IBM Cloud Object Storage System on-premises features and benefits

Object storage to help solve terabytes-and-beyond storage challenges

Highlights

- On-line scalability that offers a single storage system and namespace
- Security features include a wide range of capabilities designed to meet security requirements
- Reliability and availability characteristics of the system are configurable
- Single copy protected data with geo-dispersal creating both efficiency and manageability
- Compliance enabled vaults for when compliance requirements or locking down data is required

The IBM® Cloud Object Storage System™ is a breakthrough platform that helps solve unstructured data challenges for companies worldwide. It is designed to provide scalability, availability, security, manageability, flexibility, and lower total cost of ownership (TCO).

The Cloud Object Storage System is deployed in multiple configurations as shown in Figure 1. Each node consists of Cloud Object Storage software running on an industry-standard server. Cloud Object Storage software is compatible with a wide range of servers from many sources, including a physical or virtual appliance. In addition, IBM conducts certification of specific servers that customers want to use in their environment to help insure quick initial installation, long-term reliability and predictable performance.

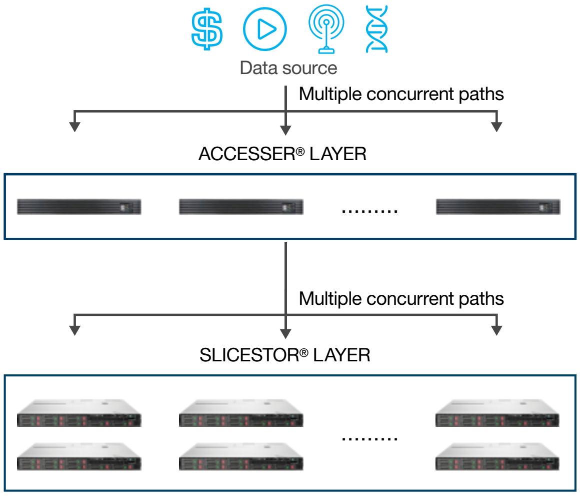
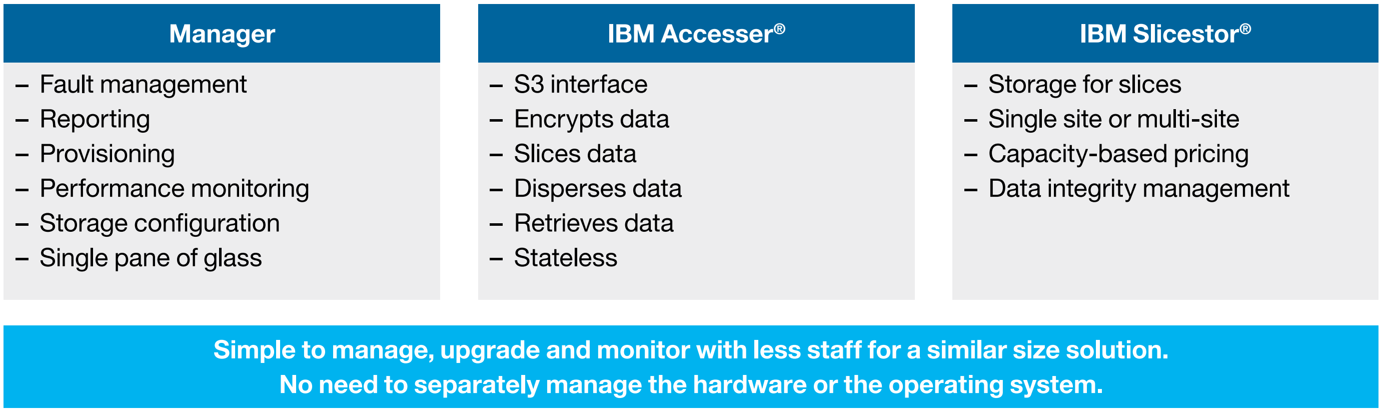


Figure 1: Multiple configurations of Cloud Object Storage System

The three types of nodes, as shown in Figure 2, are:

- IBM Cloud Object Storage Manager
- IBM Cloud Object Storage Accesser®
- IBM Cloud Object Storage Slicestor®



Manager

- Fault management
- Reporting
- Provisioning
- Performance monitoring
- Storage configuration
- Single pane of glass

IBM Accesser®

- S3 interface
- Encrypts data
- Slices data
- Disperses data
- Retrieves data
- Stateless

IBM Slicestor®

- Storage for slices
- Single site or multi-site
- Capacity-based pricing
- Data integrity management

Simple to manage, upgrade and monitor with less staff for a similar size solution.
No need to separately manage the hardware or the operating system.

