PoINT Archival **Gateway**

**Your data is
the key, so don't
lose it.**

Contents

Introduction

Growth of unstructured data is one of the biggest IT data center infrastructure challenge for enterprises, according to recent surveys of research firms. This challenge cannot be solved economically and technically meaningful with file and block storage (or NAS and SAN) based on hard disk or flash technology.

Additionally, studies show that the majority of unstructured data is inactive. This data is not frequently used, but still needs to be preserved for business or compliance reasons. It does not make sense to store huge amounts of inactive data on hard disk or flash based storage systems.

Software-defined object storage offering a standardized REST API, like Amazon S3, using standardized tape technology as storage medium, like LTO, provides a solution to this challenge.

Like file and block storage, object storage is a way to store data. The difference between file, block and object storage is that object storage has been designed for scalability, cost-effectiveness, reliability and high availability. In principle the way to store data is independent from the underlying storage media. E.g., in the same way as files can be stored on hard disk and tape in a file system structure, also objects can be stored on different storage media.

Considering the massive growth of unstructured data within the next years in combination with the fact that majority of this data becomes inactive very fast, tape is the only storage media which provides sufficient data capacity with an acceptable price ratio. In combination with its WORM capabilities tape technology also fulfills archiving requirements.

Additionally, removable media like tape create an "air gap" against malware. Thus, tape technology is perfectly suited for data protection and backup.

For these reasons, an approach which combines object storage and tape technology as storage medium provides an innovative and economic solution for the data growth problem. Additionally, compared to all the storage media available, tape technology has the potential for essential capacity improvements.

PoINT Archival Gateway is a software-defined scale-out object storage system designed to store and manage massive amounts of data on tape libraries with outstanding performance. PoINT Archival Gateway provides a standardized S3 REST API and supports a wide range of tape libraries.

In this technical white paper, a detailed technical description of PoINT Archival Gateway is provided.

