# ONTAP 概念

ONTAP 9

NetApp
April 24, 2024

# 目录

# ONTAP 概念

## 概念概述

以下概念为ONTAP数据管理软件提供了依据、包括集群存储、高可用性、虚拟化、数据保护、 存储效率、安全性和FabricPool。在配置存储解决方案之前，您应了解 ONTAP 的全部功能和优势。

对于追加信息、请参见以下内容：

- "集群和 SVM 管理"
- "高可用性(HA)对"
- "网络和 LIF 管理"
- "磁盘和聚合管理"
- "FlexVol 卷， FlexClone 技术和存储效率功能"
- "SAN 主机配置"
- NAS 文件访问
  - "NFS 管理"
  - "SMB管理"
- "灾难恢复和归档"

## ONTAP 平台

ONTAP 数据管理软件为通过块或文件访问协议读取和写入数据的应用程序提供统一存储，存储配置范围从高速闪存到价格较低的旋转介质再到基于云的对象存储。

ONTAP实施可在NetApp设计的FAS、AFF A系列和C系列以及全SAN闪存阵列ASA平台上、以及在商用硬件(ONTAP Select)和私有云、公共云或混合云(Cloud Volumes ONTAP)中运行。专业化实施可提供同类最佳的融合基础架构(FlexPod Datacenter)。

这些实施共同构成了 _NetApp Data Fabric 的基本框架，并采用通用的软件定义方法进行数据管理，以及跨平台快速高效地进行复制。

## 集群存储

ONTAP 的当前迭代最初是为 NetApp 的横向扩展 *cluster* 存储架构开发的。在 ONTAP 的数据中心实施中，您通常会发现这种架构。由于此实施可实现 ONTAP 的大部分功能，因此，您可以从了解 ONTAP 技术的概念入手。

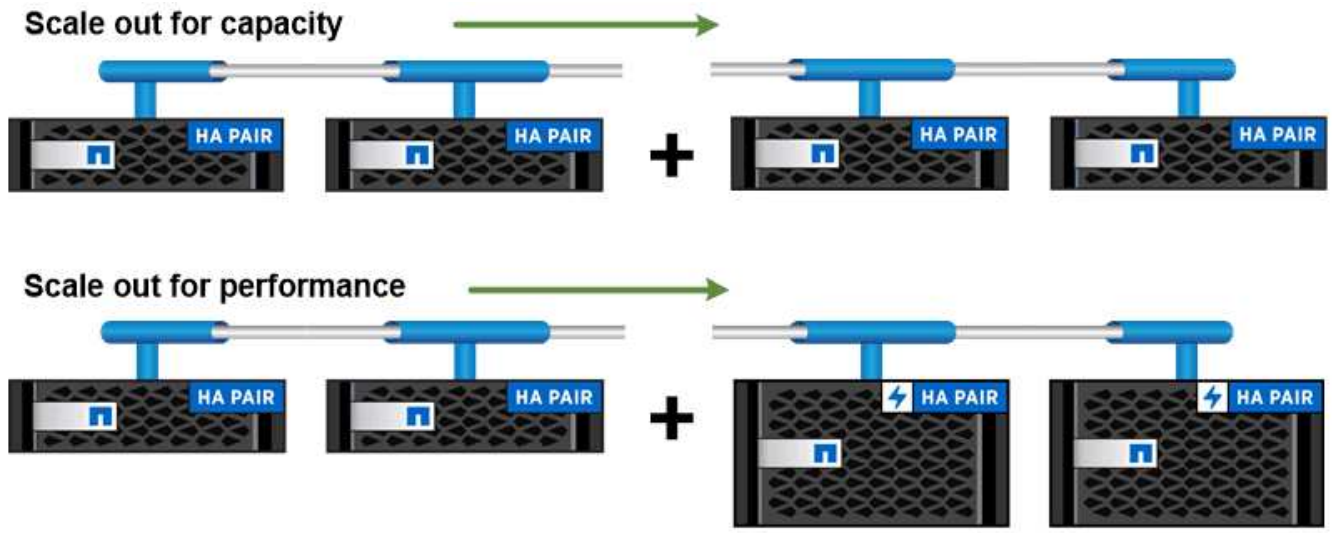
数据中心架构通常部署运行 ONTAP 数据管理软件的专用 FAS 或 AFF 控制器。每个控制器，其存储，网络连接以及在控制器上运行的 ONTAP 实例均称为 _node 。 _

节点已配对以实现高可用性（ HA ）。这些对（ SAN 最多 12 个节点， NAS 最多 24 个节点）共同构成集群。节点通过专用的专用集群互连相互通信。

根据控制器型号，节点存储由闪存磁盘，容量驱动器或两者组成。控制器上的网络端口可用于访问数据。物理存储和网络连接资源已虚拟化，仅对集群管理员可见，而不对 NAS 客户端或 SAN 主机可见。

HA 对中的节点必须使用相同型号的存储阵列。否则，您可以使用任何受支持的控制器组合。您可以通过添加具有类似存储阵列型号的节点来横向扩展容量，也可以通过添加具有高端存储阵列的节点来提高性能。

当然，您也可以采用所有传统方式进行纵向扩展，并根据需要升级磁盘或控制器。ONTAP 的虚拟化存储基础架构可以轻松无中断地移动数据，这意味着您可以在不停机的情况下纵向或横向扩展。




*You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.*

# 高可用性对

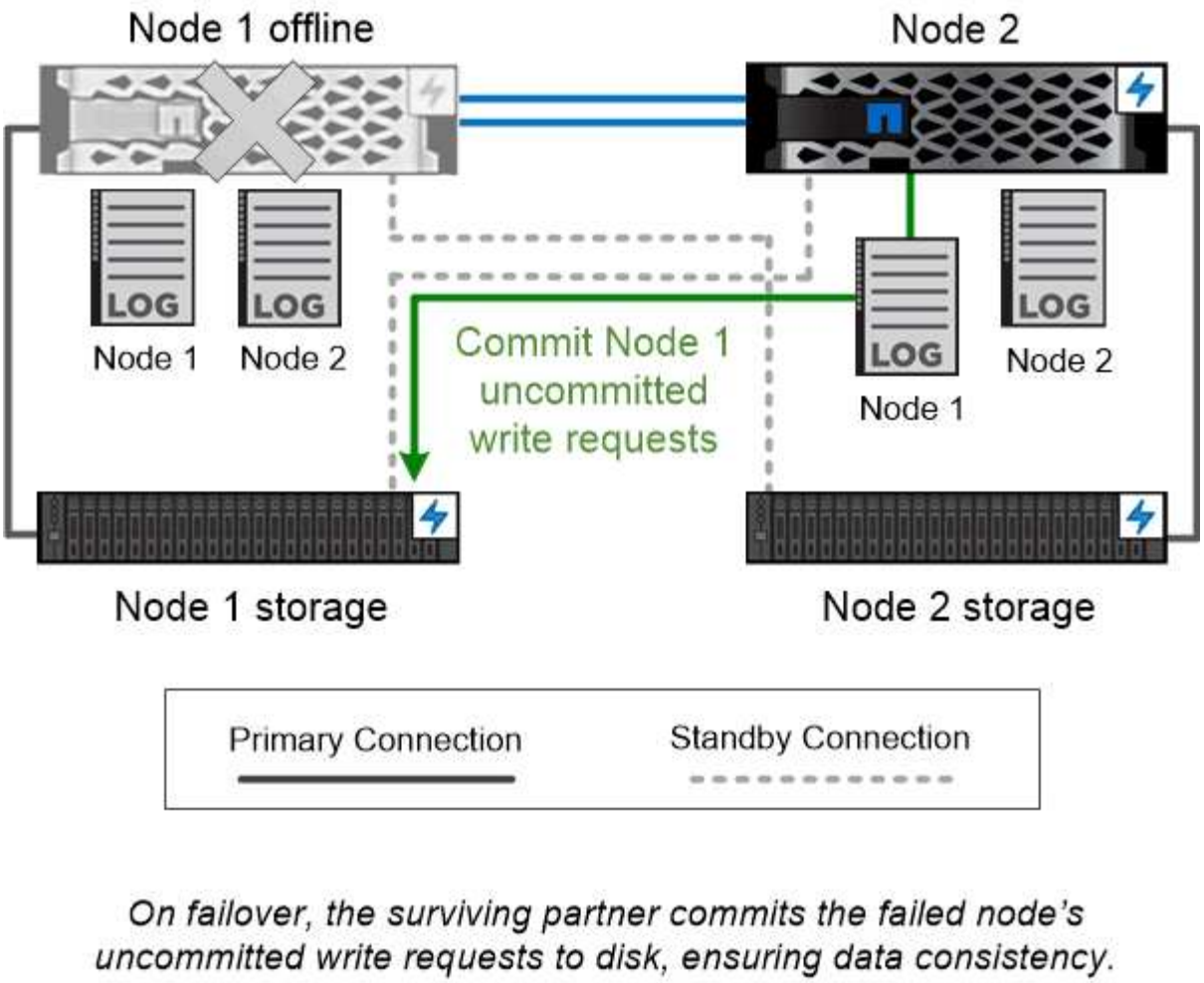
集群节点在 *High-availability* （ *HA* ）对中进行配置，以实现容错和无中断运行。如果某个节点发生故障或需要关闭某个节点以进行日常维护，其配对节点可以接管其存储并继续从中提供数据。当节点恢复联机时，配对节点 *_gives back* storage 。

HA 对始终由相似的控制器型号组成。控制器通常位于具有冗余电源的同一机箱中。

HA对是一种容错节点、可以通过不同的方式相互通信、使每个节点能够持续检查其配对节点是否正常运行、并为另一节点的非易失性内存镜像日志数据。向节点发出写入请求时，在将响应发送回客户端或主机之前，该请求会记录在两个节点上的 NVRAM 中。故障转移时，无故障配对节点会将故障节点未提交的写入请求提交到磁盘，以确保数据一致性。

通过连接到另一个控制器的存储介质，可以使每个节点在发生接管时访问另一个控制器的存储。网络路径故障转移机制可确保客户端和主机继续与正常运行的节点进行通信。

为了确保可用性，您应将任一节点上的性能容量利用率保持在 50% ，以便在故障转移情况下处理额外的工作负载。出于同样的原因，您可能希望为一个节点配置的 NAS 虚拟网络接口数量不超过最大数量的 50% 。




- 虚拟化 ONTAP 实施中的接管和交还 _*

存储不会在 `sONTAP for AWS` 或 `ONTAP Select` 等虚拟化 " 无 " Cloud Volumes ONTAP 实施中的节点之间共享。当节点发生故障时，其配对节点将继续从节点数据的同步镜像副本提供数据。它不会接管节点的存储，而是接管其数据服务功能。

# AutoSupport 和 Active IQ Digital Advisor

ONTAP 通过 Web 门户和移动应用程序提供人工智能系统监控和报告。ONTAP 的 AutoSupport 组件会发送遥测数据，并由 Active IQ Digital Advisor 进行分析。

Active IQ 通过基于云的门户和移动应用程序提供可操作的预测性分析和主动式支持，帮助您优化全球混合云中的数据基础架构。Active IQ 提供的数据驱动型洞察力和建议可供具有有效 SupportEdge 合同的所有 NetApp 客户使用（功能因产品和支持层而异）。

以下是您可以使用 Active IQ 执行的一些操作：

- 计划升级。Active IQ 可确定环境中可通过升级到较新版本的 ONTAP 来解决的问题， Upgrade Advisor 组件可帮助您规划成功升级。
- 查看系统运行状况。您的 Active IQ 信息板可报告任何健康问题，并帮助您更正这些问题。监控系统容量，

确保存储空间不会用尽。

- 管理性能。Active IQ 显示系统性能的时间比您在 System Manager 中看到的时间长。确定影响性能的配置和系统问题。
- 最大限度地提高效率。查看存储效率指标并确定如何在更少的空间中存储更多数据。
- 查看清单和配置。Active IQ 将显示完整的清单以及软件和硬件配置信息。请查看服务合同何时到期，以确保您始终可以获得服务。

相关信息

"NetApp 文档： Active IQ Digital Advisor"

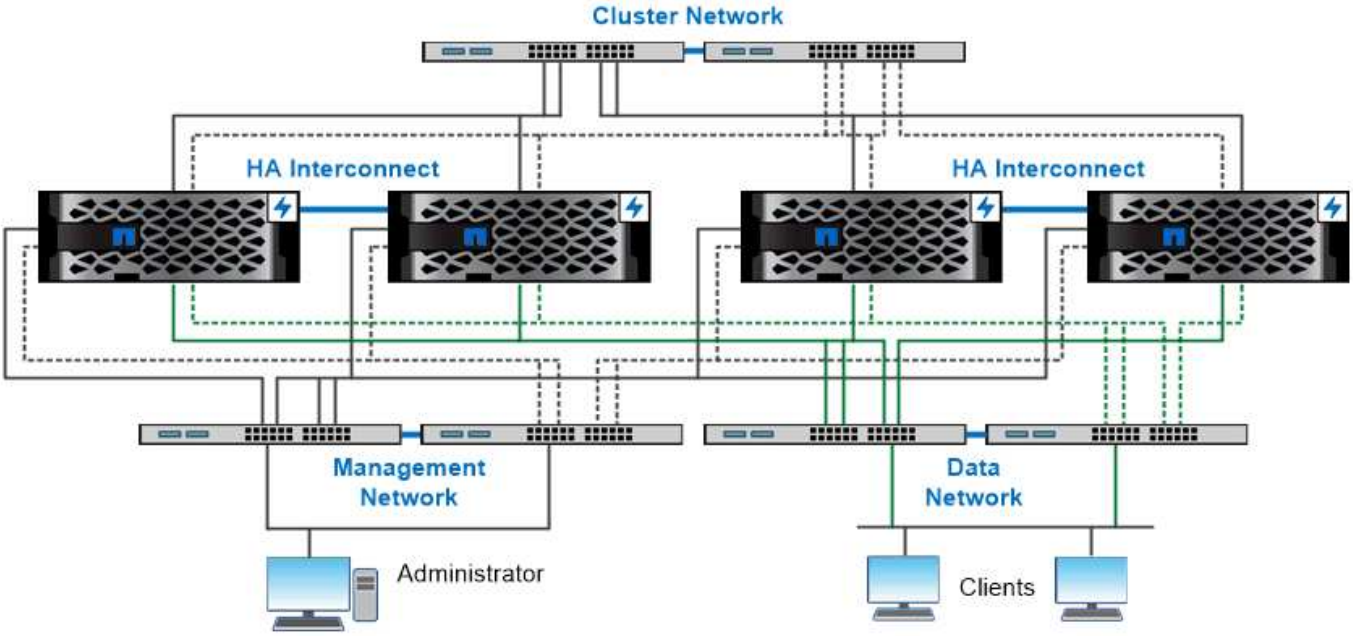
"启动 Active IQ"

"SupportEdge 服务"

# 网络架构

## 网络架构概述

ONTAP 数据中心实施的网络架构通常由集群互连，用于集群管理的管理网络和数据网络组成。NIC （网络接口卡）为以太网连接提供物理端口。HBA （主机总线适配器）为 FC 连接提供物理端口。




*The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.*

## 逻辑端口

除了每个节点上提供的物理端口之外，您还可以使用 _logical ports_来 管理网络流量。逻辑端口是接口组或 VLAN 。

接口组

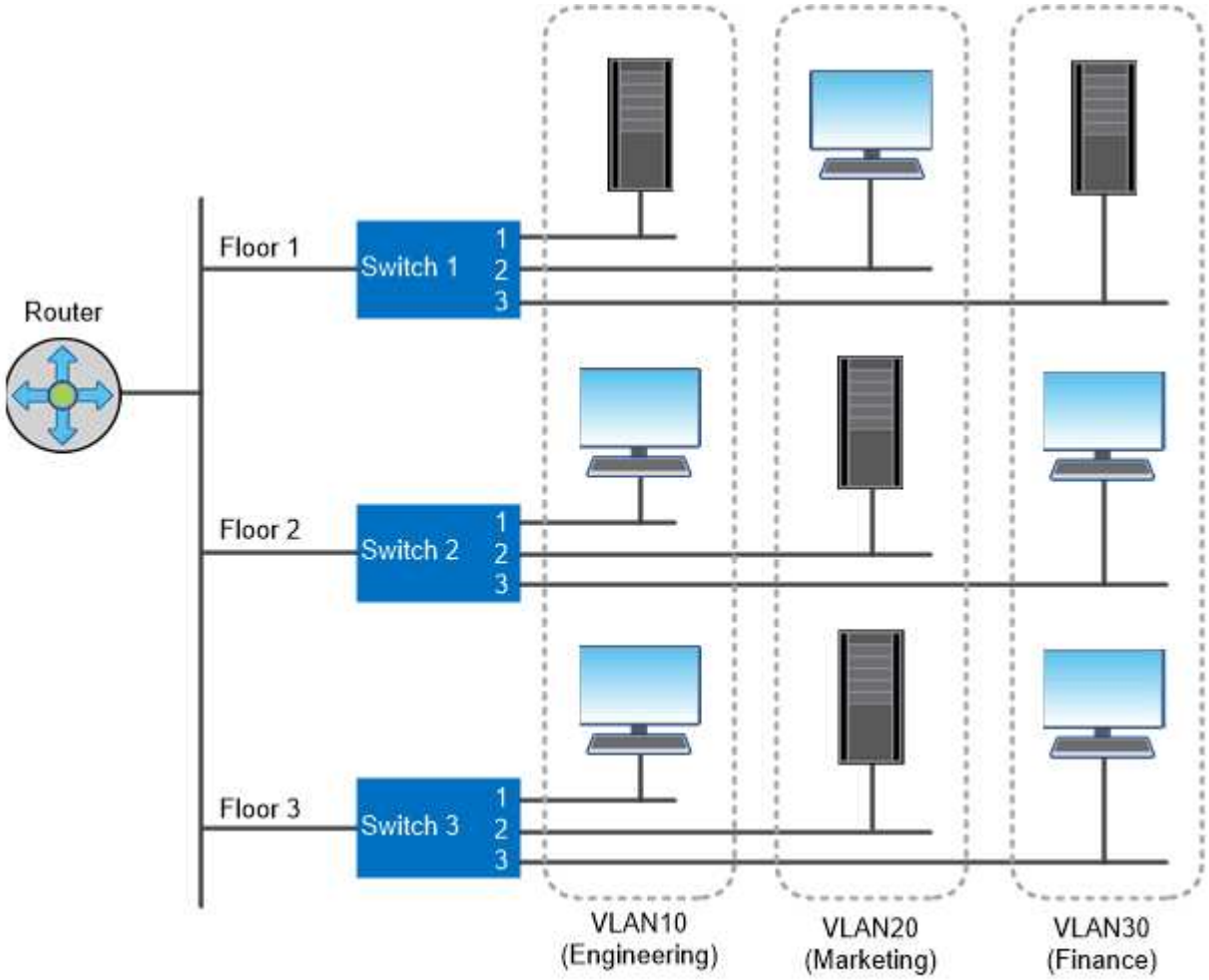
_Interface groups_将多个物理端口组合成一个逻辑"`trunk port`"。您可能需要创建一个由不同PCI插槽中NIC的端口组成的接口组、以确保不会因插槽故障而导致业务关键型流量中断。

