



使用 **S3 Object Lock** StorageGRID software

NetApp
July 23, 2026

目录

- 使用 S3 Object Lock 1
 - S3 对象锁定如何保护 StorageGRID 中的对象 1
 - 什么是 S3 Object Lock? 1
 - 将 S3 对象锁定与传统合规性进行比较 2
 - StorageGRID 中的 S3 Object Lock 工作流 3
 - StorageGRID 中的 S3 对象锁定要求 4
 - 使用全局 S3 Object Lock 设置的要求 4
 - 合规 ILM 规则的要求 4
 - ILM 策略的要求 4
 - `\${post\_edited\_translations.segment}` 5
 - `\${post\_edited\_translations.segment}` 5
 - `\${post\_edited\_translations.segment}` 5
 - 在 StorageGRID 中全局启用 S3 Object Lock 6
 - 解决在 StorageGRID 中更新 S3 Object Lock 或旧版合规性设置时的一致性错误 7

使用 S3 Object Lock

S3 对象锁定如何保护 StorageGRID 中的对象

作为网格管理员，您可以为 StorageGRID 系统启用 S3 对象锁定，并实施合规的 ILM 策略，以帮助确保特定 S3 存储桶中的对象在指定时间内不会被删除或覆盖。

什么是 S3 Object Lock？

`${post_edited_translations.segment}`

当为 StorageGRID 系统启用全局 S3 对象锁定设置时，S3 租户帐户可以创建启用或未启用 S3 对象锁定的存储桶。如果存储桶已启用 S3 对象锁定，则需要存储桶版本控制，并会自动启用。

*没有 S3 Object Lock 的存储桶*只能包含未指定保留设置的对象。所有已载入的对象均不具有保留设置。

*具有 S3 对象锁定的存储桶*可以包含具有或不具有 S3 客户端应用程序指定的保留设置的对象。已摄取的某些对象将具有保留设置。

*配置了 S3 Object Lock 和默认保留的存储桶*可以包含已指定保留设置的已上传对象以及未指定保留设置的新对象。新对象将使用默认设置，因为尚未在对象级别配置保留设置。

实际上，配置默认保留后，所有新摄入的对象都将具有保留设置。没有对象保留设置的现有对象不受影响。

保留模式

StorageGRID S3 Object Lock 功能支持两种保留模式，以对对象应用不同级别的保护。这些模式与 Amazon S3 保留模式等效。

- `${post_edited_translations.segment}`
 - 在达到其保留截止日期之前，无法删除此对象。
 - 对象的保留截止日期可以延长，但不能缩短。
 - 在达到该日期之前，无法删除对象的 `retain-until-date`。
- `${post_edited_translations.segment}`
 - 具有特殊权限的用户可以在请求中使用旁路标头来修改某些保留设置。
 - 这些用户可以在达到保留截止日期之前删除对象版本。
 - 这些用户可以增加、减少或删除对象的保留截止日期。

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- **Retain-until-date:** 如果对象版本的 `retain-until-date` 在将来，则可以检索该对象，但不能将其删除。
- **诉讼保留:** 对对象版本应用诉讼保留会立即锁定该对象。例如，您可能需要与调查或法律纠纷相关的对象进行诉讼保留。诉讼保留没有过期日期，而是会一直保持有效，直到被显式删除。诉讼保留独立于保留截止

日期。



如果对象处于合法冻结状态，则无论其保留模式如何，任何人都无法删除该对象。

有关对象设置的详细信息，请参见 ["使用 S3 REST API 配置 S3 对象锁定"](#)。

`${post_edited_translations.segment}`

如果在启用 S3 对象锁定的情况下创建了存储桶，则用户可以选择为存储桶指定以下默认设置：

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

默认存储桶设置仅适用于没有自己的保留设置的新对象。添加或更改这些默认设置时，现有存储桶对象不受影响。

请参见 ["`\${post\_edited\_translations.segment}`"](#) 和 ["更新 S3 对象锁定默认保留"](#)。

将 S3 对象锁定与传统合规性进行比较

S3 对象锁定取代了早期 StorageGRID 版本中提供的合规性功能。由于 S3 对象锁定功能符合 Amazon S3 要求，因此它弃用了专有的 StorageGRID 合规性功能，该功能现在称为"旧版合规性"。



