

PoINT Archival Gateway



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

内容

- 4 — **介绍**
- 6 — **产品一览**
 - 关键功能
- 7 — **用例**
 - S3归档至磁带
 - 分层(Tiering) /私有云ILM
 - 云或对象数据的存储备份
- 9 — **架构 (Architecture)**
 - 对象库(桶)
 - 归档存储 分区(Partition)
 - 归档存储设备
- 11 — **设计及概念**
 - 接口节点
 - 数据节点
 - 网络
- 14 — **工作流**
 - 写对象
 - 读对象
- 15 — **配置选项**
- 16 — **功能**
 - S3 REST API
 - 性能
 - 纠删码
 - 冗余
 - 数据及安全管理
 - 加密
 - 保留管理
 - 生命周期管理
 - 审计日志
 - 图形化管理界面
- 21 — **支持的归档存储设备**
 - 带库系统

介绍

最近的研究公司调查发现,企业面临的最大IT数据中心基础架构挑战,其中之一是非结构化数据(unstructured data)的爆炸式增长,使用基于硬盘或闪存技术的文件及块存储(NAS和SAN),在经济和技术上都无法解决这一挑战。

此外,这些研究还表明,大多数非结构化数据都是不活跃(inactive)数据,这些数据不经常使用,但出于业务或合规性原因,仍需要保留,但基于硬盘或闪存的存储系统上存储这样的大规模不活跃数据几乎毫无意义。

软件定义(software-defined)的对象存储,提供标准化的REST API,如Amazon S3。同时利用标准化的磁带技术,像LTO和3592这样的磁带存储介质可以解决这一难题。像文件和块存储一样,对象存储是一种存储数据的方法;文件,块和对象存储之间

的区别在于,对象存储的设计具有可伸缩性(scalability),较高的成本效益,可靠性(reliability)和高可用性(availability)的特点;原则上,存储数据的方式独立于基础存储介质,就像文件可以以文件系统结构存储在硬盘和磁带上一样,对象也可以存储在不同的存储介质上。

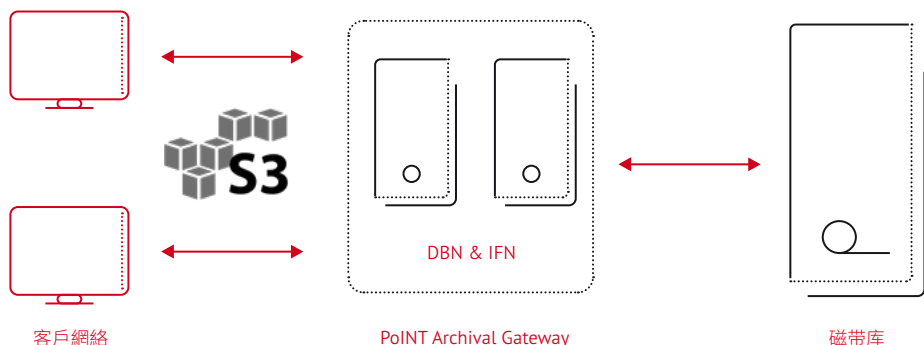
考虑到未来数年中非结构化数据的大幅度增长以及其中绝大部分数据很快变得不活跃的事实,磁带是唯一能够提供足够数据容量且成本可接受的存储介质。结合其WORM功能,磁带技术还可以满足数据归档要求。此外,像磁带这样的可移动介质也会对恶意软件产生“空隙”(air-gap)效应,故而,磁带技术非常适合数据保护和备份。此外,与所有可用的存储介质相比,磁带技术在提高其裸存储容量方面潜力无穷。