Client Network   PoINT Archival Gateway   Tape Library
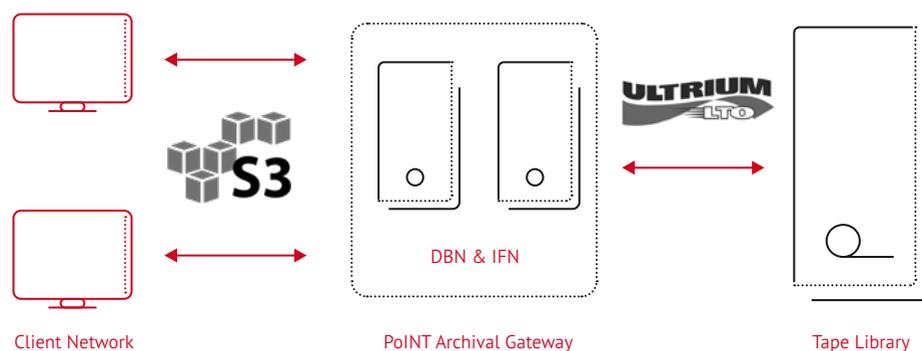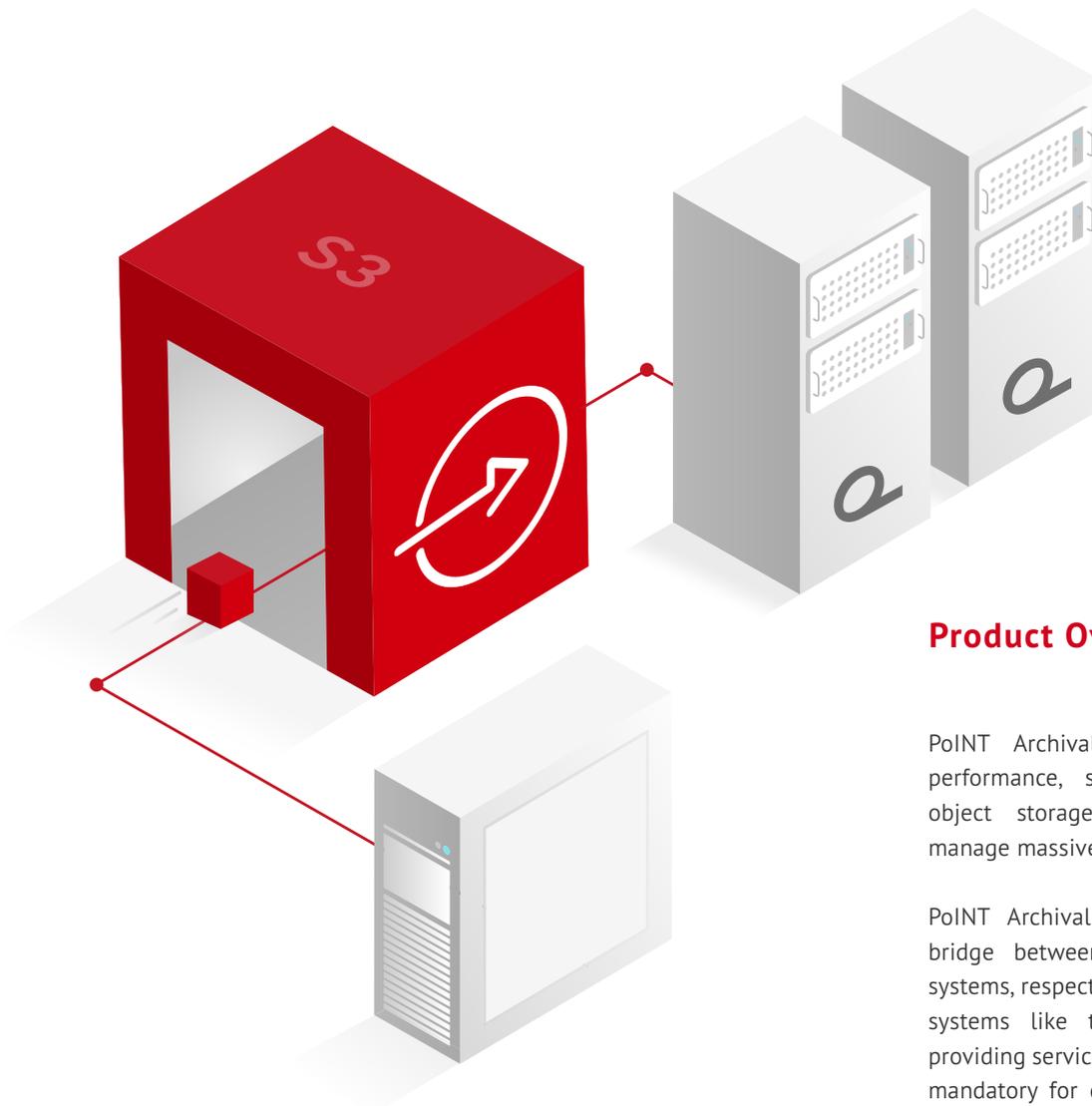
Archival Gateway

PoINT Archival Gateway offers standardized interfaces and protocols like the Amazon S3 REST API which may be used by the actual client applications for storing and reading data on the supported archival storage devices, drives and media. Essential services provided by PoINT Archival Gateway include user, data and storage management as well as access control, logging and monitoring.

Product Overview

PoINT Archival Gateway is a high-performance, scale-out, software-based object storage solution designed to manage massive amounts of data.

PoINT Archival Gateway is building a bridge between client applications or systems, respectively, and archival storage systems like tape library systems by providing services and functions which are mandatory for data archival solutions in enterprise data centers.

—— KEY FEATURES

- High performance in terms of data and object rates
- High availability and reliability
- High scalability (incl. load-balancing, redundancy and failover)
- Industry standards (S3 REST API, LTO Tape Format)
- Object versioning
- Data protection (erasure coding, authentication and encryption)
- Self-monitoring, reporting and alerting
- User management based on domain services (AD, LDAP)

Use Cases

PoINT Archival Gateway provides a solution for a wide range of requirements. With its standardized S3 REST API PoINT Archival Gateway can be used by many S3-capable applications.

The following figure gives some examples of applications and environments which can integrated with and connect to PoINT Archival Gateway.

PoINT Archival Gateway fulfils archiving and compliance requirements thanks to WORM functionality and integrated retention management. As a result, saved data is protected not just against unintended deletion, but also manipulation (e.g. from ransomware attacks).

