将 S3 对象锁定与 ILM 结合使用

StorageGRID

NetApp
April 10, 2024

目录

将 S3 对象锁定与 ILM 结合使用

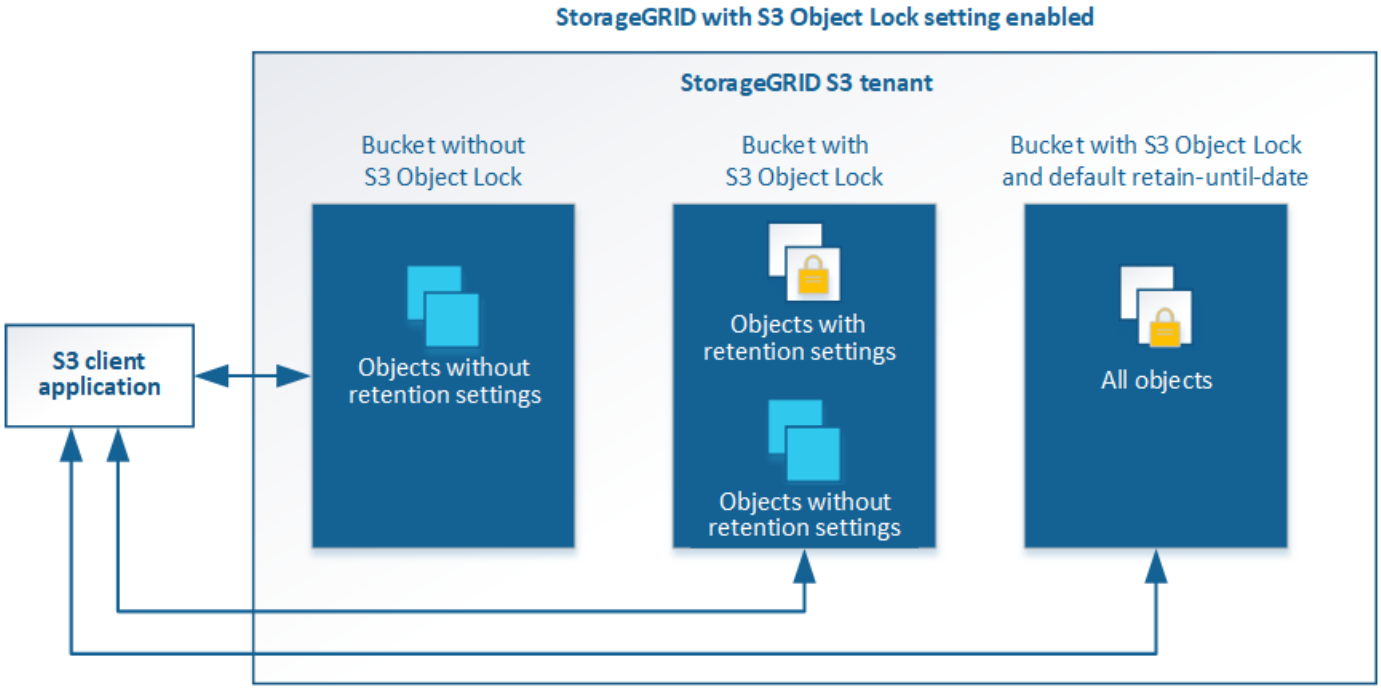
使用 S3 对象锁定管理对象

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。如果某个存储分段启用了 S3 对象锁定，则 S3 客户端应用程序可以选择为该存储分段中的任何对象版本指定保留设置。对象版本必须具有指定的保留设置，以受 S3 对象锁定的保护。此外，启用了 S3 对象锁定的每个存储分段也可以选择具有默认保留模式和保留期限，如果在没有自身保留设置的情况下将对象添加到存储分段，则此模式和保留期限适用。



StorageGRID S3 对象锁定功能提供了一种保留模式，相当于 Amazon S3 合规模式。默认情况下，任何用户都无法覆盖或删除受保护的对象版本。StorageGRID S3 对象锁定功能不支持监管模式，并且不允许具有特殊权限的用户绕过保留设置或删除受保护的对象。