Figure 2: Features of the three types of nodes

Each Cloud Object Storage System has a single Manager node, which provides out-of-band configuration, administration and monitoring capabilities. There is also one or more Accesser nodes, which provide the storage system endpoint for applications to store and retrieve data. There is one or more Slicestor nodes, which provide the data storage capacity for the Cloud Object Storage System. The Accesser is a stateless node that presents the storage interface of the Cloud Object Storage System to client applications and transforms data using an information dispersal algorithm (IDA). Slicestor nodes receive data to be stored from Accesser nodes on ingest and return data to Accesser nodes as required by reads.

The IDA transforms each object written to the system into a number of slices, such that the object can be read bit-perfectly using a subset of those slices. The number of slices created is called the IDA width. The number required to read the data is called the IDA read threshold. The difference between the width and the read threshold is the maximum number of slices that can be lost or temporarily unavailable while still maintaining the ability to read the object. For example, in a system with a width of 12 and a read threshold of seven, data can be read even if five of the 12 stored slices cannot be read.

Storage capacity is provided by a storage pool using multiple Slicestor nodes. Three or more Slicestor nodes can be grouped to create a device set which are configured to be part of a storage pool. A single Cloud Object Storage System may have one or multiple storage pools and each of the storage pools may have one or more storage device sets.

A vault is not part of the physical architecture, but is an important concept in an Cloud Object Storage System. A vault is a logical container or a virtual storage space, upon which reliability, data transformation options — for example, IBM Cloud Object Storage SecureSlice and IDA algorithm — and access control policies may be defined. Multiple vaults can be provisioned on the same storage pool.

The IDA combines encryption and erasure-coding techniques to transform data to highly reliable and available storage without making copies of the data, as would be required by traditional storage architectures. By enabling reliability and availability without storing multiple copies of the data, the Cloud Object Storage System can offer significant TCO savings.

Scalability

Storage systems should be able to handle virtually all current storage requirements. Systems should be able to scale to meet anticipated needs for many years in a single system and a single namespace, rather than through an increasing number of limited-capacity storage silos. Cloud Object Storage software has been tested at web-scale with production deployments exceeding 100 PBs of capacity in multiple deployments. It has the ability to scale to exabytes (EBs) while maintaining reliability, availability, manageability and remaining more cost-effective.

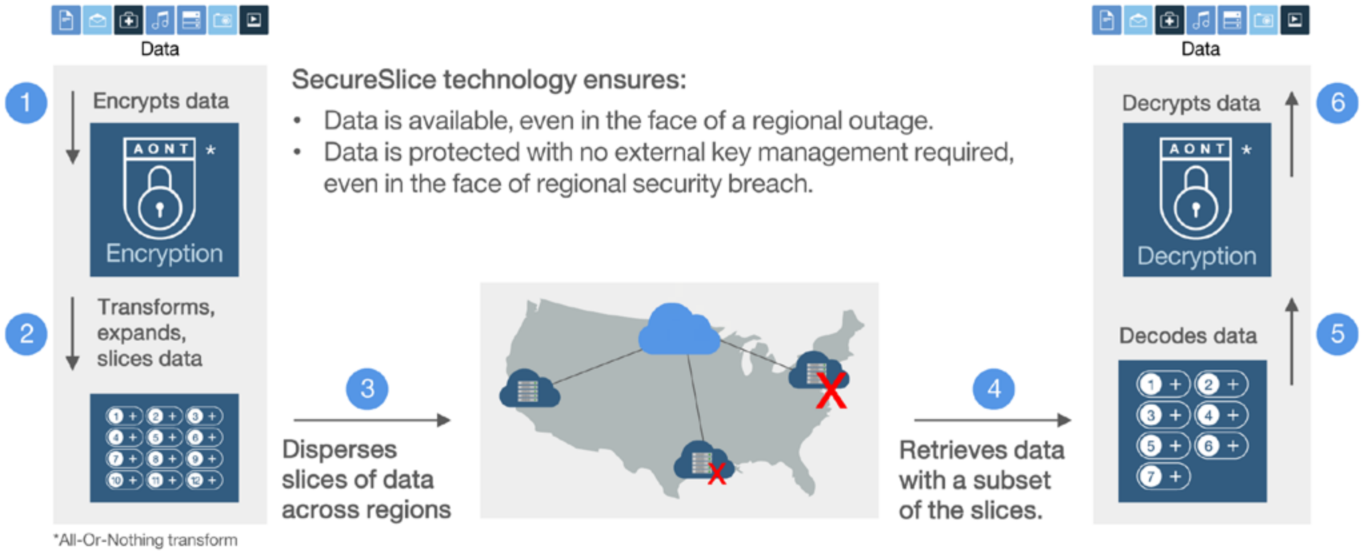
Capabilities

Whether your current needs are less than 100TB, 1 PB, 10 PBs, hundreds of PBs or even beyond an exabyte, the Cloud Object Storage solution can help meet that requirement with the following features:

- Scale-out, architecture, including distributed, shared-nothing, and peer-to-peer design.
- Yottabyte-scale global namespace with 10^{38} object IDs available per vault.
- Slicestor storage nodes increase storage capacity and performance.
- Up to thousands of Slicestor storage nodes in a single system.
- No practical limit on the number of Accessers per Cloud Object Storage System.
- Network installation of Cloud Object Storage software across the Cloud Object Storage System nodes using PXE
- Near linear increases in system throughput and HTTP operations per second as the system grows.

Security

From built-in encryption of data at rest and in motion to authentication and access control options, Cloud Object Storage includes a range of capabilities to help you meet security requirements. These security capabilities have been implemented to enable better security without compromising scalability, availability, ease of management, or economic efficiency, as shown in Figure 3.



SecureSlice technology ensures:

- Data is available, even in the face of a regional outage.
- Data is protected with no external key management required, even in the face of regional security breach.

Figure 3: SecureSlice technology

Capabilities

Transmission and storage of data is inherently private and is designed to withstand attacks from the outside and within. No copy of your data resides in any single disk, node or location. Data in motion is encrypted using total layer security (TLS). Data at rest is encrypted using SecureSlice encryption. Data can further be encrypted from the application or user to ensure security is never compromised.

SecureSlice encryption provides high-level confidentiality for data at rest on Slicestor storage nodes as long as no more than N Slicestor nodes have their data exposed, where N = IDA Read Threshold-1. In typical Cloud Object Storage System deployments, N ranges from four to 25 depending on scale and configuration. SecureSlice is a standard product feature, with no additional license fee. It can be configured to use any of the following combinations of encryption and data integrity algorithms:

- RC4-128 encryption with MD5-128 Hash for data integrity
- AES-128 encryption with MD5-128 Hash for data integrity
- AES-256 encryption with SHA-256 Hash for data integrity

TLS is supported on network connections within the Cloud Object Storage System for data-in-motion protection. TLS is supported on Client-to-Accesser networks for data-in-motion protection. Multiple authentication methods are supported for data and management access:

- Internally managed username and password
- Active directory or OpenLDAP server
- S3 secret access key
- Public key infrastructure (PKI) certificate and private key
- One user may authenticate using:
- Username and password
- Certificate and private key

Critical configuration information is communicated in a security-enhanced manner or digitally signed to prevent a potential outsider from assuming an administrator's role.

For virtually any vault, a user may be granted owner, read/write or read-only privileges. Vaults may also be configured with classless inter-domain routing (CIDR)-schemed IP Access restrictions. When vault security is not desired for a vault, it may be configured as anonymous read or anonymous read/write. This feature enables access to content in a vault without authentication.

Object-level Access Control List (ACL) support in the S3-compatible Cloud Storage Object API, enables the association of an ACL with each individual object.

Role-based Access Control in the Cloud Object Storage Manager provides managed restriction of access to functionality by role for the following six roles:

- Super user
- System administrator
- Security officer
- Operator
- Vault provisioner
- Vault user

Reliability and availability

In an Cloud Object Storage System, the reliability and availability characteristics of the system are configurable. For extremely demanding applications, reliability of 15 nines and availability of 8 nines can be provided, as shown in Figure 4. Customers can configure for more typical levels of reliability and availability and potentially achieve economic savings as a result. The configurability of the Cloud Object Storage System allows you to choose the combination of reliability, availability and economic efficiency that suits your requirements. Data durability is designed to be maintained over time by built-in integrity checking and self-repair capabilities.

70%	210%	15	100%	8
Lower Cost of Ownership[1]	Return on Investment (ROI)[1]	Nines reliability[2]	Uptime	Nines availability[2]
Save on CAPEX and OPEX costs.	Quick return on investment can be as little as 7 months	Greater than other solutions: For every 10,000 objects, one may be lost every 10 million years or more	Always on even during upgrades or component or site failure.	Less than a blink of an eye every year (0.3 second per year).