由于这些原因,结合了对象存储和磁带技术作为存储介质的方法为数据增长问题提供了一种创新且经济的解决方案。

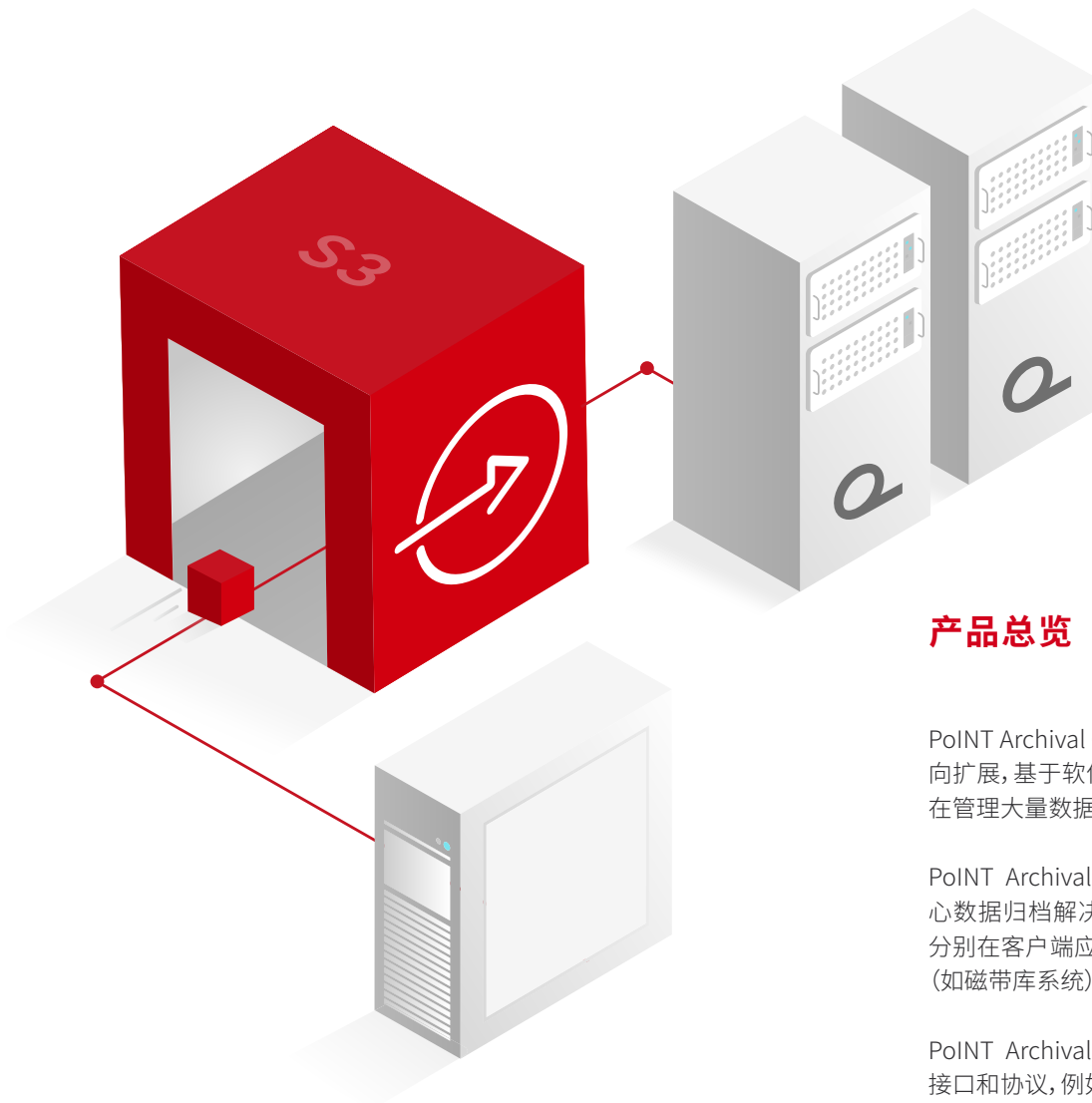
PoINT Archival Gateway是一个软件定义的横向扩展磁带库对象存储系统,旨在存储和管理带库上的大量数据,并提供出色的性能。

PoINT Archival Gateway 提供了标准化的S3 REST API,并支持各种磁带库。

本技术白皮书中,将提供了PoINT Archival Gateway的详细技术说明。



Archival Gateway



产品总览

PoINT Archival Gateway是一种高性能, 横向扩展, 基于软件的对象存储解决方案, 旨在管理大量数据。

PoINT Archival Gateway提供企业数据中心数据归档解决方案必需的服务和功能, 分别在客户端应用或系统与归档存储系统(如磁带库系统)之间架起一座桥梁。