如果存储分段启用了 S3 对象锁定，则在创建或更新对象时， S3 客户端应用程序可以选择指定以下任一或两个对象级别保留设置：

- * 保留至日期 *：如果对象版本的保留至日期为未来日期，则可以检索该对象，但无法修改或删除它。可以根据需要增加对象的保留截止日期，但不能缩短此日期。
- * 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。

有关对象保留设置的详细信息，请转到 使用 S3 对象锁定。

有关默认存储分段保留设置的详细信息，请转至 使用 S3 对象锁定默认存储分段保留。

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，因此它会弃用专有的 StorageGRID 合规性功能，现在称为 "`原有合规性 " 。`

如果您之前启用了全局合规性设置，则会自动启用全局 S3 对象锁定设置。租户用户无法再在启用了合规性的情况下创建新的分段；但是，根据需要，租户用户可以继续使用和管理任何现有的旧合规分段，其中包括执行以下任务：

- 将新对象载入已启用旧合规性的现有存储分段。
- 增加启用了旧合规性的现有存储分段的保留期限。
- 更改已启用旧合规性的现有存储分段的自动删除设置。
- 对已启用旧合规性的现有存储分段置于合法保留状态。
- 取消合法保留。

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" 有关说明，请参见。

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。

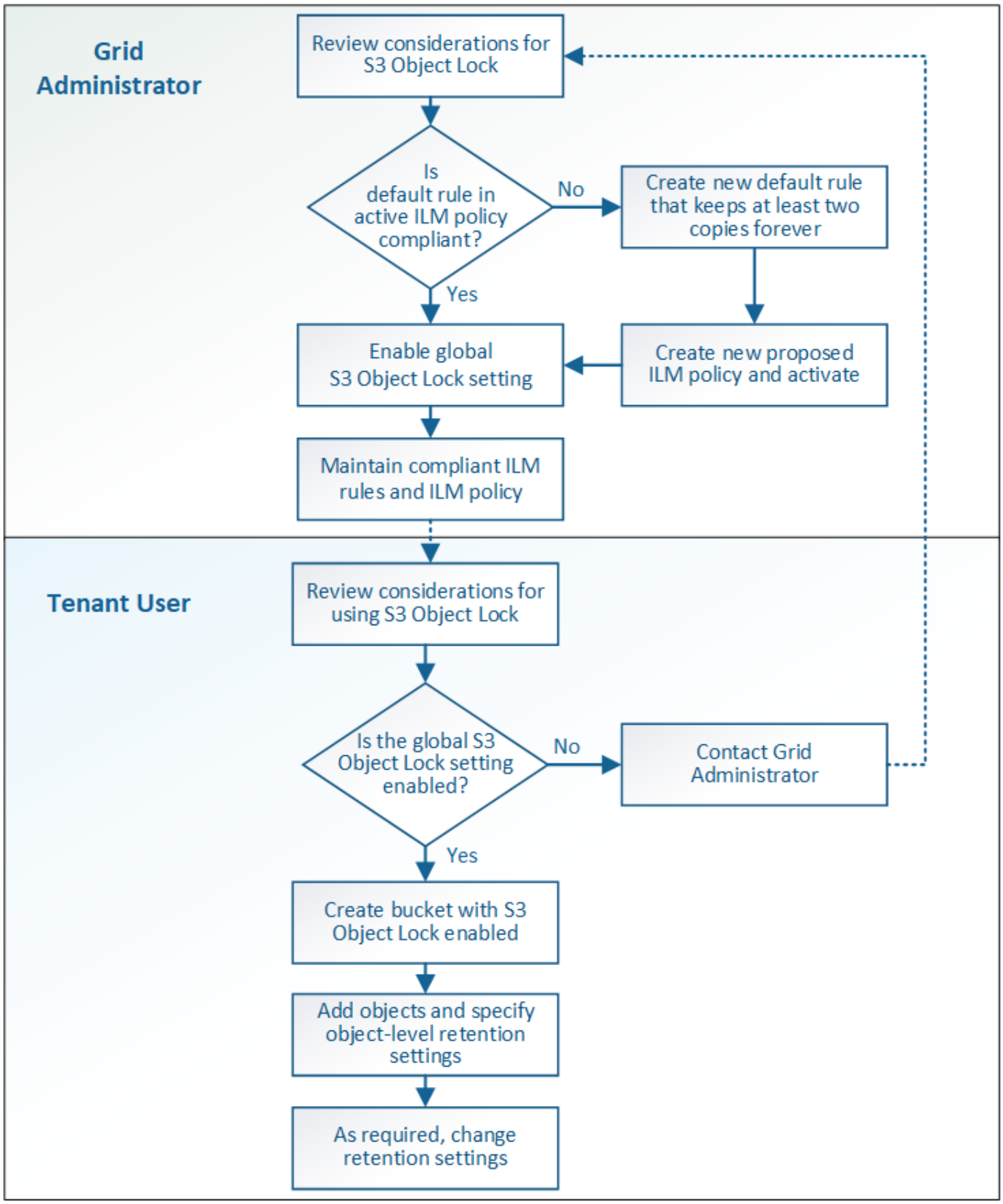
	S3 对象锁定（新增）	合规性（原有）
如何全局启用此功能?	在网格管理器中，选择 * 配置 * > * 系统 * > * S3 对象锁定 * 。	不再支持。 • 注意： * 如果您使用早期版本的 StorageGRID 启用了全局合规性设置，则在 StorageGRID 11.6 中将启用 S3 对象锁定设置。您可以继续使用 StorageGRID 管理现有合规存储分段的设置；但是，您无法创建新的合规存储分段。
如何为存储分段启用此功能?	在使用租户管理器，租户管理 API 或 S3 REST API 创建新存储分段时，用户必须启用 S3 对象锁定。	用户无法再在启用了合规性的情况下创建新的存储分段；但是，他们可以继续向现有合规存储分段添加新对象。
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。	否原有的合规性功能不允许分段版本控制。
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。	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。

