SCALITY

Data Security in the Scality RING

Overview of the Security Mechanisms in the Scality RING

Scality Technical White Paper

February 2017

Data Security in the Scality RING

Overview of the Security Mechanisms in the Scality RING

Table of Contents

Introduction

When it comes to designing a cloud-based storage infrastructure, there are more important design principles to address than simply storing files. A well-designed storage solution will take into consideration compliance needs and implement proper security protocols and best practices in the architecture. The scope of this whitepaper is to describe how the Scality RING addresses compliance needs for organizations and how security is implemented in the RING's architecture.

Chapter 1: The Impact of Security Regulations

There are many different regulatory rules out there that organizations are using. For example, HIPAA is a set of security rules set of rules and safeguards that must be implemented when working with public health information and FIPS-140-2 is used by Government organizations to list requirements and standards for encryption used. Depending on the nature of a particular business, organizations will be impacted by some form of compliance rules whether it is a regulatory compliance such as HIPAA or FIPS 140-2. IT organizations will have to adjust their solutions, services, and workflows to accommodate regulatory practices which can be intensive and chaotic at times.

The good news is that there is some common ground between compliance regulations. Here are a few common requirements that organizations take into consideration.

- **Role-based Access** - Not everyone should have privileged access to sensitive information in an organization. Different levels of access should be provided through roles such as user, admin, etc to control access to sensitive data.
- **Data Encryption** - Encryption must be used when uploading and downloading data.
- **Data Integrity** - Ensure that protections are in place to prevent data from being tampered or altered.
- **Network Security** - Firewall rules and network segmentation to protect systems and services.
- **Auditing** - A way to record all the transactions and changes made to a system.

The following chapters will explain how the Scality RING implements the compliance requirements that organizations need to remain compliant with regulations.

Chapter 2: The Scality Ring Architecture

The Scality RING architecture is composed of several layers as displayed in Figure 1. Let's explore each layer in detail to get a better understanding of the RING architecture.

2.1 Connector Layer

The Scality Ring connector layer provides support for the following protocols:

- Object: S3, REST.
- File System: FUSE, NFS, and SMB.

The connector layer is also in charge of chunking files and dispersing the chunks on the Scality Ring using file replication or erasure coding.

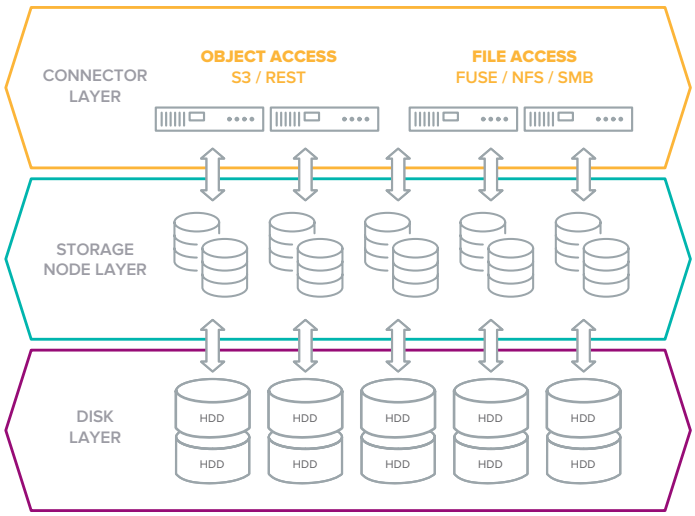

Figure 1. – Scality Ring Architecture Layers

2.2 Storage Node Layer

The Storage Node layer consists of a distributed peer-to-peer architecture that ensures files and metadata are properly distributed amongst the storage nodes and disks in the cluster. A RING installation can even span across multiple physical sites and tolerate the loss of an entire site. The RING supports data protection mechanisms such as erasure coding and replication. This intelligent architecture design provides organizations with maximum data durability.

2.3 Disk Layer

This is the layer where the file data chunks are written to SAS/SATA drives and the file metadata is written to solid-state drives (SSD's).

Chapter 3: Connector and User Interface Security

3.1 Scality S3 Connector

- The Scality S3 Connector supports AWS S3 certificate-based authentication (Signatures v2 and v4) with support for HTTPS to provide secure access to the RING storage.
- The Scality Scality S3 Connector implements IAM for Multi-Tenancy:
  - Accounts, users, and groups
  - Access/Secret Key pairs
- The Scality S3 Connector supports identity federation for delegated access to APIs:
  - Any SAML 2.0 compatible identity providers
  - Active Directory Federation (ADFS)

