SERVERCENTRAL
TURINGROUP

Managed Object Storage
Service Description

Managed Object Storage

ServerCentral Turing Group (SCTG) provides a full spectrum of Managed Cloud Storage services for our customers; this includes Managed Object Storage (MOS). SCTG 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 SCTG's global data centers, giving Customers the option to deploy resources in the most appropriate locations. SCTG's MOS service is a turnkey solution that is fully maintained and operated by the SCTG 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 SCTG 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. SCTG 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 metadata 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 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.

Wide Range of Management Features

MOS lets customers 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 Management and Monitoring

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 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 SCTG 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 SCTG 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 deletions 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 management 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 SCTG 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 SCTG’s customers are required to being 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

SCTG maintains comprehensive annual audits to support your compliance requirements for GDPR, PCI DSS, HIPAA, and more. You can learn more by visiting https://www.servercentral.com/compliance/

Object Storage Management

Managed Object Storage Services from SCTG deliver consistent operations management and predictable results by following industry-standard and proven, internal best-practices. The specific services / management functions offered by SCTG 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 SCTG'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. SCTG 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, SCTG 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 ServerCentral storage services have encryption at rest for all customers enabled by default.

Continuity Management

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

Monitoring and Reporting

With Managed Object Storage, customers have access to the data SCTG uses to manage infrastructure as well as alerts from other SCTG-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.

Service Operations

The Managed Object Storage Service, including all SCTG-operated hardware and software, is monitored by SCTG's Service Desk. Should any issues or anomalies be detected with the Service, a member of the SCTG Service Desk team will take corrective action as planned and notify the customer.

From time to time, SCTG 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, ServerCentral will use commercially reasonable efforts to notify Customer upon execution of the maintenance.

Customers may also view real time and historical graphs of the Service via the SCTG Customer Portal located at https://portal.servercentral.com.

ACCOUNT MANAGEMENT SERVICES	
Dedicated Client Relationship Manager	Included
24 X 7 MONITORING SERVICES	
Proactive Platform Monitoring (Capacity, Management, Return to Service)	Included
Platform Configuration Backup and Monitor for Changes	Included
Platform Patching and Updates	Included
24 X 7 SUPPORT (RETURN TO SERVICE & VENDOR ESCALATION)	
Change Management Coordination with Customer	Included
Access to 24x7x365 Service Desk Coverage (telephone, web and email)	Included
Access to SCTG Customer Portal with Customer-Defined Roles and Access Permissions	Included
Ticket Response Time - Promised	15 minutes

Responsibilities

The following section outlines the scope and limitation of support that SCTG offers for this Service.

SCTG RESPONSIBILITIES
SCTG will maintain all software and hardware that provides the Managed Object Storage Service.
SCTG will monitor the Managed Object Storage Service for uptime and availability. This includes any network switches, storage devices, and any other equipment necessary to provide the Service.
SCTG will retain exclusive administrative access to the hardware and infrastructure of the Managed Object Storage Service for the duration of the agreement.
SCTG will be responsible for hardware and infrastructure support, including return-to-service and vendor escalation.
SCTG will perform periodic software and security updates, install additional capacity, and replace any faulty hardware within the underlying infrastructure, per the manufacturers recommendations and industry best practices. Changes will occur during declared maintenance windows that will be agreed upon in advance with the Customer
CUSTOMER RESPONSIBILITIES
Customer is responsible for managing and securing the host operating system including any script, application, or operating system updates.
Customer is fully responsible for the installation and operation of any and all scripts and applications installed on any customer managed servers or virtual machines.
SCTG will not troubleshoot or provide any support relating to malfunctioning scripts or applications. Customer is responsible for maintaining the latest version of any and all installed scripts and applications, as well as the security of all scripts and applications installed on VMs. SCTG does not provide security auditing or disinfection of exploited software or servers. If a Customer needs support regarding a specific script or application, please contact the software vendors support resources.
Customer is responsible for monitoring the capacity thresholds of storage environments. SCTG monitors storage-level capacity, but this may not match Customer usage due to application and operating system differences.
Customer is responsible for maintaining current backups of customer-owned data. ServerCentral offers a fully managed backup service for systems utilizing Managed Object Storage. Please contact sales@servercentral.com for more information.
Customer is responsible for maintaining the list of authorized personnel on the SCTG Customer Portal. Customer is also responsible for maintaining any user accounts created for the Managed Object Storage Service. SCTG is not responsible for any unauthorized access to the Managed Object Storage Service due to out of date access list information
Customer will designate and maintain a Technical Contact who can be made available to ServerCentral for troubleshooting or questions.

Additional Questions

For more information, visit https://www.servercentral.com/cloud-storage or contact us at (312) 829-1111 and sales@servercentral.com.

About ServerCentral Turing Group (SCTG)

SCTG offers cloud-native software development, AWS consulting, managed cloud infrastructure, and global data center services. We work with companies, large and small, that see IT as their critical success factor.

SCTG is a Type II AT-101 SOC 2 audited company and PCI-DSS compliant. We are proud to be an 8-Time Inc. 5000 Honoree.

Learn more at www.servercentral.com or call us at (312) 829-1111.