PoINT Archival Gateway provides persistent data management for meeting legal and business data archival requirements. Appropriate retention rules can be enabled and specified on object repository level. The rules define how and when existing objects may be modified or deleted.
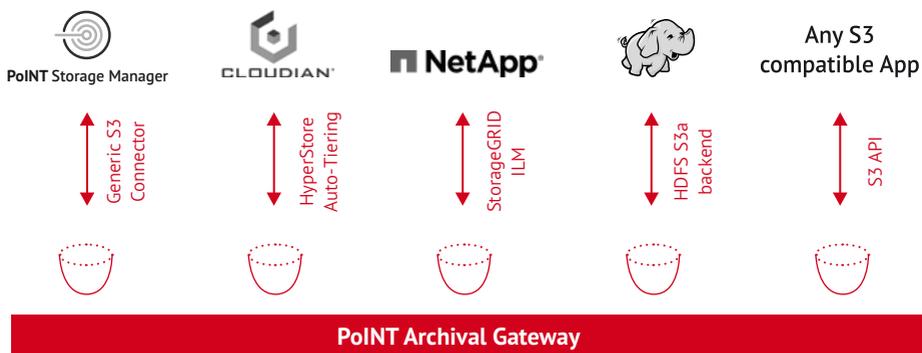
Public cloud storage providers like AWS and Microsoft Azure offer different S3 storage classes with different performance features to their customers. On premises object store products which are used as private cloud offer only one storage class which is typically hard disk based. This is inefficient because active and inactive data are stored on the same storage technology.

The combination of hard disk-based object store with PoINT Archival Gateway allows to tier inactive data from hard disk to tape. For this purpose, many object store products provide already integrated ILM functions.

Backup of cloud and object data becomes more and more important. It has already happened that public cloud providers disappeared and stored data was no longer accessible. Also, clouds are not invulnerable to malware attacks. The same applies to data on on-prem object stores. For this reason, backup of cloud and object data is essential.

PoINT Archival Gateway allows to make backups from your cloud and object data to tape in its native S3 form. Your object data will be saved in the same structure as your original data. This means saved data can be directly accessed through the S3 interface of PoINT Archival Gateway. A long retrieval process is not necessary.

PoINT Storage Manager — Generic S3 Connector

CLOUDIAN — HyperStore Auto-Tiering

NetApp — StorageGRID ILM

— HDFS S3a backend

Any S3 compatible App — S3 API

PoINT Archival Gateway

Architecture and Terms

The figure below provides an overview of the architecture and terms used in the scope of a PoINT Archival Gateway installation.

—— OBJECT REPOSITORY (BUCKET)

PoINT Archival Gateway allows to create an arbitrary number of Object Repositories (Buckets), each of which can have different settings and restrictions (e.g. size limitations, access rights). Client applications and systems can store and read objects in the Object Repositories by using the S3 REST API of PoINT Archival Gateway. Object Repositories of the same Archival Storage Partition share the same Protected Volume Arrays.

—— ARCHIVAL STORAGE PARTITION

PoINT Archival Gateway uses a logical construct called Archival Storage Partition

as management units for the entire archival storage space available on all Archival Storage Volumes which are available in the Archival Storage Devices. Multiple Archival Storage Partitions can be created, each of which having different settings and restrictions (e.g. size limitations, access rights, levels of protection, redundancy or availability) and using separate Archival Storage Volumes. By default, PoINT Archival Gateway automatically extents the size of Archival Storage Partitions by allocating additional Protected Volume Arrays (see below) when the lastly allocated array has completely been filled with data.

