使用S3物件鎖定搭配ILM

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-116/ilm/managing-objects-with-s3-object-lock.html on April 10, 2024. Always check docs.netapp.com for the latest.

目錄

使用S3物件鎖定搭配ILM

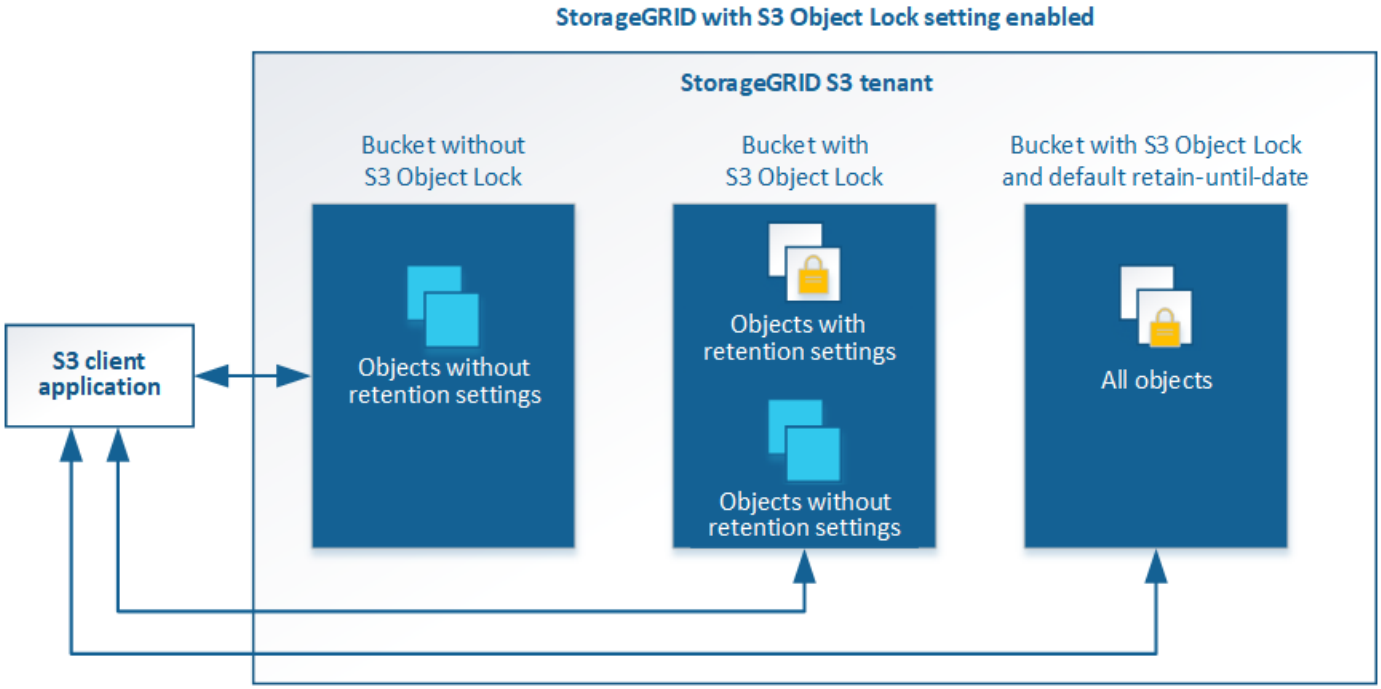
使用S3物件鎖定來管理物件

身為網格管理員、您可以為StorageGRID 您的系統啟用S3物件鎖定、並實作符合法規的ILM原則、以確保特定S3儲存區中的物件在指定時間內不會被刪除或覆寫。

什麼是S3物件鎖定？

「物件鎖定」功能是物件保護解決方案、StorageGRID 相當於Amazon Simple Storage Service（Amazon S3）中的S3物件鎖定。

如圖所示、當啟用StorageGRID 全域S3物件鎖定設定以供支援某個功能時、S3租戶帳戶可以建立啟用或不啟用S3物件鎖定的儲存區。如果某個儲存區已啟用S3物件鎖定、則S3用戶端應用程式可選擇性地指定該儲存區中任何物件版本的保留設定。物件版本必須具有指定的保留設定、才能受到S3物件鎖定的保護。此外、啟用S3物件鎖定的每個儲存區都可以選擇預設保留模式和保留期間、如果在儲存區中新增物件而不使用其本身的保留設定、則會套用此保留期間。



「S3物件鎖定」StorageGRID 功能提供單一保留模式、相當於Amazon S3法規遵循模式。依預設、受保護的物件版本無法由任何使用者覆寫或刪除。「S3物件鎖定」StorageGRID 功能不支援管理模式、也不允許具有特殊權限的使用者略過保留設定或刪除受保護的物件。

