



# 适用于**FabricPool** 的**StorageGRID** 最佳实践

## StorageGRID 11.8

NetApp  
March 19, 2024

# 目录

适用于FabricPool 的StorageGRID 最佳实践 .....	1
高可用性（HA）组的最佳实践 .....	1
FabricPool 负载均衡最佳实践 .....	1
对FabricPool 数据使用ILM的最佳实践 .....	2
StorageGRID 和 FabricPool 的其他最佳实践 .....	3

# 适用于FabricPool 的StorageGRID 最佳实践

## 高可用性（HA）组的最佳实践

在将StorageGRID 作为FabricPool 云层附加之前、请了解StorageGRID 高可用性(HA)组并查看将HA组与FabricPool 结合使用的最佳实践。

### 什么是 HA 组？

高可用性(HA)组是来自多个StorageGRID 网关节点和/或管理节点的一组接口。HA组有助于保持客户端数据连接可用。如果HA组中的活动接口发生故障、则备份接口可以管理工作负载、而对FabricPool 操作的影响微乎其微。

每个 HA 组均可提供对关联节点上共享服务的高可用性访问。例如，如果 HA 组仅包含网关节点上的接口，或者同时包含管理节点和网关节点上的接口，则可以对共享负载均衡器服务进行高可用性访问。

要了解有关高可用性组的详细信息、请参阅 ["管理高可用性\(HA\)组"](#)。

### 使用HA组

为FabricPool 创建StorageGRID HA组的最佳实践取决于工作负载。

- 如果您计划将FabricPool 与主工作负载数据结合使用、则必须创建一个至少包含两个负载均衡节点的HA组、以防止数据检索中断。
- 如果您计划使用 FabricPool snapshot-only 卷分层策略或非主本地性能层（例如，灾难恢复位置或 NetApp SnapMirror® 目标），则只能为 HA 组配置一个节点。

以下说明介绍如何为主动备份 HA 设置 HA 组（一个节点为活动节点，一个节点为备份节点）。但是，您可能更喜欢使用 DNS 轮循或主动 - 主动 HA。要了解这些其他 HA 配置的优势，请参见 ["HA 组的配置选项"](#)。

## FabricPool 负载均衡最佳实践

在将StorageGRID 作为FabricPool 云层附加之前、请查看将负载均衡器与FabricPool 结合使用的最佳实践。

要了解有关StorageGRID 负载均衡器和负载均衡器证书的常规信息、请参阅 ["负载均衡注意事项"](#)。

### 租户访问用于FabricPool 的负载均衡器端点的最佳实践

您可以控制哪些租户可以使用特定负载均衡器端点来访问其分段。您可以允许所有租户、允许某些租户或阻止某些租户。创建供FabricPool 使用的负载均衡端点时，请选择\*允许所有租户\*。ONTAP 会对StorageGRID 存储分段中的数据加密、因此这一额外的安全层几乎不会提供额外的安全性。

### 安全证书的最佳实践

在创建供FabricPool 使用的StorageGRID 负载均衡器端点时、您需要提供安全证书、以使ONTAP 能够向StorageGRID 进行身份验证。

大多数情况下、ONTAP 和StorageGRID 之间的连接应使用传输层安全(Transport Layer Security、TLS)加密。支持使用不带TLS加密的FabricPool、但不建议这样做。为StorageGRID 负载均衡器端点选择网络协议时，请选择\*HTTPS\*。然后、提供允许ONTAP 向StorageGRID 进行身份验证的安全证书。

要了解有关负载均衡端点的服务器证书的详细信息，请执行以下操作：

- ["管理安全证书"](#)
- ["负载均衡注意事项"](#)
- ["服务器证书的强化准则"](#)

## 将证书添加到ONTAP

将StorageGRID 添加为FabricPool 云层时、必须在ONTAP 集群上安装相同的证书、包括根证书颁发机构(CA)证书和任何从属证书颁发机构(CA)证书。

## 管理证书到期时间



如果用于保护ONTAP 和StorageGRID 之间连接的证书到期、FabricPool 将暂时停止工作、并且ONTAP 将暂时无法访问分层到StorageGRID 的数据。

要避免证书到期问题、请遵循以下最佳实践：

- 请仔细监控任何警告证书到期日期即将到来的警报，例如S3和Swift API\*警报的\*负载均衡器端点证书到期\*和\*全局服务器证书到期。
- 请始终保持证书的StorageGRID 和ONTAP 版本同步。如果要替换或续订用于负载均衡器端点的证书、则必须替换或续订ONTAP 用于云层的等效证书。
- 使用公共签名的CA证书。如果您使用的是由CA签名的证书、则可以使用网络管理API自动轮换证书。这样、您就可以无干扰地替换即将到期的证书。
- 如果您已生成自签名StorageGRID 证书、并且该证书即将过期、则必须在现有证书过期之前手动替换StorageGRID 和ONTAP 中的证书。如果自签名证书已过期、请在ONTAP 中关闭证书验证以防止访问丢失。

