MANAGED OBJECT STORAGE

SERVICE DESCRIPTION

SUMMIT

Service overview

Summit Managed Object Storage (MOS) is a flexible, scalable, and secure Cloud Storage service allowing customers to dynamically scale storage in response to changing business needs. MOS is delivered from Summit's global data centers, giving Customers the option to deploy resources in the most appropriate locations. Summit's MOS service is a turnkey solution that is fully maintained and operated by the Summit Managed Services team. All underlying hardware and network connectivity for the platform is administered and monitored by the Managed Services and Service Desk teams.

MOS is a highly-performant, secure, and feature-rich object storage service. With MOS, organizations of all sizes and industries can store any amount of data for any use case including applications, IoT, data lakes, analytics, backup and restore, archive, and disaster recovery. MOS has various features customers can use to organize and manage their data in ways that support specific use cases, enable cost efficiencies, enforce security, and meet compliance requirements. Data is stored as objects within containers called "buckets," and a single object can be up to 2 terabytes in size. MOS features include capabilities to append metadata tags to objects, configure and enforce data access controls, secure data against unauthorized users, and monitor data at the object and bucket levels. MOS offers multi-tenancy, Write Once Read Many (WORM), and configurable storage policies with flexible protection levels and redundancy through Intel® Intelligent Storage Acceleration Library (ISA-L) erasure coding, replication factors, data compression and server-side encryption. With MOS, seamless data management is possible, allowing users on-demand access to their data anywhere and anytime.

MOS is designed for 99.99995% durability to protect data from site-level failures, errors, and threats. MOS is designed for 99.9995% reliability so that it is always available to customer end users and applications. Customers can use MOS to store and retrieve any amount of data at any time, from anywhere on the internet. This task is accomplished using the intuitive, web-based MOS Management Console, native Summit MOS APIs and the Amazon S3 HTTP REST API*.

*Amazon has set the cloud storage standard in recent years, making it the largest object storage environment. Consequently, the Amazon S3 API is becoming the de facto standard for developers writing storage applications for cloud. Summit MOS is S3 compliant with the Amazon S3 HTTP REST API in accordance with this industry imperative. With complete S3 compatibility, MOS ensures seamless S3 integration with every available AWS/ S3 application.

Managed object storage basics

To get the most out of MOS, customers should understand a few foundational concepts for Object Storage.

- MOS stores data as objects within buckets.
- An object consists of a file and optionally any meta- data that describes that file.
- Before you can store data in MOS, you must create a bucket.
- You can create as many buckets as necessary for your configuration.
- For each bucket, you can control access to it (who can create, delete, and list objects in the bucket), view access logs for it and its objects.
- Buckets, by default, are private and can be made publicly accessible as needed.
- To store an object in MOS, you upload the file you want to store to a bucket.
- When you upload a file, you can set permissions on the object as well as any metadata associated with the file.

Key features

A managed service

Summit's Managed Services team supports the underlying hardware, software and network connectivity used to deliver the MOS Service. Customers open support requests to create or alter system configurations, or get any additional information about the service.

Durability and reliability

A durable, reliable and performant cloud storage service

- MOS is designed for 99.99995% of durability so that data is protected against site-level failures, errors, and threats.
- MOS is designed for 99.9995% reliability so that access to data is always available.

Service management features

MOS offers a wide range of management features, enabling you to manage data at the account, bucket, and object levels. MOS supports the ability to replicate, tier, query, monitor, audit, and configure access to a single object, an entire bucket, or across an entire account.

Cost-efficient storage

MOS scales on-demand and only charges customers for the storage volume used and transactions executed. The MOS system maintains comprehensive service usage data for each group and each user in the system. This usage data, which is protected by replication, serves as the foundation for MOS service billing functionality.

Storage architecture

MOS's flat, non-hierarchical structure and comprehensive management features help customers of all sizes and industries organize their data in ways that are valuable to their businesses and teams. All objects are stored in buckets and can be organized with shared names called prefixes. You can also append key-value pairs called MOS object tags to each object, which can be created, updated, and deleted throughout an object's lifecycle. To keep track of objects and their respective tags, buckets, and prefixes, customers can use an inventory report that lists their stored objects within a MOS bucket or with a specific prefix, and their respective metadata and encryption status.