如果某個儲存區已啟用S3物件鎖定、則S3用戶端應用程式可在建立或更新物件時、選擇性地指定下列任一或兩個物件層級保留設定：

- 保留截止日期：如果物件版本的保留截止日期在未來、則可擷取物件、但無法修改或刪除。視需要可增加物件的保留截止日期、但此日期不可減少。
- 合法持有：將合法持有套用至物件版本、會立即鎖定該物件。例如、您可能需要對與調查或法律爭議相關的物件保留法律。合法持有沒有到期日、但在明確移除之前、仍會保留到位。合法持有不受保留至日期的限制。

如需物件保留設定的詳細資訊、請前往 使用S3物件鎖定。

如需預設庫位保留設定的詳細資訊、請前往 使用S3物件鎖定預設儲存區保留。

比較S3物件鎖定與舊版法規遵循

S3物件鎖定取代舊StorageGRID 版的Compliance功能。由於S3物件鎖定功能符合Amazon S3的要求、因此它取代了專屬StorageGRID 的「不符合要求」功能、這項功能現在稱為「舊有法規遵循」。

如果您先前已啟用「全域符合性」設定、則會自動啟用「全域S3物件鎖定」設定。租戶使用者不再能夠在啟用「法規遵循」的情況下建立新的儲存庫、不過、根據需求、租戶使用者可以繼續使用及管理任何現有的符合舊規範的儲存庫、包括執行下列工作：

- 將新物件加入已啟用舊版法規遵循的現有儲存區。
- 延長已啟用舊版法規遵循的現有儲存庫的保留期間。
- 變更已啟用舊版法規遵循的現有儲存區的自動刪除設定。
- 合法持有已啟用舊版法規遵循的現有儲存庫。
- 解除合法持有。

請參閱 "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章" 以取得相關指示。

如果您使用StorageGRID 舊版的更新版本的支援功能、請參閱下表、瞭解其與StorageGRID 更新版本中S3物件鎖定功能的比較。

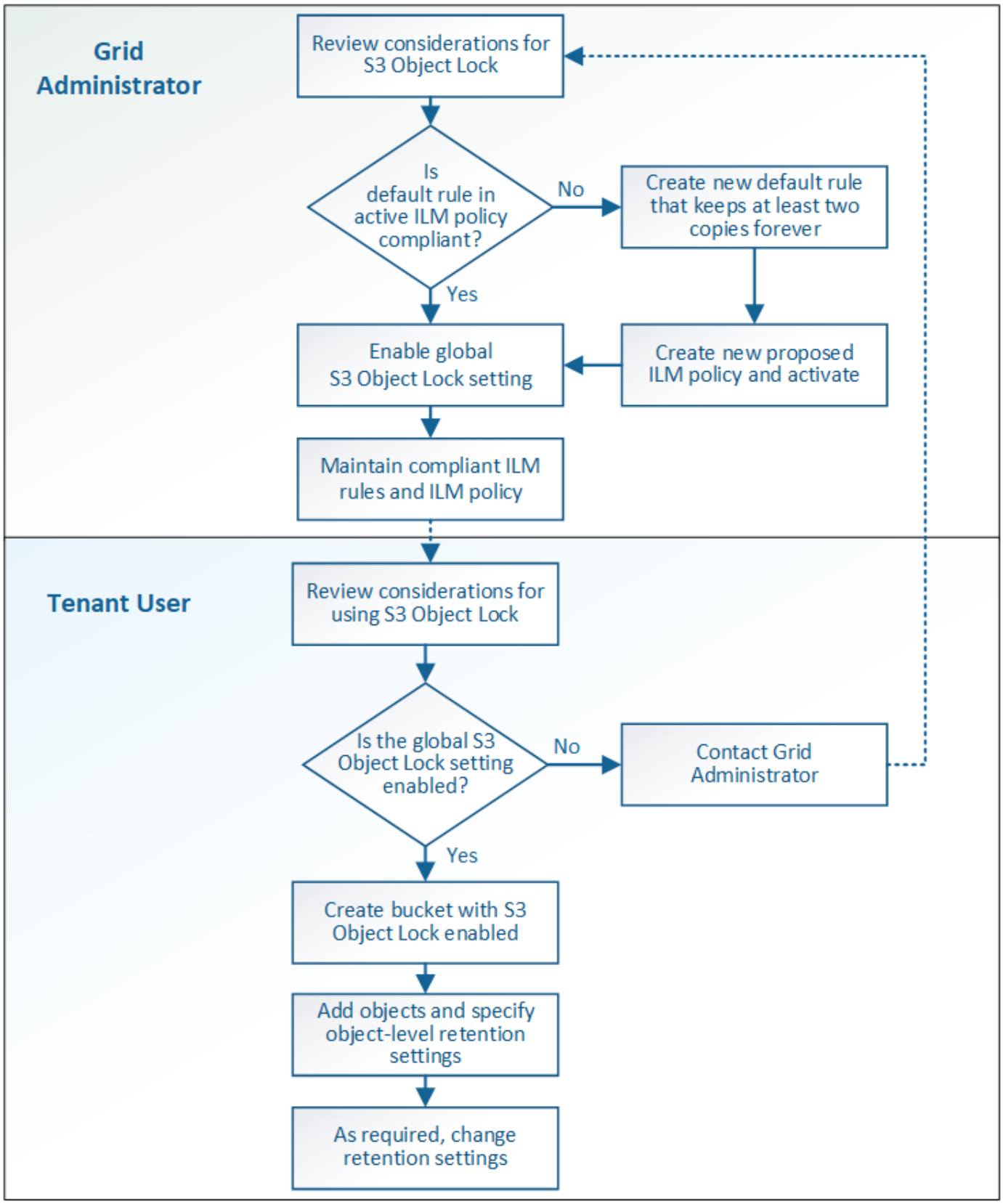
	S3物件鎖定（新增）	法規遵循（舊版）
如何在全域啟用此功能？	從Grid Manager中選擇*組態*>*系統*>* S3物件鎖定*。	不再支援。 *注意：*如果您使用舊版StorageGRID 的支援功能來啟用「全域法規遵循」設定、StorageGRID 則「S3物件鎖定」設定會在「支援支援功能」中啟用。您可以繼續使用StorageGRID 效益管理功能來管理現有的相容庫位設定、但您無法建立新的相容庫位。
此功能如何啟用儲存庫？	使用者必須啟用S3物件鎖定、才能使用租戶管理程式、租戶管理API或S3 REST API建立新的儲存區。	使用者無法再建立已啟用「符合性」的新儲存區、但仍可繼續將新物件新增至現有的「符合性」儲存區。
是否支援儲存區版本管理？	是的。儲存區版本設定是必要的、且會在啟用儲存區的S3物件鎖定時自動啟用。	不可以舊版法規遵循功能不允許庫位版本管理。