	S3 对象锁定（新增）	合规性（原有）
存储分段是否具有保留和合法保留的默认设置？	是的。启用了 S3 对象锁定的 StorageGRID 存储分段可以具有一个默认保留期限，此保留期限将应用于在载入期间未指定其自己保留设置的对象版本。	是的。
是否可以更改保留期限？	对象版本的保留日期可以增加，但不能减少。	存储分段的保留期限可以增加，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？	如果对象未处于合法保留状态，则可以在达到保留截止日期后删除该对象版本。	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. 至少创建一个合规的 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. 指定存储分段的默认保留设置，这些设置将应用于添加到存储分段中但未指定其自身保留设置的对象。
3. 向这些存储分段添加对象，并指定对象级别的保留期限和合法保留设置。
4. 根据需要更新单个对象的保留期限或更改合法保留设置。

相关信息

- 使用租户帐户
- 使用 S3
- 使用 S3 对象锁定默认存储分段保留

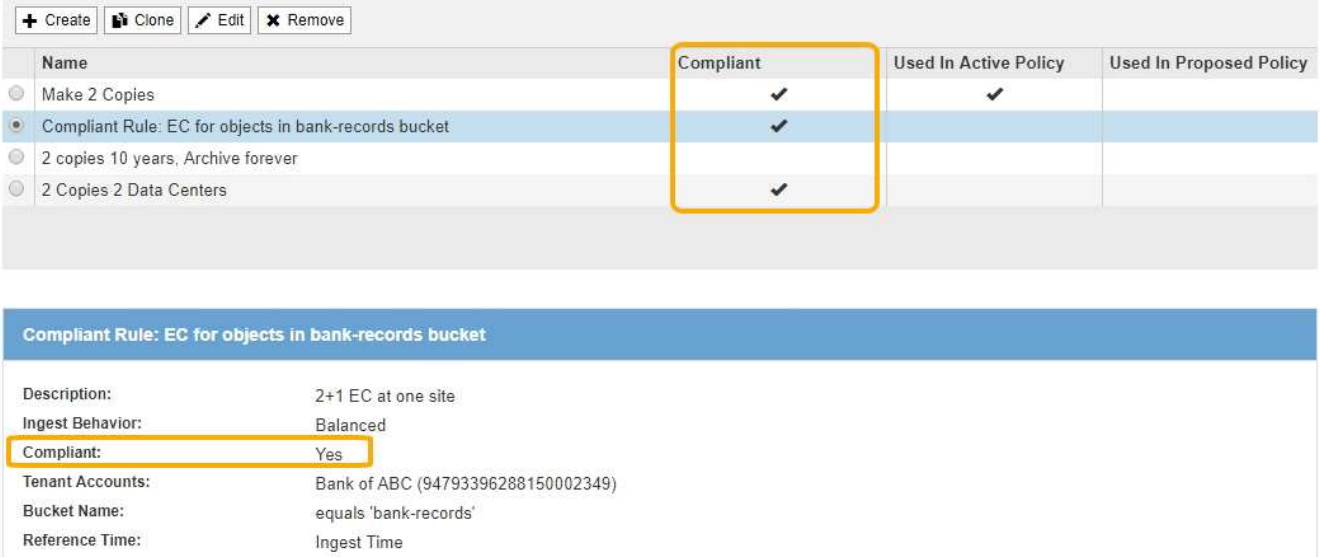
S3 对象锁定的要求

