EXECUTIVE SUMMARY

The web has transformed into an explosion of application programming interfaces (APIs), bringing all walks of technologies to the cloud and mobile-centric applications. One area in the API paradigm that has become very popular is Amazon’s S3 API de facto standard, giving applications a simple way of storing and retrieving data without having to instrument logic that is storage-system-aware. The MapR Data Platform has been expanded to support multiple data protocols, including S3. This paper will focus on the killer combination of the MapR Data Platform and the S3-Compatible API.
## CONTENTS

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>S3 BASICS</td>
<td>2</td>
</tr>
<tr>
<td>POWERED BY THE MAPR DATA PLATFORM</td>
<td>2</td>
</tr>
<tr>
<td>INTRODUCING MAPR S3 GATEWAY</td>
<td>3</td>
</tr>
<tr>
<td>ERASURE CODING</td>
<td>4</td>
</tr>
<tr>
<td>MULTIPLE PROTOCOLS</td>
<td>4</td>
</tr>
<tr>
<td>HIGHLY SCALABLE, COST-EFFECTIVE STORAGE</td>
<td>5</td>
</tr>
<tr>
<td>SINGLE VIEW GLOBAL NAMESPACE</td>
<td>5</td>
</tr>
<tr>
<td>MULTIPLE DEPLOYMENT OPTIONS</td>
<td>5</td>
</tr>
<tr>
<td>ROBUST AND UNMATCHED PROTECTION SCHEME BUILT-IN</td>
<td>6</td>
</tr>
<tr>
<td>IN SUMMARY, WHY S3 ON MAPR?</td>
<td>8</td>
</tr>
</tbody>
</table>
INTRODUCTION

S3 API capability on top of the MapR Data Platform is a killer combination. The MapR Data Platform is specifically designed as a more cost-effective way of keeping pace with the volatility and out of control state of data growth and management, which becomes even more important with data being created in a S3 paradigm.

In the past, storage was reasonably straightforward – IT had predetermined capacity size, it performed well, and the cost was well understood. Clear solutions with a consistent business model were delivered with well-defined and integrated hardware and software. Today, data proliferation is the new norm that has placed tremendous pressure on this model, which has led to a new concept of Software-Defined Storage (SDS). SDS is focused on sustained growth and reduced cost in delivering higher quality, reliability, and endurance. In fact, Gartner has rightly pointed out:

"Leaders are looking for software-defined storage products that offer the potential for better total cost of ownership, efficiency, and scalability to address exponential-data growth needs and to benefit from innovations from hardware and software players independently."

Amazon S3 API has become the de facto standard for accessing data for next-generation cloud-centric and mobile-centric applications. S3 API provides the necessary flexibility in retrieving data and storing data using a RESTful interface. S3 treats data as data objects, unlike traditional filesystems, while still using traditional files and directories. S3 removes the details of backend file system infrastructure from the application and supports basic commands such as get (read) a data object or put (write) a data object.

This paper is focused on how the value proposition of MapR in combination with Amazon S3- Compatible API brings to the market an unmatched storage solution in the industry.
S3 BASICS

The S3 API is a RESTful interface that provides applications the capability to get, put, list, and delete data. In S3, data is represented as a data object. S3 is unaware of the data format or the data structure of the data. Getting or putting of data is designed to be simple. S3 has two basic constructions: “buckets” and “data objects.” Data objects are grouped into a logical container called a “bucket.” The caller will have the flexibility to name the buckets and name the data objects. The S3 API provides the ability to create, list, or delete a bucket and provides a way to get, put, list, or delete a data object within the bucket. In addition, the S3 API has the following capabilities:

Access. Bucket access is controlled using an S3 Policy API and/or leveraging the underlying MapR File System security.

Metadata. Offers system metadata and user define information created by the user when the object is stored.

Search. Buckets can be searched with object-level granularity.

Notifications. Streaming events are used to notify changes to data from the S3 API interface.

POWERED BY THE MAPR DATA PLATFORM

MapR Data Platform is the industry’s only exabyte-scale data store for building intelligent applications.
Legacy storage solutions were built for an on-premises era of proprietary hardware, limited scale, manual control, and fragile operating environments, and fail in meeting today’s business challenges. As the power of commodity devices increased, vendors began claiming that their offerings were constructed of commodity hardware and intelligent software, yet wouldn’t allow customers to select their hardware. The reality is that a legacy storage array is extraordinarily expensive and cannot efficiently scale, given that the vendors invest money in developing custom ASICs, custom circuit boards, and custom real-time operating systems to tap into proprietary interfaces. Software-Defined Storage (SDS) takes an entirely different approach, using commodity x86 hardware and standardized operating systems, thereby leveraging existing low-cost, reliable equipment. The reality of today’s cloud is x86, Ethernet networking, PCI-e, and standardized motherboards and buses — nothing else. The MapR approach is to leverage these proven technologies and concentrate on cost-efficient storage with exabyte data scaling, high reliability, and recoverability.