—— ARCHIVAL STORAGE DEVICE

Archival Storage Devices are media changer devices (tape libraries or tape loaders) with a specific number of integrated tape drives.
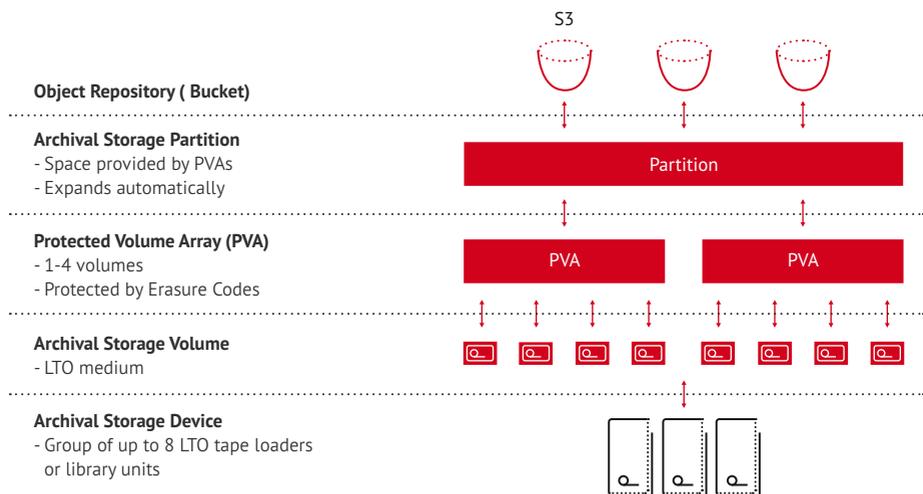
Design and Concept

PoINT Archival Gateway leverages the object storage architecture and manages data as objects. Each object includes a unique identifier of the object, the data itself as well as a variable amount of custom metadata. This architecture basically allows scalable retention of massive amounts of unstructured data on removable media like tape media in libraries.

PoINT Archival Gateway explicitly separates data and metadata. Unique identifiers and metadata are stored in common databases, while data are stored on tape media. Copies of the metadata and unique identifiers are stored on storage media, too, to support disaster recovery and verification processes.

Object storage architectures typically use databases to store metadata and unique identifiers. In contrast to other architectures (e.g. file systems and their hierarchical structures), databases do not impose any kind of limit on character sequences which can be used in unique identifiers and custom metadata or on the number

of object records. In addition, databases support arbitrary extension of existing records as well as indexes and highly performant queries covering all existing records. These features and functions are essential for supporting various kinds and versions of object storage interfaces like the S3 REST API.

This separation of data and metadata is reflected by the design of PoINT Archival Gateway which requires assigning the services to separate and dedicated server systems. Consequently, the PoINT Archival Gateway software consists of two software packages, each of which may be installed on a dedicated server system. A dedicated server system including its basic operating system software and the software package is called a gateway node. Defined by the installed software package, a gateway node serves exactly one of two possible purposes.

INTERFACE NODES

A gateway interface node (IFN) primarily is the communication partner for client applications or systems. By means of dedicated interface modules, it provides an S3 REST API for storing and reading objects to client applications and systems and transfers data between client applications or systems and the Archival Storage Volume (i.e. tape media).

In detail, the IFNs provide the following modules and services:
• HTTP service module (i.e. S3 REST API)
• Data buffering module
• Data encoding module (e.g. erasure coding, hashing, encryption)
• Driver module for tape drives
• Metadata caching module (e.g. caching of object metadata and configuration data)
• Communication module for metadata exchange with database node

DATABASE NODES

A gateway database node (DBN) primarily provides central database services to the IFNs. The database holds the index of the objects which have been stored (e.g. object keys and metadata, storage locations of object data on the Archival Storage Volume (tape medium), as well as configuration and maintenance data of PoINT Archival Gateway. Additionally, the database stores data from logging and monitoring processes and provides corresponding auditing services and log files. Further central services are

the system configuration (Admin GUI) and the management and control modules for Archival Storage Devices (tape libraries), which therefore are also located on this node.

PoINT Archival Gateway requires at least one working IFN and one working DBN to be operable.

PoINT Archival Gateway fulfills the highest levels of performance, availability and scalability requirements by means of this fully scalable and redundant design, providing scalable performance and redundancy levels for both service and data entities. Because scalability and availability of a single node is restricted due to limitations of server hardware and operating systems, PoINT Archival Gateway supports installing multiple DBNs and IFNs in a single deployment in order to build clusters for increasing performance (i.e. load balancing) and availability (i.e. failover and redundancy).

PoINT Archival Gateway automatically performs all tasks which are required to reconstitute operability and consistency of a cluster node which had been affected by a failure before, of course provided that the system administrator has re-established the operability of the server system, operating system and installed PoINT Archival Gateway software package before.

