分布式云文件存储报告

Original 常华Andy Andy730 2023-11-10 07:30 Posted on 上海

收录于合集
#存储行业趋势

147个

概要

文件存储在混合云战略中扮演着至关重要的角色，尤其是在支持协作场景方面，因此支持协作的分布式云文件存储方案正变得越来越受欢迎。这些解决方案易于获取，并可简便部署；它们以云为基础，几乎可以提供全球范围的地理位置服务；并且它们容易供终端用户操作。

从成本的角度看，这些解决方案还有助于组织从资本支出（CapEx）成本模型转向运营支出（OpEx）模型。购买方不再需要预先购置多个地点的基础设施，可以仅支付他们实际使用的容量，而不需要进行大规模的投资。

分布式云文件存储的另一个重要优势是其无处不在，这使其非常适用于远程工作。在全球COVID-19大流行之前，远程工作已经逐渐增加，但采取的突然严格措施以保护公有健康对组织和工作者的日常工作方式产生了重大而持久的影响。尽管疫情的最严重时期似乎已经过去，但它对工作方式的积极影响将长期存在，且继续需要远程数据访问的需求。

远程工作在连接企业网络并访问NAS上的文件方面已不再适用传统的集线器-辐射架构，因此需要更具可扩展性的解决方案。如今，数据必须随时随地可供访问，具备即时性和安全性，并得到保护，以防受到勒索病毒等威胁。同时，组织需要对其数据有更清晰的认识，了解哪些数据由谁生成，数据的增长速度，以及如何清晰地查看数据增长对成本的影响，管理和清理过时数据的方法，以及观察和采取行动以应对异常活动的手段。

尽管分布式云文件存储原则已经被充分确立，大多数解决方案提供了坚实的分布式架构，但新的挑战不断涌现。其中最迫切的挑战包括勒索病毒和其它高级威胁，这些威胁可能导致组织范围内的混乱和无法挽回的损害。去年已经是一个热门话题，有效的勒索病毒保护正在变得至关重要，不仅需要基本功能，如不可变快照，以便组织可以从中恢复数据，还需要主动检测和减轻恶意活动。

监管约束也对数据治理产生影响。《通用数据保护条例》（GDPR）和《加利福尼亚消费者隐私法》（CCPA）等消费者保护法律赋予客户更大的数据控制权，并影响组织管理数据的方式。

各国政府也开始认识到数据是战略资产，并开始实施严格的数据主权法规，要求数据资产必须在特定国家的边界内物理存储。为了符合政府和行业监管机构的要求，数据需要被追踪、分类和适当处理。

这是我们在关键标准和雷达报告的背景下第四次评估云文件存储领域。本报告基于我们以往的分析，并考虑了市场在过去一年中的发展情况。

这份GigaOm雷达报告突出了关键的分布式云文件存储供应商，并为IT决策者提供了选择最适合其业务和场景需求的信息。

本雷达报告中包含的所有解决方案均满足以下标准——这些是该领域广泛采纳和良好实施的能力：

- 可靠性和完整性
- 基本安全性
- 访问方式
- 快照
- Kubernetes支持

分析师观点

分布式云文件存储已经被证明是一个至关重要的能力，最初是为了确保在COVID-19大流行引发的持续中断期间维护业务连续性。这些中断不仅对劳动力及其对数据的访问产生了负面影响，还妨碍了组织提供和部署协作基础设施的能力。分布式云文件存储解决方案能够迅速缓解这些问题，这要归功于它们天生的分布式和云基础架构，以及它们对数据访问和协作的价值仍然存在。

在所有供应商中，我们没有发现关于全局命名空间、混合云和多云部署以及与对象存储的集成的关键标准存在差距或不足。此外，大多数供应商在其自身实施方面被认为要么出色，要么表现良好。

我们发现最显著差异的领域是数据管理、分析、高级安全和边缘部署。所有这些领域都很重要，但我们无法过于强调采取高级安全措施作为应对不断升级的顽固勒索病毒威胁的缓解策略的紧迫性。设计良好且多样化的边缘部署方案也至关重要，因为现在大多数组织必须适应大规模分布的劳动力。