接口组可以是单模式，多模式或动态多模式。每个模式提供不同级别的容错。您可以使用任一类型的多模式接口组来对网络流量进行负载平衡。

**VLAN**

*VLANs* 将流量从网络端口（可能是接口组）分离到基于交换机端口定义的逻辑分段中，而不是物理边界。属于 VLAN 的 _end-station_are related by function or application 。

您可以按部门（如工程和营销）或项目（如释放 1 和释放 2 ）对终端工作站进行分组。由于终端工作站的物理位置与 VLAN 无关，因此终端工作站可能位于地理位置较远程的位置。




*You can use VLANs to segregate traffic by department.*

## 支持行业标准网络技术

ONTAP 支持所有主要的行业标准网络技术。关键技术包括 IP 空间， DNS 负载平衡和 SNMP 陷阱。

中介绍了广播域，故障转移组和子网 NAS 路径故障转移。

#### IP 空间

您可以使用 *ipspaces* 为集群中的每个虚拟数据服务器创建一个不同的 IP 地址空间。这样，在管理上独立的网络域中的客户端就可以访问集群数据，同时使用来自同一 IP 地址子网范围的重叠 IP 地址。

例如，服务提供商可以为使用相同 IP 地址的租户配置不同的 IP 空间来访问集群。

#### DNS 负载平衡

您可以使用 _DNS 负载平衡 _ 在可用端口之间分布用户网络流量。DNS 服务器会根据接口上挂载的客户端数量动态选择用于流量的网络接口。

#### SNMP 陷阱

您可以使用 _SNMP 陷阱 _ 定期检查操作阈值或故障。SNMP 陷阱捕获从 SNMP 代理异步发送到 SNMP 管理器的系统监控信息。

#### FIPS合规性

对于所有 SSL 连接， ONTAP 均符合联邦信息处理标准（ FIPS ） 140-2 的要求。您可以打开和关闭 SSL FIPS 模式，全局设置 SSL 协议以及关闭 RC4 等任何弱密码。

## RDMA概述

ONTAP的远程直接内存访问(Remote Direct Memory Access、RDMA)产品支持对延迟敏感的高带宽工作负载。通过 RDMA ，可以直接在存储系统内存和主机系统内存之间复制数据，从而避免 CPU 中断和开销。

#### 基于 RDMA 的 NFS

从 ONTAP 9.10.1 开始，您可以进行配置 "基于 RDMA 的 NFS" 在具有受支持的 NVIDIA GPU 的主机上启用 NVIDIA GPUDirect 存储以处理 GPU 加速工作负载。

#### RDMA集群互连

RDMA 集群互连可减少延迟，缩短故障转移时间并加快集群中节点之间的通信速度。

从ONTAP 9.10.1开始、与X1151A集群NIC结合使用时、某些硬件系统支持集群互连RDMA。从ONTAP 9.131开始、X91153A NIC还支持集群互连RDMA。请参考下表、了解不同ONTAP版本支持哪些系统。

| 系统 | 支持的ONTAP版本 |
| --- | --- |
| • A400<br>• ASA A400 | ONTAP 9.10.1 及更高版本 |

| 系统 | 支持的**ONTAP**版本 |
| --- | --- |
| • AFF A900<br>• ASA A900<br>• FAS9500 | ONTAP 9.13.1及更高版本 |

如果设置了适当的存储系统、则无需进行其他配置即可使用RDMA互连。

# 客户端协议

## ONTAP 支持所有主要的行业标准客户端协议：NFS、SMB、FC、FCoE、iSCSI、NVMe/FC和S3。

### NFS

NFS 是 UNIX 和 Linux 系统的传统文件访问协议。客户端可以使用以下协议访问ONTAP卷中的文件。

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- pNFS

您可以使用 UNIX 模式的权限， NTFS 模式的权限或两者的混合来控制文件访问。

客户端可以使用 NFS 和 SMB 协议访问相同的文件。

### SMB

SMB 是 Windows 系统的传统文件访问协议。客户端可以使用 SMB 2.0 ， SMB 2.1 ， SMB 3.0 和 SMB 3.1.1 协议访问 ONTAP 卷中的文件。与 NFS 一样，支持混合使用多种权限模式。

SMB 1.0 可用，但在 ONTAP 9.3 及更高版本中默认处于禁用状态。

### FC

光纤通道是初始的网络块协议。块协议将整个虚拟磁盘呈现给客户端，而不是文件。传统 FC 协议使用具有专用 FC 交换机的专用 FC 网络，并要求客户端计算机具有 FC 网络接口。

LUN 表示虚拟磁盘，一个或多个 LUN 存储在 ONTAP 卷中。可以通过 FC ， FCoE 和 iSCSI 协议访问同一个 LUN ，但多个客户端只有在属于可防止写入冲突的集群时才能访问同一个 LUN 。

### FCoE

FCoE 与 FC 基本上是相同的协议，但使用数据中心级以太网网络代替传统 FC 传输。客户端仍需要 FCoE 专用的网络接口。

### iSCSI

iSCSI 是一种可在标准以太网网络上运行的块协议。大多数客户端操作系统都提供一个通过标准以太网端口运行的软件启动程序。如果您需要为特定应用程序使用块协议，但没有可用的专用 FC 网络，则 iSCSI 是一个不错的选择。

### NVMe/FC

最新的块协议 NVMe/FC 专为使用基于闪存的存储而设计。它可以提供可扩展的会话，显著降低延迟并提高并行性，因此非常适合内存数据库和分析等低延迟和高吞吐量应用程序。

与 FC 和 iSCSI 不同， NVMe 不使用 LUN 。而是使用存储在 ONTAP 卷中的命名空间。NVMe 命名空间只能通过 NVMe 协议进行访问。

### S3

从ONTAP 9.8开始、您可以在ONTAP 集群中启用ONTAP 简单存储服务(S3)服务器、从而可以使用S3存储分段在对象存储中提供数据。

ONTAP 支持在为S3对象存储提供服务时采用两种内部使用情形：

- FabricPool 层到本地集群（分层到本地分段）或远程集群（云层）上的分段。
- S3 客户端应用程序访问本地集群或远程集群上的存储分段。

> 如果您需要在现有集群上使用 S3 功能，而无需额外的硬件和管理，则 ONTAP S3 是合适的。对于 300 TB 以上的部署， NetApp StorageGRID 软件仍然是 NetApp 的旗舰级对象存储解决方案。了解相关信息 "StorageGRID"。

## 磁盘和聚合

= :allow-uri-read:

### 本地层(聚合)和RAID组

现代 RAID 技术可通过在备用磁盘上重建故障磁盘的数据来防止磁盘故障。系统会将 "`奇偶校验磁盘` " 上的索引信息与其余运行正常的磁盘上的数据进行比较，以重建缺少的数据，而无需停机或高昂的性能成本。

一个本地层(聚合)由一个或多个_RAID组_组成。本地层的_RAID type_决定RAID组中的奇偶校验磁盘数以及RAID配置可防止的并发磁盘故障数。

默认 RAID 类型 RAID-DP （ RAID-DP （ RAID-DP 双奇偶校验）要求每个 RAID 组具有两个奇偶校验磁盘，并可防止在两个磁盘同时发生故障时丢失数据。对于 RAID-DP ，建议的 RAID 组大小介于 12 到 20 个 HDD 和 20 到 28 个 SSD 之间。

您可以通过在较高的规模估算建议端创建 RAID 组来分摊奇偶校验磁盘的开销成本。SSD 尤其如此，因为 SSD 比容量驱动器更可靠。对于使用HDD的本地层、您应在最大程度地提高磁盘存储的需求与较大RAID组所需的较长重建时间等抵消因素之间取得平衡。

## 镜像和未镜像本地层(聚合)

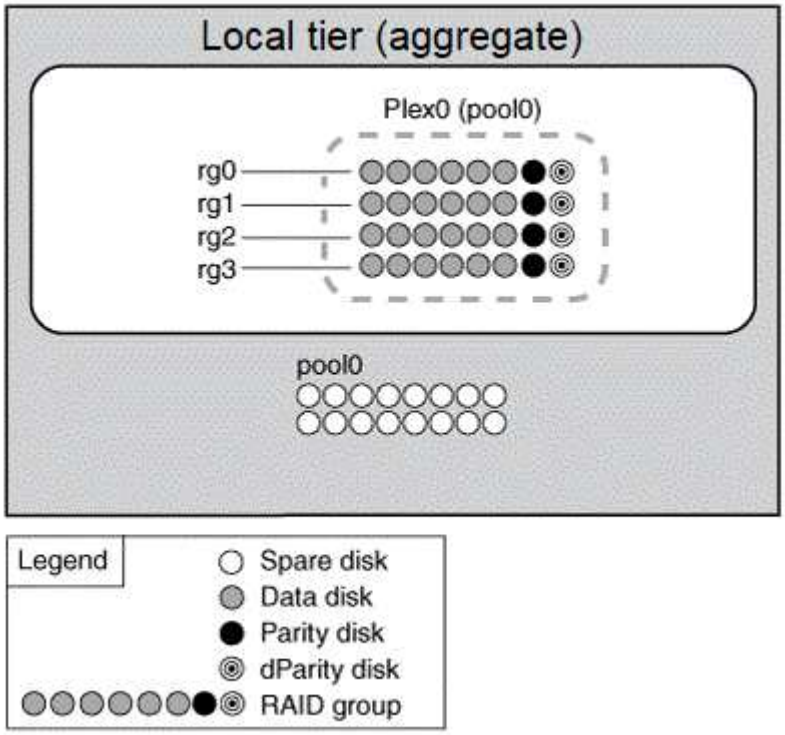
ONTAP 具有一个称为_RAID_的可选功能、您可以使用该功能同步镜像副本中的本地层(聚合)数据、也可以是存储在不同SyncMirror 组中的_plexes_。丛可确保在出现故障的磁盘数量超过 RAID 类型所能保护的磁盘数量或与 RAID 组磁盘的连接断开时防止数据丢失。

使用System Manager或CLI创建本地层时、您可以指定已镜像或未镜像本地层。

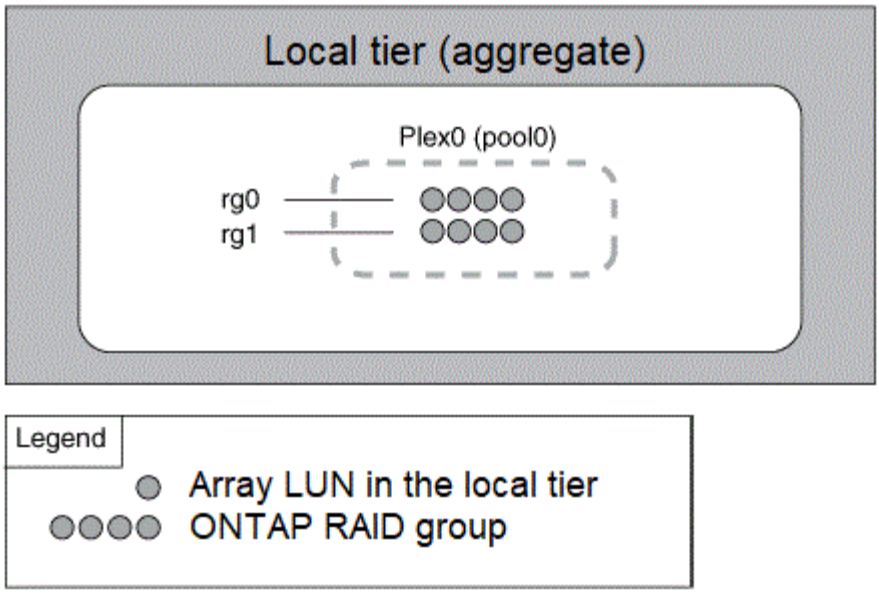
### 未镜像的本地层(聚合)的工作原理

如果未指定要镜像这些本地层、则这些本地层将创建为未镜像本地层(聚合)。未镜像的本地层只有一个_plex_(其数据的副本)、其中包含属于该本地层的所有RAID组。

下图显示了一个由磁盘组成的未镜像本地层及其一个丛。本地层包含四个RAID组：rg0、rg1、rg2和rg3。每个RAID组都有六个数据磁盘、一个奇偶校验磁盘和一个dparity (双奇偶校验)磁盘。本地层使用的所有磁盘都来自同一个池"`pool0`"。




下图显示了一个具有阵列LUN的未镜像本地层及其一个丛。它具有两个 RAID 组： rg0 和 rg1 。本地层使用的所有阵列LUN均来自同一个池"`pool0`"。




镜像本地层(聚合)的工作原理

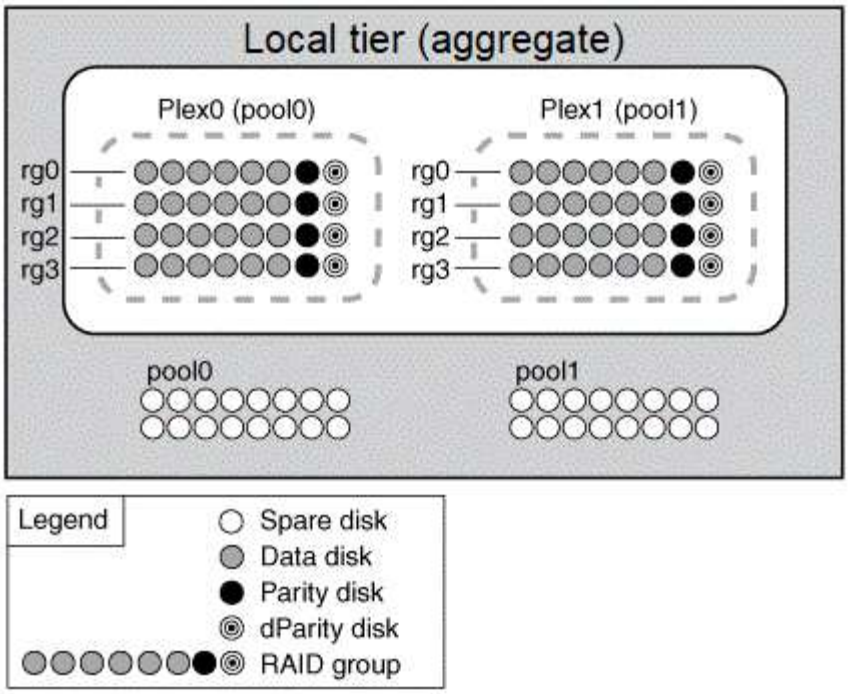
镜像聚合具有两个 *plexes* （其数据的副本），这两个聚合使用 SyncMirror 功能复制数据以提供冗余。

创建本地层时、您可以指定它是镜像本地层。 此外、您还可以向现有未镜像本地层添加另一个丛、使其成为镜像层。使用SyncMirror 功能、ONTAP 会将原始丛(plex0)中的数据复制到新丛(plex1)中。丛在物理上是分开的（每个丛都有自己的 RAID 组和池），并且丛会同时更新。