The following picture illustrates the design of PoINT Archival Gateway and the networks used by the solution by showing a sample deployment.
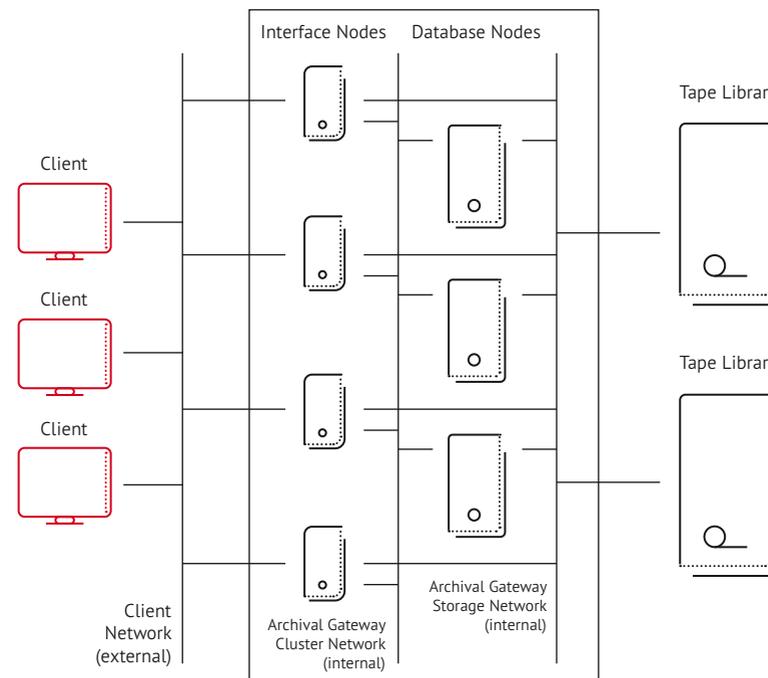
NETWORKS

The storage network of the PoINT Archival Gateway can be an iSCSI or Fibre Channel network connecting Archival Storage Devices (e.g. tape libraries with tape drives) to the gateway nodes, while typically the other networks are Ethernet networks.

Workflow

Clients connect to the interface modules of the IFNs, which currently is the HTTP service module providing the S3 REST API. Clients can send their requests to any IFN, and the IFNs either process the request and send the final response, or they instruct the clients to send the requests to another IFN by sending a special redirection response.

Redirection responses can occur if the original request transfers object data to or from tape media (e.g. GET or PUT requests). In this case, the appropriate Archival Storage Volume (i.e. tape medium) have to be loaded in free tape drive, and the request typically has to be redirected to the specific IFN that is connected to these tape drive because this IFN can read or write the data.

—— WRITING OBJECTS

When a client desires to write a new object, it sends an appropriate PUT request including the object data. Provided that redirection is not required, the HTTP service module of the addressed IFN receives the object data and stores it in data buffers in memory (q.v. data buffering module). In addition, the IFN computes a hash code of the data and adds it to the metadata of the object. Optionally, the IFN compares its hash code to a hash code which has been computed and transferred by the client in the request header, and

sends a specific error response if the hash codes do not match. Then, it forwards the request and its associated data buffers to the driver module for the tape drive to write it to the tape media. In this module, the original data buffers are reorganized, interleaved with data buffers from other objects, protected by adding erasure codes and logical block protection codes, optionally encrypted, and written to the Archival Storage Volume (tape media). Finally, after the data have successfully been written to the Archival Storage Volume, the HTTP service module stores the object metadata and the location of the object data on Archival Storage Volume in the database and sends a positive response to the clients.

—— READING OBJECTS

For reading an existing object, a client sends an appropriate GET request. Provided that redirection is not required, the HTTP service module of the addressed IFN first reads the object metadata and the location of the object data from the database. Then, it forwards the request to the driver module for the drive units to read the object data from the Archival Storage Volume (tape medium). This module regenerates the object data from the data on the Archival Storage Volume, copies it to data buffers in memory, and immediately sends the data buffers to the client.