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，您将无法禁用此设置。
- 除非活动 ILM 策略中的默认规则为 *compliant* （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，除非策略中的默认规则合规，否则您无法创建新的建议 ILM 策略或激活现有建议的 ILM 策略。启用全局 S3 对象锁定设置后， "ILM 规则 " 和 "ILM 策略 " 页面将指示符合哪些 ILM 规则。

  在以下示例中， "ILM 规则 " 页面列出了与启用了 S3 对象锁定的存储分段兼容的三个规则。

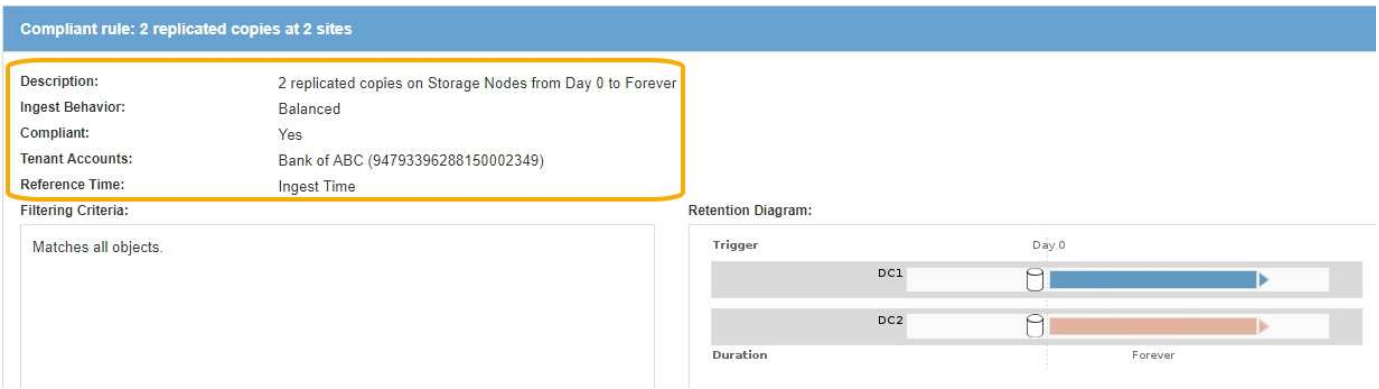


符合 ILM 规则的要求

如果要启用全局 S3 对象锁定设置，必须确保活动 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。
- 对象副本无法保存在云存储池中。
- 无法将对象副本保存在归档节点上。
- 放置说明中至少有一行必须从第 0 天开始，并使用 * 载入时间 * 作为参考时间。
- 放置说明中至少一行必须为 "`forever 。` "

例如，此规则满足启用了 S3 对象锁定的分段的要求。它会存储从载入时间（第 0 天）到 "`Forever " 的两个复制对象副本。` 这些对象将存储在两个数据中心的存储节点上。