尽管数据管理和分析可能看似次要，但它们也是关键的业务智能启用者，不仅因为能够重复使用数据以实现改进的结果，而且由于更高效的资源使用和支出控制。

尽管在关键标准方面评估的解决方案表现出色，但目前尚未提供与GigaOm报告“评估云文件存储解决方案的关键标准”中突出显示的新兴技术相关的功能，即数据分类、数据合规性和数据主权。这些解决方案可能以某种

方式提供实施这些能力所需的组件的覆盖范围，例如对存储位置的手动“分段”以实现地理主权或对文件添加元数据的能力。然而，总体而言，分类、合规性和数据主权的编排是不存在的。

供应商定位：市场细分和部署模型

	MARKET SEGMENT			DEPLOYMENT MODEL	
	SMB	Large Enterprise	Specialized	SaaS	Hybrid & Multicloud
CTERA	++	+++	+++	+	+++
Hammerspace	++	+++	+++	–	+++
LucidLink	++	++	+++	+++	++
Nasuni	+++	+++	++	+	+++
Panzura	+++	+++	++	+	+++
Peer Software	++	+	–	–	++

关键标准对比

	KEY CRITERIA						
	Global Namespace	Hybrid & Multicloud Support	Integration with Object Storage	Data Management	Analytics	Cyber Resiliency	Edge Deployments
CTERA	+++	+++	+++	++	+++	+++	+++
Hammerspace	+++	+++	+++	+++	++	++	++
LucidLink	++	+++	+++	+	+	++	+++
Nasuni	+++	+++	++	++	+++	+++	+++
Panzura	+++	+++	+++	+++	++	+++	++
Peer Software	++	++	++	+	++	++	++

评估指标对比

	EVALUATION METRICS						
	Architecture	Scalability	Flexibility	Efficiency	Performance	Ease of Use	Security Approach
CTERA	+++	+++	+++	+++	+++	+++	+++
Hammerspace	+++	+++	+++	+++	+++	+++	++
LucidLink	++	++	++	++	+++	++	+++
Nasuni	+++	+++	++	+++	+++	+++	+++
Panzura	+++	+++	++	++	+++	+++	+++
Peer Software	++	++	++	++	++	++	++