Configuration Options

Typically, the software packages and thus the services of PoINT Archival Gateway should be installed on separate server systems because this kind of deployments provides the maximum levels of scalability, availability and performance.

However, for systems which are not required to provide the maximum levels, a special software package allows installing one database and one interface service on the same server system. In this case, the database and interface service functions are combined in a single and compact service module to optimize the common use of resources and to remove overhead caused by inter-service communication.

Client Network

DBN & IFN

PoINT Archival Gateway

Tape Library
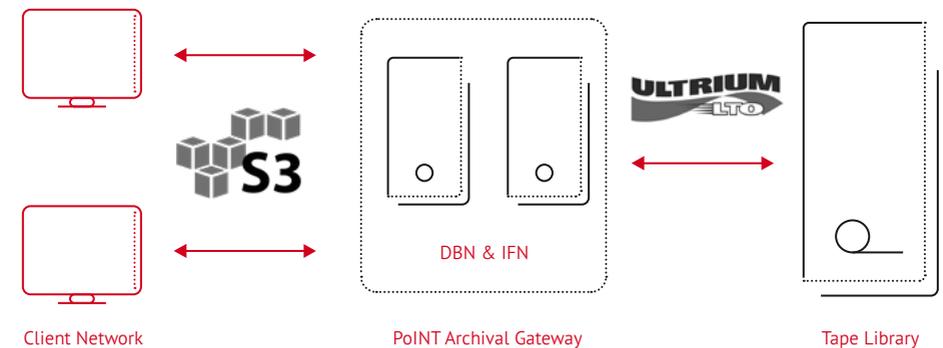
Functionality

The PoINT Archival Gateway offers a standardized S3 REST API. This makes the software suitable for use with the rapidly rising number of applications that support object-based storage using S3 REST.

The PoINT Archival Gateway's design is independent of the storage technology or system used, meaning that users can choose and swap out such systems with confidence. The PoINT Archival Gateway's highly scalable S3 REST web service enables almost unlimited parallelization and very high data transfer rates.

The PoINT Archival Gateway is a software-based, high-performance object storage system. It supports mass storage media such as tape libraries. This combination makes it possible to store and archive hundreds of petabytes of data. The decisive factor that makes this possible is the way the PoINT Archival Gateway quickly receives data and securely writes it to Archival Storage Volume (tape media) in a format that means this data can also be quickly read again afterwards.

The PoINT Archival Gateway's high level of scalability means it can handle transfer rates of over 1 PB per day.

The following table gives some numerical examples for three configurations for achievable read/write rates under optimum conditions regarding server and network components.

#Libraries	#LTO-8 Drives per Library	Read/Write Rates
1	8	up to 7.200 MB/s[1])
4	4	up to 14.400 MB/s[1])
8	32	*up to 230.400 MB/s[1])* *(theoretically)*

[1] May be limited by insufficient FC or Ethernet bandwidth or by maximum performance of clients.

Data security is ensured by an erasure coding process. This saves data blocks redundantly on multiple media, meaning that data is not lost even if a medium fails.

Erasure code rates supported by PoINT Archival Gateway are 1/2, 1/3, 1/4, 2/3, 2/4 and 3/4. In combination with erasure coding, the level of data protection and redundancy can further be advanced by using two, three or four Archival Storage Devices (tape libraries) in parallel. A Protected Volume Array consisting of N tape media may span N libraries.

In the following two figures the write path and read path are illustrated in case a erasure coding rate of 3/4 has been selected.

