使用 S3 对象锁定

StorageGRID 11.8

NetApp
March 19, 2024

目录

使用 S3 对象锁定

使用 S3 对象锁定管理对象

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存储分段中的对象在指定时间内不会被删除或覆盖。

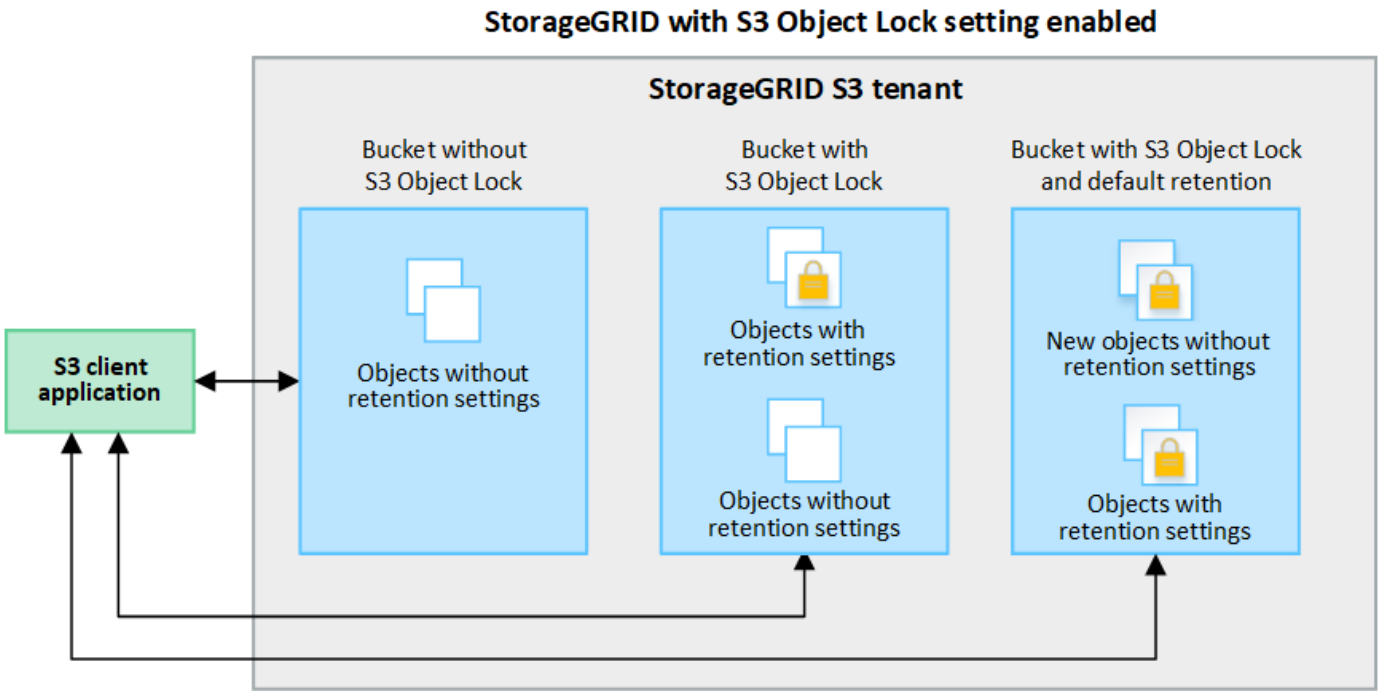
什么是 S3 对象锁定?

StorageGRID S3 对象锁定功能是一种对象保护解决方案，相当于 Amazon Simple Storage Service （ Amazon S3 ）中的 S3 对象锁定。

如图所示，如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则 S3 租户帐户可以在启用或不启用 S3 对象锁定的情况下创建存储分段。如果存储分段启用了S3对象锁定、则需要执行存储分段版本控制、并会自动启用此功能。

如果存储分段启用了S3对象锁定、S3客户端应用程序可以选择为保存到该存储分段的任何对象版本指定保留设置。

此外、启用了S3对象锁定的分段还可以选择具有默认保留模式和保留期限。默认设置仅适用于添加到存储分段的对象、这些对象没有自己的保留设置。



保留模式

StorageGRID S3对象锁定功能支持两种保留模式、可对对象应用不同级别的保护。这些模式相当于Amazon S3保留模式。

- 在合规模式下：
  - 在达到保留截止日期之前、无法删除此对象。

- 对象的保留截止日期可以增加、但不能减少。
- 在达到该日期之前、无法删除对象的保留截止日期。

- 在监管模式下：
  - 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。

对象版本的保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以使用S3客户端应用程序为添加到该存储分段的每个对象指定以下保留设置(可选)：