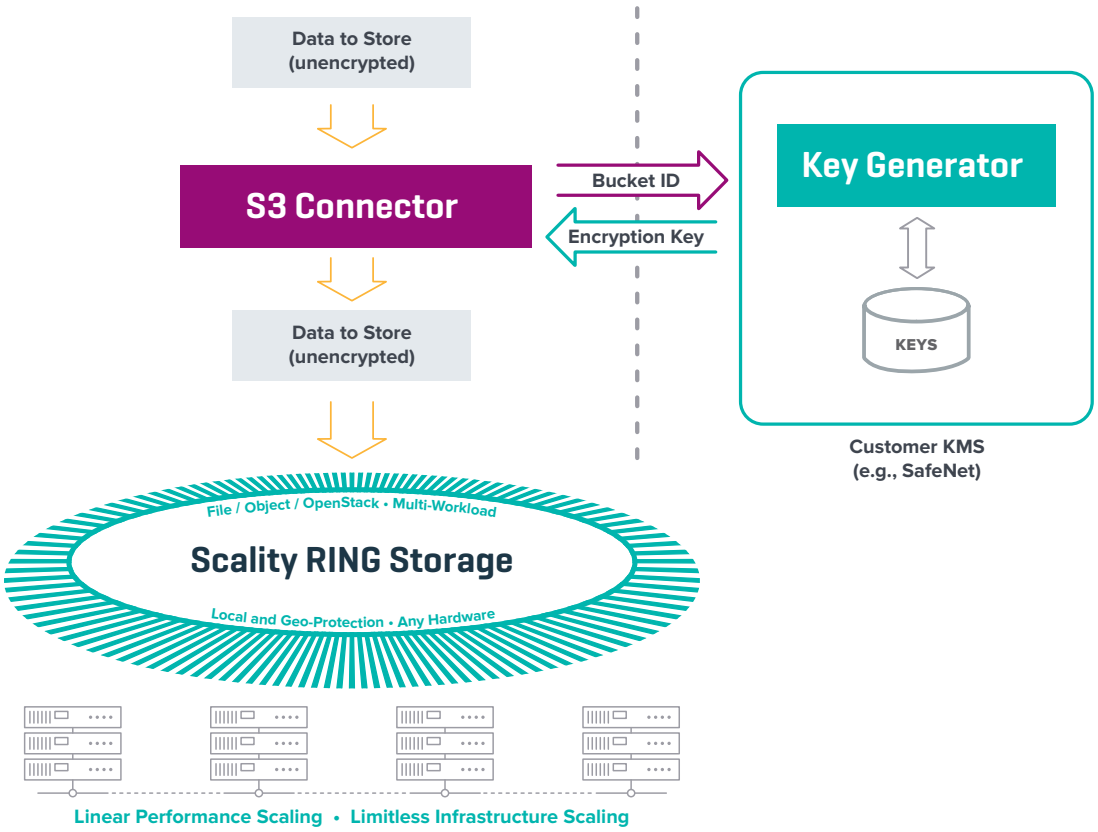

Figure 2. – S3 Connector Architecture

3.2 REST Protocol

The REST protocol supports HTTPS and can be configured to use basic authentication with the Apache web server to require a username and password.

3.3 File System Protocols

- The Scality NFS v3 connector supports Kerberos KDC.
- The Scality SMB connector provides Active Directory Server integration and support for simple Windows ACL's (user and group).

Chapter 4: Core RING Security

4.1 Logging

All actions performed by a user are in the Supervisor Web Administration console are logged to a file (by default /var/log/scality/dsup/audit.log) on the Supervisor server and can also be set to another location. The audit log file provides detailed information on the user, date and time, name of the action performed (e.g. list, retrieve, delete, modify), RING component (Supervisor, Connector, Storage Node) on which the action was performed, result of the action (successful or not), duration of the action, and the detailed error message if the action wasn't successful.

4.2 Versioning and WORM

As mentioned earlier in this paper, data integrity requirements are in place to ensure that information is not tampered or altered. The S3 connector for the RING supports the versioning features from the Amazon S3 API. If enabled, this feature will allow users to keep track of different versions of a file on the RING storage. Using the standard S3 API calls, organizations will have the ability to view the modification dates and times of each file and it's checksum as well as the ability to download previous versions of a file.

Versioning is not always enough to address compliance requirements so organizations look for solutions that support Write once read many (WORM) operations. If an organization uses a solution that supports WORM, they can be assured that data will be read only and can not be altered. To help address this compliance requirement, Scality created a joint solution with iTernity that can meet legal and industry-specific regulations to provide a compliant long-term archiving solution.

For more information, please check out the link to the solution sheet with iTernity in Appendix A.

4.3 Checksums

The Scality RING uses a built-in CRC-32 checksum mechanism to ensure that the data being read is the same that was originally written to the RING. Upon reading replicated or Erasure Coded chunks on the disks, the RING calculates a CRC-32 checksum for each of the chunks it has to read and compares it to the CRC-32 checksum that was calculated upon writing the chunk (and stored in metadata with the chunk). If any of the chunks are found to be corrupted, (meaning the checksums do not match), the RING does two things:

1. Uses another replica or EC chunk to serve the requested data
2. Launches a chunk repair operation to repair the corrupted chunk (basically to replace the replica chunk by another replica or recalculates an Erasure Coded chunk).