Write Path

Read Path
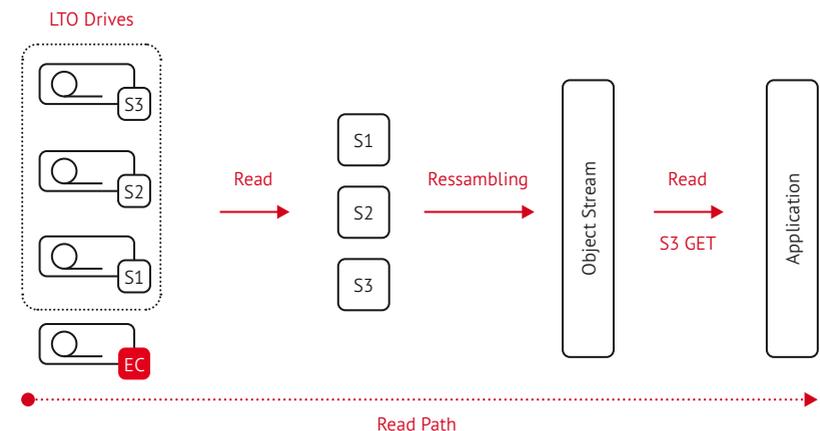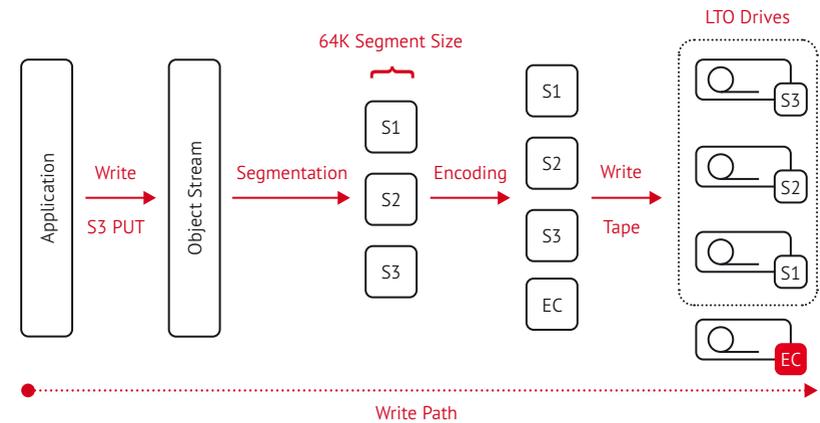
REDUNDANCY

Redundant server nodes automatically managed by PoINT Archival Gateway mean that the server systems running the PoINT Archival Gateway remain stable.

DATA AND MANAGEMENT SECURITY

The system's approach to management security is made possible by user and permission management concept. Access rights can be assigned for these guidelines. To this end, the administrative interface provides functionality for creating local security guidelines for users and groups. The system can also inherit external guidelines from an Active Directory domain.

Access rights for the objects in an Object Repository are granted by adding a local principal of type user or an external security principal to the list of authorized object repository principals. While adding a principal, a security manager may define granular access rights by specifying if the principal shall be allowed to a list, read, write or delete objects in the object repository.

Principals created and used for providing access rights to object repositories may, but do not need to have management roles.

Access to the objects in object repositories is exclusively possible through the client interfaces and protocols, where the individual interface or protocol,

respectively, defines how principals must authenticate themselves by providing their credentials.

ENCRYPTION

Data and metadata of objects may optionally be encrypted by PoINT Archival Gateway before they are written to the Archival Storage Volumes (tape media). Encryption leverages cipher blocks chaining algorithms, is applied on block level and can be enabled or disabled on Archival Storage Partition level. For encryption, either a common system key or a partition specific key may be used. The encryption algorithms supported by PoINT Archival Gateway use cryptographic keys of 128 (AES-1) and 256 (AES-2) bits length.

RETENTION MANAGEMENT

PoINT Archival Gateway provides persistent data management for meeting legal and business data archival requirements. Appropriate retention rules can be enabled and specified on Object Repository level and apply to all objects in the repository. The rules define how and when existing objects in the object repository may be modified or deleted.

The retention rules basically allow specifying retention periods and to issue or retire legal holds and can be managed by means of the system configuration GUI.

Once enabled, retention rules cannot be disabled again, and affected object repositories cannot be deleted before the retention periods of all contained objects has expired. However, retention periods can be extended at any time and, in addition, administrative deletion of retained objects is possible, but PoINT Archival Gateway unconditionally logs administrative deletion of objects.

LIFECYCLE MANAGEMENT

In addition to data retention management as described above, PoINT Archival Gateway provides a set of lifecycle management functions of Amazon S3.

In particular, PoINT Archival Gateway supports policies defining expiration actions on objects and incomplete multi-part uploads. Expiration policies cannot be filtered, but can only be applied to an entire bucket. Policies defining transition actions are ignored by PoINT Archival Gateway.