- 保留模式：合规性或监管。
- **retain**至日期：如果某个对象版本的retain至日期为未来版本，则可以检索该对象，但不能将其删除。
- * 合法保留 * ：对对象版本应用合法保留时，会立即锁定该对象。例如，您可能需要对与调查或法律争议相关的对象进行法律保留。合法保留没有到期日期，但在明确删除之前始终有效。合法保留与保留日期无关。

> 如果某个对象处于合法保留状态、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"。

存储分段的默认保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以选择为此存储分段指定以下默认设置：

- 默认保留模式：合规或监管。
- 默认保留期限：添加到此存储分段的新对象版本应保留多长时间、从添加之日开始。

默认分段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、现有存储分段对象不会受到影响。

请参见 "创建 S3 存储区。" 和 "更新S3对象锁定默认保留"。

比较 S3 对象锁定与原有合规性

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、因此会弃用专有的StorageGRID合规性功能、该功能现在称为"原有合规性"。

> 已弃用全局合规性设置。如果使用早期版本的StorageGRID 启用此设置、则会自动启用S3对象锁定设置。您可以继续使用StorageGRID 管理现有合规存储分段的设置、但不能创建新的合规存储分段。有关详细信息，请参见 "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"。

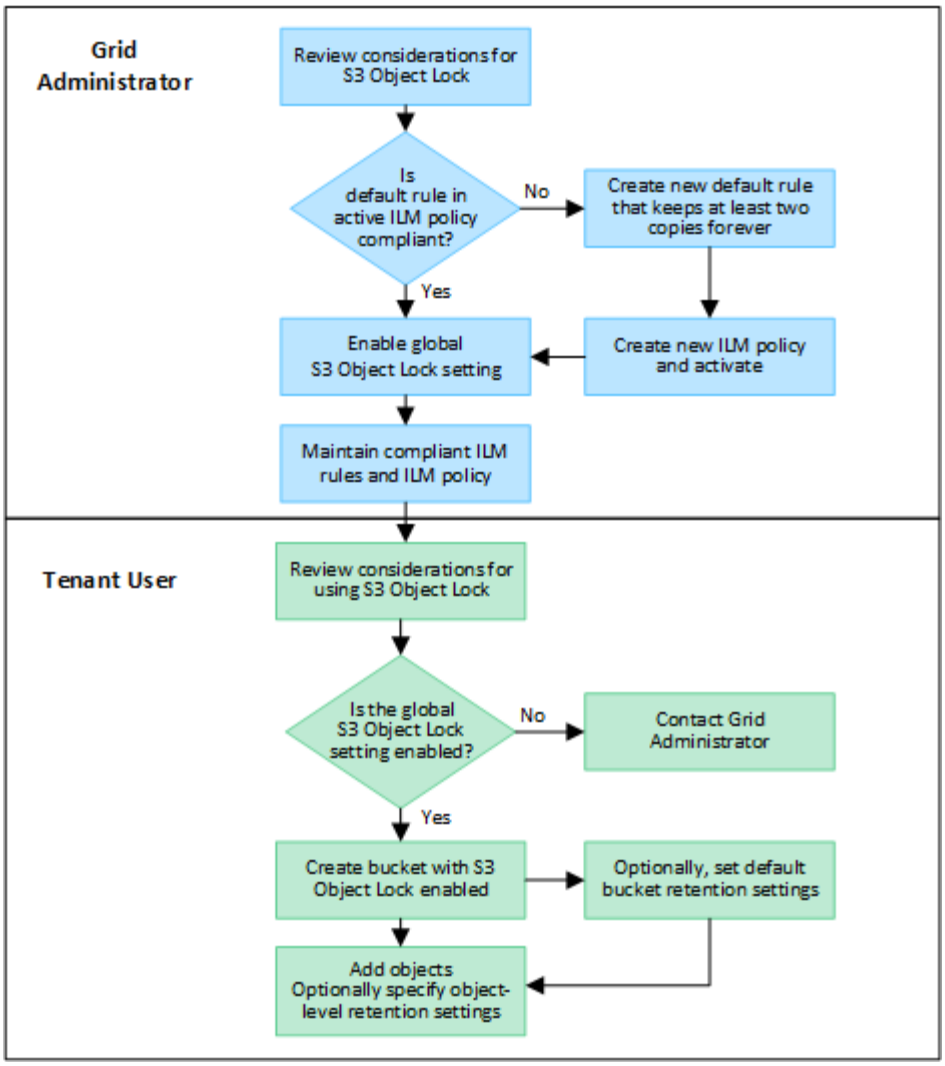
如果您在先前版本的 StorageGRID 中使用了原有的合规性功能，请参见下表，了解它与 StorageGRID 中的 S3 对象锁定功能的比较情况。