Storage configuration management

With MOS bucket names, prefixes, object tags, and MOS Inventory, you have a range of ways to categorize and report on your data. MOS also supports features that help maintain data version control, and prevent accidental deletions. With MOS versioning, customers can easily preserve, retrieve, and restore every version of an object stored in in the system, which allows them to recover from unintended user actions and application failures. For an additional fee, users can take advantage of the Multi-Site Replication (MSR), which allows customers to replicate objects (and their respective metadata and object tags) into other Summit locations for reduced latency, increased redundancy, compliance, security, disaster recovery, and other use cases. MOS MSR is configured to a source bucket and replicates objects into a destination bucket in another Summit location.

You can also enforce write-once, read-many (WORM) policies with MOS. MOS supports applying a WORM policy to a bucket via native tools or an advanced S3 extension. When a WORM policy is implemented for a bucket, objects in the bucket cannot be altered or deleted through MOS S3 interfaces until the object age exceeds a specified retention period. WORM is implemented on a per-bucket basis and therefore offers great multi-tenancy retention flexibility.

This management feature blocks object version deletion during the customer-defined retention period so that customers can enforce retention policies as an added layer of data protection or to meet compliance obligations. Customers can configure MOS Object Lock at the object- and bucket-levels to prevent object version dele- tions prior to a pre-defined Retain Until Date or Legal Hold Date. To track which objects are blocked from version deleting, customers can refer to a MOS Inventory report that includes the WORM status of objects.

Storage monitoring

In addition to these management capabilities, customers can use MOS features to monitor and control how their MOS resources are being used. Customers can apply tags to MOS buckets in order to increase the granularity of their system management and administration. Additionally, notifications can be set and accessed via the Customer Portal and the Managed Object Storage API for common notification variables including, but not limited to:

- Storage Bytes
- Storage Objects
- All Requests
- Get/Head Requests
- Put/Post Requests
- Delete Requests
- Data Transfer In Bytes
- Data Transfer Out Bytes

Storage classes

Currently, MOS employs a single level of storage classification.

Access management, security and compliance

Access management

To protect customer data in MOS, by default, users only have access to the MOS resources they create. Customer administrators can grant access to other users by using one or a combination of the following access manage- ment features: MOS Identity and Access Management (IAM) to create users and manage their respective access; Access Control Lists (ACLs) to make individual objects accessible to authorized users; and bucket policies to configure permissions for all objects within a single MOS bucket. MOS also supports Audit Logs that list the requests made against your MOS resources for complete visibility into who is accessing what data.

Security

MOS offers flexible security features to prevent unauthorized users from accessing data. MOS supports both server-side encryption and client-side encryption for data uploads. Customers can use MOS Inventory to check the encryption status of their MOS objects.

Users can configure and enforce finely-tuned access policies to sensitive data with MOS user- and resource-based policies. Customers can use MOS to restrict all access requests to their data stored in MOS. The service also supports different encryption options for data in transit and at rest.

Two server-side encryption methods (SSE/SSE-c, Keysecure) are implemented to ensure that the data is always protected. MOS also supports the option of using a third-party Key Management System to generate and manage the encryption key (KMS). This relieves administrators from the burden of encryption key management and eliminates the risk of data loss occurring due to lost keys. Encryption can be managed granularly—either at a bucket level or down to an individual object.

MOS can also provide public access, if desired. This is achieved via a set of security controls that ensures MOS buckets and objects do not have public access. With a few clicks in the MOS Management Controls located in the Summit Customer Portal, customers can apply the public access settings to all buckets within their account or to specific buckets. Once the settings are applied to an account, any existing or new buckets and objects associated with that account inherit the settings that prevent public access. MOS public access settings override other MOS access permissions, making it easy for the account administrator to enforce a “no public access” policy regardless of how an object is added, how a bucket is created, or if there are existing access permissions. Block Public Access controls are auditable, providing a further layer of control.