活动的和建议的 ILM 策略的要求

启用全局 S3 对象锁定设置后，活动和建议的 ILM 策略可以同时包含合规和不合规的规则。

- 活动 ILM 策略或任何建议 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。

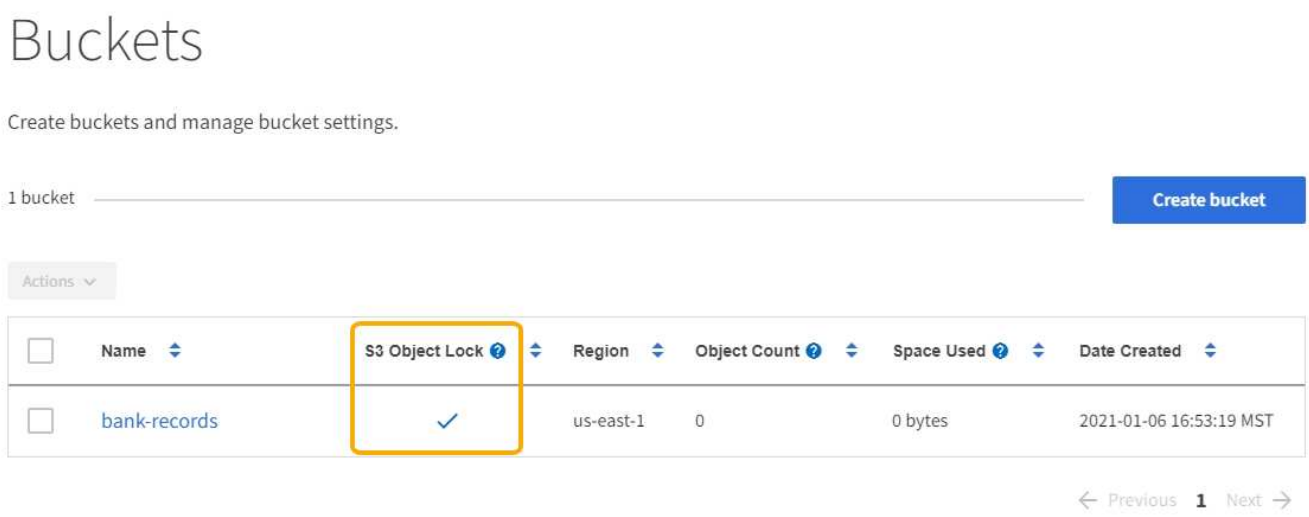
合规的 ILM 策略可能包括以下三个规则：

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。

  此租户管理器示例显示了一个已启用 S3 对象锁定的存储分段。



- 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。
- S3 对象锁定需要分段版本。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。
- 在启用了 S3 对象锁定的情况下创建存储分段后，无法禁用 S3 对象锁定或暂停该存储分段的版本控制。
- 您也可以为存储分段配置默认保留。上传对象版本时，默认保留将应用于对象版本。您可以通过在上传对象版本的请求中指定保留模式和保留至日期来覆盖存储分段默认值。
- S3 对象生命周期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， S3 客户端应用程序必须配置存储分段默认保留，或者在每个上传请求中指定保留设置。
- 您可以增加对象版本的保留截止日期，但不能减小此值。
- 如果您收到有关待定法律诉讼或监管调查的通知，则可以通过对对象版本进行法律保留来保留相关信息。如果对象版本处于合法保留状态，则无法从 StorageGRID 中删除该对象，即使该对象已达到保留日期。一旦取消合法保留，如果已达到保留日期，则可以删除对象版本。
- S3 对象锁定需要使用版本控制的分段。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

保存在启用了 S3 对象锁定的存储分段中的每个对象将经历三个阶段：

1. * 对象载入 *
   - 在启用了 S3 对象锁定的情况下向存储分段添加对象版本时， S3 客户端应用程序可以使用默认存储分段保留设置，也可以指定对象的保留设置（保留至日期，合法保留或两者）。然后， StorageGRID 会为此对象生成元数据，其中包括唯一对象标识符（ UUID ）以及载入日期和时间。
   - 载入具有保留设置的对象版本后，将无法修改其数据和 S3 用户定义的元数据。
   - StorageGRID 存储的对象元数据与对象数据无关。它会为每个站点上的所有对象元数据维护三个副本。
2. * 对象保留 *
   - StorageGRID 会存储该对象的多个副本。副本的确切数量和类型以及存储位置取决于活动 ILM 策略中的合规规则。
3. * 对象删除 *
   - 达到保留截止日期后，可以删除对象。
   - 无法删除处于合法保留状态的对象。