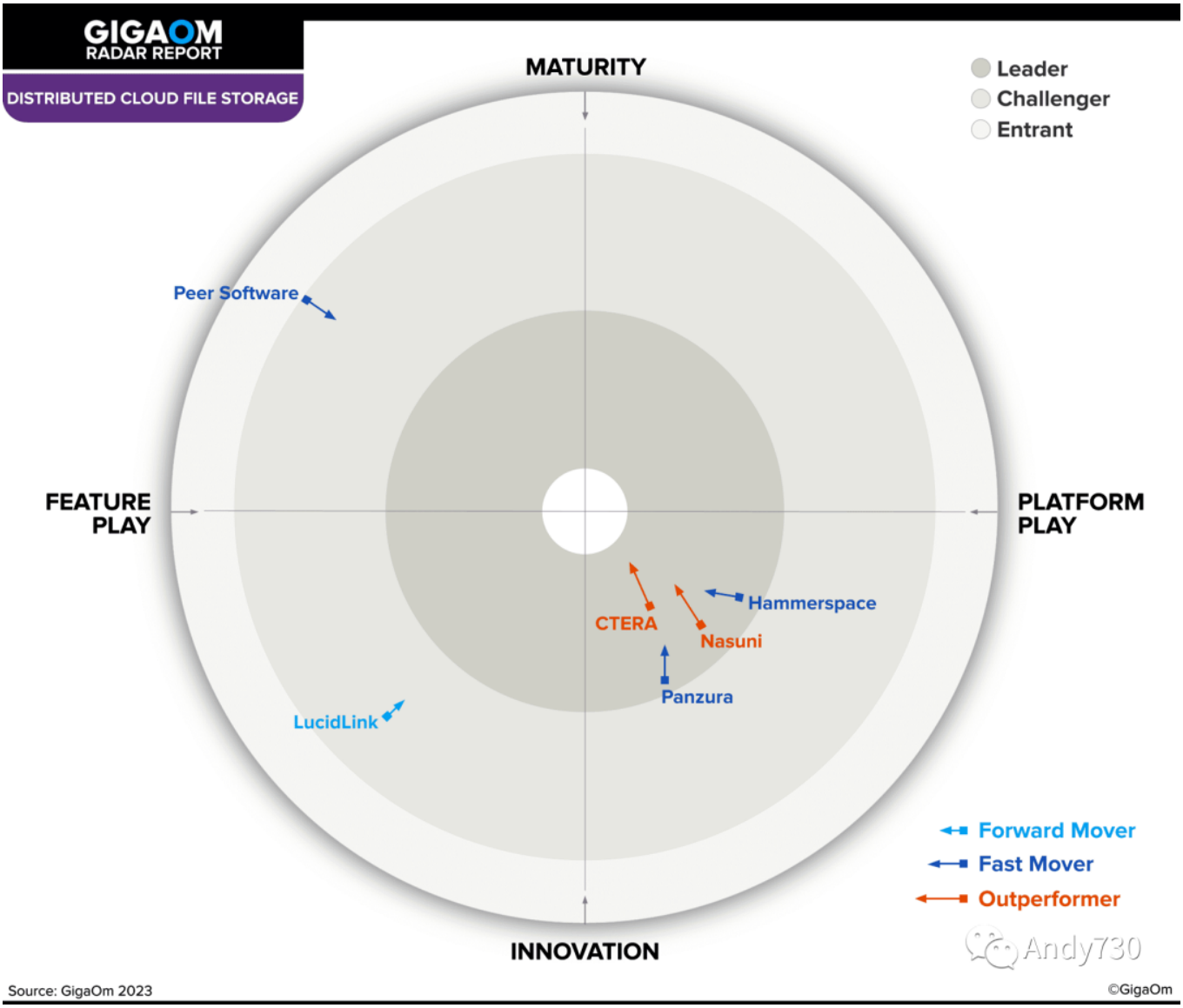
新兴技术对比

	EMERGING TECHNOLOGIES		
	Data Classification	Data Privacy Compliance Support	Data Sovereignty Requirements Support
CTERA	–	+	+++
Hammerspace	++	+	++
LucidLink	–	–	–
Nasuni	++	++	–
Panzura	++	++	–
Peer Software	–	–	+

综合评估

在本报告中，我们通过分析关键标准以及它们对评估指标的影响，提供了如图1中的GigaOm雷达图所示的信息。这些图表代表了对所有供应商的前瞻性视角，基于其产品的技术能力和功能集。

GigaOm雷达将供应商的解决方案绘制在一系列同心圆环上，靠近中心的位置表示整体价值更高。图表分为两个轴线：成熟度与创新平衡，以及功能性与平台性。此外，还提供了一个箭头，用于预测每个解决方案未来12到18个月的发展趋势。



如图所示，今年有两家供应商被评为表现优异。尽管技术和解决方案已经相对成熟，但大多数供应商在未来18到24个月内都有出色的路线图。

右下角区域包括四家注重创新的平台型解决方案：CTERA、Hammerspace、Nasuni和Panzura。

CTERA在勒索病毒保护方面取得了重大创新，通过开发内置的基于人工智能的勒索病毒检测引擎，推动了解决方案的能力增强。此外，它还引入了许多其它安全相关的改进，但未来需要更多地关注数据管理能力的发展。Hammerspace提供了最佳的全局命名空间实施，拥有无缝的基于策略的数据编排功能，用于复制和分层。该公司在2023年收购RozoFS，进一步提高了对高性能实施的支持。Nasuni一直致力于提供平衡和精心设计的平台，具有大规模扩展性和出色的勒索病毒保护能力。该公司最近加强了数据管理能力，以提升其功能集。Panzura提供了高度可扩展的解决方案，拥有全面的功能集，包括主动勒索病毒保护和高级数据管理套件。

左侧区域包括两家供应商：LucidLink和Peer Software。LucidLink位于创新部分，专注于全球即时可访问数据，带有强大的数据流传输能力，使其适用于需要远程访问大规模多TB文件的行业和场景，如媒体和娱乐行

业。尽管该解决方案在架构方面表现出创新，但在今年没有引入显著提升。

Peer Software位于成熟度部分，提供了一个经过验证的架构，允许组织在现有存储基础设施之上构建抽象的分布式文件服务，同时支持云中的可扩展性。公司有一个雄心勃勃的路线图，最近推出了一个新的分析引擎，但需要时间来实现路线图。

CTERA

CTERA提供一种分布式云文件存储平台，基于其高度可扩展的CTERA全局文件系统（GFS）。这一解决方案可以同时存在于云端和本地基础设施中。CTERA的GFS在前端呈现文件界面，并在后端充分利用私有或公有云S3对象存储。