PoINT Archival Gateway提供了标准化的接口和协议, 例如Amazon S3 REST API ,

客户端应用可以使用这些接口协议来存储或读取那些数据。 PoINT档案网关提供的基本服务包括用户, 数据和存储管理以及访问控制, 日志记录和监视。

— 关键功能

- 高性能
- 高可用及可靠性
- 高扩展性 (包括负载均衡, 冗余及容错)
- 行业标准: S3 REST API, LTO 及3592磁带机
- 对象版本控制 (versioning)
- 数据保护 (纠删码, 身份验证及加密)
- 自我监控, 报告及告警
- 基于域服务的用户管理(AD, LDAP)

用例

PoINT Archival Gateway提供了满足各种要求的解决方案, 凭借其标准化的S3 REST API, PoINT Archival Gateway可被许多支持S3的应用所使用。

下图给出了可以与PoINT Archival Gateway集成和连接的应用程序和环境的的一些示例。

— S3 归档至磁带

基于WORM功能和集成的保留(retention)管理功能, PoINT Archival Gateway满足了归档和合规性要求。结果, 不仅保护了已保存的数据不受意外删除, 而且还防止了人为操纵 (例如, 免受勒索软件攻击)。

PoINT Archival Gateway提供持久的数据管理能力, 以满足法规和商业数据归档的要求, 如可在对象存储库(object repository)级别启用并指定适当的保留(retention)规则, 这些规则定义了如何以及何时可以修改或删除现有的对象。

— 私有对象存储分层 / 生命周期管理(ILM)

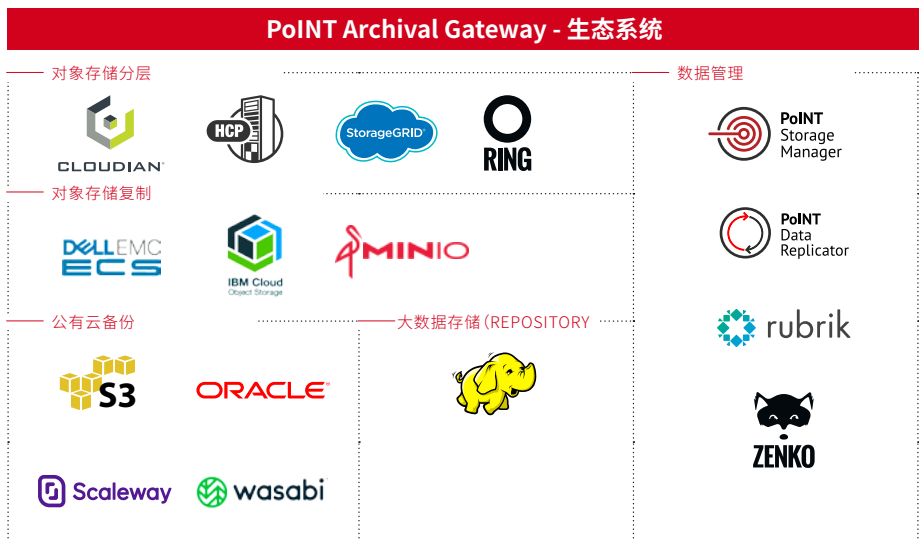
AWS和Microsoft Azure等公共云存储提供商已向其客户提供具有不同性能的不同S3存储服务类别, 然而, 用作私有云的对象存储产品往往仅提供一种存储类型, 通常基于硬盘, 活动数据和非活动数据存储在不同的存储介质上, 这样的方式往往效益不佳。

基于硬盘的对象存储与PoINT Archival Gateway相结合, 可以将非活动数据从硬盘到磁带进行分层, 为此目的, 许多对象存储产品已经提供了集成的ILM功能。

— 云及对象存储备份

云和对象数据的备份变得越来越重要。公有云提供商消失了, 存储其云上的数据则变得不可访问, 另外, 云并非不受恶意软件攻击。这同样适用于私有对象存储上的数据, 因此, 云和对象数据的备份至关重要。

允许您以原生S3格式从云和对象数据备份到磁带, 您的对象数据将以与原始数据相同的结构保存, 这也意味着可以通过PoINT Archival Gateway的S3接口直接访问保存的数据, 并不需要很长的恢复(retrieval)过程。



架构及术语

PoINT Archival Gateway所用的架构和术语一览如下：

对象库 (OBJECT REPOSITORY或BUCKET)