	S3 对象锁定	合规性（原有）
如何全局启用此功能?	在网格管理器中，选择 * 配置 * > * 系统 * > * S3 对象锁定 * 。	不再支持。
如何为存储分段启用此功能?	在使用租户管理器，租户管理 API 或 S3 REST API 创建新存储分段时，用户必须启用 S3 对象锁定。	不再支持。
是否支持存储分版本控制?	是的。需要分段版本控制，并且在为分段启用 S3 对象锁定时会自动启用分段版本控制。	否
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、也可以为每个存储分段设置默认保留期限。	用户必须为整个存储分段设置一个保留期限。保留期限适用场景 存储分段中的所有对象。
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增加、但不能减少。 • 在监管模式下、具有特殊权限的用户可以减少甚至删除对象的保留设置。	存储分段的保留期限可以延长、但不能缩短。
合法保留在何处?	用户可以对存储分段中的任何对象版本进行合法保留或取消合法保留。	合法保留放置在存储分段上，并影响存储分段中的所有对象。
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、前提是对象不处于合法保留状态。 • 在监管模式下、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、前提是该对象不处于合法保留状态。	可以在保留期限到期后删除对象，前提是存储分段未处于合法保留状态。可以自动或手动删除对象。
是否支持存储分段生命周期配置?	是的。	否

S3 对象锁定的工作流

作为网格管理员，您必须与租户用户密切协调，以确保对象受到保护，并满足其保留要求。

工作流图显示了使用 S3 对象锁定的高级步骤。这些步骤由网格管理员和租户用户执行。



网格管理员任务

如工作流图所示，网格管理员必须执行两项高级任务， S3 租户用户才能使用 S3 对象锁定：

1. 至少创建一个合规ILM规则、并将该规则设置为活动ILM策略中的默认规则。
2. 为整个 StorageGRID 系统启用全局 S3 对象锁定设置。

租户用户任务

启用全局 S3 对象锁定设置后，租户可以执行以下任务：

1. 创建已启用 S3 对象锁定的分段。
2. (可选)指定存储分段的默认保留设置。任何默认分段设置仅应用于没有自己的保留设置的新对象。
3. 将对象添加到这些分段中、并可选择指定对象级别保留期限和合法保留设置。
4. 根据需要、更新存储分段的默认保留、或者更新单个对象的保留期限或合法保留设置。

S3 对象锁定的要求

您必须查看启用全局 S3 对象锁定设置的要求，创建合规 ILM 规则和 ILM 策略的要求以及 StorageGRID 对使用 S3 对象锁定的分段和对象所施加的限制。

使用全局 S3 对象锁定设置的要求

- 您必须先使用网格管理器或网格管理 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 对象锁定的分段。
- 启用全局 S3 对象锁定设置后，所有 S3 租户帐户都可以在启用了 S3 对象锁定的情况下创建存储分段。
- 启用全局S3对象锁定设置后、无法禁用该设置。
- 除非所有活动ILM策略中的默认规则均为_兼容_(即、默认规则必须符合启用了S3对象锁定的分段的要求)、否则无法启用全局S3对象锁定。
- 启用全局S3对象锁定设置后、您无法创建新的ILM策略或激活现有ILM策略、除非该策略中的默认规则合规。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规则合规。

符合 ILM 规则的要求

如果要启用全局S3对象锁定设置、则必须确保所有活动ILM策略中的默认规则合规。合规规则可满足启用了 S3 对象锁定的两个存储分段以及启用了旧合规性的任何现有存储分段的要求：

- 它必须至少创建两个复制的对象副本或一个经过纠删编码的副本。
- 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存储节点上。
- 无法将对象副本保存在云存储池中。
- 无法将对象副本保存在归档节点上。
- 至少一行放置指令必须从第0天开始、并使用*内嵌时间*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策略可以同时包含合规和不合规规则。

- 活动或非活动ILM策略中的默认规则必须合规。
- 不合规规则仅适用于未启用S3对象锁定或未启用原有合规性功能的分段中的对象。
- 合规规则可以应用于任何存储分段中的对象；不需要为此存储分段启用 S3 对象锁定或原有合规性。

合规的 ILM 策略可能包括以下三个规则：

1. 一种在启用了 S3 对象锁定的情况下为特定分段中的对象创建经过擦除编码的副本的合规规则。EC 副本从第 0 天一直存储在存储节点上。
2. 一种不合规的规则，在存储节点上创建两个复制的对象副本一年，然后将一个对象副本移动到归档节点并永久存储该副本。此规则仅适用于未启用S3对象锁定或原有合规性的适用场景 分段、因为它仅永久存储一个对象副本、并且使用归档节点。
3. 一种默认的合规规则，用于在存储节点上创建从 0 天到永久的两个复制对象副本。此规则适用场景 任何分