全局合规性设置已弃用。如果使用以前版本的 StorageGRID 启用了此设置，则会自动启用 S3 对象锁定设置。您可以继续使用 StorageGRID 来管理现有兼容存储桶的设置；但是，您无法创建新的兼容存储桶。有关详细信息，请参见 ["NetApp 知识库：如何在 StorageGRID 11.5 中管理旧版兼容存储桶"](#)。

如果您在以前版本的 StorageGRID 中使用了旧版合规性功能，请参见下表，了解它与 StorageGRID 中的 S3 对象锁定功能的比较。

	S3 对象锁定	合规性（旧版）
如何在全球范围内启用此功能？	在网格管理器中，选择 Configuration > System > S3 Object Lock 。	不再支持。
如何为存储桶启用此功能？	用户必须在使用 Tenant Manager、租户管理 API 或 S3 REST API 创建新存储桶时启用 S3 对象锁定。	不再支持。
是否支持存储区版本控制？	是的。存储区版本控制为必填字段，当为存储区启用 S3 Object Lock 时会自动启用。	目标卷
如何设置对象保留？	用户可以为每个对象版本设置保留截止日期，也可以为每个存储桶设置默认保留期限。	用户必须为整个存储桶设置保留期。保留期适用于存储桶中的所有对象。

	S3 对象锁定	合规性（旧版）
是否可以更改保留期限？	- 在合规模式下，对象版本的保留截止日期可以延长，但不能缩短。 - 在治理模式下，具有特殊权限的用户可以减少甚至删除对象的保留设置。	存储桶的保留期限可以增加，但不能减少。
法律保留在哪里受到控制？	用户可以对存储桶中的任何对象版本进行法律冻结或解除法律冻结。	合法冻结放置在存储桶上，并影响存储桶中的所有对象。
何时可以删除对象？	- 在合规模式下，可以在达到保留截止日期后删除对象版本，前提是对象未处于合法持有状态。 - 在治理模式下，具有特殊权限的用户可以在达到保留截止日期之前删除对象，前提是该对象未处于合法持有状态。	在保留期到期后，假设存储桶未处于合法冻结状态，则可以删除对象。对象可以自动或手动删除。
是否支持存储桶生命周期配置？	是	否

StorageGRID 中的 S3 Object Lock 工作流

作为网格管理员，您必须与租户用户密切协调，以确保以满足其保留要求的方式保护对象。



`${post_edited_translations.segment}`

以下网格管理员和租户用户列表包含使用 S3 对象锁定功能的高级任务。

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- 确保信息生命周期管理 (ILM) 策略是_合规_的；也就是说，它们符合"`${post_edited_translations.segment}`"。
- 根据需要，允许租户将 Compliance 用作保留模式。否则，仅允许使用 Governance 模式。
- 根据需要，为租户设置最长保留期限。

租户用户

- `${post_edited_translations.segment}`
- 根据需要，联系网格管理员以启用全局 S3 Object Lock 设置并设置权限。
- 创建启用了 S3 Object Lock 的存储桶。
- 可选地，为存储桶配置默认保留设置：
 - `${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- 使用 S3 客户端应用程序添加对象，并可选择设置对象特定的保留：
 - 保留模式。治理或合规性（如果网格管理员允许）。
 - 保留截止日期：必须小于或等于网格管理员设置的最大保留期限所允许的值。

StorageGRID 中的 S3 对象锁定要求

您必须查看启用全局 S3 Object Lock 设置的要求、创建合规 ILM 规则和 ILM 策略的要求，以及 StorageGRID 对使用 S3 Object Lock 的存储桶和对象施加的限制。