MapR supports the most stringent speed, scale, and reliability requirements across multiple edges, on-premises, and cloud environments. The MapR Data Platform makes it easy to store any data at exabyte-scale and supports trillions of files, provides enterprise-grade features to be the system of record for large global enterprises, and uniquely combines analytics and operations into a single platform, enabling intelligent application development.

**INTRODUCING MAPR S3 GATEWAY**

The MapR Object Store with S3- Compatible API Gateway for S3 is built on top of the MapR Data Platform to combine the best data platform and the capabilities of S3. MapR has built-in capabilities for multiple protocol support, erasure coding, and global namespace. The MapR Gateway conforms to the Amazon S3 de facto standard RESTful API, supporting a wide range of S3 capabilities, including:

- **Global Namespace**
- **Multi-Tenancy Support**
- **Works with AWS SDK & Client**
- **User-Defined Metadata**
- **S3-Compatible Error Codes**
- **Data Secure TLS (HTTPS)**
- **Multipart Upload**
- **Multiprotocol Support [NFS, POSIX, S3]**
- **Support Blend of S3 Policy Security and MapR Security**
- **Drill Integration to Search on Tags and Metadata**
- **Event Notifications (a Kafka API-Based Pub/Sub System)**
ERASURE CODING

MapR Erasure Coding (EC) brings additional value to the S3 paradigm. S3 objects typically need higher reliability and lesser storage footprint. Optionally, EC can be enabled for your S3 data objects to reduce S3 storage footprint by roughly 50%. EC technology reduces storage footprint and maintains data protection by breaking the data into fragments that are expanded and encoded with a configurable number of redundant pieces of data, stored by striping the data across different disk locations.

MULTIPLE PROTOCOLS

One of the most significant advantages of the MapR Data Platform is its support for multiple protocols. Data is useless without tangible ways to reach it. MapR supports NFS, HDFS, POSIX, Fuse, SMB, SQL, and S3-Compatible API. This provides the most flexible option in terms of providing multiple access protocols to your data. For example, a cloud-centric application can collect and write data to MapR Object Store using S3-Compatible API, and then a legacy batch program can access the same data via NFS. Applications that read and write files using standard operating system calls can use S3-Compatible API to upload data into MapR.
HIGHLY SCALABLE, COST-EFFECTIVE STORAGE

The MapR SDS design provides a high-scale, reliable, globally distributed data store that creates a data fabric for managing files and containers, leveraging existing, low-cost commodity x86 hardware and standardized operating systems. MapR supports the most stringent speed, scale, and reliability requirements across multiple edges, on-premises, and cloud environments. MapR makes it easy to store any data using any protocol at exabyte-scale and supports trillions of files, provides enterprise-grade features to be the system of record for large global enterprises, and uniquely combines analytics and operations into a single platform, enabling intelligent application development.

SINGLE VIEW GLOBAL NAMESPACE

MapR global namespace capability can be leveraged when using multiple clusters, generally used for disaster recovery purposes, which can be very useful for MapR Object Store Data. The global namespace facilitates access to files on any remote cluster as if they were part of the local cluster, regardless of their physical location. The global namespace offers a number of benefits:

Copy Data Management. The need to move files from one cluster to another reduces significantly. You can reduce the number of copies of files by extending the permissions to users that need the information.

Data Security. An application hosted in New York is able to access a file located in Chicago. Sometimes data is not allowed to leave certain regions, due to security. The MapR global namespace preserves boundary regulations while still allowing other authorized departments located elsewhere to access the data.

Mirroring. Volumes across geographically remote areas take longer to access. With MapR, it’s possible to mirror volume across the pond to facilitate faster access. Delta changes are mirrored (after compression) to optimize bandwidth. Mirroring is also an industry-standard method for disaster recovery.

MULTIPLE DEPLOYMENT OPTIONS

The MapR highly scalable S3 solution is designed with the MapR Object Store Gateway instance, responsible in the management of all the inbound S3 requests into the MapR Data Platform and conforming to the Amazon S3 de facto standard. The MapR Object Store with S3-Compatible API Gateway will communicate with the MapR Data Platform as it handles the retrieving or storing of data to the file system.

The Gateway for the MapR Object Store can be deployed within MapR cluster nodes or can be deployed on the edge as well as in a containerized environment. The Gateway can be deployed along with applications on edge nodes or in a container.