段中未被前两个规则筛选出的任何对象。

启用了 **S3** 对象锁定的存储分段的要求

- 如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以使用租户管理器，租户管理 API 或 S3 REST API 创建启用了 S3 对象锁定的分段。
- 如果您计划使用 S3 对象锁定，则必须在创建存储分段时启用 S3 对象锁定。您不能为现有存储分段启用S3对象锁定。
- 为存储分段启用 S3 对象锁定后， StorageGRID 会自动为该存储分段启用版本控制。您不能禁用存储分段的S3对象锁定或暂停版本控制。
- 您也可以使用租户管理器、租户管理API或S3 REST API为每个存储分段指定默认保留模式和保留期限。存储分段的默认保留设置仅适用于添加到存储分段中但没有自己的保留设置的新对象。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。
- 启用了S3对象锁定的分段支持分段生命周期配置。
- 启用了 S3 对象锁定的存储分段不支持 CloudMirror 复制。

启用了 **S3** 对象锁定的分段中的对象的要求

- 要保护对象版本、您可以为存储分段指定默认保留设置、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。
- 保留设置适用于各个对象版本。对象版本可以同时具有保留截止日期和合法保留设置，但不能具有其他设置，或者两者均不具有。为对象指定保留日期或合法保留设置仅保护请求中指定的版本。您可以创建新版本的对象，而先前版本的对象仍保持锁定状态。

启用了 **S3** 对象锁定的存储分段中的对象生命周期

在启用了S3对象锁定的情况下保存在存储分段中的每个对象都会经历以下阶段：

1. * 对象载入 *

   将对象版本添加到启用了S3对象锁定的存储分段时、将按如下所示应用保留设置：

   - 如果为对象指定了保留设置、则会应用对象级别设置。系统将忽略任何默认存储分段设置。
   - 如果没有为对象指定保留设置、则会应用默认存储分段设置(如果存在)。
   - 如果没有为对象或存储分段指定保留设置、则对象不受S3对象锁定保护。

   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会受到保护。

2. 对象保留和删除

   StorageGRID 会在指定的保留期限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。是否可以在达到保留截止日期之前删除受保护对象取决于其保留模式。

   - 如果某个对象处于合法保留状态、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

- "创建 S3 存储区。"

- "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： S3 对象锁定的兼容 ILM 策略"

全局启用 S3 对象锁定

如果 S3 租户帐户在保存对象数据时需要遵守法规要求，则必须为整个 StorageGRID 系统启用 S3 对象锁定。启用全局 S3 对象锁定设置后，任何 S3 租户用户都可以使用 S3 对象锁定创建和管理存储分段和对象。

开始之前

- 您拥有 "root访问权限"。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已查看S3对象锁定工作流、并了解注意事项。
- 您已确认活动ILM策略中的默认规则合规。请参见 "创建默认 ILM 规则" 了解详细信息。

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 对象锁定的新分段。启用此设置后、将无法禁用它。

> 已弃用全局合规性设置。如果使用早期版本的StorageGRID 启用此设置、则会自动启用S3对象锁定设置。您可以继续使用StorageGRID 管理现有合规存储分段的设置、但不能创建新的合规存储分段。有关详细信息，请参见 "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"。

步骤

1. 选择 * 配置 * > * 系统 * > * S3 对象锁定 * 。

   此时将显示 "S3 Object Lock Settings" 页面。

2. 选择 * 启用 S3 对象锁定 * 。
3. 选择 * 应用 * 。

   此时将显示一个确认对话框、提醒您在启用S3对象锁定后无法禁用它。

4. 如果确实要为整个系统永久启用 S3 对象锁定，请选择 * 确定 * 。

   选择 * 确定 * 时：

   - 如果活动ILM策略中的默认规则合规、则会为整个网格启用S3对象锁定、并且无法禁用。
   - 如果默认规则不合规、则会显示错误。您必须创建并激活一个新的ILM策略、其中包括一个合规规则作为其默认规则。选择 * 确定 * 。然后、创建一个新策略、对其进行模拟并将其激活。请参见 "创建 ILM 策略" 有关说明，请参见。

解决更新 S3 对象锁定或原有合规性配置时出现的一致性错误

如果一个站点上的一个数据中心站点或多个存储节点不可用，您可能需要帮助 S3 租户用户对 S3 对象锁定或原有合规性配置进行更改。

启用了 S3 对象锁定（或原有合规性）的存储分段的租户用户可以更改某些设置。例如，使用 S3 对象锁定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 存储分段或对象版本的设置时， StorageGRID 会尝试立即更新整个网格中的存储分段或对象元数据。如果由于数据中心站点或多个存储节点不可用而导致系统无法更新元数据、则系统将返回错误：

```
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. 尝试尽快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网格中一致地应用更改。
3. 解决底层问题描述 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"