[1] IBM Cloud Object Storage on-prem solution delivers >70% lower TCO than traditional on-premise storage. Source: Forrester Total Economic Impact Study, 2015. IBM Cloud
[2] Numbers shown for availability and reliability are for deployments greater than three sites and require specific supported configurations

Figure 4: Extremely high availability and reliability numbers

Capabilities

The Cloud Object Storage IDA is designed to enable durable storage, helping provide reliability and availability without storing multiple copies of the data. Availability and reliability are maintained regardless of a potential failure of hard drives and other components, complete failure of Cloud Object Storage System nodes and site outage or destruction.

The IDA can be configured to provide high levels of reliability (15 nines) or availability (8 nines), or to provide a lower level of reliability or availability with less physical storage capacity needed for the same usable capacity. The system allows the flexibility to use different IDA configurations for different vaults.

Distributed Rebuilder uses all Slicestor nodes in the system to identify slices that are missing or corrupt and perform the necessary repair, such as:

- Slice data lost due to failure
- Slice data corrupted by a disk-level
- Unrecoverable Read Error

Disk lifecycle management—low-level monitoring of disk health in Slicestor nodes—allows data to be moved from a failing drive to a healthy drive before the drive fails.

Multi-level data integrity incorporates checksums to handle physical media errors that often occur in large-scale storage systems. Integrity is checked at both the slice and object levels. Corrupted slices are not used and are repaired by the Distributed Rebuilder.

Manageability

The manageability of a Cloud Object Storage System enables storage administrators to handle up to 15 times the storage capacity of a traditional storage system, freeing time for them to invest in other tasks. The Cloud Object Storage System provides always-on availability for storage applications while completing tasks that would require scheduled downtime in traditional storage systems. Software upgrades, hardware maintenance, storage capacity expansion, hardware refresh and physical relocation of the storage system are all supported with zero downtime. Object storage systems are designed to keep versions of files or object simplifying management further by not requiring the need for snapshot and constantly protecting against changed blocks or files. The design of an object system makes it simpler, with fewer tasks to perform or activities to monitor.

Capabilities

The Cloud Object Storage Manager is an out-of-band management console for the entire system. It provides robust configuration, administration, event monitoring and reporting, as well as Role-Based Access Control support. The Cloud Object Storage Manager can be accessed through a web GUI, which provides a unified display into the Cloud Object Storage System. It can also be viewed and through a set of management APIs.

A robust set of management and monitoring APIs help enable integration with customer-provided management or monitoring tools:

- Cloud Object Storage Manager REST API
- SNMPv3
- RESTful device state and statistics interface
- syslog
- Report export through HTTP command

It is designed for always on operations with virtually no downtime required to:

- Upgrade to a new version of Cloud Object Storage software
- Add Slicestors to increase storage capacity
- Add Accesser to increase access layer throughput
- Perform hardware maintenance
- Refresh hardware Move hardware to a new site/data center
- Change the number of sites or data centers across which the system is deployed

There is a top-level indicator of the health of physical hardware with drill-down capability to see more detailed information on any individual servers in the Cloud Object Storage System.

The Cloud Object Storage Manager provides the following information for each Manager, Accesser, or Slicestor node:

- Node health
- IP Address
- Model
- Software version

The following information is available for each Slicestor data drive:

- Drive health
- Drive capacity
- Drive model
- Drive serial number
- Drive firmware

The Cloud Object Storage Manager provides the following information for each vault:

- Name
- Description
- Creation date
- Vault health
- Capacity used (raw and usable)
- IDA width and read threshold
- Soft quota
- Hard quota
- SecureSlice enabled or disabled
- Object versioning enabled/or disabled—Delete restricted yes or no

The Cloud Object Storage Manager provides the following information for each storage pool:

- Name
- Capacity
- Slicestor nodes used for vaults

Graphs provide visualization of key performance, system health, and use indicators. The same data used to create these graphs is available through a REST interface for processing by other tools. Graphs provide information on the following:

- Storage pool capacity and use
- Vault space used
- Client-to-Accesser throughput
- Accesser-to-Slicestor throughput
- Rebuild activity
- Node disk use (MB/s)
- Node CPU use
- Node network usage
- CPU temperature
- Fan speeds
- Hard drive temperature

Near real-time incident streams provide a to-do list of issues requiring operator attention to maintain the health of the Cloud Object Storage System at the current time.

Near real-time event stream provides a historical record system including conditions impacting nodes (Cloud Object Storage Manager, Accesser, or Slicestor), vaults, and storage pools. Event stream data can be filtered in a variety of ways when looking for specific events or patterns.

Generate alerts using:

- email
- SNMP traps
- syslog forwarding from incidents and events.