A single Gateway can handle roughly 4000 reads per second or 1200 writes per second, assuming a 1 GB file, which is sufficient to handle many workloads. The Gateway is also protected using MapR Warden, which manages automatic restarting in the unlikely event of an unexpected server failure.
ROBUST AND UNMATCHED PROTECTION SCHEME BUILT-IN

The MapR security model is built directly into the platform from day one, supporting the ability to apply security protection directly as data comes into and out of the platform without requiring an external security manager server or a particular security plugin into each ecosystem component. MapR security semantics are applied automatically by design for data being retrieved or stored by any ecosystem, application, or users out of the box.

In addition to the MapR built-in security scheme, S3 bring another layer called S3 policy security. It secures data coming in and out of the RESTful API, using its define structure (called “policy”). A customer has the flexibility to use the MapR built-in security scheme alongside the S3 policy security.

MapR built-in security consists of authentication, authorization, auditing, and data protection, using platform-level capabilities that don’t require external security tools or plugins. Such a solution is therefore complete and cannot be bypassed by components that have not been carefully altered to work with an external security tool.

A secured MapR cluster provides for network-safe authentication. All access to the system (both user-to-service and service-to-service) must be authenticated. MapR supports Kerberos as well as the similar MapR native security equally – customers can choose which best meets their needs. Kerberos authentication, of course, can integrate into an existing enterprise Kerberos infrastructure, while the advantage of MapR native security is that it is built into the product and does not require additional software and external management complexity. In any case, once authenticated, all access is done using secured RPCs, which leverage the MapR tickets to authenticate in a network-safe manner. When the MapR Data Platform is used primarily for native file access, either NFSv3-based access (with its weak, host-based authentication) or MapR POSIX Client can be used, which authenticates securely from the client node to the cluster while still allowing native Unix applications to access the file system data without any explicit use of MapR security. MapR security seamlessly leverages and is compatible with standard Linux user information. The MapR authentication process uses Linux PAM to validate passwords and Linux nsswitch for user and group information – making MapR behave just like any native Linux application.

All access to data stored in MapR has access control checks. MapR supports both POSIX mode bits and more advanced MapR Access Control Expressions (ACEs) to protect all files and directories. For those leveraging the full power of the converged platform, ACEs can also safeguard tables and streams.
Access Control Expressions are a unique, advanced feature of the MapR Data Platform. ACEs are Boolean logic expressions that use the standard Boolean operators – AND, OR, NOT – to express an access constraint. While obviously more powerful than the primitive Unix mode bits found in old-school file systems, ACEs are also more powerful than the more recent Access Control Lists (ACLs). ACLs, while adequate to protect data, are not very expressive – they make it difficult to express seemingly trivial access control requirements. For example, using ACEs, one can easily say “only members of groupA AND groupB can access this volume.” That cannot be said with ACLs; instead, the administrators have to create a new group called groupAB and put all of the right users in that group. This is both cumbersome and hard to scale.

In support of proper multi-tenant isolation, MapR controls access at the volume level using ACEs as well. This makes it easy for a system administrator to ensure that all data in a volume is accessed or modified only by a specific set of users, regardless of what individual file and directory permissions may say. When building a multi-tenant environment, where tenant access isolation is crucial, this capability is essential.

Finally, S3 policy security can work in conjunction with MapR Data Platform security, as outlined above. S3 provides a layer of protection at the S3 API layer, and MapR security provides industrial-strength security at the fabric layer.

All storage-related traffic in MapR travels over the network using the MapR highly efficient RPC protocol. When security is enabled, the header of all RPCs are encrypted, and the entire message, including all data, can be encrypted as well. Full data encryption can be controlled on a per-file basis, enabling flexible control of security behaviors. All encryption is done automatically, using the Intel AES-NI hardware for optimal performance. In addition, MapR offers an option to encrypt data at rest. MapR supports standard encryption methods, which include AES256/GCM and Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol that secures several channels of HTTP traffic, supporting TLS 1.2.

MapR includes robust, high-performance auditing built directly into the product without any complex add-ons. When auditing is enabled, all data access (file, directory, table, stream) generates audit records to a Kafka API-based pub/sub system, supporting a real-time processing of audit data. Audit records record both metadata modifications and any read or write actions. Auditing introduces very low overhead as records are coalesced in memory with duplicates automatically suppressed within a configurable interval before writing to disk. Auditing is also highly configurable and can be enabled on a per volume or per file basis. Finally, all administrative operations against the storage system (which are coordinated by the CLDB) generate audit records, ensuring that all administrative operations can be monitored appropriately.
IN SUMMARY, WHY S3 ON MAPR?

The addition of the S3-Compatible API to the list of multiple protocols provided by the MapR Data Platform is a killer combination. Data can be written to the MapR Object Store with S3-Compatible API and processed using a wide range of data protocols, including S3. In addition, MapR is specifically designed as a more cost-effective way of keeping pace with the volatility and out-of-control state of data growth and management, which becomes even more important with data being created in an S3 paradigm. And, when combined with erasure coding technology, it reduces storage footprint and maintains data protection.