Encryption

Encryption of data stored within the MOS platform is available via self-service. To enable encryption of the storage bucket Summit's customers are required to bring their own keys. Customers can choose to either encrypt the data before it is uploaded to the MOS platform or set the encryption keys on the bucket using the S3-compatible API.

Compliance

Summit maintains comprehensive annual audits to support your compliance requirements for GDPR, PCI DSS, HIPAA, and more. You can learn more by visiting:
https://www.summithq.com/services/cloud-hosting/object-storage/

Day-to-day management

Managed Object Storage Services from Summit deliver consistent operations management and predictable results by following industry-standard and proven, internal best-practices. The specific services / management functions offered by Summit as part of the Service include:

Change management

Managed Object Storage provides simple and efficient means to make controlled changes to customer storage environments. Storage system changes are serviced by the Managed Services Team through support requests. Changes follow a well-defined approval process, and most changes can be executed quickly by Summit's Managed Services Team.

Incident management

Managed Object Storage includes the monitoring of the overall health of the storage platform and the handling of the daily activities of investigating and resolving alarms or incidents. Summit creates pre-defined playbooks that are used to rectify alarms and incidents in a way that minimizes disruption to each customer's storage environment.

Provisioning management

Designed to meet a customer's application needs, Managed Object Storage allows customers to reconfigure storage resources and allocate additional storage to support applications in either test or production environments through the timely handling of submitted support requests by our Managed Services Team.

Patch management

Managed Object Storage takes care of all infrastructure system patching activities to help keep resources current and secure. When updates or patches are released from infrastructure vendors, Summit applies them in a timely and consistent manner to minimize the impact on customer business.

Access management

Managed Object Storage Services enables customers to securely connect to the storage platform in the manner they require – be it API access, HTTPS, Cross Connects or Dedicated Physical Connectivity. Our team will make sure that the connection is maintained.

Security management

Managed Object Storage protects customer information assets and helps keep storage infrastructure secure. All storage volumes are logically separated and only available to the appropriate host systems. All Summit storage services have encryption at rest for all customers enabled by default.

Continuity management

Summit can provide Managed Backup and Recovery as an additional service in support of MOS environments. In the event of a failure or outage that impacts the customer's business, or at their request, Summit can perform a restore of these backups as needed.

Monitoring and reporting

With Managed Object Storage, customers have access to the data Summit uses to manage infrastructure as well as alerts from other Summit-supplied monitoring systems. In addition, customers receive time series reports for storage volume, data volume transfer, and transactions as well as recommendations to optimize platform usage.

What makes this service unique?

Your business is unique, so is our service

We work with you to understand your data storate needs and configure the MOS parameters to support your unique business, financial, and technological requirements.

Native and AWS S3 APIs

MOS provides native APIs and the Amazon S3 HTTP REST API* support enabling you to choose the best integration process for your business.

Custom backup and recovery services

You can choose to implement custom backup, replication and recovery services and just the frequency of policies, encryption methods, and data locations to fit these requirements.

Custom replication strategies

You may also choose to have backup data replicated to a second Summit-operated data center to provide physical redundancy should security , governance or compliance requirements dictate.

Roles, responsibilities and process

Successful Managed Services are the result of transparency and collaboration. Clearly defined processes and a detailed outline of roles and responsibilities are where this collaboration begins.

Our Managed Object Storage Service is preceded by defined Consult and Plan, Design and Build processes. These critical steps establish the foundation for the execution of the Service and align these critical processes with your unique business needs.

Consult

We follow a proven, structured process of automated data collection and personal interviews with key business stakeholders, IT infrastructure, and application teams to successfully complete the Discovery process.

The outcome of these efforts includes identification of identification of business drivers and the discovery / analysis of your existing environment including Business and IT Governance processes, Infrastructure configurations and Networking and Security policies.

Discovery sessions are conducted with your company's subject matter experts (SMEs) and our Managed Services team. This collaboration helps us prioritize your goals and ensure that all critical success factors are met.

Plan, design and build

The data gathered and objectives defined in Consult inform the configuration and process requirements for your Service. Plan, Design and Build brings these to life.