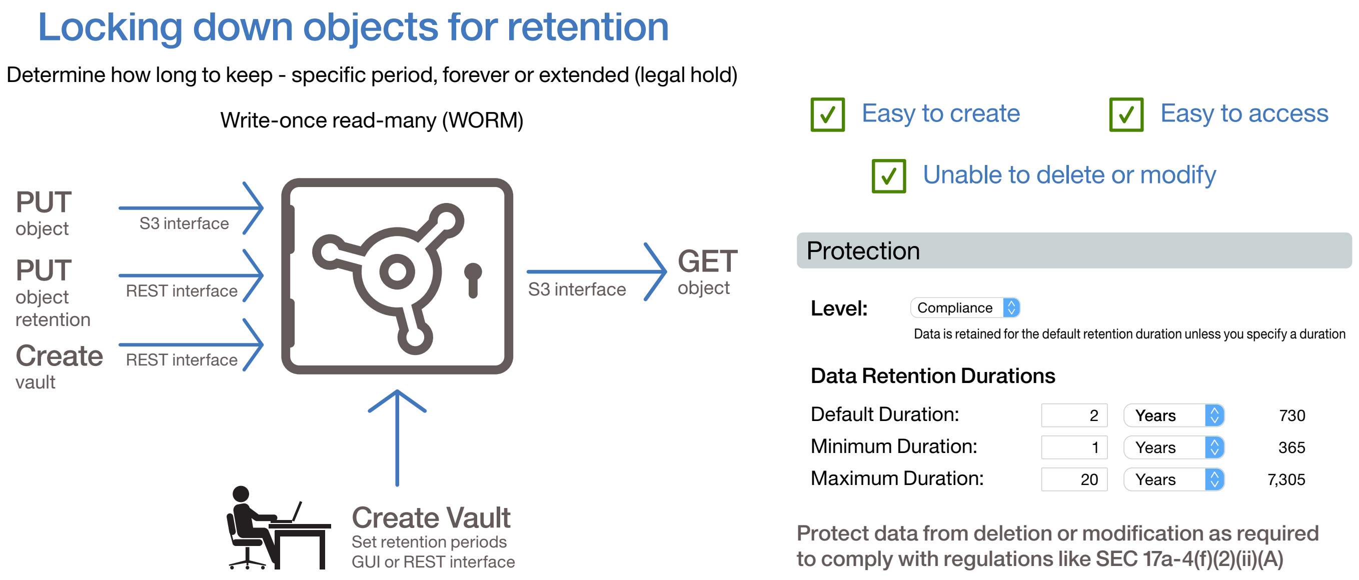
System-provided reports provide information on Cloud Object Storage System health and configuration, which can be viewed through the Cloud Object Storage Manager or exported. Export can be done from the Cloud Object Storage Manager or through a RESTful interface. The following reports are available:

- Disk drive and devices
- Cloud Object Storage System compliance
- Storage pool use
- Vault summary
- Device summary
- Failed FRU report
- Event report
- Firmware report

Phone Home capability delivers relevant system information to IBM's support organization to enable proactive maintenance and help reduce issue resolution time.

Read-only retention periods

For companies that require the ability to store data with specific policy based retention rules, retention periods can now be set. See Figure 5.This capability allows for the creation of data vaults designed per government mandated compliance SEC Rule 17a-4(f) to help meet the requirement that "electronic records must be preserved exclusively in a non-rewritable and non-erasable format." Once set, the data cannot be overwritten or deleted. IBM will enforce the controls and will protect data per the controls (including a predefined retention period) by an application or vault creator. Setting retention is done with a simple click on a screen or using an S3-compatible API.



Locking down objects for retention

Determine how long to keep - specific period, forever or extended (legal hold)

Write-once read-many (WORM)

Protection

Level: Compliance

Data is retained for the default retention duration unless you specify a duration

Data Retention Durations

Default Duration:	2	Years	730
Minimum Duration:	1	Years	365
Maximum Duration:	20	Years	7,305

Protect data from deletion or modification as required to comply with regulations like SEC 17a-4(f)(2)(ii)(A)

Figure 5: Summary of retention periods

One cannot change the data after it is set. However, you can still alter and configure the access controls that are not related to compliance by using a separate read only access policy. For example, you can grant read access to business partners or designated third parties (as sometimes required by regulations).

In most cases, a vault should be created, a protection level applied, and then data is uploaded to the vault where it will be governed by the designed policy.