请参见 ["NetApp知识库：如何在现有ONTAP FabricPool 部署上配置新的StorageGRID 自签名服务器证书"](#) 有关说明，请参见。

## 对FabricPool 数据使用ILM的最佳实践

如果要使用FabricPool 将数据分层到StorageGRID 、则必须了解对FabricPool 数据使用StorageGRID 信息生命周期管理(ILM)的要求。



FabricPool 不了解 StorageGRID ILM 规则或策略。如果 StorageGRID ILM 策略配置不当，可能会发生数据丢失。有关详细信息、请参见 ["创建ILM规则：概述"](#) 和 ["创建ILM策略：概述"](#)。

## 将ILM与FabricPool 结合使用的准则

使用FabricPool设置向导时、该向导会自动为您创建的每个S3存储分段创建一个新的ILM规则、并将该规则添加到非活动策略中。系统将提示您激活此策略。自动创建的规则遵循建议的最佳实践：在单个站点上使用2+1纠删

编码。

如果您要手动配置StorageGRID、而不是使用FabricPool 设置向导、请查看这些准则、以确保您的ILM规则和ILM策略适合FabricPool 数据和您的业务需求。您可能需要创建新规则并更新活动ILM策略、以符合这些准则。

- 您可以使用复制和纠删编码规则的任意组合来保护云层数据。

建议的最佳实践是，在站点内使用 2+1 纠删编码，以实现经济高效的数据保护。纠删编码使用的 CPU 较多，但提供的存储容量明显低于复制。4+1 和 6+1 方案使用的容量小于 2+1 方案。但是，如果您需要在网络扩展期间添加存储节点，4+1 和 6+1 方案的灵活性将会降低。有关详细信息，请参见 ["为经过纠删编码的对象添加存储容量"](#)。

- 应用于 FabricPool 数据的每个规则都必须使用纠删编码，或者必须至少创建两个复制副本。



如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

- 如果需要 ["从StorageGRID中删除FabricPool数据"](#)下，使用ONTAP检索FabricPool卷的所有数据并将其提升到性能层。



为避免数据丢失、请勿使用将过期的ILM规则或删除FabricPool云层数据。将每个ILM规则中的保留期限设置为\*永久\*、以确保StorageGRID ILM不会删除FabricPool对象。

- 请勿创建将FabricPool 云层数据从存储分段移动到其他位置的规则。您不能使用云存储池将FabricPool 数据移动到其他对象存储。同样、您也不能使用归档节点将FabricPool 数据归档到磁带。



不支持将云存储池与 FabricPool 结合使用，因为从云存储池目标检索对象会增加延迟。

- 从 ONTAP 9.8 开始，您可以选择创建对象标记来帮助对分层数据进行分类和排序，以便于管理。例如，您只能在连接到 StorageGRID 的 FabricPool 卷上设置标记。然后，在 StorageGRID 中创建 ILM 规则时，您可以使用对象标记高级筛选器选择并放置此数据。

## StorageGRID 和 FabricPool 的其他最佳实践

在配置StorageGRID 系统以与FabricPool 结合使用时、您可能需要更改其他StorageGRID 选项。在更改全局设置之前、请考虑此更改会对其他S3应用程序产生何种影响。

### 审核消息和日志目标

FabricPool 工作负载的读取操作率通常较高、从而可能会生成大量审核消息。

- 如果您不需要FabricPool 或任何其他S3应用程序的客户端读取操作记录，可选择进入\*configuration\*>\*Monitoring\*>\*Audit and syslog server\*。将“\*客户端读取\*”设置更改为“\*错误\*”，以减少审核日志中记录的审核消息数。请参见 ["配置审核消息和日志目标"](#) 了解详细信息。
- 如果您的网格很大、可以使用多种类型的S3应用程序、也可以保留所有审核数据、配置外部系统日志服务器并远程保存审核信息。使用外部服务器可以最大限度地降低审核消息日志记录对性能的影响、而不会降低审核数据的完整性。请参见 ["外部系统日志服务器的注意事项"](#) 了解详细信息。

## 对象加密

配置StorageGRID 时、您可以选择启用 "用于存储对象加密的全局选项" 其他StorageGRID 客户端需要进行数据加密。从 FabricPool 分层到 StorageGRID 的数据已加密，因此不需要启用 StorageGRID 设置。客户端加密密钥归 ONTAP 所有。

## 对象压缩

配置StorageGRID 时、请勿启用 "用于压缩存储对象的全局选项"。已对从 FabricPool 分层到 StorageGRID 的数据进行压缩。使用StorageGRID 选项不会进一步减小对象的大小。

## 存储分段一致性

对于FabricPool存储分段、建议的存储分段一致性为\*新写入后读取\*、这是新存储分段的默认一致性。请勿编辑FabricPool存储分段以使用\*可用\*或\*强站点\*。

## FabricPool 分层

如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。例如，如果 StorageGRID 节点正在 VMware 主机上运行，请确保为 StorageGRID 节点的数据存储库提供支持的卷未启用 FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。



切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。