During this phase we will deliver the official, comprehensive analysis of the current environment. This docmentation includes, but is not limited to, Infrastructure Diagrams and network connectivity requirements, identifying how is accessed, used and managed today, and where risks are present.

We will also develop and deliver a Remediation Plan for the current environment or a Development Plan for a net-new environment to ensure industry and Summit best practices are in place to support your business today and tomorrow, especially as your storage needs grow.

Once the recommended Remediation Plan / Development Plan has been vetted and approved, we will move on to complete the Remediation / Development Process using the documentation and decisions identified, and agreed upon, by both parties.

Run and operate

Now that your environment is successfully configured and verified as ready for production, the official Managed Object Storage Service can begin. This is where we begin delivery of proactive day-to-day management, administration, monitoring, and support for your object storage environment and processes.

Optimize and evolve

The final component of our Managed Object Storage Service for is the ongoing optimization and evolution of your environment. This phase has us focused on infrastructure performance and cost management. Monthly or quarterly reviews provide updates and opportunities for additional environment optimizations based upon changing business requirements and environment performance. Any opportunities identified are shared directly with your IT and leadership teams to inform strategy and decisions.

Customer success and service operations

The foundation of every Summit Managed Object Storage Service is collaboration. All customer success and service operations workflows have been designed to minimize response time, mitigate risk and optimize collaboration so knowledge transfer occurs when and where necessary.

We recognize your business, and your customers, operate 24x7x365. We have designed and operate our business to be here for you, whenever and however necessary to ensure your success.

Customer success team

Summit provides each customer with comprehensive resources to deliver ongoing service and support for your cloud environment. From sales, solution architecture and certified engineer support on our Service Desk, to customer success and executive management sponsorship, you will have experts with you every step of the way.

How to contact Summit support

Summit uses cases to identify incidents and provide support to our clients until the incident is resolved. Case identification and review is conducted using the Summit Customer Portal. Each Summit client is supplied with accounts that are permissioned to create, update and view their cases.

Case Creation – Customer Portal

Support cases submitted to Summit are submitted using the Summit Customer Portal. The portal is accessible at: https://www.summithq.com/login-and-support/.

To create a support case:

- Log into the Summit Customer Portal.
- Select “Create Case”.
- You receive an automatic confirmation of the successful case creation, including the case number.
- Summit Service Desk staff review the case for accuracy, confirm the Severity Level, and send acknowledgement of case receipt to you.
- Summit Service Desk agent & Cloud Services Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Creation – Telephone

We recognize there may be times when a support case required the immediacy only a phone call can provide. Support cases may be created by calling the Summit Service Desk at +1 312-829-1111, Ext. 2. Telephone submitted support cases utilize a similar support operation, with a few modifications.

To create a support case:

- Call the Summit Service Desk at +1 312-829-1111, Ext. 2.
- Summit Service Desk Agent verifies caller identity, captures relevant information, creates the support case, and assigns a Severity Level.
- Summit Service Desk agent & Cloud Services Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Escalation Paths

Summit provides several, formal options for support case escalation. Escalations occur to set a support case to a desired Severity Level, as outlined below.

Primary Escalation Path - This method is preferred as it is the most efficient method for raising the Severity Level of a case. To create a support case, you will:

- Log into the Summit Customer Portal.
- Navigate to the appropriate case.
- Click the “Escalate Case” link.
- Select the desired Severity Level and submit.

Alternate Case Escalation Path(s) - Additional Case Escalation paths are also available. However, it is important to note that Alternate Case Escalation Paths will not be as expedient as the Preferred Escalation Path.

Alternate Escalation – Case Response

You may submit a response to an existing case and simply request an escalation to the desired Severity Level. The Severity Level will be raised once a Service Desk Agent has reviewed and processed the request.

Alternate Escalation Path - Phone Support

- You may call the Summit Service Desk at +1 312-829-1111, Ext. 2.
- The Summit Service Desk Agent will verify the caller’s identity and the support case number. You verbally request escalation to the desired Severity Level.
- The Summit Service Desk Agent updates the case accordingly.