使用全局 S3 Object Lock 设置的要求

- 必须使用 Grid Manager 或 Grid Management API 启用全局 S3 对象锁定设置，然后任何 S3 租户才能创建启用了 S3 对象锁定的存储桶。
- 启用全局 S3 Object Lock 设置允许所有 S3 租户帐户在启用 S3 Object Lock 的情况下创建存储桶。
- 启用全局 S3 Object Lock 设置后，无法禁用该设置。
- 除非所有活动 ILM 策略中的默认规则都符合，否则无法启用全局 S3 Object Lock（即，默认规则必须符合启用了 S3 Object Lock 的存储桶的要求）。
- 启用全局 S3 对象锁定设置后，除非策略中的默认规则符合要求，否则无法创建新的 ILM 策略或激活现有的 ILM 策略。启用全局 S3 对象锁定设置后，ILM 规则和 ILM 策略页面将指示哪些 ILM 规则是合规的。

合规 ILM 规则的要求

如果要启用全局 S3 Object Lock 设置，必须确保所有活动 ILM 策略中的默认规则均符合要求。合规规则满足已启用 S3 Object Lock 的存储桶以及已启用旧版合规性的任何现有存储桶的要求：

- 必须至少创建两个复制对象副本或一个纠删编码副本。
- 这些副本必须在放置说明中每行的整个持续时间内存在于 Storage Nodes 上。
- 对象副本无法保存在云存储池中。
- 至少有一行放置说明必须从第 0 天开始，使用 **Ingest time** 作为参考时间。
- 放置说明中至少有一行必须为“永久”。

ILM 策略的要求

启用全局 S3 对象锁定设置后，活动和非活动 ILM 策略可以包括合规和不合规规则。

- 活动或非活动 ILM 策略中的默认规则必须符合合规要求。
- 不合规规则仅适用于未启用 S3 Object Lock 或未启用旧版合规性功能的存储桶中的对象。
- 合规规则可以应用于任何存储桶中的对象；不需要为存储桶启用 S3 Object Lock 或旧版合规性。

["S3 对象锁定合规 ILM 策略示例"](#)

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- 如果您计划使用 S3 Object Lock，则必须在创建存储桶时启用 S3 Object Lock。您无法为现有存储桶启用 S3 Object Lock。
- 为存储桶启用 S3 Object Lock 时，StorageGRID 会自动为该存储桶启用版本控制。您无法禁用 S3 Object Lock，也无法暂停该存储桶的版本控制。
- （可选）您可以使用 Tenant Manager、Tenant Management API 或 S3 REST API 为每个存储桶指定默认保留模式和保留期。存储桶的默认保留设置仅适用于添加到该存储桶且自身没有保留设置的新对象。您可以通过在上传每个对象版本时为其指定保留模式和保留截止日期来覆盖这些默认设置。
- 已启用 S3 Object Lock 的存储桶支持存储桶生命周期配置。
- CloudMirror 复制不支持启用了 S3 Object Lock 的存储桶。

`${post_edited_translations.segment}`

- 要保护对象版本，您可以为存储桶指定默认保留设置，也可以为每个对象版本指定保留设置。可以使用 S3 客户端应用程序或 S3 REST API 指定对象级保留设置。
- 保留设置适用于单个对象版本。一个对象版本可以同时具有保留截止日期和法定保留设置，也可以仅具有其中之一，或者两者都不具有。为对象指定保留截止日期或法定保留设置仅会保护请求中指定的版本。您可以创建该对象的新版本，而该对象的上一个版本仍保持锁定状态。

`${post_edited_translations.segment}`

在启用了 S3 Object Lock 的存储桶中保存的每个对象都会经历以下阶段：

1. 对象载入

`${post_edited_translations.segment}`

- 如果为对象指定了保留设置，则应用对象级别设置。任何默认存储桶设置都将被忽略。
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

如果应用了保留设置，则对象和任何 S3 用户定义的元数据都将受到保护。

2. 对象保留和删除

StorageGRID 会在指定的保留期内存储每个受保护对象的多个副本。对象副本的确切数量和类型以及存储位置由活动 ILM 策略中的合规规则决定。受保护对象在达到其保留截止日期之前是否可以被删除，取决于其保留模式。