Capabilities

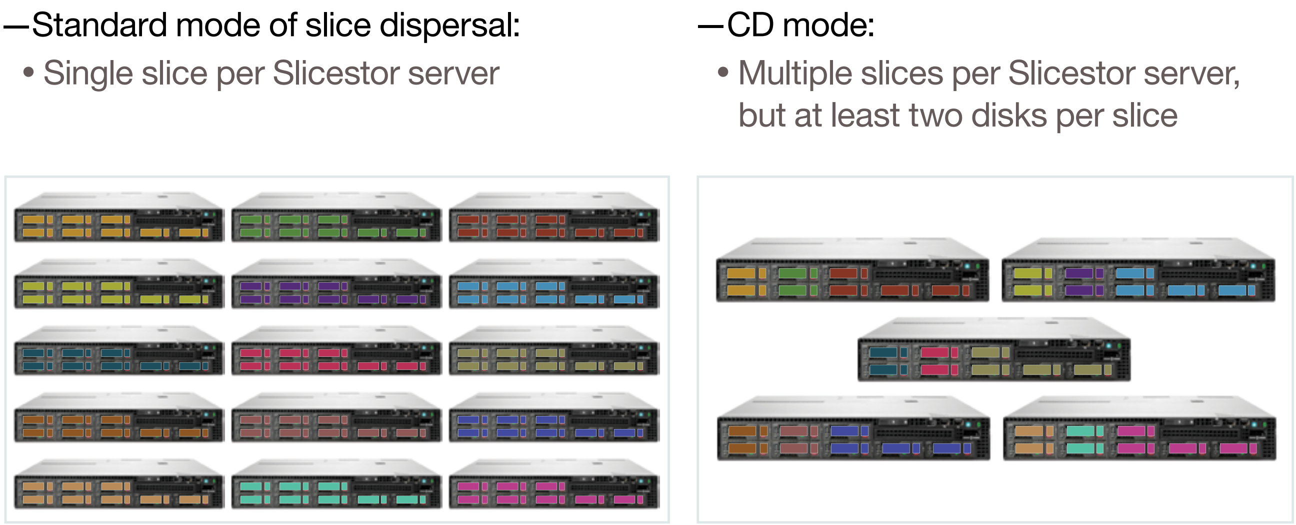
Locking down data (no deletion or changes) for a specific period of time (retention period) starts by creating a vault either with the GUI or through a REST API. A default retention period along with a minimum and maximum retention period can be initially set. Retention periods can also be set at the object level through the REST API. Access to objects either creating or reading objects is still using the S3-compatible API. Some of the features include:

- Protected objects cannot be deleted until the retention period has expired and all legal holds are removed
- Singe-click GUI management for creation of vaults and default retention periods
- Data tampering will be detected and prevented
- All data can be securely accessed using standard S3 interface
- Support for variable user-defined retention policies for different data sets (minimum, maximum and default)
- Retention of data past retention period when required by subpoena, legal hold or other similar circumstances
- S3-compatible API extensions for setting and viewing retention intervals at a bucket and object level
- Letter of Assessment Report from Cohasset Associates or SEC, FINRA and CFTC compliance

Concentrated dispersal

An object stored on a Cloud Object Storage system is dispersed into slices on multiple storage nodes. By default—standard mode—slices are distributed on separate storage nodes for each object. Concentrated Dispersal (CD) mode provides a way to distribute multiple slices of an object on the same storage node. This concentration of slices allows a complete scalable storage solution starting with only three nodes and 72 TB of useable capacity versus a starting configuration of six nodes for standard mode. When using either mode there are multiple capacity options available and each one maintains the ability to grow online to exabyte+ capacity

These new features maintain IBM's ability to access data during any growth in capacity or hardware or software upgrade. IBM engineers set out to scale down its object storage but maintain its high reliability factor of 15 nines. It also maintains its high availability standards of a system with built in redundancy and security. The minimum system configuration can be deployed in a single data center or distributed across three different data centers. Other CD mode configurations allow for different combinations of one, two, three or more data center configurations, as shown in Figure 6. With the new CD mode, IBM can create configurations that use 75% less resources than previous minimal configurations and that better align to customer requirements for private cloud storage.