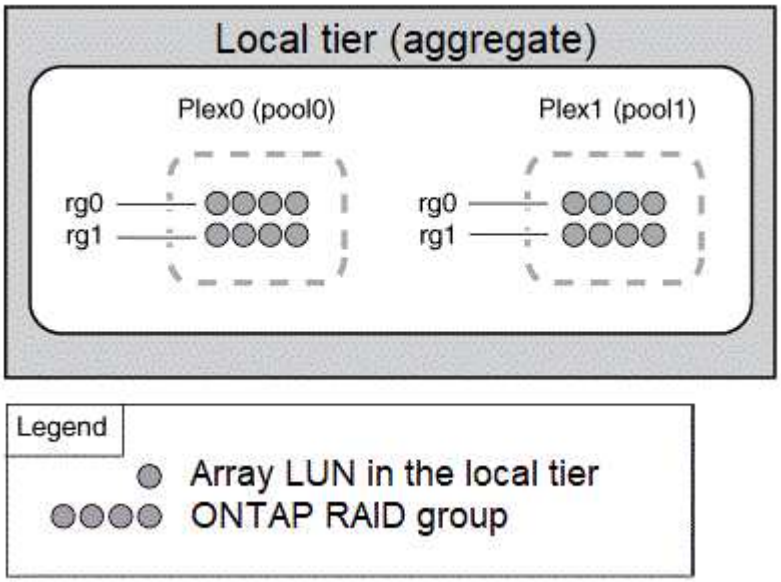
如果出现故障的磁盘数超过聚合所保护的RAID级别、或者连接断开、则此配置可提供额外的保护、防止数据丢失、因为在修复故障发生原因 期间、未受影响的丛会继续提供数据。修复出现问题的丛后，两个丛将重新同步并重新建立镜像关系。

系统上的磁盘和阵列LUN分为两个池：“pool0`"和"`pool1”。Plex0 从 pool0 获取其存储，而 Plex1 从 pool1 获取其存储。

下图显示了一个由启用并实施了SyncMirror 功能的磁盘组成的本地层。已为本地层创建第二个丛"`plex1`" 。plex1 中的数据是 plex0 中的数据副本， RAID 组也是相同的。32个备用磁盘将使用每个池的16个磁盘分配给pool0或pool1。




下图显示了一个由已启用并实施SyncMirror 功能的阵列LUN组成的本地层。已为本地层创建第二个丛"`plex1`" 。Plex1 是 plex0 的副本， RAID 组也相同。




建议为镜像聚合至少保留20%的可用空间、以获得最佳存储性能和可用性。虽然建议对非镜像聚合使用10%的空间、但文件系统可以使用额外的10%空间来吸收增量更改。由于ONTAP采用基于Snapshot的写时复制架构、增量更改可提高镜像聚合的空间利用率。不遵守这些最佳实践可能会对性能产生负面影响。

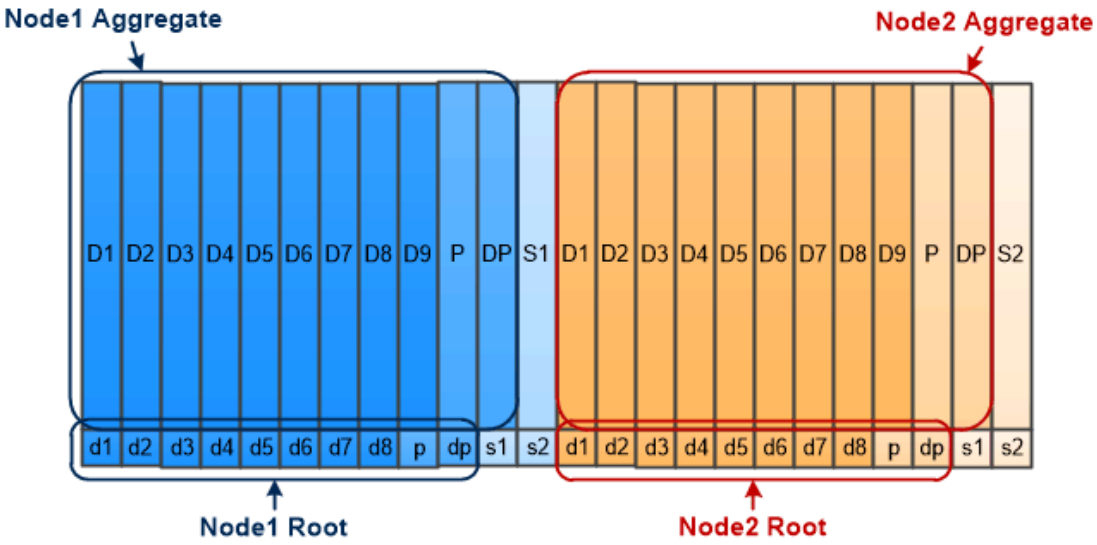
## 根数据分区

每个节点都必须具有存储系统配置文件的根聚合。根聚合具有数据聚合的 RAID 类型

System Manager 不支持根 - 数据或根 - 数据 - 数据分区。

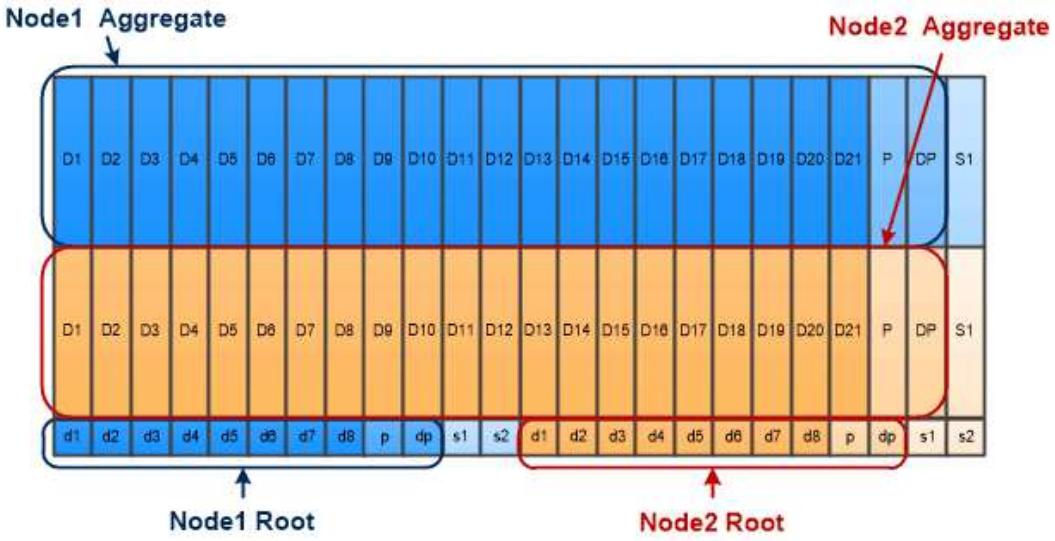
RAID-DP 类型的根聚合通常由一个数据磁盘和两个奇偶校验磁盘组成。如果系统已为聚合中的每个 RAID 组预留两个磁盘作为奇偶校验磁盘，则要为存储系统文件支付 "`奇偶校验税` " 是一项重大的费用。

根 - 数据分区 _ 通过在磁盘分区之间分配根聚合，在每个磁盘上保留一个小分区作为根分区，并为数据保留一个大分区来减少奇偶校验费用。




*Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.*

如图所示，用于存储根聚合的磁盘越多，根分区越小。这种情况也适用于一种名为 *root-data-data partition* 的根 - 数据分区形式，它会创建一个小分区作为根分区，并为数据创建两个大小相等的较大分区。




*Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.*

这两种类型的根数据分区均属于 ONTAP 高级驱动器分区（ADP） _ 功能的一部分。这两种配置在出厂时均已配置：入门级 FAS2xxx， FAS9000， FAS8200， FAS80xx 和 AFF 系统的根数据分区，仅适用于 AFF 系统的根数据数据分区。

了解更多信息 "高级驱动器分区"。

驱动器已分区并用于根聚合

已分区以在根聚合中使用的驱动器取决于系统配置。

了解用于根聚合的驱动器数量有助于确定为根分区预留的驱动器容量以及可用于数据聚合的容量。

入门级平台、全闪存FAS 平台以及仅连接SSD的FAS 平台均支持根数据分区功能。

对于入门级平台、仅对内部驱动器进行分区。

对于纯闪存FAS 平台和仅连接SSD的FAS 平台、系统初始化时连接到控制器的所有驱动器都会进行分区、每个节点最多可分区24个驱动器。在系统配置后添加的驱动器不会进行分区。

# 卷， qtree ，文件和 LUN

ONTAP 从名为 _Volume FlexVol 的逻辑容器向客户端和主机提供数据。 _ 由于这些卷只是与其包含的聚合松散耦合，因此与传统卷相比，它们在管理数据方面提供了更大的灵活性。

您可以将多个 FlexVol 卷分配给一个聚合，每个卷专用于不同的应用程序或服务。您可以扩展和缩减 FlexVol 卷，移动 FlexVol 卷以及为 FlexVol 卷创建高效副本。您可以使用 *qtree* 将 FlexVol 卷分区为更易于管理的单元，并使用 *quotas* 限制卷资源使用量。

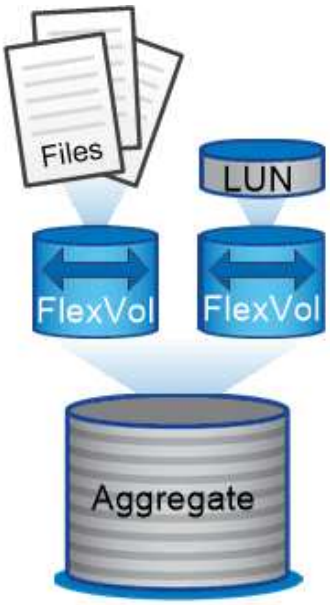
卷包含 NAS 环境中的文件系统和 SAN 环境中的 LUN 。LUN （逻辑单元号）是一个由 SAN 协议寻址的名为 *logical unit* 的设备的标识符。

LUN 是 SAN 配置中的基本存储单元。Windows 主机将存储系统上的 LUN 视为虚拟磁盘。您可以根据需要无中断地将 LUN 移动到不同的卷。

除了数据卷之外，您还需要了解一些特殊卷：

- 节点根卷 _ （通常为 "`vol0` " ）包含节点配置信息和日志。
- SVM 根卷 _ 充当 SVM 提供的命名空间的入口点，并包含命名空间目录信息。
- 系统卷 _ 包含特殊元数据，例如服务审核日志。

您不能使用这些卷来存储数据。




*Volumes contain files in a NAS environment and LUNs in a SAN environment.*

- ； FlexGroup volumes_*

在某些企业中，单个命名空间可能需要数 PB 的存储，甚至远远超过 FlexVol 卷的 100 TB 容量。

FlexGroup 卷 _ 包含 200 个成分卷，支持多达 4000 亿个文件，这些卷协同工作，可以在所有成员之间均匀地动态平衡负载和空间分配。

FlexGroup 卷不需要维护或管理开销。您只需创建 FlexGroup 卷并与 NAS 客户端共享即可。ONTAP 可执行其余操作。

# 存储虚拟化

## 存储虚拟化概述

您可以使用 _storage virtual machine （ SVM ） _ 向客户端和主机提供数据。与虚拟机管理程序上运行的虚拟机一样， SVM 也是一个逻辑实体，用于抽象化物理资源。通过 SVM 访问的数据不会绑定到存储中的某个位置。对 SVM 的网络访问不会绑定到物理端口。

SVM以前称为Vserver。 ONTAP 命令行界面仍使用术语"vServer"。

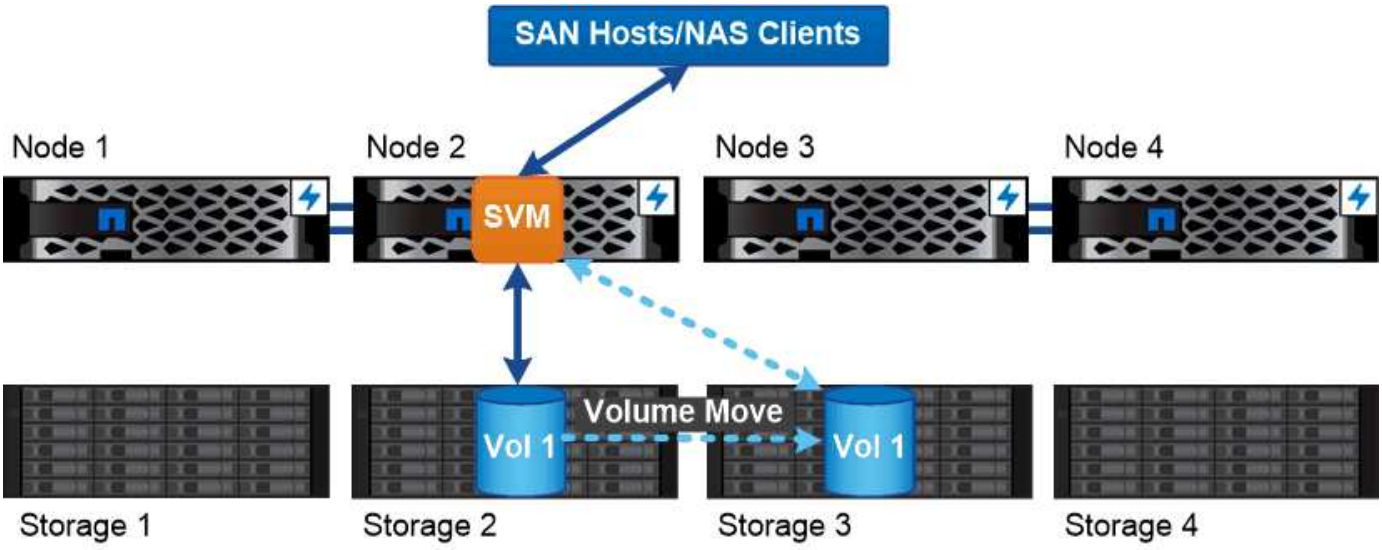
SVM 通过一个或多个网络逻辑接口（ LIF ） _ 从一个或多个卷向客户端和主机提供数据。可以将卷分配给集群中的任何数据聚合。LIF 可以由任何物理或逻辑端口托管。无论您是执行硬件升级，添加节点，平衡性能还是优化聚合间的容量，都可以在不中断数据服务的情况下移动卷和 LIF 。

同一 SVM 可以具有一个用于 NAS 流量的 LIF 和一个用于 SAN 流量的 LIF 。客户端和主机只需要 LIF 的地址（ NFS ， SMB 或 iSCSI 的 IP 地址； FC 的 WWPN ）即可访问 SVM 。LIF 会在移动时保留其地址。端口可以托管多个 LIF 。每个 SVM 都有自己的安全性，管理和命名空间。

除了数据 SVM 之外， ONTAP 还部署了用于管理的特殊 SVM：

- 设置集群时会创建一个 *admin SVM* 。
- 当节点加入新的或现有的集群时，会创建 *node SVM* 。
- 系统会自动在 IP 空间中为集群级别的通信创建 *system SVM* 。

您不能使用这些 SVM 来提供数据。此外，集群内部和之间的流量以及集群和节点管理也有特殊的 LIF 。




*Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.*

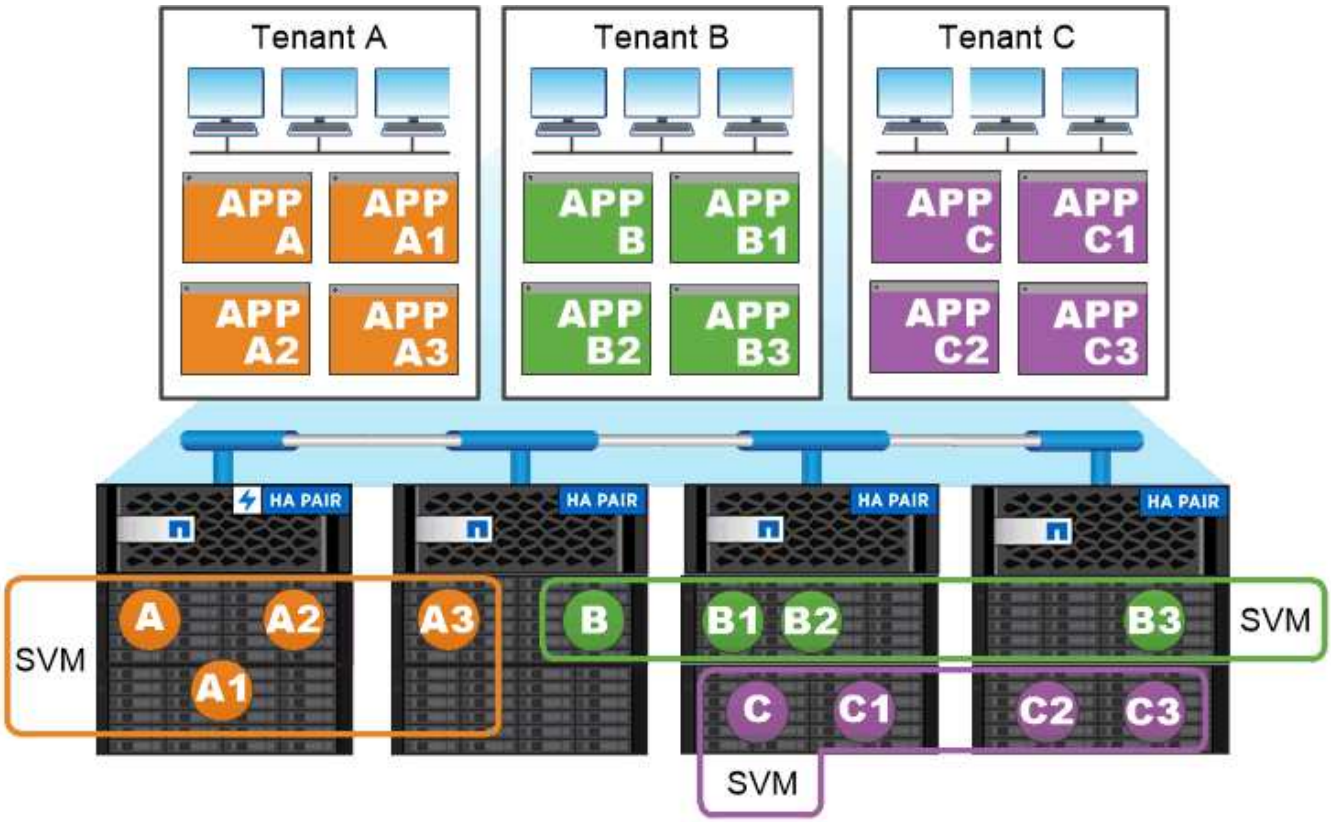
为什么**ONTAP**就像中间件

ONTAP 用于存储管理任务的逻辑对象符合精心设计的中间件包的常见目标：保护管理员免受低级实施详细信息的影响，并使配置不受节点和端口等物理特性变化的影响。基本理念是，管理员应该能够轻松移动卷和 LIF ，重新配置几个字段，而不是整个存储基础架构。