相关信息

- 使用租户帐户
- 使用 S3
- 比较 S3 对象锁定与原有合规性
- 示例 7： S3 对象锁定的兼容 ILM 策略
- 查看审核日志
- 使用 S3 对象锁定默认存储分段保留。

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。

您需要的内容

- 您具有 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，必须了解注意事项。
- 活动 ILM 策略中的默认规则合规。
  - 创建默认 ILM 规则
  - 创建 ILM 策略

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，便无法将其禁用。

> 如果您使用先前版本的 StorageGRID 启用了全局合规性设置，则 StorageGRID 11.6 中会启用 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；但是，您无法创建新的合规存储分段。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。

   S3 Object Lock Settings

   Enable S3 Object Lock for your entire StorageGRID system if S3 tenant accounts need to satisfy regulatory compliance requirements when saving object data. After this setting is enabled, it cannot be disabled.

   S3 Object Lock

   Before enabling S3 Object Lock, you must ensure that the default rule in the active ILM policy is compliant. A compliant rule satisfies the requirements of buckets with S3 Object Lock enabled.

   - It must create at least two replicated object copies or one erasure-coded copy.
   - These copies must exist on Storage Nodes for the entire duration of each line in the placement instructions.
   - Object copies cannot be saved on Archive Nodes.
   - At least one line of the placement instructions must start at day 0, using Ingest Time as the reference time.
   - At least one line of the placement instructions must be "forever".

   ☐ Enable S3 Object Lock

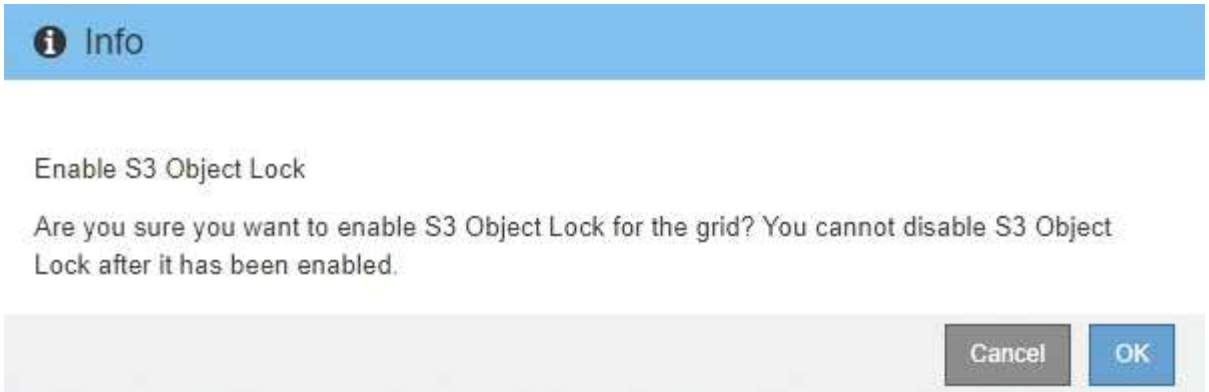
   Apply

   如果您已使用先前版本的 StorageGRID 启用了全局合规性设置，则此页面将包含以下注意事项：

   The S3 Object Lock setting replaces the legacy Compliance setting. When this setting is enabled, tenant users can create buckets with S3 Object Lock enabled. Tenants who previously created buckets for the legacy Compliance feature can manage their existing buckets, but can no longer create new buckets with legacy Compliance enabled. See Managing objects with information lifecycle management for information.