—Standard mode of slice dispersal:

- Single slice per Slicestor server

—CD mode:

- Multiple slices per Slicestor server, but at least two disks per slice

Figure 6: Standard dispersal mode slices versus CD mode slices

Capabilities

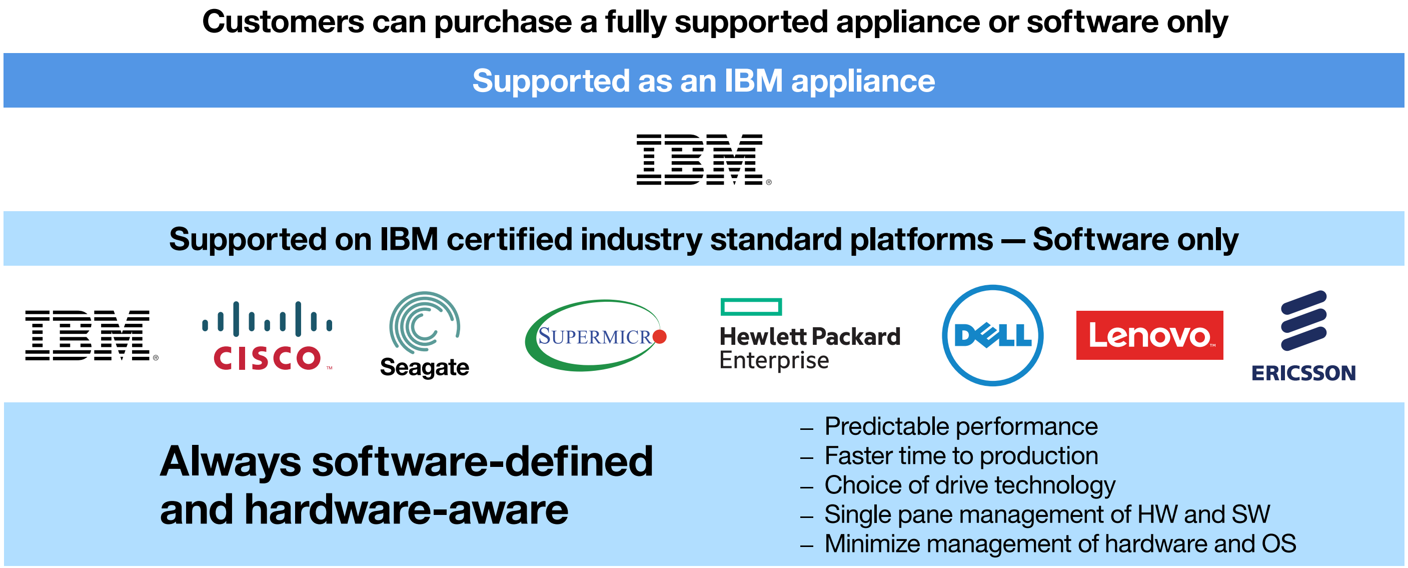
CD mode allows for the creation of a consolidated configuration using three or more servers, which is 75% less than a previous minimal configuration for most multi-site deployments. This option automatically detects the number of servers and—based on your requirements—will choose either CD mode or Standard mode when configuring storage pools.

CD mode features include:

- Cost effective to be deployed with a little as 72 TB (6u) of capacity with 5 nines availability and 15 nines of reliability.
- Automatic detection of optimal configuration depending on number of nodes configured.
- Same software and hardware for new CD mode. Grow online to exabyte+ capacity.
- Existing Cloud Object Storage-certified solutions are compatible with CD mode.
- Works seamlessly with CEVs, bringing new capacity and price points for compliance requirements.
- A single system can maintain both CD mode and Standard mode configurations with ability to combine modes online if desired.
- Transparent operation of modes with no effect on user and application interface or use.

Flexibility

Cloud Object Storage's software-defined storage solution requires no IBM-specific or proprietary hardware. Using Cloud Object Storage software with industry-standard hardware systems enables an IT organization to potentially achieve a significantly lower cost per usable terabyte curve. This helps the organization to economically manage rapidly increasing storage capacity requirements. See Figure 7.



Customers can purchase a fully supported appliance or software only

Supported as an IBM appliance

Supported on IBM certified industry standard platforms — Software only

Always software-defined and hardware-aware

– Predictable performance
– Faster time to production
– Choice of drive technology
– Single pane management of HW and SW
– Minimize management of hardware and OS

Figure 7: Certified hardware vendors available for software deployments

Capabilities

Software-defined storage allows Cloud Object Storage to run on a wide range of industry standard hardware platforms that are certified by IBM. All major hardware vendors are supported, including Cisco, Dell, HPE, IBM, Lenovo, Seagate, SuperMicro.

This certification includes integration with IBM's hardware component health monitoring and Disk Lifecycle Management functionality including:

- IBM testing of the specific combination of hardware and software you deploy can result in significantly reduced time to production on initial deployment.
- IBM guidance on optimal configuration of certified platforms.
- Close monitoring of hardware health delivers timely notification of hardware issues needing attention.
- Disk Lifecycle Management allows data to be migrated off a failing Slicestor hard drive before that drive fails, reducing the amount of data that must be rebuilt due to disk failure.
- IBM support staff are familiar with the combination of hardware and software you are using.