PoINT Archival Gateway允许创建任意数量的对象库(bucket)，每个对象库可以具有不同的设置和限制(例如大小限制，访问权限)。客户端应用和系统可以使用PoINT Archival Gateway的S3 REST API在对象库中存储和读取对象。相同归档存储分区的对象库共享相同的受保护卷阵列(PVA: Protected Volume Array)。

归档存储分区(ARCHIVAL STORAGE PARTITION)

PoINT Archival Gateway使用称为“归档存储分区”的逻辑结构作为管理单元,用于管理归档存储设备可用的所有存储卷的存储

空间, 可以创建多个归档存储分区, 每个分区具有不同的设置和限制(例如大小限制, 访问权限, 保护级别, 冗余或可用性), 并使用单独的归档存储卷。默认情况下, 当最后分配的阵列被数据完全填充时, PoINT Archival Gateway会通过分配其他受保护的卷阵列(请参见下文)来自动扩展归档存储分区的容量。

归档存储设备 ARCHIVAL STORAGE DEVICE

归档存储设备是具有特定数量的具备磁带驱动器的介质更换器设备(磁带库或磁带加载器)。

设计与概念

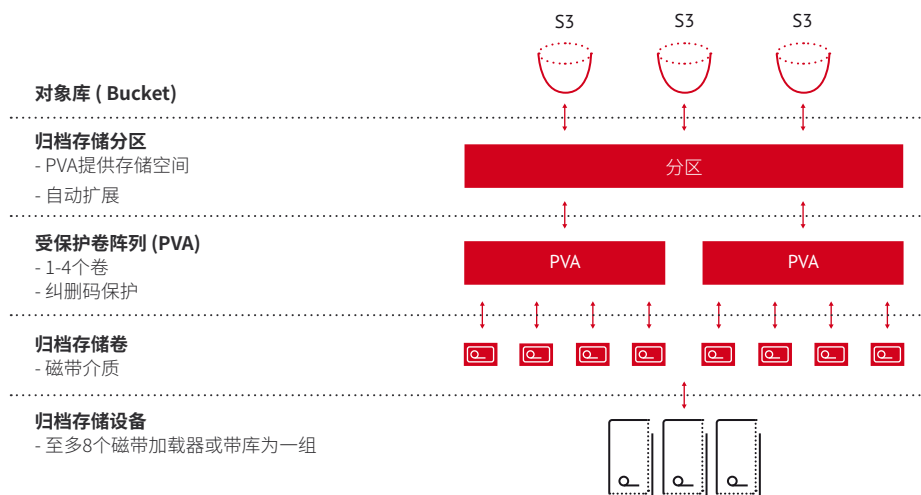
PoINT Archival Gateway利用对象存储体系结构并将数据作为对象进行管理。每个对象都包含对象的唯一标识符, 数据本身以及可变数量的自定义元数据。该体系结构基本上允许可伸缩地将大量非结构化数据保留在可移动介质(例如库中的磁带介质)上。

PoINT Archival Gateway明确地将数据和元数据分开。唯一标识符和元数据存储于公用数据库中, 而数据存储于磁带介质上。元数据和唯一标识符的副本也存储在存储介质上, 以支持灾难恢复和数据验证。

对象存储架构通常使用数据库来存储元数据和唯一标识符。与其他架构(如文件系统及其分层结构)相比, 数据库对对象记录可用于唯一标识符和自定义元数据以及数字中的字符序列没有任何限制。此外, 数据库

支持现有记录的任意扩展, 以及覆盖所有现有记录的索引和高性能查询。这些特性和功能对于支持各种类型和版本的对象存储接口(例如S3 REST API)至关重要。

PoINT Archival Gateway的设计反映了这种数据和元数据的分离, 该设计要求将服务分配给单独的专用服务器系统。因此, PoINT Archival Gateway软件由两个软件包组成, 每个软件包都可以安装在专用服务器系统上。包含其基本操作系统软件和软件包的专用服务器系统称为网关节点。网关节点由已安装的软件包定义, 正好可以满足两个可能目的之一。



— 网关接口节点 INTERFACE NODES (IFN)

网关接口节点 (IFN) 主要是客户端应用或系统的通信伙伴, 通过专用接口模块, 它提供了S3 REST API, 用于将对象存储和读取到客户端应用和系统, 并在客户端应用或系统与归档存储卷(即磁带介质)之间传输数据。

详细来说, IFN提供以下模块和服务:

- HTTP服务模块(即S3 REST API)
- 数据缓冲模块
- 数据编码模块(如纠删码, 哈希, 加密)
- 磁带机的驱动模块
- 元数据缓存(如对象元数据和配置缓存)
- 通信模块, 用于与数据库节点交换元数据

— 数据库节点 DATABASE NODES (DBN)

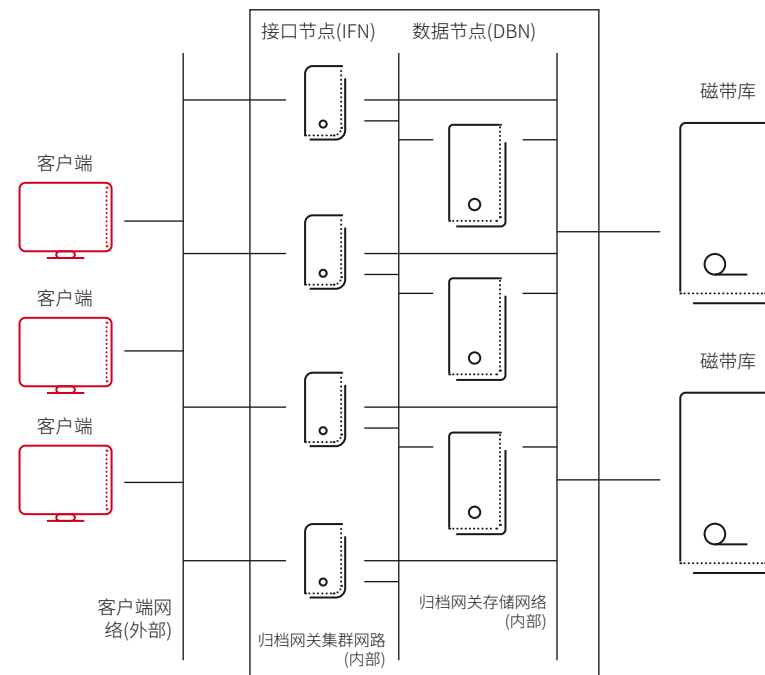
数据库节点 (DBN) 主要为IFN提供集中数据库服务, 数据库保存已存储对象的索引(如对象密钥和元数据), 对象数据在归档存储卷(磁带介质)上的存储位置, 以及PoINT Archival Gateway的配置和维护数据。更进一步, 归档存储设备(磁带库)的系统配置界面 (Admin GUI), 管理和控制模块, 也位于此节点上。

PoINT Archival Gateway需要至少一个IFN和一个DBN才能运行。

PoINT Archival Gateway通过这种完全可扩展和冗余的设计来满足最高级别的性能, 可用性和可扩展性要求, 为服务和数据实体提供可扩展的性能和冗余水平; 由于服务器硬件和操作系统的限制, 单个节点的可扩展性和可用性受到限制, 因此PoINT Archival Gateway支持在单个部署中安装多个DBN和IFN, 以便构建集群以提高性能(即负载均衡)和可用性(即故障转移和冗余)。

归档网关软件可自动重构受故障影响的群集节点, 包括可操作性和一致性所需的所有任务, 当然前提是系统管理员已重建服务器系统, 操作系统并安装之前的PoINT Archival Gateway软件包。

下图说明了PoINT档案网关的设计以及样例部署中的网络情况。



— 网络

PoINT Archival Gateway的存储网络可以是归档存储设备(磁带库)连接到网关节点的iSCSI或光纤通道网络, 而其他网络通常是以太网。

工作流程

客户端连接到IFN的接口模块,目前是提供S3 REST API的HTTP服务模块。客户端可以将其请求发送到任何IFN,而IFN要么处理该请求并发送最终响应,要么通过发送特殊的重定向响应来指示客户将请求发送给另一个IFN。

如果原始请求将对象数据传输到磁带介质或从磁带介质传输回来(例如GET或PUT请求),则可能会发生重定向(redirectation)响应。在这种情况下,必须将适当的归档存储卷(即磁带介质)加载到空闲的磁带机中,并且通常必须将该请求重定向到连接至该磁带机的特定IFN,因为只有该IFN可以读取或写入数据。