该解决方案依赖于CTERA Direct，这是一种加速的边缘到云的双向同步协议，通过增加并行性和提供从边缘到区域对象存储桶的直接数据路径，增强了现有的基于源的去重和压缩功能。此外，该协议还支持流式传输，从而实现了对媒体和娱乐行业通常使用的多TB文件的即时访问。

由于CTERA实施了全局命名空间，组织可以为不同部门或租户定义专用区域。管理员可以定义细粒度的权限，围绕区域和授权用户进行详细的设置。这些区域还可以将数据在地理上分隔，以满足每个租户的需求，或者满足特定司法管辖区内的数据主权要求。

全局命名空间对终端用户是完全透明的。管理员可以使用CTERA Migrate内置的迁移引擎，从NAS系统中发现、评估和自动导入文件共享。现有文件系统可以通过Windows、Linux、macOS和移动设备上的本机文件同步和共享功能来实现。

这一解决方案提供了广泛的部署可选，涵盖边缘、核心基础设施和云端。它同时支持多个云，并允许用户在云端之间或与本地对象存储之间实现无缝数据迁移。

当客户使用AWS S3作为CTERA的后端对象存储时，该解决方案可以利用AWS S3智能层级划分功能，实现更好的成本节省。此外，CTERA可以完全部署在符合数据安全客户严格安全要求的私有架构中。

CTERA Insight提供了数据分析能力。这种数据可视化服务通过类型、大小和使用趋势分析文件资产，并通过一个良好组织、可定制的用户界面呈现信息。除了数据洞察，该界面还提供了关于中央组件和边缘设备的实时使用、健康和监控能力。CTERA的SDK允许API集成和S3连接，以支持微服务执行数据管理任务（CTERA支持生产中的Kafka）。

这一解决方案拥有一系列抗网络攻击能力，包括不可变快照（也在云端持续复制到不可变对象存储中）、一次写多次读（WORM）文件夹、CTERA Ransom Protect的主动基于AI的勒索病毒检测、AWS跨帐户存储桶复制和多因子身份验证（MFA）能力。对于恢复，即时灾难恢复文件夹功能允许部署CTERA文件夹并立即投入运行，同时元数据同步在后台进行，实现了对勒索病毒攻击的快速恢复。这一全面的功能集已经在GigaOm Sonar报告中广泛介绍了基于文件的初级存储勒索病毒保护。

从合规性的角度来看，该解决方案包括云存储路由以符合数据主权合规性和符合GDPR"被遗忘权"的安全数据清除功能，此外，它还可以指定WORM文件夹以符合HIPAA、SOX和FINRA等法规。数据分类不是内置的，而是通过与第三方工具（Varonis和Microsoft Purview Information Protection）的集成来提供。

该解决方案的架构允许在小型分支机构或远程管理的CTERA HC100 Edge设备上进行边缘部署，以满足小型分支机构或重度远程办公（WFH）用户的需求。

值得一提的是，CTERA正在与Hitachi Vantara合作，通过OEM合作伙伴关系将分布式云文件存储能力赋能Hitachi Content Platform。

- **优势**：CTERA展示了多种访问其GFS的方法和多个选择和解决方案，专为边缘场景打造。在安全性和网络攻击抗性能力方面有出色的关注和执行（包括遵循严格的安全标准），在多个功能领域有有前瞻的路线图。
- **挑战**：尽管提供了非常全面和令人满意的功能集，但仍有进一步提高数据管理能力的机会，通过实施高级功能，如全文索引和数据分类。

Hammerspace

Hammerspace通过创建一个全局命名空间，实现了全局数据环境，自动化数据编排可确保数据在需要的时间和地点提供。它将并行全局文件系统与企业NAS数据服务结合在一起，提供了高性能的数据访问，无论数据位于何处，都不会牺牲企业数据治理、保护和合规需求。Hammerspace通过提供单一的文件系统，解决了混合云、多云区域和多云文件存储的封闭特性，并通过将控制平面（元数据）与数据平面（数据的实际位置）分离来实现这一目标。它支持多个版本的NFS和SMB协议，同时提供对NFSv4.2的RDMA支持。