The Cloud Object Storage System can be deployed in a single site with data protection through information dispersal without RAID and without replication. A system can be deployed across two sites using a vault- mirroring configuration. This configuration provides site level fault tolerance by maintaining a copy of the data in each of the two sites. A system can be deployed across three or more sites with information dispersal providing site-level fault tolerance without replication.

The number of sites used can be changed in the future in a way that requires no system downtime. For example, a system initially deployed across two sites can be later reconfigured and deployed across three sites. A system can also change storage modes such as changing from Concentrated Dispersal mode to Standard mode without any disruption to any data.

The flexibility to specify different configurations across vaults sharing the same pool of Slicestor storage nodes enables the Cloud Object Storage System to support multiple applications and workloads with different requirements and characteristics. Vault-level settings include the following:

- IDA width and read threshold
- Soft quota
- Hard quota
- SecureSlice enabled or disabled
- Object versioning enabled or disabled
- Delete restricted yes or no
- Accesser devices provisioned

The best IDA configuration varies based on factors like capacity (1, 10, 100 or 1000 PBs) and how many sites will be used for deployment, such as 1, 2, 3 or more sites. Support for a wide range of different IDA widths and read thresholds can provide valuable flexibility that is not present in replication-based storage systems or systems offering only a few erasure-coding settings.

Multiple storage interfaces are supported, including the following:

- Cloud Storage Object API (an Amazon S3-compatible RESTful interface)
- CR API setting and managing the retention capabilities of an object in a CEV
- NFS through cloud storage gateway from one of IBM's technology collaborators
- SMB/CIFS/iSCSI from one of IBM's technology collaborators

When your storage needs grow, there are two ways to increase storage capacity:

- Add a new storage pool and create new vaults in the storage pool
- Increase the capacity of an existing storage pool making more capacity available for new and existing vaults

Support for multiple storage pools in a single Cloud Object Storage System offers flexibility to provision different combinations of performance, durability or cost for different applications or workloads. This is within a single Cloud Object Storage System rather than deploying application-specific storage systems.

The SmartRead feature optimizes read performance and allows consistent performance to be maintained even if some storage system components are impaired. The SmartWrite feature improves availability and allows consistent performance even when some individual components are slow to respond. The SmartRead adaptively increases the number of active WAN connections if latency becomes too high.

Packed Slice Storage optimizes performance and storage efficiency for small objects allowing the Cloud Object Storage System to efficiently handle a wide range of workloads including those with significant numbers of small objects.

Economics/TCO

IDAs protect digital assets, rather than relying on storage of multiple copies, which can reduce the physical storage capacity required by more than 50%. The IDA encodes the data before storing it so that data remains available regardless of numerous hard drive or server failures and site outages, while storing a single copy of that data. Also, the Cloud Object Storage System may use up to 99% of its usable capacity without the drop-off in performance that is typical in most traditional storage systems as use increases.

Cloud Object Storage Systems can achieve TCO savings of up to 70% compared to most traditional storage systems as well as public cloud storage. TCO savings reflect not only reduced acquisition cost, but savings on power, cooling and space due to the smaller hardware footprint, as well as lower manpower costs in storage management and operations.

About IBM Cloud Object Storage

Cloud Object Storage provides organizations the flexibility, scale and simplicity required to store, manage and access today's rapidly growing unstructured data in a hybrid cloud environment. Relied upon by some of the world's largest repositories, Cloud Object Storage turns storage challenges into business advantage. It does this by reducing storage costs while reliably supporting both traditional and emerging cloud-born workloads for enterprise mobile, social, analytics and cognitive computing.

For more information

Call 1-866-398-7638 or visit the IBM Cloud Object Storage website: **ibm.com**/software/products/en/object-storage-on-prem

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
October 2017

IBM, the IBM logo, ibm.com, Accesser, Cloud Object Storage System, and Slicestor are 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.

This document is current as of the initial date of publication and may be changed by IBM at any time.

Not all offerings are available in every country in which IBM operates. The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Actual available storage capacity may be reported for both uncompressed and compressed data and will vary and may be less than stated.

♻ Please Recycle

[1] Learn more about Information Dispersal in "The Definitive Guide to IBM Cloud Object Storage Dispersed Storage", in the Resources section at: www.ibm.com/software/products/en/object-storage-on-prem.

[2] "The Total Economic Impact of IBM Cloud Object Storage," a Forrester Total Economic Impact Study Commissioned by IBM, Forrester Research, Inc., March 2015, ibm.co/2wZccZG.