Response time

All Summit customers can set the severity level of their support cases. The severity level you select will determine the response time. You can select the following severity levels when submitting a support case:

Infrastructure Administration (Proactive Services)

Severity Level	Description	Response Time SLA
Critical / Level 1	Critical Issues include business-critical system outages or issues causing extreme business impact.	15-minute response time
High / Level 2	High Severity Level issues include the impairment of production systems, impaired application performance, and moderate business impact.	30-minute response time
Normal / Level 3	Normal Severity Level issues include standard service issue requests and minimal business impact.	1-hour response time
Low / Level 4	Low Severity Level issues include general information requests, questions and guidance from Summit team members, arranging prescheduled maintenance activities.	4-hour response time
Informational / Level 5	Informational Issues include general questions, how-to style requests, or reports.	24-hour response time

As standard business practice, Summit's Service Desk acknowledges all support cases within 15 minutes of case creation. The response times identified in the table above represent the average time required to remediate such issues. Please note the response time to resolution of your issue may vary based upon circumstances and configurations unique to your business and your cloud architecture. Any support cases created without a severity level selected will be set to "Level 3 – Normal" by default.

Service level agreements

Summit provides two Availability SLAs for Cloud MSP customers.

Standard Cloud Application Management

We provide the following uptime SLA: 99.95% availability of the Cloud Application to respond to incoming requests from all endpoints for Standard Cloud Application configurations. If the Cloud Application's availability is disrupted, and the disruption lasts for more than 21 minutes, you shall be eligible for a credit.

High Availability Cloud Application Management

We provide the following uptime SLA: 99.99% availability of the Cloud Application to respond to incoming requests from all endpoints for High Availability Cloud Application configurations. If the Cloud Application's availability is disrupted, and the disruption lasts for more than six (6) minutes, you shall be eligible for a Credit as set forth below.

The SLA for Cloud Resources will be dependent upon the Cloud Platform(s) selected by Summit and you. You can find current version of the Cloud Application Management SLA on our website.

Account reviews

Summit offers quarterly and annual Account Reviews for all Managed Service Partnerships. These collaborative sessions aim to provide greater visibility into the technical, operational, financial and business aspects of your company and your Cloud. Account Reviews also provide you with a way to offer direct feedback, including areas of improvement, on the status of your Partnership with Summit.

An Account Review agenda includes:

- Introductions
- Technical, Operational, Business Updates
- Service & Performance Metrics/Dashboard Review Optimization Recommendations
- SLA Adherence & Support Ticket Review
- Access Control List (ACL) Review Q&A/Discussion

Upon completion of each account review, you should be confident that we are flexing our services and approach to meet you where you are and have a plan to take you where want to go so that you can focus on what matters most for your customers and your business.

Responsibility matrix

We are committed to solving your Object Storage challenges so you can focus on what matters most.

Each Summit Managed Services Partnership operates with the understanding that there are two parties involved in supporting your environment: your in-house experts and ours.

The MOS Service, including all Summit-operated hardware and software, is monitored by our Managed Services Team and Service Desk. Should any issues or anomalies be detected with the Service, a member of the Summit Managed Services Team or Service Desk team will take corrective action as planned and notify the customer.

From time to time, we will perform scheduled maintenance activities on the infrastructure supporting the service. Customers will be notified in advance for all scheduled maintenance. Emergency maintenance may be required and performed without advance notice. Should a service-impacting emergency maintenance be required, we will use commercially reasonable efforts to notify Customer upon execution of the maintenance.

The following responsibility matrix defines the roles and responsibilities for each party:

Managed Object Storage Responsibilities

Managed Service	SUMMIT	Customer
MOS Software and Hardware Maintenance	Y	N
MOS Software and Hardware Monitoring	Y	N
MOS Software and Hardware Administration	Y	N
MOS Software and Hardware Updates	Y	N
Host Operating System Management and Administration	N	Y
Custom Script Development, Management, Support	N	Y
Mointiroing Account Capacity Thresholds	N	Y
Maintaining Backups of Customer-Owned Data	N	Y
Maintaining List of MOS and Customer Portal Authorized Personnell	N	Y

Tired of tech that underdelivers?

Let's fix that. Get IT infrastructure that works at summithq.com.