Hammerspace在2023年5月收购了RozoFS，并将RozoFS技术整合到其解决方案中。客户现在可以部署新的DSX EC-Groups，这些群组提供了高性能的数据存储，由于采用了纠删码，数据效率显著提高。Hammerspace解决方案旨在提供高性能和可扩展的数据存储，以满足HPC和AI训练、检查点和推理工作负载的需求。

该解决方案允许客户使用基于目标的策略自动化，使他们可以通过单一全局命名空间在全球范围内使用、访问、存储、保护和放置数据，用户无需了解资源的物理位置。系统实时监视数据和存储的使用，以确保其符合

策略目标，并以无缝透明的方式执行自动化的合规性纠正。通过本地元数据的使用，为远程应用程序、AI模型、计算农场和用户提供了高性能的本地访问，这些本地元数据在不同位置之间保持一致同步。即使数据正在传输到新位置，用户和应用程序也可以在数据传输过程中进行读/写操作并使用其文件。

该产品智能使用跨文件系统标准的元数据，包括遥测数据（如IOPS、吞吐量和延迟），以及用户定义和分析获取的元数据，使用户或集成的应用程序能够快速查看、过滤和搜索元数据，而不依赖文件名。此外，Hammerspace通过Hammerspace Metadata Plugin支持用户自定义元数据。Hammerspace解释自定义元数据，并将其用于数据分类、数据放置、灾难恢复或数据保护策略。

Hammerspace可以在边缘、本地或云端进行部署，支持AWS、Azure、GCP、Seagate Lyve、Wasabi和其它几个云平台。它可以使用自己的存储节点、数据中心中的任何现有第三方供应商的块、文件或对象存储系统，或各种云存储进行数据存储。它提供了共享级别的快照功能以及全面的复制能力，允许文件通过Hammerspace策略引擎在不同站点之间自动复制。基于策略的复制活动也可以根据需要进行配置。这些功能使组织能够实施多站点的主动灾难恢复，实现自动切换和切换回。

Hammerspace的网络攻击抗性策略依赖于原生的不可变性功能、监视和第三方检测能力。缓解功能包括"撤销删除"和文件版本控制，允许用户还原到未受勒索病毒相关数据损害影响的文件版本。Hammerspace的自动化数据编排以进行恢复也是其功能集的核心组成部分。

Hammerspace已发布到AWS、Azure和Google Cloud市场，并与Snowflake集成。

- **优势**：Hammerspace的并行全局文件系统结合了强大的元数据功能，提供了一个非常平衡的功能集，同时具备复制和混合云的能力。
- **挑战**：目前尚未内置主动勒索病毒检测功能。

LucidLink

LucidLink Filespace是一款旨在克服NFS和SMB协议限制的高效云文件系统，专为分布式任务而设计。作为SaaS解决方案，它将文件存储在与S3对象存储兼容的后端，根据需要进行文件的流式传输。在LucidLink中，文件的元数据与内容数据分离，内容数据被拆分成多个段，每个数据段都是后端的一个独立S3对象。

对于处理大量数据的企业，尤其是媒体、娱乐和创意产业，LucidLink为文件流式传输提供了无缝的解决方案。应用程序可继续将文件视为一个统一的实体，而LucidLink则在后台静默地进行数据流式传输，并按需提供给应用程序，无需担心性能或带宽问题。这种创新的数据管理方法消除了完整文件复制或同步的需求，使快速访问大型数据集变得更加容易，提高了整体工作流效率。

LucidLink解决方案由两个组件组成：LucidLink客户端和LucidLink服务。客户端组件在桌面和服务器的操作系统级别运行（未来计划在移动平台上实施）。其主要功能是使文件看起来像是本地文件，同时管理加密、缓存、预取以及可选的压缩。

提供的解决方案拥有一个全局命名空间，旨在共享，具备完整的文件系统语义。在云上运行的LucidLink服务能够精确地管理元数据协调、文件锁定、垃圾回收、快照以及其它优化功能。客户端加密元数据，然后同步到所有连接的客户端，确保LucidLink和云服务商都不具备任何数据或元数据的知识。实际文件数据存储在对象存储中。

LucidLink的主要关注点是充分利用公有云对象存储提供商，使组织能够创建容量为PB级的卷，每个卷包含数亿个文件。该解决方案旨在支持任何S3对象存储，无论其位于本地、云端还是在Microsoft Azure Blob上。

