SDS Object Storage – 7 Key Data Security and Protection Features

Object storage used to be just the slow final resting place for archive data. That is no longer true. As enterprises shift to cloud-native technologies, object storage is often used for active data. Fast flash-based object storage is even displacing primary storage for some use cases and applications.

With the growing importance of object storage in the enterprise, and the trend toward software-defined storage (SDS) solutions, organizations would do well to pay special attention to the data security and data protection features of SDS object storage solutions.

Object Storage – 7 Key Data Security and Protection Features to Evaluate

To that end, here are seven data security and data protection features enterprises should consider for SDS Object Storage. For this article, we define data security as securing data against unauthorized access and data protection as protecting data from loss.

Data Security Features

Access control – Access control features ensure only authorized persons to manage the SDS solution and access your data. One way these products do this is through directory services integration. Organizations can authenticate its data users and administrators through its existing directory
services application. Directory service protocols of interest include AD, LDAP, IAM authentication, and Object-level Access Control Lists.

**Encryption** – Encrypting scrambles data such that it cannot be deciphered without the assigned encryption key. At a minimum, storage solutions should encrypt data at rest. Many solutions support data in-flight encryption (that is, while data is transmitted over a network). Key lengths vary; however, many providers support AES-256 encryption key lengths. One clarifying question for your solution provider: Who owns the encryption keys for data managed on-premises and in the cloud?

**Multitenancy** – As an additional security wall, some organizations require multitenancy features to isolate different business units’ storage from each other. Solution providers depend on this feature to keep its customer’s data segregated. If your organization contains different business units or legal entities, you will want to ask about this feature.

**Data Protection Features**

**Replication** – Replication protects an organization’s data by making redundant copies stored in different locations. The object storage application maintains access to data for users and applications in case of failures such as those from hardware, site, or network outages. SDS object storage applications often provide multiple replication options. Enterprises will need to consider the options best suited for their priorities.

**Erasure coding** – Erasure coding protects data by breaking data up, expanding it, encoding it, and storing it as chunks distributed across multiple drives. Should data corruption or component failure occur, data can be rebuilt from remaining
chunks. Like replication, erasure coding options can be configured based on the availability priorities of the organization.

**Data immutability** – Data immutability protects object data from being modified or deleted. Through their SDS application, customers can select immutability profiles for their object storage. This may be beneficial for legal or other business reasons. IT departments value data immutability in the event of ransomware attacks. While not circumventing ransomware attacks per se, data immutability helps minimize an attack from becoming a catastrophe by offering a means for recovery. See Jerome Wendt’s article on Immutable Storage Options in a Ransomware World.

**The Triple AAA’s to Compliment Data Security and Protection**

AAA’s – APIs, analytics, and auditing – API’s, analytics, and auditing features complement data security and protection. API’s enable integration into existing automation frameworks. Analytics enable some solutions to issue alerts when suspicious activity occurs. Auditing tracks the who, what, and when of data access and modification. By helping organizations identify which files need to be rolled back to a previous version. Auditing also helps enterprises identify the path attackers used to get to the data.

**DCIG is Researching SDS Object Storage**

Given the growing importance of object storage, it behooves enterprises to consider how SDS object storage solutions they are considering secure and protect their data.

DCIG is initiating research into the SDS Object Storage marketplace. DCIG invites SDS object storage providers to
participate in the survey research taking place through August 31st, 2021. DCIG plans to publish results in the 4th quarter as one or more DCIG TOP 5 reports. These reports help IT decision-makers save valuable time through its succinct independent analysis of solutions.

**IT professionals**

Readers interested in the research results should sign up for the DCIG weekly newsletter. Subscribers to DCIG newsletters will receive an announcement of the TOP 5 SDS Object Storage providers, and other upcoming DCIG reports may publish. Announcements will include links enabling individuals to download the reports at no cost. Sign Up for the free weekly DCIG Newsletter.

**Attention SDS object storage solution providers**

The invitation to participate in the survey research is open to providers with an SDS product supporting object storage protocols as of August 1st, 2021. SDS vendors can ensure they receive an invitation to participate by contacting DCIG through the Contact Us page.

Technology providers interested in licensing DCIG TOP 5 reports or having DCIG produce custom reports, please contact DCIG for more information.