—— 写入对象

当客户端希望写入新对象时,它将发送一个包含对象数据的适当PUT请求。如果不需要重定向,则被寻址IFN的HTTP服务模块将接收对象数据并将其存储在内存中的数据缓冲区中(数据缓冲模块)。此外,IFN计算数据的哈希码,并将其添加到对象的

元数据中,IFN还可将其哈希码与客户端在请求头中计算并传输的哈希码进行比较,并且如果哈希码不匹配,则发送特定的错误反馈。之后,它将请求及其关联的数据缓冲区转发到磁带机的驱动模块,以将其写入磁带介质。在此模块中,原始数据缓冲区将进行重组,与其他对象的数据缓冲区进行交织,通过添加擦除代码和逻辑块保护代码(也可选择进行加密)进行保护,并写入归档存储卷(磁带介质);最后,在将数据成功写入归档存储卷之后,HTTP服务模块将对象元数据以及对象数据在归档存储卷上的位置信息存储在数据库中,并向客户端发送已写入响应。

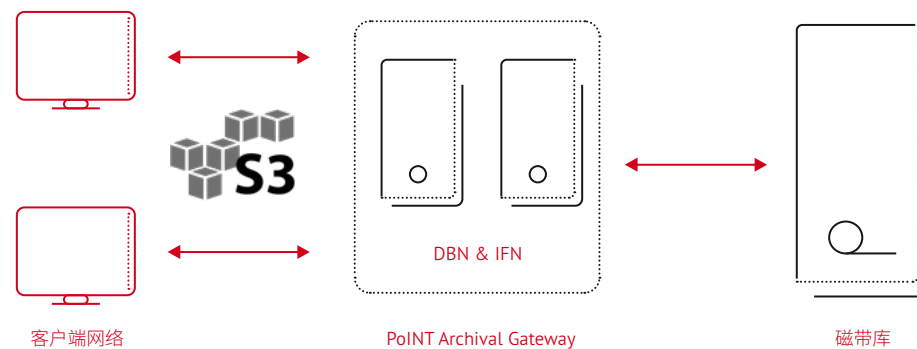
—— 读取对象

为了读取现有对象,客户端发送适当的GET请求,如果不需要重定向,则被寻址IFN的HTTP服务模块首先从数据库中读取对象元数据和对象数据的位置。随即,它将请求转发给驱动器模块,以供磁带驱动器从归档存储卷(磁带介质)读取对象数据。HTTP服务模块从归档存储卷上的数据中重新生成对象数据,将其复制到内存中的数据缓冲区中,然后即将数据缓冲区发送给客户端。

配置选项

通常,应该将PoINT Archival Gateway的软件包以及相应的服务安装在单独的服务器系统上,因为这种部署提供了最大程度的可伸缩性,可用性及性能。

对于不需要提供最大效能的系统,可以使用特殊的软件包将数据库和接口服务软件安装在同一服务器系统上,在这种情况下,数据库和接口服务功能组合在一个紧凑的服务模块中,可使资源优化并消除由服务间通信引起的网络开销。



功能

— S3 REST API

PoINT Archival Gateway提供了标准化的S3 REST API。这使得该软件与那些支持S3 Rest API的应用天然适配，这些应用在迅速增长之中。

PoINT Archival Gateway归档网关的设计与所使用的存储技术或系统并无绑定关系，这意味着用户可以放心地选择和更换此类系统。另外，PoINT档案网关的高度可扩展的S3 REST网络服务可实现几乎无限的并行化和很高的数据传输率。

— 性能

PoINT Archival Gateway是基于软件的高性能对象存储系统，它支持海量存储介质，例如磁带，这种组合使得可以存储和归档数百PB的数据。做到这一点的决定性因素是PoINT Archival Gateway可快速接收数据并将其安全地写入到归档存储卷(磁带介质)中，同时意味着此数据随后也可以再次被快速读取。