从安全性角度来看，LucidLink采用零信任访问模型，支持完全的客户端端到端加密和多租户。组织可以使用自己的密钥管理系统，用户在初始化文件空间时创建自己的加密密钥。数据是按租户加密，并在文件系统级别通过不可变、只读的快照进行保护。设计决策采用了零知识安全模型，即数据完全由客户提供的加密密钥进行加密，这提供了卓越的安全性，但也限制了数据管理和数据分析功能的范围，因为LucidLink无法访问客户数据。

LucidLink的管理界面设计良好，但分析和监控功能仍有改进的潜力，许多高级功能仍在路线图上，考虑到前述的架构限制。

- **优势**：通过LucidLink，用户能够轻松访问全局数据，特别适合远程工作和协作。API、自动化支持以及数据分层的改进正在进行中。
- **挑战**：尽管该解决方案的架构考虑了安全性和端到端加密，但也许可以探索一些方法来增强其数据管理和数据分析功能，而不会影响其安全性措施。

Nasuni

Nasuni提供了一种专为企业文件数据服务设计的SaaS解决方案。该解决方案拥有一个基于对象的全局文件系统，支持多种文件接口，包括SMB和NFS，作为其核心引擎。它无缝集成了所有主要云服务商，并兼容本地S3对象存储。Nasuni的SaaS解决方案为企业文件数据服务的管理提供了可靠和高效的平台，有助于企业简化数字业务运营。

Nasuni的解决方案包括一个核心平台，囊括多个领域的附加服务，包括勒索病毒保护和混合工作，同时还计划提供数据管理和内容智能服务。许多Nasuni的客户已经采用该解决方案来替代传统的NAS系统和Windows文件服务器，因为它的特点使用户能够替代其它基础设施组件，如备份、灾难恢复、数据复制服务和归档平台。

Nasuni提供了一个名为UniFS的全局文件系统，它提供了一个层次结构，将文件与存储资源分离，管理公有云或私有云对象存储中的一份主副本的数据，并分发数据访问。全局文件系统管理所有元数据，包括版本控制、访问控制、审计记录和锁定，通过标准协议如SMB和NFS提供对文件的访问。正在使用的文件使用Nasuni的Edge Appliances进行缓存，因此用户可以通过现有的驱动映射和共享点获得高性能的访问。所有文件，包括那些在多个本地缓存中使用的文件，都将其主要副本存储在云对象存储中，因此可以从全球任何访问点进行访问。

Nasuni管理控制台提供了对全局边缘设备、卷、快照、恢复、协议、共享等的集中管理。这个基于Web的界面可用于点对点配置，但Nasuni还提供了REST API方法，用于跨任意数量的站点进行自动监控、配置和报告。此外，Nasuni Health Monitor向Nasuni管理控制台报告CPU、目录服务、磁盘、文件系统、内存、网络、服务、NFS、SMB等的健康状况。Nasuni还与Grafana和Splunk等工具集成，以进行进一步的分析，并最近宣布与Microsoft Sentinel更正式的集成，用于共享来自Nasuni Edge Appliance（NEA）设备的安全、网络威胁和其它事件信息。数据管理功能正在集成中，得益于Nasuni在2022年6月收购数据管理公司Storage Made Easy，未来几个月将会有更多的集成。

Nasuni通过Nasuni Continuous File Versioning和其Rapid Ransomware Recovery功能在其核心平台提供了勒索病毒保护。为了进一步缩短恢复时间，该公司最近推出了Nasuni Ransomware Protection，作为一个付费的附加解决方案，通过不可变的快照增加了预防性检测和自动化缓解能力。该服务根据签名定义分析恶意扩展名、勒索笔记和可疑的传入文件，这些定义被推送到Nasuni Edge Appliances，自动停止攻击，并为管理员提供了一个最新干净快照的地图以进行恢复。该解决方案的未来版本（已在路线图上）将在边缘设备上实施基于AI/ML的分析。

Nasuni Edge Appliances是轻量级虚拟机（VM）或硬件设备，可以使用Windows、macOS和Linux客户端的SMB或NFS访问缓存频繁访问的文件，以实现良好的性能。它们可以在本地或云端部署，以替代传统的文件服务器和NAS设备。它们对文件进行加密和去重，然后以频繁的间隔将它们快照到云中，以只读格式写入对象存储。