## SVM 使用情形

服务提供商在安全多租户配置中使用 SVM 隔离每个租户的数据，为每个租户提供自己的身份验证和管理，并简化成本分摊。您可以将多个 LIF 分配给同一 SVM 以满足不同的客户需求，并且可以使用 QoS 防止租户工作负载 "`抢占` " 其他租户的工作负载。

管理员在企业中使用 SVM 的目的类似。您可能希望将数据与不同部门隔离，或者将主机访问的存储卷保留在一个 SVM 中，而将用户共享卷保留在另一个 SVM 中。某些管理员将 iSCSI/FC LUN 和 NFS 数据存储库放置在一个 SVM 中，而将 SMB 共享放置在另一个 SVM 中。




*Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.*

## 集群和 **SVM** 管理

集群管理员 _ 访问集群的管理 SVM 。具有预留名称的管理SVM和集群管理员 `admin` 在设置集群时自动创建。

使用默认值的集群管理员 `admin` 角色可以管理整个集群及其资源。集群管理员可以根据需要创建具有不同角色的其他集群管理员。

SVM 管理员 _ 访问数据 SVM 。集群管理员根据需要创建数据 SVM 和 SVM 管理员。

为SVM管理员分配了 `vsadmin` 默认情况下的角色。集群管理员可以根据需要为 SVM 管理员分配不同的角色。

- 基于角色的访问控制（RBAC） _*

分配给管理员的 *role* 用于确定管理员有权访问的命令。您可以在为管理员创建帐户时分配角色。您可以根据需要分配其他角色或定义自定义角色。

## 命名空间和接合点

nas_namespaces_ 是指在 *junction points* 处联合在一起的卷的逻辑分组，用于创建单个文件系统层次结构。具有足够权限的客户端可以访问命名空间中的文件，而无需指定文件在

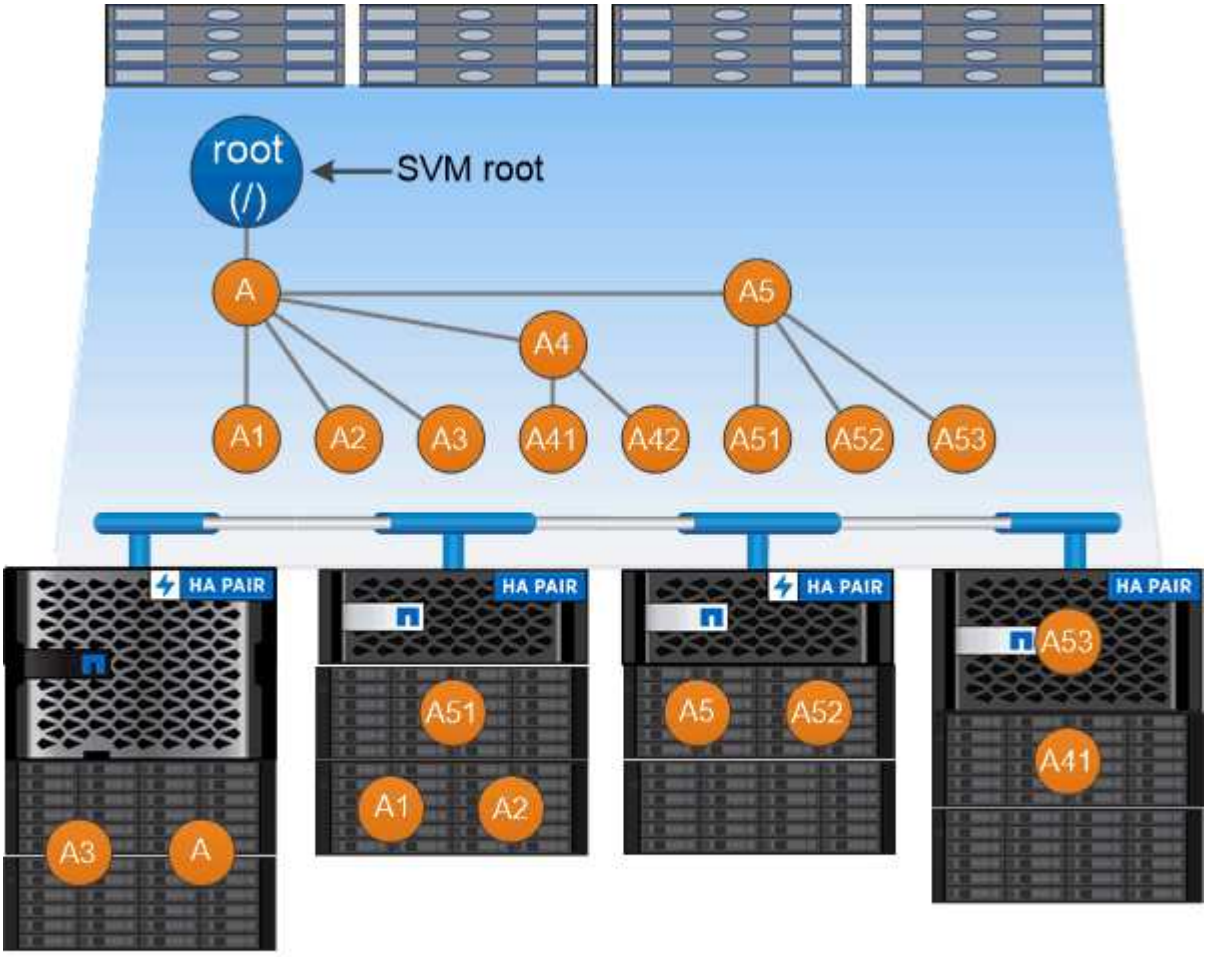
存储中的位置。集群中的任何位置都可以驻留未分配的卷。

NAS 客户端不会挂载包含相关文件的每个卷，而是挂载 nfs *export* 或访问 SMB _share 。 _ 导出或共享表示整个命名空间或命名空间中的中间位置。客户端仅访问挂载在其访问点下方的卷。

您可以根据需要向命名空间添加卷。您可以直接在父卷接合下方或卷中的目录上创建接合点。名为"`vol3`"的卷的卷接合路径可能为 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`，甚至 `/dir1/dir2/vol3`。此路径称为 _junction path…

每个 SVM 都有一个唯一的命名空间。SVM 根卷是命名空间层次结构的入口点。

> 要确保在发生节点中断或故障转移时数据仍然可用，您应为 SVM 根卷创建一个 *load-sharing mirror* 副本。




*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

示例

以下示例将在` SVM VS1上创建一个具有接合路径的名为"`home"的卷 `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

# 路径故障转移

## 路径故障转移概述

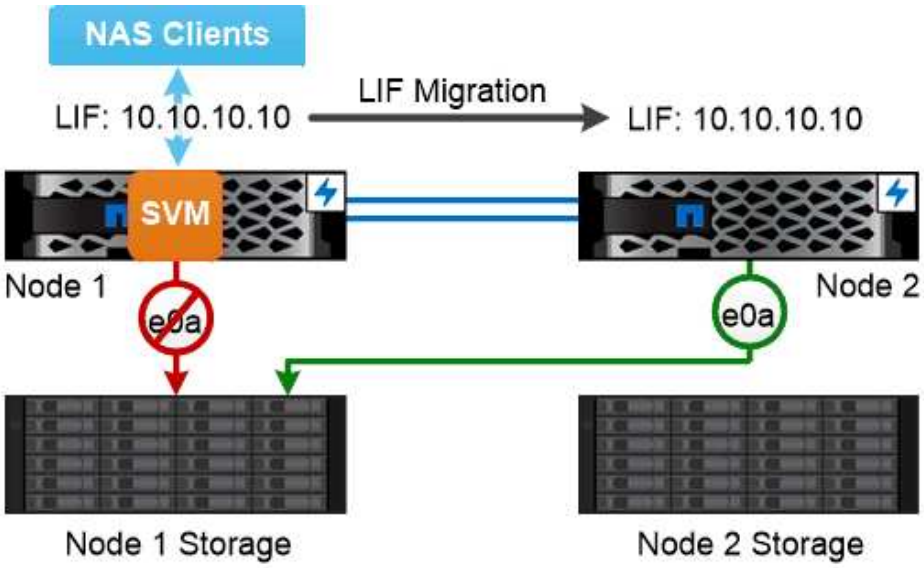
ONTAP 在 NAS 和 SAN 拓扑中管理路径故障转移的方式存在重要差异。链路出现故障后， NAS LIF 会自动迁移到其他网络端口。SAN LIF 不会迁移（除非您在发生故障后手动移动）。相反，主机上的多路径技术会将流量转移到同一 SVM 上的其他 LIF ，但会访问不同的网络端口。

### NAS 路径故障转移

在 NAS LIF 的当前端口出现链路故障后，该 LIF 会自动迁移到正常运行的网络端口。LIF 迁移到的端口必须是 LIF 的 *failover group* 的成员。故障转移组策略 _ 可将数据 LIF 的故障转移目标缩小至数据所属节点及其 HA 配对节点上的端口。

为了便于管理， ONTAP 会为网络架构中的每个 *broadcast domain* 创建一个故障转移组。广播域对属于同一第 2 层网络的端口进行分组。例如，如果您使用 VLAN 按部门（工程，营销，财务等）隔离流量，则每个 VLAN 都会定义一个单独的广播域。每次添加或删除广播域端口时，与广播域关联的故障转移组都会自动更新。

几乎始终最好使用广播域定义故障转移组，以确保故障转移组保持最新。但是，有时可能需要定义与广播域不关联的故障转移组。例如，您可能希望 LIF 仅故障转移到广播域中定义的部分端口中的端口。




*A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.*

- 子网 _*

*subnet* 会在广播域中保留一个 IP 地址块。这些地址属于同一个第 3 层网络，并在创建 LIF 时分配给广播域中的端口。与指定 IP 地址和网络掩码相比，在定义 LIF 地址时指定子网名称通常更简单，更不容易出错。

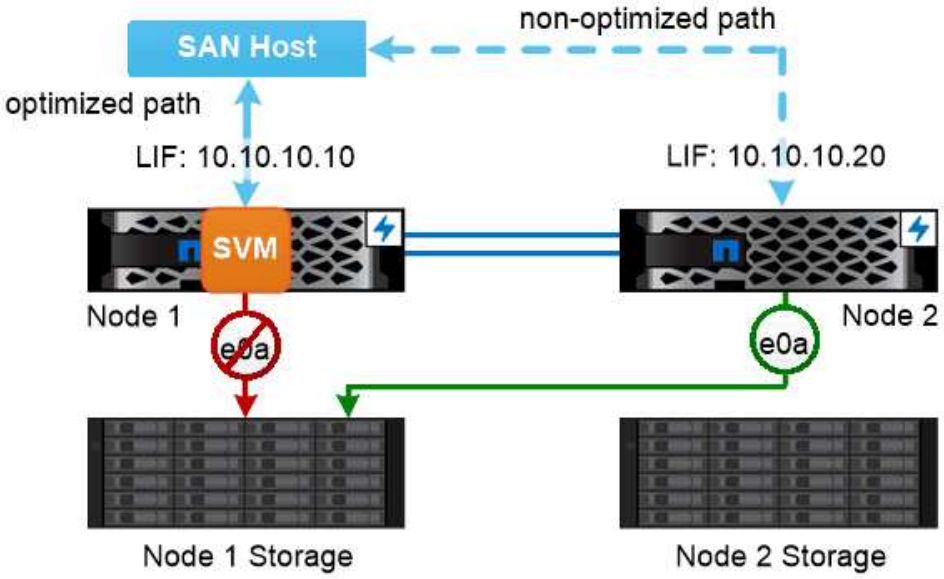
## SAN路径故障转移

在链路出现故障后， SAN 主机使用 ALUA （非对称逻辑单元访问）和 MPIO （多路径 I/O ）将流量重新路由到运行正常的 LIF 。预定义的路径可确定 SVM 所提供的 LUN 的可能路由。

在 SAN 环境中，主机被视为向 lun *targets* 发出请求的 _*initiator* 。 _ MPIO 可启用从启动程序到目标的多个路径。ALUA 标识最直接的路径，称为 _optim优化 的路径。 _

通常，您可以为 LUN 所属节点上的 LIF 配置多个优化路径，并为其 HA 配对节点上的 LIF 配置多个非优化路径。如果所属节点上的一个端口发生故障，则主机会将流量路由到运行正常的端口。如果所有端口都发生故障，主机将通过非优化路径路由流量。

默认情况下， ONTAP 选择性 LUN 映射（ SLM ）会限制从主机到 LUN 的路径数。新创建的 LUN 只能通过 LUN 所属节点或其 HA 配对节点的路径进行访问。您还可以通过在 *port set* 中为启动程序配置 LIF 来限制对 LUN 的访问。




*A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.*

在 SAN 环境中移动卷 _*

默认情况下， ONTAP 选择性 LUN 映射（ SLM ） _ 会限制从 SAN 主机到 LUN 的路径数。新创建的 LUN 只能通过 LUN 所属节点或其 HA 配对节点的路径访问，即 LUN 的 *reporting nodes* 。

这意味着，将卷移动到另一个 HA 对上的节点时，您需要将目标 HA 对的报告节点添加到 LUN 映射中。然后，您可以在 MPIO 设置中指定新路径。卷移动完成后，您可以从映射中删除源 HA 对的报告节点。

# 负载平衡

当节点上的工作量超过可用资源时，工作负载的性能开始受到延迟的影响。您可以通过增加可用资源（升级磁盘或 CPU ）或减少负载（根据需要将卷或 LUN 移动到不同节点）来管理过载节点。

您还可以使用 ONTAP _storage Quality of Service （ QoS ） _ 来保证关键工作负载的性能不会因争用工作负载而降级：

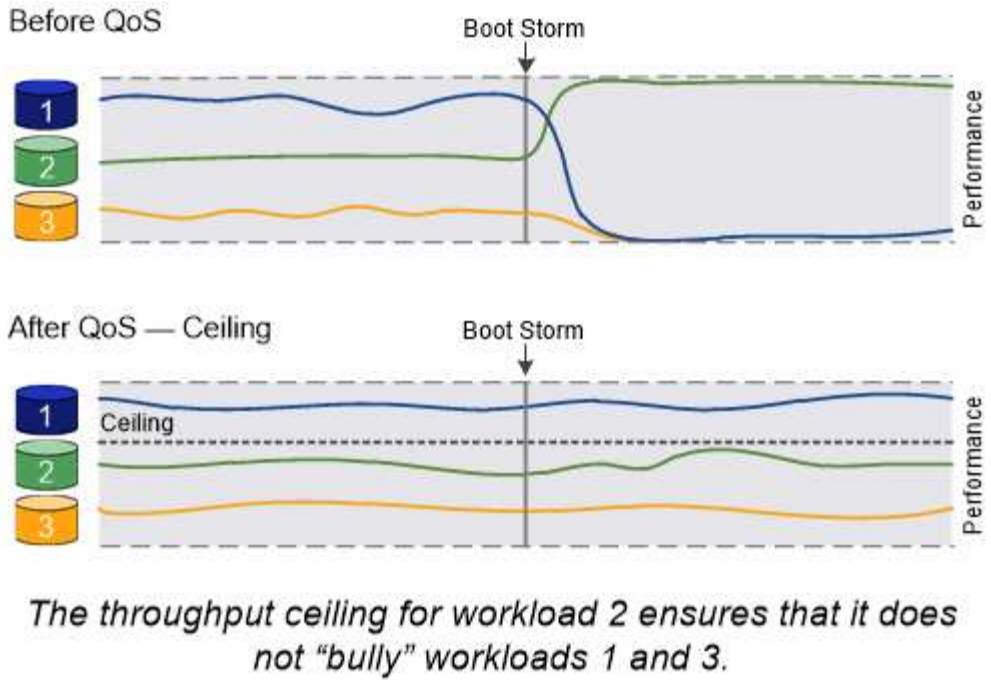
- 您可以为争用资源的工作负载设置 QoS 吞吐量上限，以限制其对系统资源的影响（ QoS 最大值）。
- 您可以为关键工作负载设置 QoS 吞吐量 *floor* ，以确保其满足最小吞吐量目标，而不管争用工作负载的需求如何（ QoS 最小值）。
- 您可以为同一工作负载设置 QoS 上限和下限。