PoINT档案网关的高度可扩展性意味着它每天可以处理超过1 PB的数据。

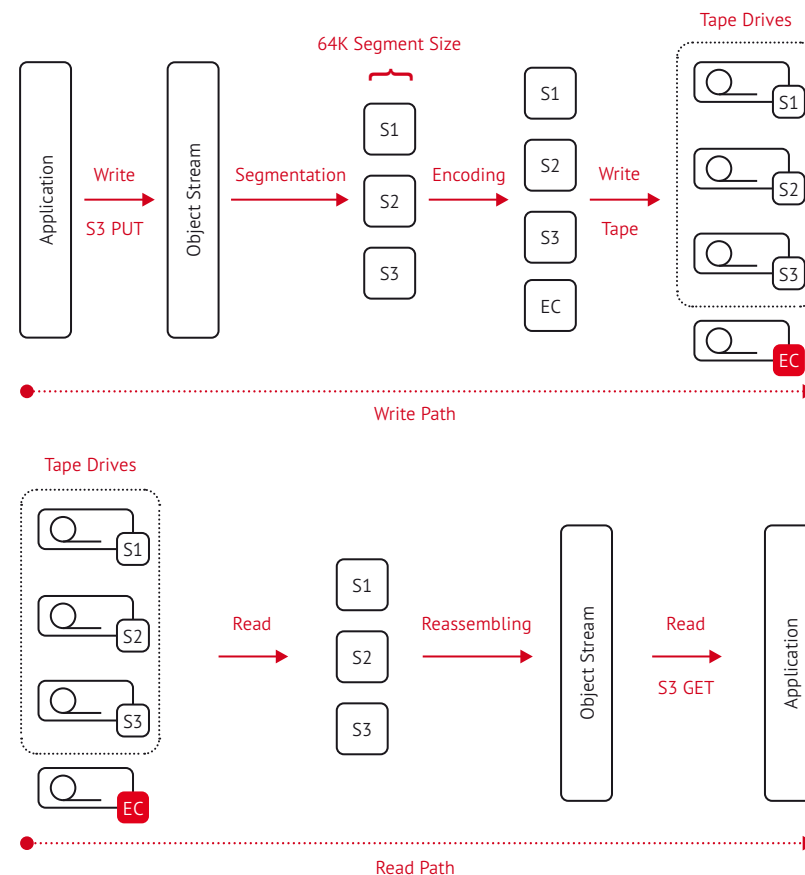
— 纠删码 (EC)

PoINT Archival Gateway的数据安全性由纠删码技术提供，这样可以将数据块冗余地保存在多个介质上，这意味着即使介质发生故障，数据也不会丢失。

支持的纠删码为1/2、1/3、1/4、2/3、2/4和3/4，结合纠删码，可以通过并行使用两个，三个或四个归档存储设备(磁带库)来进一步提高数据保护和冗余级别。

由N个磁带组成的受保护卷阵列(PVA)可以跨越N个磁带库。

下列两个图示为选择3/4纠删码情况下的写入路径和读取路径。



—— 冗余

由PoINT Archival Gateway自动管理的冗余服务器节点意味着整个系统保持稳定。

—— 数据和管理安全

用户和权限管理将使系统的管理安全性成为可能，访问权限基于这些准则(guidelines)分配，为此，管理界面提供了用于为用户和组创建本地安全准则的功能，系统还可以从 Active Directory域承继外部准则。

通过将类型为用户的本地主体或外部安全主体添加到授权的对象库规则列表中，可以授予对象存储库中对象的访问权限。在添加主体时，安全管理者(security manager)可以通过指定是否应允许此主体对对象库中的对象进行列表，读取，写入或删除来定义粒度访问权限。

创建并用于提供对对象库访问权限的主体可以但不必具有管理角色。

只能通过客户端接口和协议来访问对象库中的对象，其中各个接口或协议分别定义了主体必须如何通过提供其凭据来对自身进行身份验证。

—— 加密

在将对象的数据和元数据写入归档存储卷(磁带介质)之前，可以选择通过PoINT Archival Gateway对其进行加密；加密利用密码块链接算法，应用于块(block)级别，并且可以在归档存储分区级别启用或禁用；加密可以使用公用系统密钥或分区专用密钥。PoINT Archival Gateway支持的加密算法使用128 (AES-1)和256 (AES-2)位长度的加密密钥。

—— 保留 (RETENTION) 管理

PoINT Archival Gateway提供持久的数据管理，以满足法规和商业数据归档的要求。可以在对象库级别上启用和指定适当的保留规则，并将其应用于库中的所有对象。规则定义了对象库中现有对象如何修改和何时删除。