Nasuni的附加服务Nasuni Access Anywhere提供本地同步功能、安全便捷的文件共享（包括组织外的共享），并与Microsoft Teams完全集成。此外，边缘设备还提供搜索和文件加速服务。

- **优势**：Nasuni的文件系统解决方案安全、可扩展，并提供了防勒索病毒保护。边缘设备使用户能够快速安全地访问频繁使用的数据。适合寻求高效可靠文件存储的企业。
- **挑战**：目前，Nasuni在有效管理数据方面还有一些不足之处。然而，团队正在努力开发和实施数据管理服务，将在不久的将来提供。

Panzura

Panzura提供了一个高性能的混合云全局文件系统，基于其CloudFS文件系统构建。该解决方案在各个站点（包括公有云和私有云）之间协同工作，为用户提供一个单一的数据平面，具备本地文件操作性能、自动文件锁定和实时全球数据一致性。最近，Panzura对其解决方案进行了重新设计，引入了一个模块化架构，逐步允许更多数据服务与核心Panzura平台进行无缝集成。Panzura最近发布了Panzura Edge，这是CloudFS文件的移动网关，突显了该公司对广泛分布的团队的持续关注，这些团队依赖移动设备进行大文件协作，例如医疗保健领域的临床现场以及遥远工地上的建筑和工程项目。

该解决方案实现了一个全局命名空间，并通过全局文件锁定机制满足数据完整性的要求，无论用户在全球的哪个地点访问文件，都能实现实时数据一致性。此外，它还提供了高效的快照管理，包括版本控制，并允许管理员根据需要进行配置和保留策略的设定。备份和灾难恢复功能也得以提供。

Panzura利用S3对象存储，并与各种对象存储解决方案兼容，无论是托管在公有云中还是本地。其一个关键功能，云镜像，允许用户将数据写入到次要云存储提供商，以确保在一个提供商发生故障时数据可用。此外，Panzura还提供了分层和存档数据的方案。

Panzura通过其Panzura数据服务提供了高级的分析能力。这一系列功能包括全局搜索、用户审计、监控功能和一键文件还原。这些服务提供了核心指标和存储消耗数据，如访问频率、活跃用户和环境健康状况。Panzura还提供了多个数据管理的API服务，允许用户将他们的数据管理工具与Panzura连接起来。Panzura数据服务可以检测到不经常访问的数据，从而使用户可以采取适当的措施。

Panzura数据服务提供了强大的安全功能，以保护数据免受勒索病毒攻击。勒索病毒保护是通过不可变数据（WORM S3后端）和全局文件级别每60秒进行一次只读快照的结合来处理的，定期将数据移动到不可变对象存储中，以允许在勒索病毒攻击发生时通过与正常情况下恢复数据所使用的相同机制——备份——进行无缝数据恢复。这些功能还有Panzura Protect的补充，目前支持检测勒索病毒攻击并提供主动警报。未来，Panzura Protect还将支持端用户异常检测以检测可疑活动。

该解决方案还包括一个安全擦除功能，可以删除所有已删除的文件版本，并使用零覆盖已删除的数据，即使在云端对象存储上也可以使用该功能。

解决方案的新功能之一是Panzura Edge，它将Panzura的CloudFS直接扩展到用户的本地计算机。

- **优势**：Panzura提供了一个混合云全局文件系统，具有本地访问性能、全球可用性、数据一致性、分层存储和高级分析，有助于组织更有效地管理其数据足迹。
- **挑战**：Panzura Edge是产品的一个相对较新的附加功能，承诺为移动协作和数据管理提供强大的解决方案。然而，鉴于其最近的推出，确认或独立验证其在实施之前是否足够重要，以确保它满足您的需求和期望。

Peer Software

Peer Software采用一种独特的方法来应对分布式云文件存储的挑战。其全局文件服务（GFS）解决方案与其它供应商的解决方案不同，其它供应商通常在现有文件系统之上实现其专有的全局分布式文件系统，而Peer Software则在不同存储供应商的现有文件系统之上实现了一个分布式服务。该解决方案的关键特点包括全局文件锁定、站点之间的主动-主动数据复制、高可用性和集中式备份。

PeerGFS架构由两个关键组件组成：PeerGFS代理和PeerGFS管理中心。PeerGFS管理中心负责配置、管理和监控，同时还作为消息代理，与其它消息代理和PeerGFS代理进行通信。PeerGFS可以配置文件以在集线器和分支拓扑或点对点拓扑中进行复制，适用于需要数据留在特定地理区域以满足数据主权法规的情况。