PoINT Archival Gateway removes expired objects and aborts incomplete multipart uploads one day after the specified date has been reached. This process runs once per day and automatically starts at the end of a day (i.e. at midnight local time).

Expiration actions cannot delete objects of which the retention period has not yet elapsed. In such a case, the expiration action is performed at earliest as soon as the retention period has been elapsed.

—— AUDIT LOGS

PoINT Archival Gateway supports data access audit logs and security audit logs.

Accesses to the data objects of an Object Repository are logged in associated access audit log files. Log records include identifier, time stamp and kind of access as well as an identifier of the principal who performed the access.

In addition, all logon actions of managers and all modifications applied by security managers or either way related to security settings are logged in a protected security audit log file. This log file includes information about the principals, including details about the modification.
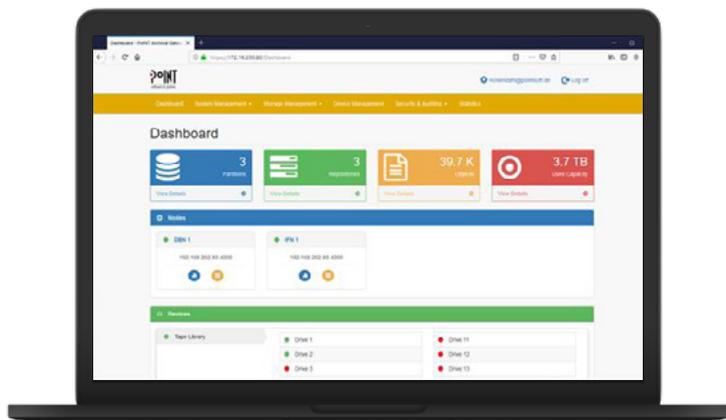
—— ADMIN GUI

The primary configuration interface is the Admin GUI provided by an HTTP service of PoINT Archival Gateway.

The service is hosted by Microsoft Internet Information Server instances running on the DBNs. The Admin GUI communicates with the configuration module via a local network connection. The configuration module forwards configuration data and

corresponding changes to the affected nodes.

The service is hosted by Microsoft Internet Information Server instances running on the DBNs. The Admin GUI communicates with the configuration module via a local network connection. The configuration module forwards configuration data and corresponding changes to the affected nodes.

Supported Archival Storage Devices

The PoINT Archival Gateway supports a wide range of tape libraries and PoINT works closely with leading manufacturers. As a result, the list of supported products is being expanded all the time.

—— TAPE SYSTEMS

The following table provides an overview about the currently supported tape systems (loaders and libraries) which are supported.

Vendor	Product	
actidata	actilib Library 2U	
BDT	FlexStor II	
Cristie	GigaStreamT8	GigaStream T24
	GigaStreamT48	GigaStream T24
HPE	MSL2024	MSL8096
	StoreEver MSL6480	
IBM	TS3100 Tape Library	TS3200 Tape Library
	TS3500 Tape Library	TS4300 Tape Library
	TS4500 Tape Library	
Qualstar	RLS-8560	RLS-85120
	XLS-832700	
Quantum	Scalar i3	Scalar i6
	Scalar i6000	

The listed tape systems are supported using tape technologies LTO 5 through 8.

Please contact PoINT Software & Systems GmbH for support of tapes systems which are not yet listed.

PoINT Archival Gateway directly supports and integrates tape libraries. No additional drivers or software products are required.

A PoINT Archival Gateway installation supports up to 8 tape libraries with a maximum number of 256 tape drives.

PoINT Software & Systems ——

PoINT Software & Systems is specialized in the development of software solutions for storage and management of data using all available mass storage technologies like cloud and object storage, hard disk, magnetic tape and optical. Close collaboration with leading hardware manufacturers enables an early support of innovative storage technologies. Besides complete solutions PoINT also offers its know-how as Toolkits, which can be easily integrated in other applications by the programming interface. Furthermore we project entire storage solutions and provide consultancy with our long-term and versatile experience.

PoINT products are distributed in more than 25 countries world-wide and have been installed successfully in more than two million installations. Our customers range from end users expecting a compact and secure solution to large corporations, which comply with our solutions their complex demands by providing the necessary reliability and perfection.