## 吞吐量上限

吞吐量上限会将工作负载的吞吐量限制为最大 IOPS 数或 MB/ 秒在下图中，工作负载 2 的吞吐量上限可确保它不会 "`抢占` " 工作负载 1 和 3 。

策略组定义了一个或多个工作负载的吞吐量上限。工作负载表示 _storage 对象： _ 卷，文件或 LUN 或 SVM 中的所有卷，文件或 LUN 的 I/O 操作。您可以在创建策略组时指定上限，也可以等到监控工作负载之后再指定上限。

> 工作负载的吞吐量可能会超出指定上限 10% ，尤其是在工作负载的吞吐量发生快速变化时。要处理突发事件，上限可能会超过 50% 。



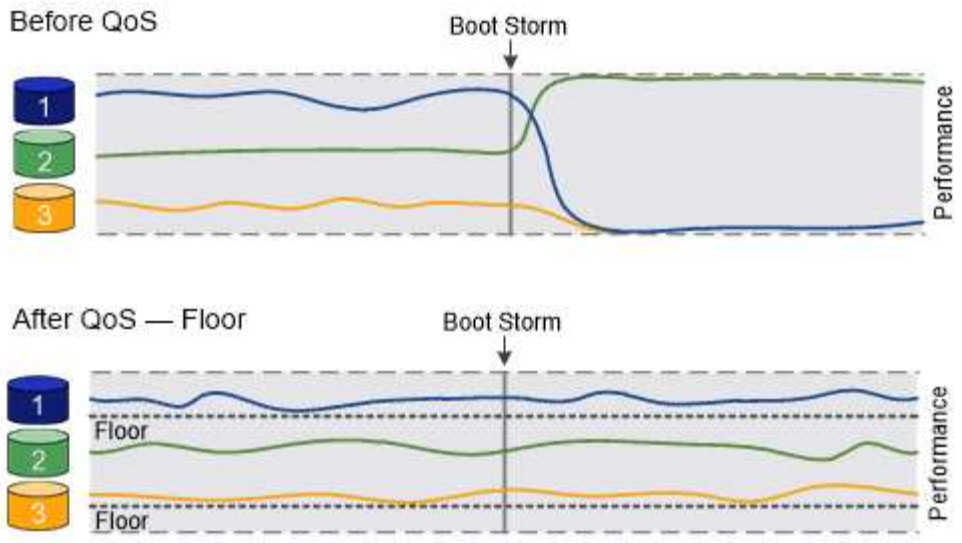

## 吞吐量下限

吞吐量下限可确保工作负载的吞吐量不会低于最小 IOPS 数。在下图中，工作负载 1 和工作负载 3 的吞吐量下限可确保满足最小吞吐量目标，而不管工作负载 2 的需求如何。

> 如示例所示，吞吐量上限会直接限制吞吐量。吞吐量下限会优先考虑设置了下限的工作负载，从而间接限制吞吐量。

工作负载表示卷， LUN 或从 ONTAP 9.3 开始的文件的 I/O 操作。定义吞吐量下限的策略组不能应用于 SVM 。您可以在创建策略组时指定下限，也可以等到监控工作负载之后再指定下限。

> 如果节点或聚合上的性能容量(余量)不足、或者在执行等关键操作期间、工作负载的吞吐量可能会低于指定的下限 `volume move trigger-cutover`。即使有足够的可用容量且未执行关键操作，工作负载的吞吐量也可能会低于指定的下限，最高可达 5% 。




*The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.*

### 自适应 QoS

通常，分配给存储对象的策略组值是固定的。当存储对象的大小发生变化时，您需要手动更改此值。例如，增加卷上的已用空间量通常需要相应地增加为卷指定的吞吐量上限。

*Adaptive QoS* 会自动将策略组值扩展到工作负载大小，并在工作负载大小发生变化时保持 IOPS 与 TBSGB 的比率。如果您要在大型部署中管理数百或数千个工作负载，则这是一项显著优势。

通常，您可以使用自适应 QoS 来调整吞吐量上限，但也可以使用它来管理吞吐量下限（当工作负载大小增加时）。工作负载大小表示为存储对象分配的空间或存储对象使用的空间。

> 在 ONTAP 9.5 及更高版本中，已用空间可用于吞吐量下限。在 ONTAP 9.4 及更早版本中，吞吐量下限不支持此功能。

+ 从ONTAP 9.13.1开始、您可以使用自适应QoS在SVM级别设置吞吐量下限和上限。

- 已分配空间策略会根据存储对象的标称大小保持 IOPS/TBGB 比率。如果此比率为 100 IOPS/GB ，则只要 150 GB 卷保持此大小，其吞吐量上限将为 15 ， 000 IOPS 。如果将卷大小调整为 300 GB ，则自适应 QoS 会将吞吐量上限调整为 30 ， 000 IOPS 。
- 已用空间策略（默认值）会根据存储效率之前存储的实际数据量保持 IOPS/TBGB 比率。如果此比率为 100 IOPS/GB ，则存储了 100 GB 数据的 150 GB 卷的吞吐量上限为 10 ， 000 IOPS 。随着已用空间量的变化，自适应 QoS 会根据比率调整吞吐量上限。

## Replication

### Snapshot 副本

传统上， ONTAP 复制技术可满足灾难恢复（ DR ）和数据归档的需求。随着云服务的出现， ONTAP 复制已进行了调整，可适应 NetApp Data Fabric 中端点之间的数据传输。所有这些用途的基础是 ONTAP Snapshot 技术。

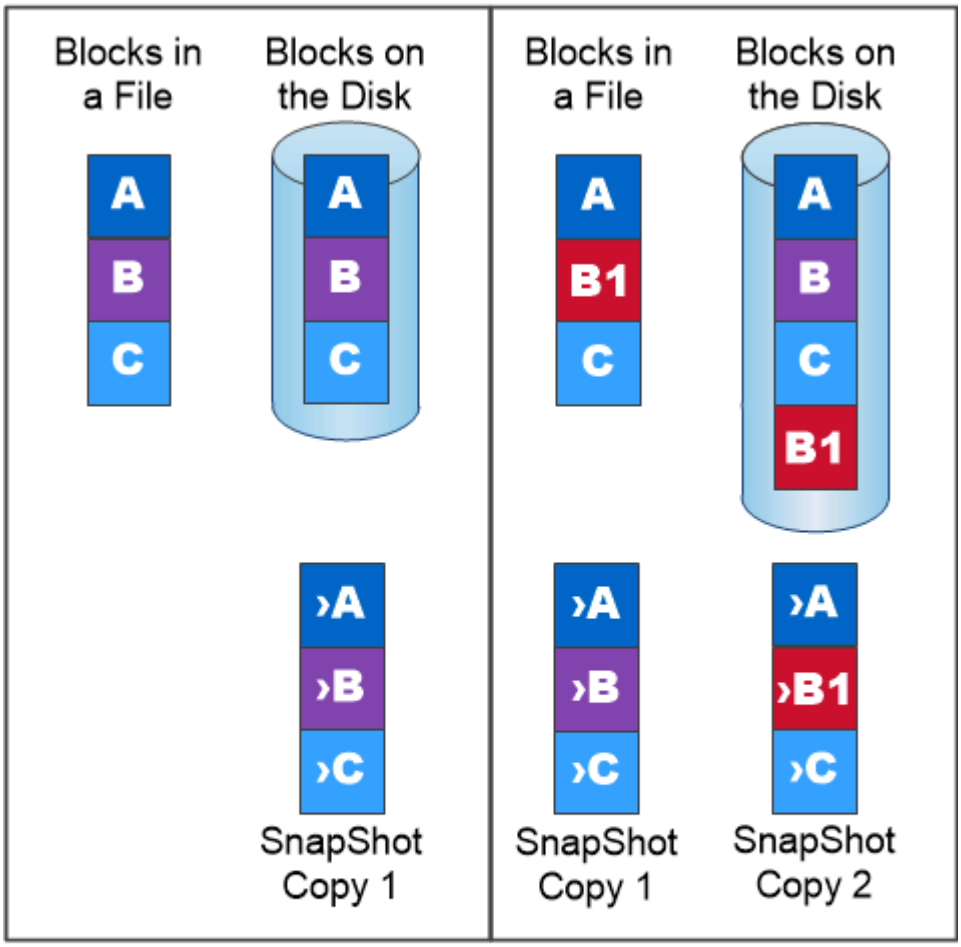
_Snapshot 副本 _ 是卷的只读时间点映像。创建Snapshot副本后、活动文件系统和Snapshot副本将指向相同的磁盘块；因此、Snapshot副本不会使用额外的磁盘空间。随着时间的推移、该映像占用的存储空间极少、并且性能开销可以忽略不计、因为它仅会记录自上次创建Snapshot副本以来对文件所做的更改。

Snapshot 副本的效率归功于 ONTAP 的核心存储虚拟化技术—任意位置写入文件布局（ WAFL ）。 _ 与数据库一样， WAFL 使用元数据指向磁盘上的实际数据块。但是，与数据库不同， WAFL 不会覆盖现有块。它会将更新后的数据写入新块并更改元数据。

Snapshot副本非常高效、因为在创建Snapshot副本时、ONTAP会引用元数据、而不是复制数据块。这样可以避免其他系统在查找要复制的块时所花费的"寻道时间"以及自行创建副本的成本。

您可以使用 Snapshot 副本恢复单个文件或 LUN ，或者还原卷的整个内容。ONTAP 会将 Snapshot 副本中的指针信息与磁盘上的数据进行比较，以重建缺少或损坏的对象，而不会造成停机或高昂的性能成本。

_Snapshot 策略 _ 用于定义系统如何创建卷的 Snapshot 副本。此策略用于指定何时创建 Snapshot 副本，要保留的副本数量，如何为其命名以及如何为其添加标签以进行复制。例如，系统可能会在每天中午 12： 10 创建一个 Snapshot 副本，保留两个最新副本，将其命名为 " `daily` " （附加时间戳），并将其标记为 " `daily` " 以进行复制。




*A Snapshot copy records only changes to the active file system since the last Snapshot copy.*

## SnapMirror 灾难恢复和数据传输

*snapmirror* 是一种灾难恢复技术，用于从主存储故障转移到地理位置偏远的站点上的二级存储。顾名思义， SnapMirror 会在二级存储中为您的工作数据创建一个副本（或 _mirror ） _ ，当主站点发生灾难时，您可以从该副本继续提供数据。

数据在卷级别进行镜像。主存储中的源卷与二级存储中的目标卷之间的关系称为 _data 保护关系。 _ 卷所在的集群以及从这些卷提供数据的 SVM 必须为 _peered 。 _ 对等关系可使集群和 SVM 进行交换 数据安全。

> 您还可以在 SVM 之间创建数据保护关系。在此类关系中，系统会复制 SVM 的全部或部分配置，从 NFS 导出和 SMB 共享到 RBAC ，以及 SVM 所拥有的卷中的数据。

从 ONTAP 9.10.1 开始，您可以使用 S3 SnapMirror 在 S3 存储分段之间创建数据保护关系。目标存储分段可以位于本地或远程 ONTAP 系统上，也可以位于非 ONTAP 系统上，例如 StorageGRID 和 AWS 。

首次调用 SnapMirror 时，它会执行从源卷到目标卷的 *baseline transfer* 。基线传输通常涉及以下步骤：

- 为源卷创建 Snapshot 副本。
- 将 Snapshot 副本及其引用的所有数据块传输到目标卷。
- 将源卷上剩余的较晚 Snapshot 副本传输到目标卷，以便在 "`active` " 镜像损坏时使用。

基线传输完成后， SnapMirror 仅将新的 Snapshot 副本传输到镜像。更新是异步的，遵循您配置的计划。保留会镜像源上的 Snapshot 策略。您可以在主站点发生灾难时激活目标卷，并尽可能减少中断，并在服务还原后重新激活源卷。

由于 SnapMirror 仅在创建基线后传输 Snapshot 副本，因此复制速度快，不会造成中断。如故障转移使用情形所示，二级系统上的控制器应与主系统上的控制器等效或接近等效，以便从镜像存储高效地提供数据。


*A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.*

- 使用 SnapMirror 进行数据传输 _*

您还可以使用 SnapMirror 在 NetApp Data Fabric 的端点之间复制数据。创建 SnapMirror 策略时，您可以选择一次性复制或重复复制。

## SnapMirror Cloud 备份到对象存储

*SnapMirror Cloud* 是一种备份和恢复技术，专为希望将数据保护工作流过渡到云的 ONTAP 用户而设计。从传统备份到磁带架构迁移的企业可以使用对象存储作为长期数据保留和归档的备用存储库。SnapMirror Cloud 在增量永久备份策略中提供了 ONTAP 到对象存储复制功能。

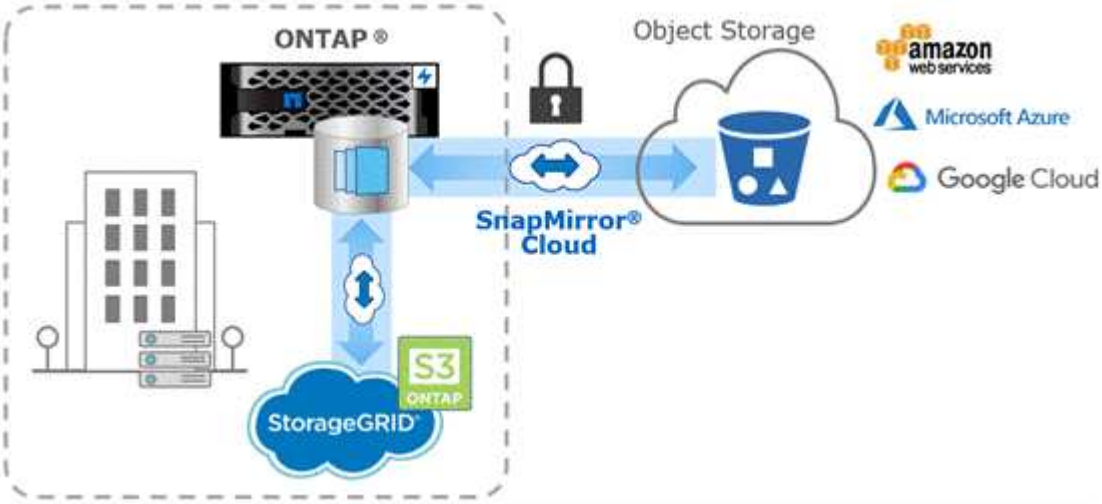
ONTAP 9.8 引入了 SnapMirror 云，作为 SnapMirror 复制技术系列的扩展。虽然 SnapMirror 经常用于 ONTAP 到 ONTAP 备份，但 SnapMirror Cloud 使用同一个复制引擎将 ONTAP 的 Snapshot 副本传输到符合 S3 的对象存储备份。

SnapMirror Cloud 针对备份使用情形，支持长期保留和归档工作流。与 SnapMirror 一样，初始 SnapMirror Cloud 备份会对卷执行基线传输。对于后续备份， SnapMirror Cloud 会生成源卷的快照副本，并将仅包含已更改数据块的快照副本传输到对象存储目标。

SnapMirror云关系可以在ONTAP系统和选定内部和公共云对象存储目标(包括Amazon S3、Google Cloud Storage和Microsoft Azure Blot Storage)之间配置。其他内部对象存储目标包括StorageGRID和ONTAP S3。

SnapMirror 云复制是一项获得许可的 ONTAP 功能，需要经过批准的应用程序来编排数据保护工作流。可通过多种业务流程选项管理 SnapMirror Cloud 备份：

- 支持 SnapMirror 云复制的多个第三方备份合作伙伴。可从获取参与的供应商 "NetApp 博客"。
- 适用于ONTAP环境的NetApp原生解决方案的BlueXP备份和恢复
- 用于为数据保护工作流开发自定义软件或利用自动化工具的 API




## SnapVault 归档

SnapMirror 许可证用于支持用于备份的 SnapVault 关系和用于灾难恢复的 SnapMirror 关

系。从ONTAP 9.3开始、SnapVault许可证已弃用、SnapMirror许可证可用于配置存储、镜像以及镜像和存储关系。SnapMirror 复制用于从 ONTAP 到 ONTAP 复制 Snapshot 副本，支持备份和灾难恢复使用情形。

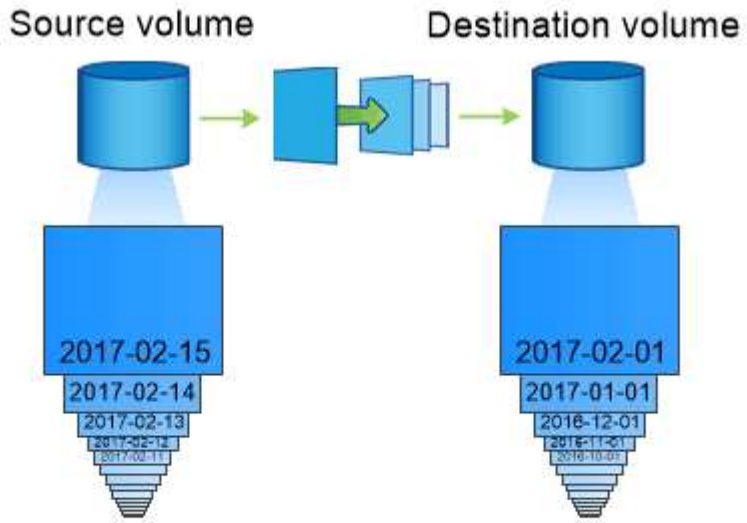
*Snapshot* 是一种归档技术，专为磁盘到磁盘 SnapVault 副本复制而设计，可满足标准要求并用于其他监管相关目的。与目标通常仅包含源卷中当前 Snapshot 副本的 SnapMirror 关系不同， SnapVault 目标通常会保留较长时间内创建的时间点 Snapshot 副本。