PeerGFS在几个方面独具特色。与其它供应商不同，它使用Microsoft DFS在混合云和多云环境中创建命名空间，而不是实现专有的全局命名空间。用户可以将此解决方案部署在本地或云端。PeerGFS支持绝大多数带有SMB支持的硬件文件系统，同时也支持Azure Blob和任何S3兼容的公有云存储，最近还增加了对NFS的支持。此外，PeerGFS兼容AWS FSx for NetApp ONTAP、Dell Apex Files和Nutanix Cloud Clusters等云存储解决方案。

Peer Software的解决方案采用双活架构，在数据中心和云之间复制数据。它还支持多云实施和跨可用性区域的复制。为了节省带宽并加速传输，PeerGFS仅复制增量更改，同时通过全局文件锁定防止文件版本冲突。

此外，该解决方案还提供了数据迁移功能。数据可以备份到兼容S3的对象存储和公有云平台。备份的数据以单个文件形式存储，这使得可以进行文件级别的恢复，允许立即重用数据，适用于基于文件的数据集场景。

除了PeerGFS管理界面提供的监控功能外，Peer Software最近推出了PeerIQ，这是一个独立的解决方案，旨在提供存储可观察性功能，包括实时事件流监控、分析、警报和报告功能。这个基础版本提供了信息丰富的可定制仪表板，并将通过持续的更新进一步改进。

目前，Peer Software的抵御勒索病毒的能力主要集中在检测用户或应用程序在分布式文件服务上的活动方面。Peer Malicious Event Detection（MED）是一款用于分析和检测恶意活动的引擎，包括勒索病毒攻击。进一步的勒索病毒保护措施尚未实施。至于不可变性，该解决方案目前没有本地支持，而是依赖于第三方S3存储的不可变性功能，以实现文件数据的复制。要实现这一点，客户需要使用Peer Software的S3连接器进行备份。

此外，Peer Software还提供另一解决方案PeerFSA，用于提供有关组织环境的洞察，并生成关于基于时间的指标/使用情况、目录、用户和文件类型的报告。这些报告是静态的，以Excel格式提供。

一些组织使用PeerGFS作为云文件存储服务的替代和经济高效的文件缓存解决方案。然而，值得注意的是，PeerGFS本身不提供任何边缘缓存存储硬件，通常缓存的文件存储在客户的Windows文件服务器上。

- **优势**：Peer Software通过在现有基础设施之上实现分布式云文件存储解决方案，创建了一个组织现有资源的单一命名空间。这可以为用户节省时间和费用，因为它们不需要替换现有工具。此外，该解决方案具有出色的恶意活动检测能力，并在监控和分析领域取得了显著的提升。
- **挑战**：PeerGFS的设计依赖于底层硬件和软件能力，因为它是构建在现有硬件之上的分布式文件服务层。此外，该解决方案目前不支持本地不可变性功能，而依赖于第三方S3存储的不可变性。

Source: Max Mortillaro, Arjan Timmerman, GigaOm Radar for Distributed Cloud File Storagev4.0, Nov 8, 2023

---【本文完】---

近期受欢迎的文章：
- 2023年非结构化数据管理报告
- 文件/块存储勒索病毒解决方案报告
- 2023年全球AI趋势报告
- 探寻通用存储之道（测试报告）
- 【报告】闪存存储垄断被打破了吗？

我们正处于数十年未见之大机遇中
新技术爆发式发展，催生新产品
然而，颠覆式创新并非简单的技术堆叠
而是异常复杂的系统工程
需要深度洞察
欢迎一起分享思考和见解


常华Andy
上海 徐汇

扫一扫上面的二维码图案，加我为朋友。

Andy730

收录于合集 #存储行业趋势 147

上一篇

分布式文件系统和对象存储魔力象限：五年演进（2019-2023）

下一篇

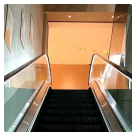
HPC/AI与存储领域简讯

Read more

People who liked this content also liked

【一句】CXL SSD 箭在铉上（几篇文章）
Andy730

分布式文件系统和对象存储魔力象限：五年演进（2019-2023）
Andy730



Transformer模型：介绍与目录（全）
Andy730