- 如果对象处于合法冻结状态，则无论其保留模式如何，任何人都无法删除该对象。

相关信息

- ["\\${post_edited_translations.segment}"](#)
- ["更新 S3 对象锁定默认保留"](#)
- ["使用 S3 REST API 配置 S3 对象锁定"](#)

- ["示例 7：针对 S3 对象锁定的合规 ILM 策略"](#)

在 StorageGRID 中全局启用 S3 Object Lock

如果 S3 租户帐户在保存对象数据时需要遵守监管要求，则必须为整个 StorageGRID 系统启用 S3 对象锁定。启用全局 S3 对象锁定设置允许任何 S3 租户用户使用 S3 对象锁定创建和管理存储区和对象。

开始之前

- 您有 ["root 访问权限"](#)。
- 您已使用 ["支持的 Web 浏览器"](#) 登录到网格管理器。
- 您已查看 S3 Object Lock 工作流程，并了解注意事项。
- 您已确认活动 ILM 策略中的默认规则是合规的。有关详细信息，请参见 ["创建默认 ILM 规则"](#)。

关于此任务

网格管理员必须启用全局 S3 对象锁定设置，以允许租户用户创建启用了 S3 对象锁定的新存储桶。启用此设置后，无法将其禁用。

启用全局 S3 对象锁定设置后，请检查现有租户的合规性设置。启用此设置时，每个租户的 S3 对象锁定设置取决于创建租户时的 StorageGRID 版本。



全局合规性设置已弃用。如果使用以前版本的 StorageGRID 启用了此设置，则会自动启用 S3 对象锁定设置。您可以继续使用 StorageGRID 来管理现有兼容存储桶的设置；但是，您无法创建新的兼容存储桶。有关详细信息，请参见 ["NetApp 知识库：如何在 StorageGRID 11.5 中管理旧版兼容存储桶"](#)。

步骤

1. 选择 **配置 > 系统 > S3 对象锁定**。

此时将显示"S3 对象锁定设置"页面。

2. 选择 **Enable S3 Object Lock**。
3. 选择*应用*。

此时将显示一个确认对话框，提醒您在启用 S3 对象锁定后无法将其禁用。

4. 如果您确定要为整个系统永久启用 S3 对象锁定，请选择 **OK**。

选择*确定*时：

- 如果活动 ILM 策略中的默认规则符合要求，则现在将为整个网格启用 S3 Object Lock，且无法禁用。
- 如果默认规则不合规，则会出现错误。您必须创建并激活一个新的 ILM 策略，其中包含一个合规规则作为其默认规则。选择 **OK**。然后，创建新策略，模拟并激活它。有关说明，请参阅 ["创建 ILM 策略"](#)。

解决在 StorageGRID 中更新 S3 Object Lock 或旧版合规性设置时的一致性错误

如果一个数据中心站点或站点上的多个存储节点不可用，则可能需要帮助 S3 租户用户将更改应用于 S3 对象锁定或旧版合规性配置。

拥有已启用 S3 Object Lock（或旧版合规性）的存储桶的租户用户可以更改某些设置。例如，使用 S3 Object Lock 的租户用户可能需要将对象版本置于合法保留状态。

当租户用户更新 S3 存储区或对象版本的设置时，StorageGRID 尝试立即跨网格更新存储区或对象元数据。如果系统由于某个数据中心站点或多个存储节点不可用而无法更新元数据，则会返回错误：

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

要解决此错误，请执行以下步骤：

1. 尽快尝试使所有存储节点或站点重新可用。
2. 如果您无法在每个站点提供足够的存储节点，请联系技术支持，他们可以帮助您恢复节点，并确保在整个网格中始终如一地应用更改。
3. 解决潜在问题后，提醒租户用户重试其配置更改。

相关信息

- ["使用租户帐户"](#)
- ["使用 S3 REST API"](#)
- ["恢复和维护"](#)

版权信息

版权所有 © 2026 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，本文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。