您可能希望在 20 年的时间内保留数据的每月 Snapshot 副本，例如，为了符合政府对您企业的会计规定。由于无需从存储提供数据，因此您可以在目标系统上使用速度较慢，成本较低的磁盘。

与 SnapMirror 一样， SnapVault 会在您首次调用时执行基线传输。它会为源卷创建 Snapshot 副本，然后将该副本及其引用的数据块传输到目标卷。与 SnapMirror 不同， SnapVault 不会在基线中包含较早的 Snapshot 副本。

更新是异步的，遵循您配置的计划。您在关系的策略中定义的规则可确定更新中要包含哪些新 Snapshot 副本以及要保留多少副本。在策略中定义的标签（ m例如 " 每月， "）必须与源上 Snapshot 策略中定义的一个或多个标签匹配。否则，复制将失败。

SnapMirror 和 SnapVault 共享相同的命令基础架构。您可以指定在创建策略时要使用的方法。这两种方法都需要对等集群和对等 SVM 。




*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

## 云备份以及对传统备份的支持

除了SnapMirror和SnapVault数据保护关系(仅适用于ONTAP 9.7及更早版本的磁盘到磁盘关系)之外、现在还有多种备份解决方案可为长期数据保留提供成本更低的替代方案。

许多第三方数据保护应用程序为 ONTAP 管理的数据提供传统备份。Veeam ， Veritas 和 Commvault 等均可为 ONTAP 系统提供集成备份。

从 ONTAP 9.8 开始， SnapMirror Cloud 可将 Snapshot 副本从 ONTAP 实例异步复制到对象存储端

点。SnapMirror 云复制要求使用许可的应用程序来协调和管理数据保护工作流。ONTAP 系统支持通过 SnapMirror 云关系来选择内部部署和公有云对象存储目标，包括 AWS S3 ， Google 云存储平台或 Microsoft Azure Blob 存储，从而通过供应商备份软件提高效率。有关受支持的认证应用程序和对象存储供应商列表，请联系您的 NetApp 代表。

如果您对云原生数据保护感兴趣、可以使用BlueXP在内部卷和公有 云中的Cloud Volumes ONTAP 实例之间配置SnapMirror或SnapVault 关系。

此外、BlueXP还可以使用软件即服务(SaaS)模式备份Cloud Volumes ONTAP 实例。用户可以使用 NetApp Cloud Central 上的 Cloud Backup 将其 Cloud Volumes ONTAP 实例备份到 S3 和 S3 兼容的公有云对象存储。

"Cloud Volumes ONTAP 和BlueXP文档资源"

"NetApp Cloud Central"

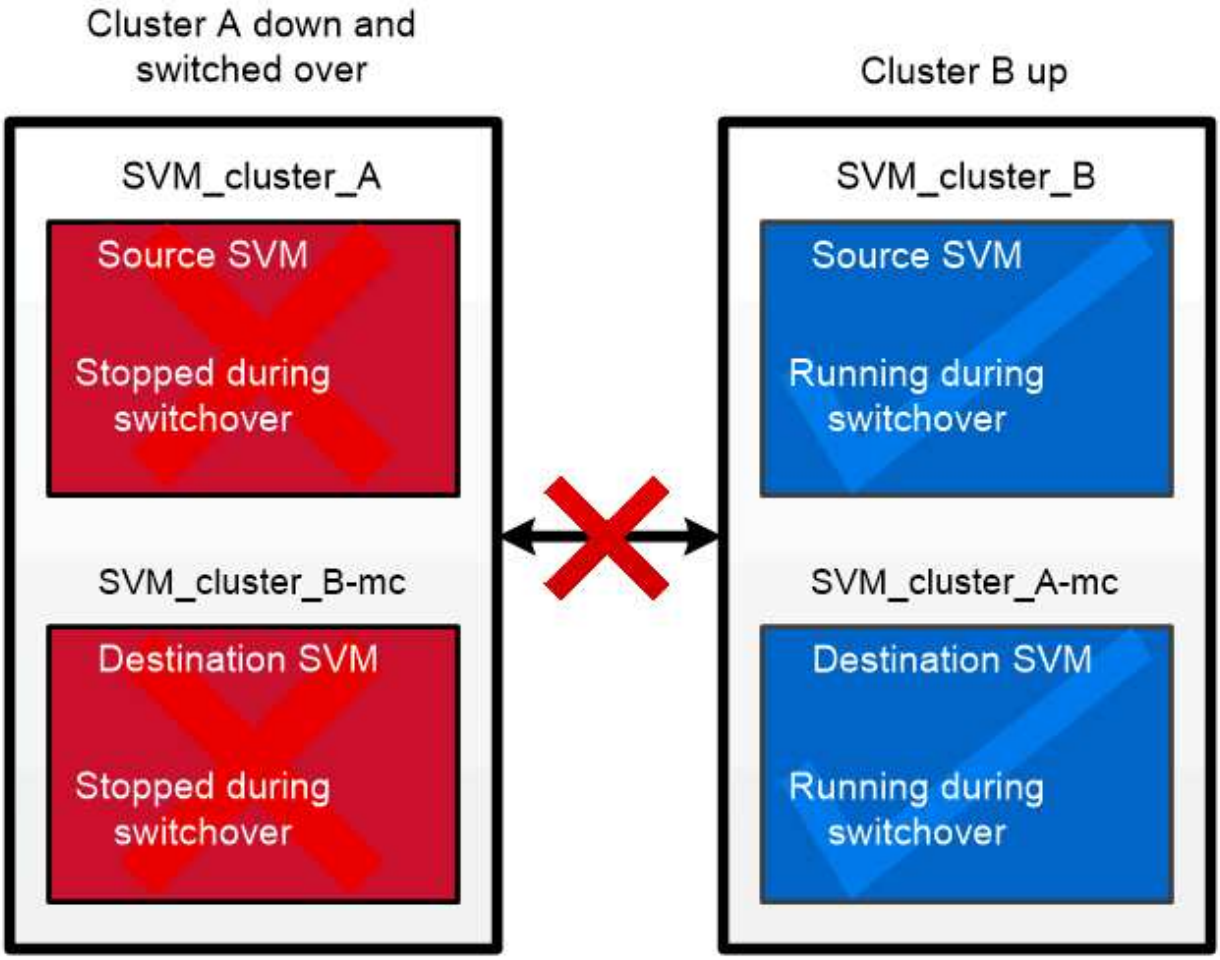
## MetroCluster 持续可用性

MetroCluster 配置通过实施两个物理上独立的镜像集群来保护数据。每个集群会同步复制另一个集群的数据和 SVM 配置。如果某个站点发生灾难，管理员可以激活镜像的 SVM 并开始从正常运行的站点提供数据。

- 光纤连接的 MetroCluster 配置支持城域范围的集群。
- 延伸型 MetroCluster 配置支持校园范围的集群。

无论哪种情况，集群都必须建立对等关系。

MetroCluster 使用名为 *plex* 的 ONTAP 功能 SyncMirror 在副本或另一集群存储中同步镜像每个集群的聚合数据。如果发生切换，则正常运行的集群上的远程丛会联机，并且二级 SVM 会开始提供数据。




*When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.*

**_在非MetroCluster实施中使用SyncMirror _**
您可以选择在非MetroCluster实施中使用SyncMirror、以便在出现故障的磁盘数量超过RAID类型所能保护的数量时或与RAID组磁盘的连接断开时防止数据丢失。此功能仅适用于 HA 对。

聚合数据镜像到存储在不同磁盘架上的丛中。如果其中一个磁盘架不可用，则在修复故障发生原因期间，不受影响的丛将继续提供数据。

请注意，使用 SyncMirror 镜像的聚合所需的存储容量是未镜像聚合的两倍。每个丛所需的磁盘数与其镜像的丛所需的磁盘数相同。例如，要镜像 1 ， 440 GB 的聚合，需要 2 ， 880 GB 的磁盘空间，每个丛需要 1 ， 440 GB 。

借助SyncMirror、建议您为镜像聚合至少保留20%的可用空间、以获得最佳存储性能和可用性。虽然建议对非镜像聚合使用10%的空间、但文件系统可以使用额外的10%空间来吸收增量更改。由于ONTAP采用基于Snapshot的写时复制架构、增量更改可提高镜像聚合的空间利用率。不遵守这些最佳实践可能会对SyncMirror重新同步性能产生负面影响、进而间接影响非共享云部署的NDU和MetroCluster部署的切回等运营工作流。

> SyncMirror 也可用于 FlexArray 虚拟化实施。

# 存储效率

## ONTAP存储效率概述

存储效率衡量存储系统如何通过优化存储资源、最大限度地减少空间浪费以及减少写入数据的物理占用空间来有效利用可用空间。通过提高存储效率、您可以以尽可能低的成本在尽可能小的空间中存储最大数量的数据。例如、利用可检测和消除重复数据块和填充为零的数据块的高效存储技术、可以减少所需的总物理存储量并降低总成本。

ONTAP提供了广泛的存储效率技术、可减少数据占用的物理硬件或云存储量、并显著提高系统性能、包括加快数据读取速度、加快数据集副本速度以及加快VM配置速度。

**ONTAP**存储效率技术包括：

- * 精简配置 *

  精简配置 用于根据需要在卷或LUN中分配存储、而不是预先预留存储。 这样、您可以根据潜在使用情况过度分配卷或LUN、而无需预留当前未使用的空间、从而减少所需的物理存储量。

- * 重复数据删除 *

  重复数据删除 可通过三种不同的方式减少卷所需的物理存储量。

  - 零块重复数据删除

    零块重复数据删除可检测并消除全零数据块、并且仅更新元数据。然后、零块通常使用的空间将节省100%。 默认情况下、所有经过重复数据删除的卷都会启用零块重复数据删除。

  - 实时重复数据删除

    实时重复数据删除会检测重复的数据块、并在将数据写入磁盘之前将其替换为对唯一共享块的引用。实

时重复数据删除可将VM配置速度加快20%到30%。 实时重复数据删除可在卷或聚合级别使用、具体取决于您的ONTAP版本和平台。 默认情况下、AFF和ASA系统会启用此功能。您需要在FAS系统上手动启用实时重复数据删除。

  - 后台重复数据删除

    后台重复数据删除还会检测重复的数据块、并将其替换为对唯一共享块的引用、但在将数据写入磁盘后会进一步提高存储效率。 您可以将后台重复数据删除设置为在存储系统满足特定条件时运行。例如、您可以在卷利用率达到10%时启用后台重复数据删除。 您也可以手动触发后台重复数据删除、或者将其设置为按特定计划运行。默认情况下、AFF和ASA系统会启用此功能。您需要在FAS系统上手动启用后台重复数据删除。

  重复数据删除在卷内部以及聚合内的卷之间均受支持。 读取经过重复数据删除的数据通常不会对性能产生任何影响。

- * 数据压缩 *

  压缩 通过将数据块合并到数据压缩组中(每个数据块存储为一个块)、减少卷所需的物理存储量。收到读取或覆盖请求时、只会读取一小组块、而不会读取整个文件。此过程可优化读取和覆盖性能、并提高所压缩文件大小的可扩展性。

  数据压缩可以实时运行、也可以后处理运行。 实时数据压缩可在将数据写入磁盘之前压缩内存中的数据、从而立即节省空间。后处理压缩首先将块以未压缩格式写入磁盘、然后按计划压缩数据。您需要手动启用数据压缩。

- 压缩

  数据缩减可通过采集存储在4 KB块中但大小小于4 KB的数据块并将其合并为一个块来减少卷所需的物理存储量。数据缩减是在数据仍位于内存中时进行的、因此磁盘上不会占用不必要的空间。 默认情况下、AFF和ASA系统会启用此功能。您需要手动在FAS系统上启用数据缩减。

- **FlexClone**卷、文件和**LUN**

  FlexClone技术 利用Snapshot元数据为卷、文件或LUN创建可写时间点副本。副本与其父副本共享数据块、在将更改写入副本或其父副本之前、除了元数据所需的存储外、不会占用任何存储。 写入更改时、仅存储增量。

  传统的数据集副本可能需要几分钟甚至几小时才能创建、而FlexClone技术甚至可以让您近乎瞬时地复制最大的数据集。

- 对温度敏感的存储效率

  ONTAP提供 "对温度敏感的存储效率" 通过评估卷数据的访问频率并将该频率映射到应用于该数据的压缩程度、可以获得优势。对于不常访问的冷数据、将压缩较大的数据块；对于频繁访问且覆盖频率更高的热数据、将压缩较小的数据块、从而提高流程效率。

  ONTAP 9.8中引入了温度敏感型存储效率(TSSE)、此功能会在新创建的精简配置AFF卷上自动启用。

您可以轻松地在日常运营中实现这些技术的优势。 例如、假设您需要为5、000个用户提供主目录存储、并且您估计任何用户所需的最大空间为1 GB。您可以提前预留一个5 TB的聚合、以满足总的潜在存储需求。 但是、您也知道、您的组织中的主目录容量要求差别很大。 您可以创建2 TB聚合、而不是为组织预留5 TB的总空间。 然后、您可以使用精简配置为每个用户分配1 GB的存储、但仅在需要时分配存储。 您可以随时主动监控聚合、并根据需要增加实际物理大小。

在另一个示例中、假设您使用的虚拟桌面基础架构(Virtual Desktop Infrastructure、VDI)在虚拟桌面之间存在大量重复数据。重复数据删除可自动删除VDI中重复的信息块、并将其替换为指向原始块的指针、从而降低存储使用量。数据压缩等其他ONTAP存储效率技术也可以在后台运行、而无需您干预。

ONTAP磁盘分区技术还可以提高存储效率。 RAID DP技术可防止出现双磁盘故障、而不会影响性能或增加磁盘镜像开销。ONTAP 9的高级SSD分区功能可将可用容量提高近20%。

NetApp提供与云中的内部ONTAP相同的存储效率功能。将数据从内部ONTAP迁移到云时、现有的存储效率将得以保留。例如、假设您有一个SQL数据库、其中包含要从内部系统迁移到云的业务关键型数据。 您可以在BlueXP中使用数据复制来迁移数据、并且在迁移过程中、您可以为云中的Snapshot副本启用最新的内部策略。

## 精简配置

除了 Snapshot 副本之外， ONTAP 还提供了一系列存储效率技术。关键技术包括精简配置，重复数据删除，数据压缩以及 FlexClone 卷，文件， 和 LUN 。与 Snapshot 副本一样，所有副本都基于 ONTAP 的任意位置写入文件布局（ Write Anywhere File Layout ， WAFL ）构建。

精简配置卷或 LUN 不会预先预留存储。而是根据需要动态分配存储。删除卷或 LUN 中的数据后，可用空间将释放回存储系统

假设您的组织需要为 5 ， 000 个用户提供主目录存储。您估计最大的主目录将占用 1 GB 的空间。

在这种情况下，您可以购买 5 TB 的物理存储。对于存储主目录的每个卷，您需要预留足够的空间来满足最大使用者的需求。

但实际上，您还知道，社区中的主目录容量要求差别很大。对于每个大型存储用户来说，十个用户占用的空间很少或没有空间。

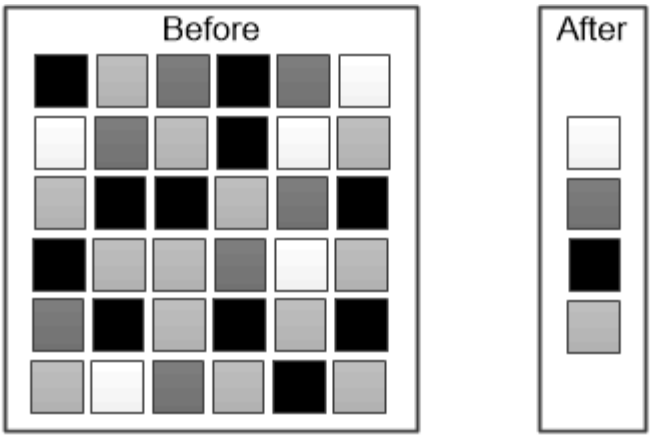
通过精简配置，您可以满足大型存储使用者的需求，而无需购买可能从未使用的存储。由于存储空间在耗尽之前不会分配，因此您可以 "`过量使用` " 一个 2 TB 的聚合，方法是名义上为该聚合包含的 5 ， 000 个卷中的每个卷分配 1 GB 的大小。

只要您正确地确定轻用户与重用户的比例为 10： 1 ，并且只要您在监控聚合上的可用空间方面发挥积极作用，您就可以确信卷写入不会因空间不足而失败。

## 重复数据删除

_ded重复 数据删除 _ 通过丢弃重复块并将其替换为对单个共享块的引用，减少卷（或 AFF 聚合中的所有卷）所需的物理存储量。读取经过重复数据删除的数据通常不会对性能产生任何影响。除了过载的节点之外，写入所产生的费用可以忽略不计。

由于数据是在正常使用期间写入的，因此 WAFL 会使用批处理过程创建 _block signatures 目录。 _ 开始重复数据删除后， ONTAP 会比较目录中的签名以识别重复块。如果存在匹配项，则会逐个字节进行比较，以验证候选块自创建目录以来是否未发生更改。只有当所有字节匹配时，才会丢弃重复块并回收其磁盘空间。




*Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.*

压缩

*compression* 通过将数据块组合到 _compression groups_中 来减少卷所需的物理存储量，每个数据块都存储为一个块。与传统压缩方法相比，压缩数据的读取速度更快，因为 ONTAP 仅解压缩包含所请求数据的压缩组，而不是解压缩整个文件或 LUN 。

您可以单独或组合执行实时或后处理压缩：

- *Inline compression* 在将数据写入磁盘之前压缩内存中的数据，从而显著减少卷的写入 I/O 量，但可能会降低写入性能。性能密集型操作将延迟到下一个后处理压缩操作（如果有）为止。
- *postprocess compression* 按照与重复数据删除相同的计划，在数据写入磁盘后对其进行压缩。

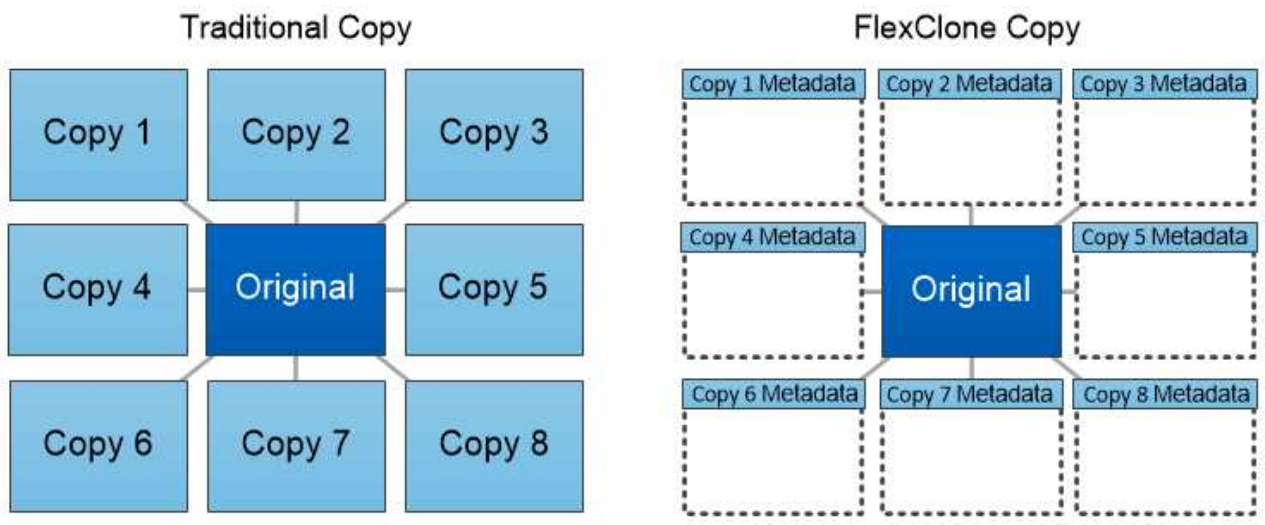
**_Inline data** 能力缩减 **_** 小文件或填充零的 I/O 存储在 4 KB 块中，无论它们是否需要 4 KB 的物理存储。_Inline 数据缩减 _ 将通常占用多个 4 KB 块的数据块组合到磁盘上的一个 4 KB 块中。数据缩减是在数据仍位于内存中时进行的，因此最适合速度更快的控制器。

## FlexClone 卷，文件和 LUN

_FlexClone _ 技术引用 Snapshot 元数据来创建卷的可写时间点副本。副本与其父级共享数据块，在将更改写入副本之前，除了元数据所需的存储外，不会占用任何其他存储。FlexClone 文件和 FlexClone LUN 使用相同的技术，只是不需要备份 Snapshot 副本。

传统副本可能需要几分钟甚至几小时才能创建，而 FlexClone 软件可以让您几乎即时复制最大的数据集。因此，如果您需要相同数据集的多个副本（例如，虚拟桌面部署）或数据集的临时副本（针对生产数据集测试应用程序），则这种情况是理想之选。

您可以克隆现有 FlexClone 卷，克隆包含 LUN 克隆的卷或克隆镜像和存储数据。您可以将 FlexClone 卷从其父卷拆分，在这种情况下，会为该副本分配自己的存储。




*FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.*

## System Manager 中的容量测量

系统容量可以用物理空间或逻辑空间来衡量。从ONTAP 9.7开始、System Manager可提供物理容量和逻辑容量的测量结果。

以下说明介绍了这两个测量值之间的差异：

- 物理容量：物理空间是指卷或本地层中使用的物理存储块。由于存储效率功能（例如重复数据删除和数据压缩）中的数据减少，物理已用容量值通常小于逻辑已用容量值。
- 逻辑容量：逻辑空间是指卷或本地层中的可用空间(逻辑块)。逻辑空间是指在不考虑重复数据删除或数据压缩结果的情况下如何使用理论空间。 已用逻辑空间值是从已用物理空间量加上已配置的存储效率功能（例如重复数据删除和数据压缩）节省的空间得出的。 此度量值通常会大于已用物理容量，因为它包括 Snapshot 副本，克隆和其他组件，并且不会反映数据压缩以及物理空间的其他缩减。因此，总逻辑容量可能会高于配置的空间。

> 在 System Manager 中，容量表示不考虑根存储层（聚合）容量。

已用容量的测量值

已用容量的测量值会根据您使用的 System Manager 版本而有所不同，如下表所述：

| System Manager 版本 | 容量术语 | 引用的容量类型 |
| --- | --- | --- |
| 9.9.1 及更高版本 | 已用逻辑容量 | 已用逻辑空间<br>如果已启用存储效率设置) |
| 9.7 和 9.8 | 已用 | 已用逻辑空间<br>(如果已启用存储效率设置) |

| | | |
|---|---|---|
| 9.5和9.6<br>(经典视图) | 已用 | 已用物理空间 |

容量测量术语

在描述容量时，使用以下术语：

- 已分配容量：已为Storage VM中的卷分配的空间量。
- 可用：可用于在Storage VM或本地层中存储数据或配置卷的物理空间量。
- 卷间容量：Storage VM上所有卷的已用存储与可用存储之和。
- 客户端数据：客户端数据(物理或逻辑)使用的空间量。
  - 从ONTAP 9.13.1开始、客户端数据使用的容量称为*逻辑使用容量*、Snapshot副本使用的容量将单独显示。
  - 在ONTAP 9.12.1及更早版本中、添加到Snapshot副本所用容量中的客户端数据所使用的容量称为*逻辑使用容量*。
- 已提交：本地层的已提交容量。
- 数据精简：
  - 从ONTAP 9.13.1开始、数据精简率显示如下：
    - "容量"面板上显示的数据精简值是指逻辑已用空间与物理已用空间之比、而不考虑使用Snapshot副本等存储效率功能时所实现的显著缩减。
    - 显示详细信息面板时、您将看到概览面板上显示的比率以及所有逻辑已用空间与物理已用空间之比的总体比率。 此值称为*使用Snapshot副本*、包括使用Snapshot副本和其他存储效率功能所带来的优势。
  - 在ONTAP 9.12.1及更早版本中、数据精简率显示如下：
    - "容量"面板上显示的数据精简值是所有逻辑已用空间与物理已用空间之比、其中包括使用Snapshot副本和其他存储效率功能所带来的优势。
    - 显示详细信息面板时，您将看到“概览”面板上显示的*总体*比率，以及仅由客户端数据使用的逻辑已用空间与仅由客户端数据使用的物理已用空间之比(称为*不使用Snapshot副本和克隆*)。
- 逻辑使用量：
  - 从ONTAP 9.13.1开始、客户端数据使用的容量称为*逻辑使用容量*、Snapshot副本使用的容量将单独显示。
  - 在ONTAP 9.12.1及更早版本中、添加到Snapshot副本已用容量中的客户端数据所使用的容量称为*逻辑使用容量*。
- 逻辑已用**%**：当前已用逻辑容量与配置大小之比的百分比、不包括Snapshot预留。 此值可以大于 100% ，因为它包括卷中的效率节省。
- 最大容量：为Storage VM上的卷分配的最大空间量。
- 物理已用：卷或本地层的物理块中已用的容量。
- 物理已用**%**：卷的物理块中已用容量与配置大小之比。
- 已配置容量：已从Cloud Volumes ONTAP系统分配并已准备好存储用户或应用程序数据的文件系统(卷)。
- 预留：为本地层中已配置卷预留的空间量。

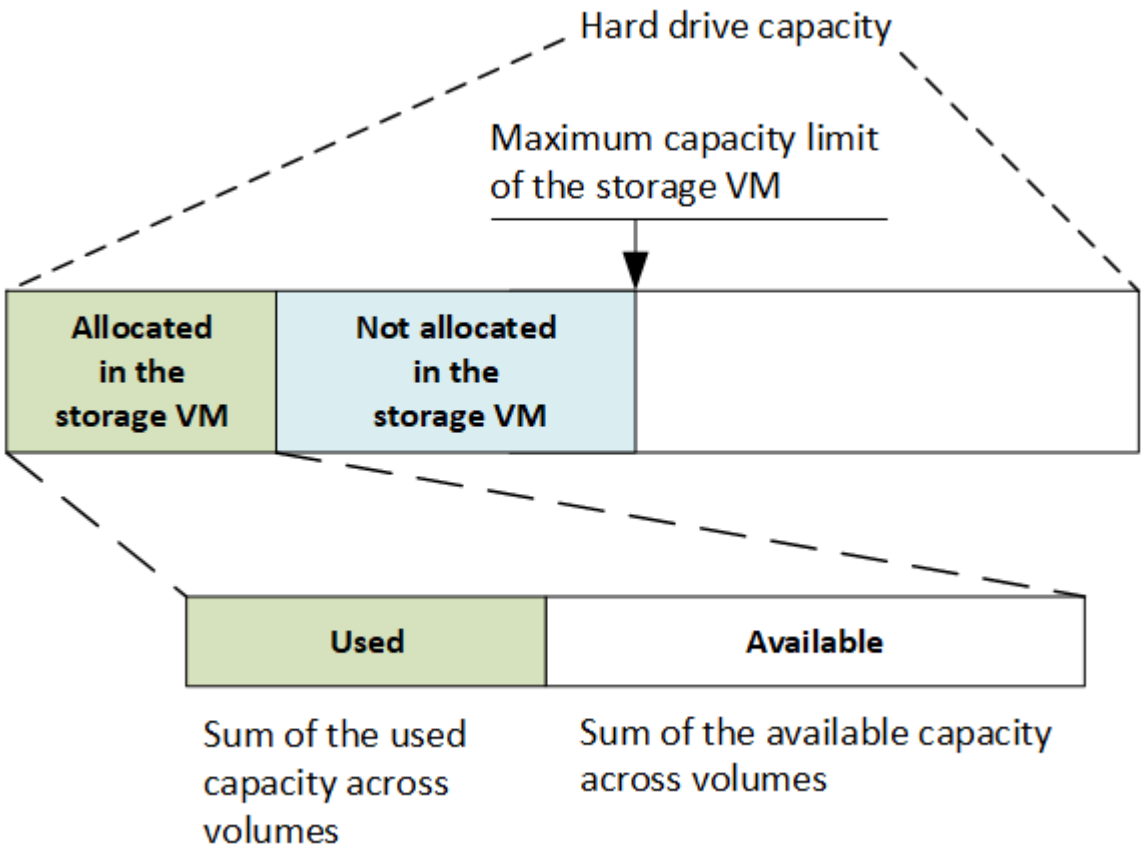
- 已用：包含数据的空间量。
- 已用和预留：已用物理空间与预留空间之和。

**Storage VM的容量**

Storage VM的最大容量由为卷分配的总空间加上剩余的未分配空间决定。

- 为卷分配的空间等于已用容量与FlexVol 卷、FlexGroup 卷和FlexCache 卷的可用容量之和。
- 即使卷在删除后受到限制、脱机或位于恢复队列中、卷的容量也会计入总和。
- 如果为卷配置了自动增长、则会在总和中使用卷的最大自动大小值。 如果不使用自动增长、则会使用卷的实际容量作为总和。

下图说明了卷间容量的衡量指标与最大容量限制之间的关系。




从ONTAP 9.13.1开始、集群管理员可以执行此操作 "为Storage VM启用最大容量限制"。但是、对于包含用于数据保护的卷的Storage VM、在SnapMirror关系或MetroCluster 配置中、不能设置存储限制。此外、不能将配额配置为超过Storage VM的最大容量。

设置最大容量限制后、不能将其更改为小于当前分配的容量的大小。

当Storage VM达到其最大容量限制时、无法执行某些操作。System Manager可为中的后续步骤提供建议 "洞察力 "。

容量测量单位

System Manager 会根据 1024 （ $2^{10}$ ）字节的二进制单元计算存储容量。

- 从ONTAP 9.10.1开始、存储容量单位在System Manager中显示为KiB、MiB、GiB、TiB和PIB。
- 在ONTAP 9.10.0及更早版本中、这些单位在System Manager中显示为KB、MB、GB、TB和PB。

> 对于所有版本的 ONTAP ， System Manager 中用于吞吐量的单位仍为 KB/ 秒， MB/ 秒， Gb/ 秒， TB/ 秒和 PB / 秒。

| 对于 ONTAP 9.10.0 及更早版本，System Manager 中会显示容量单位 | 对于ONTAP 9.10.1 及更高版本、System Manager中显示的容量单位 | 计算 | 以字节为单位的值 |
|---|---|---|---|
| 知识库 | KiB | 1024 | 1024 字节 |
| MB | MIB | 1024 * 1024 | 1 ， 048 ， 576 字节 |
| GB | GIB | 1024 * 1024 * 1024 | 1 ， 073 ， 741 ， 824 字节 |
| TB | TIB | 1024 * 1024 * 1024 * 1024 | 1 ， 099 ， 511 ， 627 ， 776 字节 |
| PB | PIB | 1024 * 1024 * 1024 * 1024 * 1024 | 1、125、899、905、843、024 字节 |

相关信息

"在 System Manager 中监控容量"

"卷的逻辑空间报告和强制实施"

## 温度敏感型存储效率概述

ONTAP 通过评估卷数据的访问频率并将该频率映射到应用于该数据的压缩程度、可提供对温度敏感的存储效率优势。对于不常访问的冷数据、将压缩较大的数据块；对于频繁访问且覆盖频率更高的热数据、将压缩较小的数据块、从而提高流程效率。

ONTAP 9.8中引入了温度敏感型存储效率(TSSE)、此功能会在新创建的精简配置AFF卷上自动启用。您可以在现有AFF卷和精简配置的非Af DP卷上启用对温度敏感的存储效率。

### 引入"默认"和"高效"模式

从ONTAP 9.10.1开始、仅为AFF 系统引入了两种卷级存储效率模式、即_default_和_高效_。这两种模式提供了两种选择：文件压缩(默认)(创建新AFF卷时的默认模式)或温度敏感型存储效率(高效)(启用温度敏感型存储效率)。与ONTAP 9.10.1配合使用、 "必须明确设置对温度敏感的存储效率" 启用自动自适应数据压缩。但是、默认情况下、AFF 平台会在默认和高效模式下启用数据缩减、自动重复数据删除计划、实时重复数据删除、跨卷实时重复数据删除和跨卷后台重复数据删除等其他存储效率功能。

启用了FabricPoool的聚合以及所有分层策略类型均支持这两种存储效率模式(默认和高效)。

在**C**系列平台上启用对温度敏感的存储效率

默认情况下、在AFF C系列平台上、以及使用卷移动或SnapMirror将卷从非TSSE平台迁移到启用了TSSE的C系列平台时、如果目标上安装了以下版本、则会启用对温度敏感的存储效率：

- ONTAP 9.12.1P4及更高版本
- ONTAP 9.13.1及更高版本

有关详细信息，请参见 "卷移动和SnapMirror操作的存储效率行为"。

对于现有卷、不会自动启用对温度敏感的存储效率、但您可以这样做 "修改存储效率模式" 手动更改为高效模式。

> 将存储效率模式更改为高效后、您将无法再更改回该模式。

通过连续打包连续物理数据块提高存储效率

从ONTAP 9.13.1开始、对温度敏感的存储效率功能可添加连续物理块的顺序打包功能、从而进一步提高存储效率。将系统升级到ONTAP 9.13.1后、启用了对温度敏感的存储效率的卷会自动启用顺序打包。启用顺序打包后、您必须执行此操作 "手动重新打包现有数据"。

升级注意事项

升级到ONTAP 9.10.1及更高版本时、系统会根据现有卷上当前启用的压缩类型为这些卷分配存储效率模式。在升级期间，启用了数据压缩的卷将分配默认模式，启用了温度敏感型存储效率的卷将分配高效模式。如果未启用数据压缩，存储效率模式将保持空白。

# 安全性

## 客户端身份验证和授权

### ONTAP 使用标准方法来保护客户端和管理员对存储的访问，并防止病毒的侵害。高级技术可用于对空闲数据进行加密以及对 WORM 存储进行加密。

ONTAP 通过向可信源验证客户端计算机和用户的身份来对其进行身份验证。ONTAP 通过将用户凭据与文件或目录上配置的权限进行比较来授权用户访问文件或目录。

身份验证

您可以创建本地或远程用户帐户：

- 本地帐户是指帐户信息驻留在存储系统上的帐户。
- 远程帐户是指帐户信息存储在 Active Directory 域控制器， LDAP 服务器或 NIS 服务器上的帐户。