2. 选择 * 启用 S3 对象锁定 * 。
3. 选择 * 应用 * 。

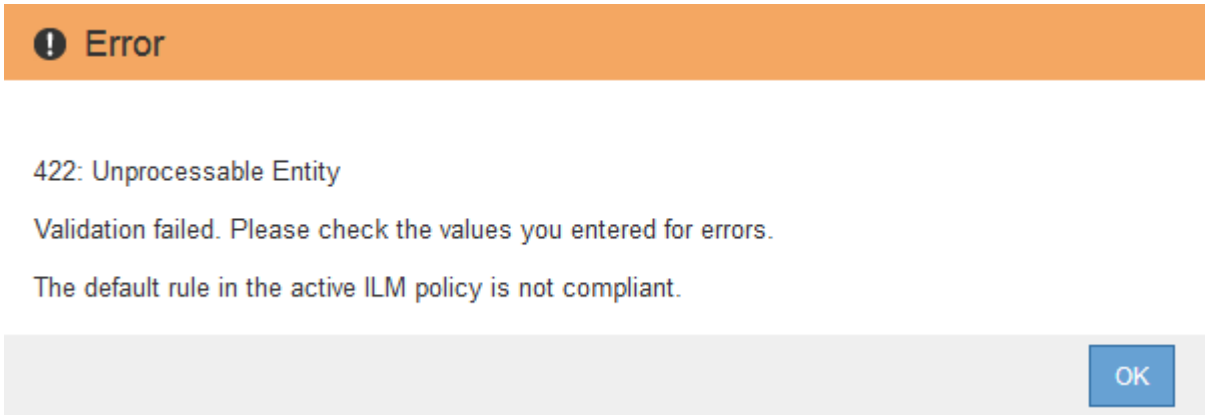
   此时将显示一个确认对话框，提醒您在启用 S3 对象锁定后无法禁用它。



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，则现在将为整个网格启用 S3 对象锁定，并且无法禁用。
   - 如果默认规则不符合要求，则会显示一个错误，指示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 * 确定 * ，然后创建新的建议策略，对其进行模拟并激活。



完成后

启用全局 S3 对象锁定设置后，您可能需要执行此操作 创建默认规则 合规和 创建 ILM 策略 合规。启用此设置后， ILM 策略可以选择同时包含合规的默认规则和不合规的默认规则。例如，您可能希望使用一个不合规规则，该规则不会筛选未启用 S3 对象锁定的分段中的对象。

相关信息

- 比较 S3 对象锁定与原有合规性

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

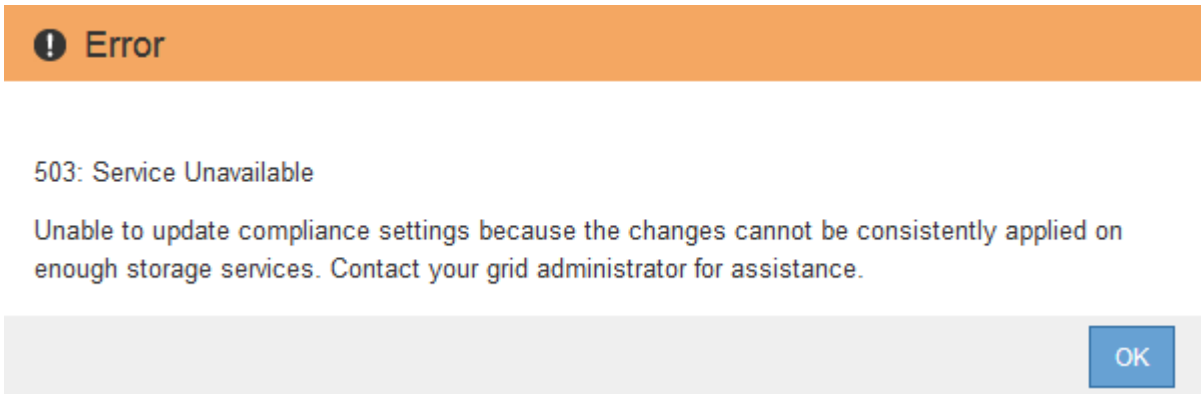
如果一个站点上的一个数据中心站点或多个存储节点不可用，您可能需要帮助 S3 租户用户对 S3 对象锁定或原有合规性配置进行更改。

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。如果系统由于数据中心站点或多个存储节点不可用而无法更新元数据，则会显示一条错误消息。具体

而言：

- 租户管理器用户会看到以下错误消息：



- 租户管理 API 用户和 S3 API 用户收到响应代码 `503 Service unavailable` 并显示类似的消息文本。

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
- 恢复和维护