4.4 Data Encryption

Encryption on the disk level can be done today from array controllers or with encrypted

drives. The Scality S3 connector supports bucket level encryption via an API extension which is a customized HTTP header used when a file is uploaded. The files are encrypted using OpenSSL with the AES-256 standard and the RING uses an external Key Management Service (KMS) to manage the encryption keys.

4.5 Supervisor Security

The Supervisor is the web-based GUI for managing, monitoring, and provisioning resources on the RING. The Supervisor has the following security mechanisms:

1. HTTPS with password authentication.
2. Role-based Access Control (RBAC).

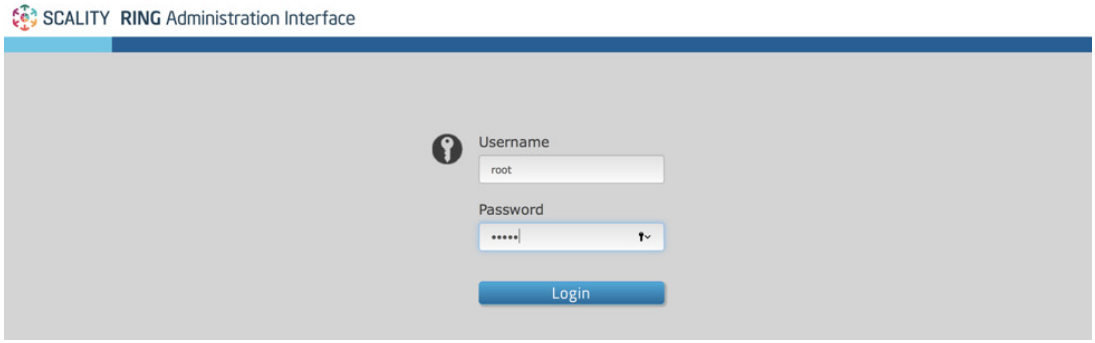

Figure 3. – Scality Ring Supervisor Login Screen

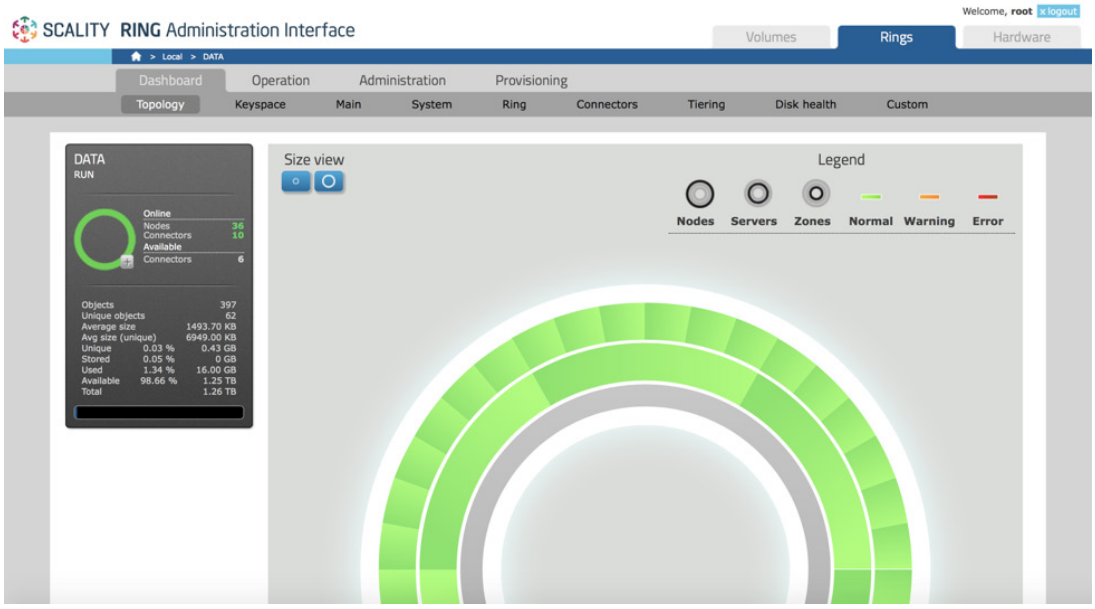

Figure 4. – Scality Ring Supervisor Ring Overview

Summary

This paper explained what it takes to have a compliant storage solution built for the enterprise and went over the impact of security regulations and common compliance requirements. The security mechanisms of the Scality RING architecture was explained in detail ranging from the application layer to the storage layer. We hope that you now have a better idea of the Scality RING architecture and how we implemented common compliance features and security.

Appendix A

A.1 Going beyond this White Paper

1. Information on Scality products and use cases can be found here:
http://www.scality.com

2. For more information on the Scality Ring, please view the technical white paper:
http://storage.scality.com/white-paper-scality-technical-wp.html

3. Get more information on the S3 Connector in the following white paper:
http://storage.scality.com/white-paper-scality-ring-s3-connector.html

4. Get more information on the joint solution with iTernity:
http://www.scality.com/partners/iternity/

WPSR1-1702