ONTAP 使用本地或外部名称服务查找主机名，用户，组，网络组和名称映射信息。ONTAP 支持以下名称服务：

- 本地用户

- DNS
- 外部 NIS 域
- 外部LDAP域

名称服务切换表 _ 用于指定搜索网络信息的源以及搜索这些源的顺序（提供 UNIX 系统上 /etc/nsswitch.conf 文件的等效功能）。当 NAS 客户端连接到 SVM 时， ONTAP 会检查指定的名称服务以获取所需的信息。

***kerberos support*** Kerberos 是一种网络身份验证协议，可通过在客户端 - 服务器实施中加密用户密码来提供 " s强身份验证 " 。ONTAP 支持使用完整性检查的 Kerberos 5 身份验证（ krb5i ）和使用隐私检查的 Kerberos 5 身份验证（ krb5p ）。

**Authorization**

ONTAP 会评估三个安全级别，以确定实体是否有权对 SVM 上的文件和目录执行请求的操作。在评估安全级别后，访问权限由有效权限决定：

- 导出（ NFS ）和共享（ SMB ）安全性

  导出并共享对给定 NFS 导出或 SMB 共享的安全适用场景客户端访问。具有管理权限的用户可以管理 SMB 和 NFS 客户端的导出和共享级别安全性。

- 存储级别访问防护文件和目录安全性

  存储级别访问防护安全性适用场景 SMB 和 NFS 客户端对 SVM 卷的访问。仅支持 NTFS 访问权限。要使 ONTAP 对 UNIX 用户执行安全检查，以访问应用了存储级别访问防护的卷上的数据， UNIX 用户必须映射到拥有该卷的 SVM 上的 Windows 用户。

- NTFS ， UNIX 和 NFSv4 原生文件级安全性

  表示存储对象的文件或目录具有原生文件级安全性。您可以从客户端设置文件级安全性。无论使用 SMB 还是 NFS 访问数据，文件权限都是有效的。

使用**SAML**进行身份验证

ONTAP支持使用安全断言标记语言(SAML)对远程用户进行身份验证。支持多种常见的身份提供程序(IDPs)。有关支持的IdPs的详细信息以及启用SAML身份验证的说明、请参见 "配置 SAML 身份验证"。

**OAuth2.0**与**ONTAP REST API**客户端

从ONTAP 9.14开始、可支持开放授权(OAuth2.0)框架。当客户端使用REST API访问ONTAP时、您只能使用OAuth2.0进行授权和控制访问决策。但是、您可以使用任何ONTAP管理界面(包括命令行界面、System Manager和REST API)配置和启用此功能。

标准OAuth2.0功能与多个常用授权服务器一起受支持。您可以使用基于相互TLS的受发件人限制的访问令牌进一步增强ONTAP安全性。此外、还提供了多种授权选项、包括独立范围以及与ONTAP REST角色和本地用户定义的集成。请参见 "ONTAP OAuth2.0实施概述" 有关详细信息 …

## 管理员身份验证和 **RBAC**

管理员可以使用本地或远程登录帐户向集群和 SVM 进行身份验证。基于角色的访问控制（Role-Based Access Control， RBAC）可确定管理员有权访问的命令。

身份验证

您可以创建本地或远程集群和 SVM 管理员帐户：

- 本地帐户是指帐户信息，公有密钥或安全证书驻留在存储系统上的帐户。
- 远程帐户是指帐户信息存储在 Active Directory 域控制器， LDAP 服务器或 NIS 服务器上的帐户。

除了 DNS 之外， ONTAP 使用与对客户端进行身份验证相同的名称服务来对管理员帐户进行身份验证。

**RBAC**

分配给管理员的 *role* 用于确定管理员有权访问的命令。您可以在为管理员创建帐户时分配角色。您可以根据需要分配其他角色或定义自定义角色。

## 病毒扫描

您可以在存储系统上使用集成的防病毒功能，防止数据受到病毒或其他恶意代码的侵害。称为 *Vscan* 的 ONTAP 病毒扫描将同类最佳的第三方防病毒软件与 ONTAP 功能相结合，让您可以灵活地控制扫描哪些文件以及何时扫描。

存储系统将扫描操作卸载到托管第三方供应商提供的防病毒软件的外部服务器。ONTAP 防病毒连接器 _ 由 NetApp 提供并安装在外部服务器上，用于处理存储系统与防病毒软件之间的通信。

- 当客户端通过 SMB 打开，读取，重命名或关闭文件时，您可以使用 _on-access scanning-来 检查病毒。文件操作将暂停，直到外部服务器报告文件的扫描状态为止。如果文件已扫描，则 ONTAP 允许执行文件操作。否则，它将从服务器请求扫描。

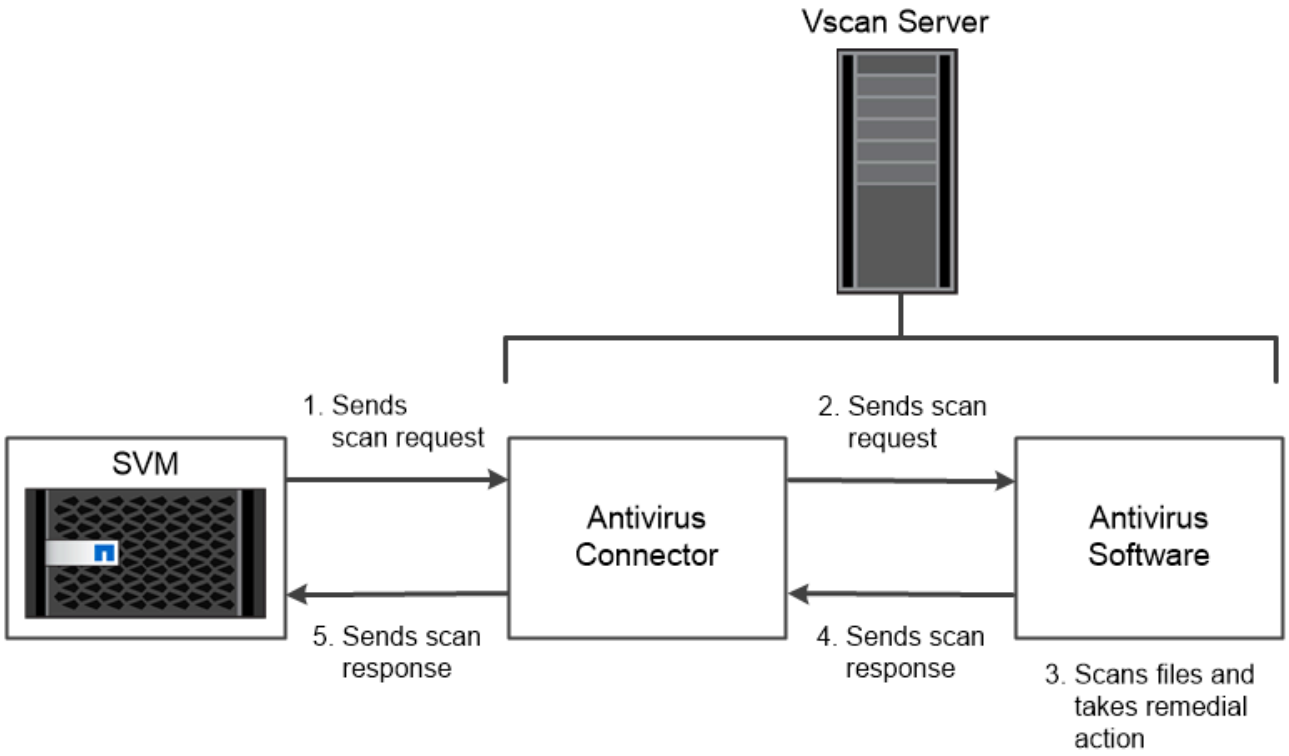
  NFS 不支持实时扫描。

- 您可以使用 _on-Demand scanning-立即 或按计划检查文件中的病毒。例如，您可能只想在非高峰时段运行扫描。外部服务器会更新已检查文件的扫描状态，以便下次通过 SMB 访问这些文件时，通常会缩短这些文件的文件访问延迟（假设这些文件尚未修改）。

  您可以对 SVM 命名空间中的任何路径使用按需扫描，即使是仅通过 NFS 导出的卷也是如此。

通常，您可以在 SVM 上同时启用这两种扫描模式。在任一模式下，防病毒软件都会根据软件中的设置对受感染的文件采取补救措施。

| |
|---|
| 灾难恢复和 MetroCluster 配置中的 * 病毒扫描 _*<br><br>对于灾难恢复和 MetroCluster 配置，您必须为本地集群和配对集群设置单独的 Vscan 服务器。 |




*The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.*

## 加密

ONTAP 提供了基于软件和基于硬件的加密技术，可确保在存储介质被重新利用，退回，放置在不当位置或被盗时无法读取空闲数据。

对于所有 SSL 连接， ONTAP 均符合联邦信息处理标准（ FIPS ） 140-2 的要求。您可以使用以下加密解决方案：

- 硬件解决方案：
  - NetApp 存储加密（ NSE ）

    NSE 是一种使用自加密驱动器（ SED ）的硬件解决方案。

  - NVMe SED

    ONTAP 为未获得 FIPS 140-2 认证的 NVMe SED 提供全磁盘加密。

- 软件解决方案：
  - NetApp 聚合加密（ NAE ）

    NAE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个聚合都使用唯一的密钥启用数据卷。

  - NetApp 卷加密（ NVE ）

NVE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个卷都有一个唯一的密钥。

使用软件（ NAE 或 NVE ）和硬件（ NSE 或 NVMe SED ）加密解决方案实现空闲双加密。存储效率不受 NAE 或 NVE 加密的影响。

**NetApp** 存储加密

NetApp 存储加密（ NetApp Storage Encryption ， NSE ）支持 SED 在写入数据时对数据进行加密。如果磁盘上未存储加密密钥，则无法读取数据。而加密密钥只能由经过身份验证的节点访问。

在发出 I/O 请求时，节点会使用从外部密钥管理服务器或板载密钥管理器检索到的身份验证密钥向 SED 进行自我身份验证：

- 外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为节点提供身份验证密钥。
- 板载密钥管理器是一个内置工具，可从与数据相同的存储系统为节点提供身份验证密钥。

NSE 支持自加密 HDD 和 SSD 。您可以将 NetApp 卷加密与 NSE 结合使用，对 NSE 驱动器上的数据进行双重加密。

> 如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

**NVMe** 自加密驱动器

NVMe SED 没有 FIPS 140-2 认证，但这些磁盘使用 AES 256 位透明磁盘加密来保护空闲数据。

数据加密操作（例如生成身份验证密钥）在内部执行。存储系统首次访问磁盘时会生成身份验证密钥。之后，磁盘将通过在每次请求数据操作时要求存储系统身份验证来保护空闲数据。

**NetApp** 聚合加密

NetApp 聚合加密（ NAE ）是一种基于软件的技术，用于对聚合上的所有数据进行加密。NAE 的一个优势是，卷包含在聚合级别重复数据删除中，而 NVE 卷则不包括在内。

启用 NAE 后，可以使用聚合密钥对聚合中的卷进行加密。

从ONTAP 9.7开始、如果您有、则新创建的聚合和卷会默认进行加密 "NVE许可证" 以及板载或外部密钥管理。

**NetApp** 卷加密

NetApp 卷加密（ NVE ）是一种基于软件的技术，用于一次对一个卷上的空闲数据进行加密。只有存储系统可以访问的加密密钥可确保在底层设备与系统分离时无法读取卷数据。

包括 Snapshot 副本和元数据在内的数据都会进行加密。数据访问由一个唯一的 XTS-AES-256 密钥提供，每个卷一个。内置的板载密钥管理器可保护数据所在系统上的密钥。

您可以在任何类型的聚合（ HDD ， SSD ，混合，阵列 LUN ）上使用任何 RAID 类型以及任何受支持的 ONTAP 实施（包括 ONTAP Select ）中使用 NVE 。您还可以将 NVE 与 NetApp 存储加密（ NetApp Storage Encryption ， NSE ）结合使用，对 NSE 驱动器上的数据进行双重加密。

***When to use KMIP servers*** 尽管使用板载密钥管理器成本较低且通常更方便，但如果满足以下任一条件，则应设置 KMIP 服务器：

- 您的加密密钥管理解决方案必须符合联邦信息处理标准（FIPS） 140-2 或 OASIS KMIP 标准。
- 您需要一个多集群解决方案。KMIP 服务器支持多个集群，并可集中管理加密密钥。

  KMIP 服务器支持多个集群，并可集中管理加密密钥。

- 您的企业需要将身份验证密钥存储在系统或与数据不同的位置，从而提高安全性。

  KMIP 服务器将身份验证密钥与数据分开存储。

相关信息

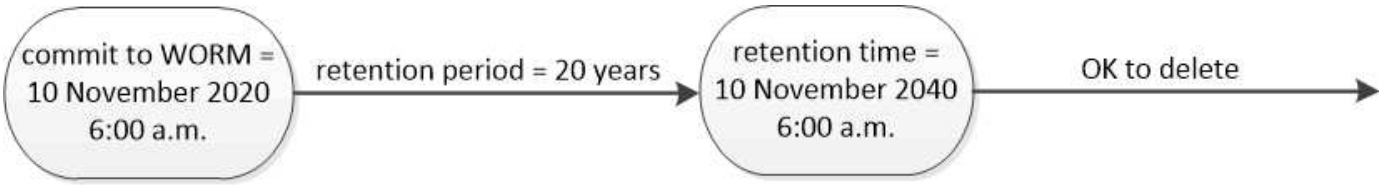
"常见问题解答—NetApp卷加密和NetApp聚合加密"

### WORM 存储

*WORM* 是一种高性能合规解决方案，适用于使用 _write once ， read many （SnapLock ） _ 存储以未经修改的形式保留关键文件以满足监管要求的组织。

通过一个许可证，您可以在 Stric_Compliance 模式 _ 下使用 SnapLock ，以满足 SEC 规则 17a-4 等外部要求，并可在宽松 *Enterprise* 模式 _ 下使用，以满足保护数字资产的内部规定。*SnapLock* 使用防篡改 _*ComplianceClock* 来确定 WORM 文件的保留期限何时已过。

您可以使用 *Snapshot SnapLock for Snapshot* 来保护二级存储上的 SnapVault 副本。您可以使用 SnapMirror 将 WORM 文件复制到其他地理位置，以实现灾难恢复和其他目的。




*SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.*

## 应用程序感知型数据管理

您可以通过应用程序感知型数据管理来描述要通过 ONTAP 部署的应用程序，具体体现在应用程序方面，而不是存储方面。通过使用 System Manager 和 REST API ，可以对应用程序进行配置并使其能够以最少的输入快速提供数据。

通过应用程序感知型数据管理功能，可以在各个应用程序级别设置，管理和监控存储。此功能整合了相关的 ONTAP 最佳实践，可优化配置应用程序，并根据所需性能服务级别和可用系统资源平衡放置存储对象。

应用程序感知型数据管理功能包括一组应用程序模板，其中每个模板都包含一组参数，这些参数共同描述了应用程序的配置。这些参数通常预设为默认值，用于定义应用程序管理员在 ONTAP 系统上配置存储时可以指定的特

征，例如数据库大小，服务级别， LIF 等协议访问元素以及本地保护标准和远程保护标准。ONTAP 会根据指定的参数为应用程序配置大小和服务级别适当的存储实体，例如 LUN 和卷。

您可以对应用程序执行以下任务：

- 使用应用程序模板创建应用程序
- 管理与应用程序关联的存储
- 修改或删除应用程序
- 查看应用程序
- 管理应用程序的 Snapshot 副本
- 创建 一致性组 通过在同一卷或不同卷中选择多个 LUN 来提供数据保护功能

# FabricPool

许多 NetApp 客户都存储了大量很少访问的数据。我们称之为 *cold* 数据。客户还可以经常访问数据，我们将这些数据称为 *hot* data 。理想情况下，您希望将热数据保存在速度最快的存储上，以获得最佳性能。只要冷数据在需要时立即可用，它就可以移至速度较慢的存储。但是，您如何知道数据中哪些部分是热的，哪些部分是冷的？

FabricPool 是一项 ONTAP 功能，可根据访问模式在高性能本地层（聚合）和云层之间自动移动数据。分层可将昂贵的本地存储释放出来用于存储热数据，同时使冷数据随时可从云中的低成本对象存储中访问。FabricPool 会持续监控数据访问并在层之间移动数据，以获得最佳性能并最大程度地节省空间。

使用 FabricPool 将冷数据分层到云是提高云效率和创建混合云配置的最简单方法之一。FabricPool 可在存储块级别运行，因此可同时处理文件和 LUN 数据。

但是， FabricPool 不仅仅是将内部数据分层到云。许多客户使用 Cloud Volumes ONTAP 中的 FabricPool 将冷数据从昂贵的云存储分层到云提供商中成本较低的对象存储。从 ONTAP 9.8 开始，您可以使用捕获启用了 FabricPool 的卷上的分析 "文件系统分析" 或 "对温度敏感的存储效率"。

使用数据的应用程序不知道数据是分层的，因此不需要对应用程序进行更改。分层是完全自动的，因此无需持续管理。

您可以将冷数据存储在主要云提供商之一的对象存储中。或者，选择 NetApp StorageGRID 将冷数据保存在您自己的私有云中，以获得最高性能并全面控制您的数据。

相关信息

"FabricPool 系统管理器文档"

"BlueXP层"

"NetApp TechComm TV 上的 FabricPool 播放列表"