保留规则基本上允许指定保留期限并发布或撤消合法保留，并且可以通过系统配置 GUI进行管理。

保留规则一旦启用，则无法再次禁用。在保留期限到期之前，无法删除受影响的对

象存储库。但是，保留期可以随时延长，此外，可以对保留的对象进行管理性删除，但是PoINT Archival Gateway会无条件记录这些对对象的管理删除。

—— 生命周期管理

除了如上所述的数据保留管理之外，PoINT Archival Gateway还提供了Amazon S3的一组生命周期管理功能。

尤其是，PoINT Archival Gateway支持很多策略，这些策略如定义对象的到期操作(expiration actions)以及不完整的分段上传(multi-part uploads)，到期策略无法过滤(filter)，只能应用于整个存储桶(bucket)。PoINT Archival Gateway会忽略那些定义过渡操作(transition actions)的策略。

过期的对象会被移除，不完整的分段上传也会在指定日期的一天后中止，此过程每天运行一次，并在当天结束时(即当地时间午夜)自动开始。

到期操作无法删除尚未超过保留期的对象。但只要超过了保留期限，就会立即执行。

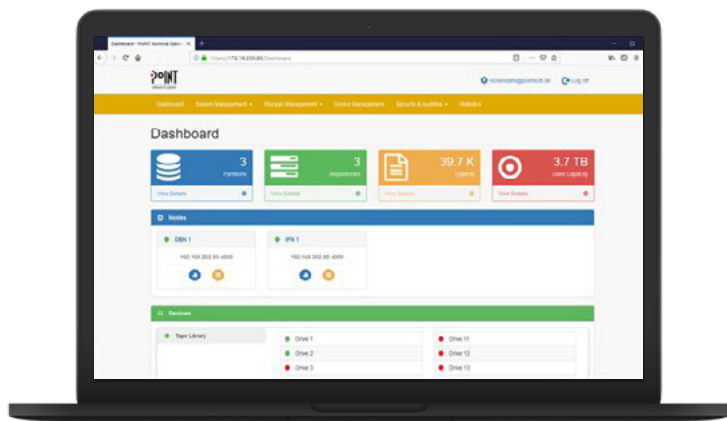
—— 审计日志

PoINT Archival Gateway支持数据访问审计日志和安全审计日志。

对对象库的数据对象的访问记录在关联的访问审计日志文件中。日志记录包括标识符, 时间戳和访问类型, 以及执行访问主体的标识符。

此外, 管理者的所有登录操作以及安全管

理者应用的所有修改或与安全设置有关的任何一种方式都会被记录在受保护的安全审计日志文件中。该日志文件包含有关主体的信息, 也包括有关修改的详细信息。



—— 管理界面

主配置界面是PoINT Archival Gateway的HTTP服务提供的Admin GUI。

该服务由在DBN上运行的Microsoft Internet Information Server实例托管。Admin GUI通过本地网络连接与配置模块通信。配置模块将配置数据和相应的更改转发到受其影响的节点。

支持的归档存储设备

—— 磁带系统

PoINT Archival Gateway支持各种磁带库, PoINT与领先的制造商紧密合作, 所支持的产品列表也一直在扩展。

表为当前所支持的磁带系统(加载器和磁带库):

厂商	产品	
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	

PoINT Archival Gateway支持LTO及3592磁带机。

PoINT Archival Gateway直接支持和集成磁带库, 不需其他驱动程序或软件产品。

不在列表中的磁带机系统, 请联络PoINT Software & Systems GmbH。

单个安装实例最大可支持8个磁带库, 最大管理磁带驱动器为256个。

PoINT Software & Systems



PoINT Software & Systems致力于使用所有可用大容量存储技术(例如云和对象存储, 硬盘, 磁带和光盘)开发用于存储和管理数据的软件解决方案。与领先的硬件制造商的紧密合作可以为创新性存储技术提供早期支持。除了完整的解决方案, PoINT还提供其专有技术(know-how)作为工具包, 可以通过编程接口轻松地集成到其他应用程序中。此外, 我们计划整个存储解决方案, 并以长期和多角度的经验为您提供咨询。

PoINT产品分布于全球超过25个国家, 并已有超过200万次成功安装。我们的客户范围, 涉及哪些希望提供紧凑安全解决方案的最终用户, 也包括大规模部署的大型企业, 这些企业需要提供必要的可靠性和完善性来满足复杂的需求。

PoINT Software & Systems GmbH
Eiserfelder Straße 316
57080 Siegen, Germany

P +49 271 3841-0
M info@point.de
W www.point.de