	S3物件鎖定（新增）	法規遵循（舊版）
如何設定物件保留？	使用者可以為每個物件版本設定保留截止日期。	使用者必須為整個儲存庫設定保留期間。保留期間適用於貯體中的所有物件。
桶是否有保留和合法持有的預設設定？	是的。啟用S3物件鎖定的各個區段可以有預設保留期間、套用至物件版本、而物件版本在擷取期間並未指定其保留設定。StorageGRID	是的
保留期間可以變更嗎？	物件版本的保留截止日期可以增加、但不會減少。	可延長庫位的保留期間、但不會縮短。
合法持有控制在哪裡？	使用者可以合法持有或撤銷貯體中任何物件版本的合法持有。	合法持有會置於貯體上、並影響貯體中的所有物件。
何時可以刪除物件？	物件版本可在達到保留截止日期後刪除、前提是物件未處於合法持有狀態。	保留期間到期後、如果儲存區未處於合法保留狀態、則可刪除物件。物件可以自動或手動刪除。
是否支援庫位生命週期組態？	是的	否

S3物件鎖定的工作流程

身為網格管理員、您必須與租戶使用者密切協調、以確保物件受到保護、並符合其保留需求。

工作流程圖顯示使用S3物件鎖定的高階步驟。這些步驟由網格管理員和租戶使用者執行。



網格管理工作

如工作流程圖所示、網格管理員必須先執行兩項高層級工作、S3租戶使用者才能使用S3物件鎖定：

1. 建立至少一個相容的ILM規則、並將該規則設為作用中ILM原則中的預設規則。

2. 為整個StorageGRID 支援系統啟用全域S3物件鎖定設定。

租戶使用者工作

啟用全域S3物件鎖定設定之後、租戶即可執行下列工作：

1. 建立啟用S3物件鎖定的儲存區。
2. 指定儲存區的預設保留設定、套用至新增至儲存區但未指定其本身保留設定的物件。
3. 將物件新增至這些儲存區、並指定物件層級的保留期間和合法的保留設定。
4. 視需要更新保留期間、或變更個別物件的合法保留設定。

相關資訊

- 使用租戶帳戶
- 使用S3
- 使用S3物件鎖定預設儲存區保留

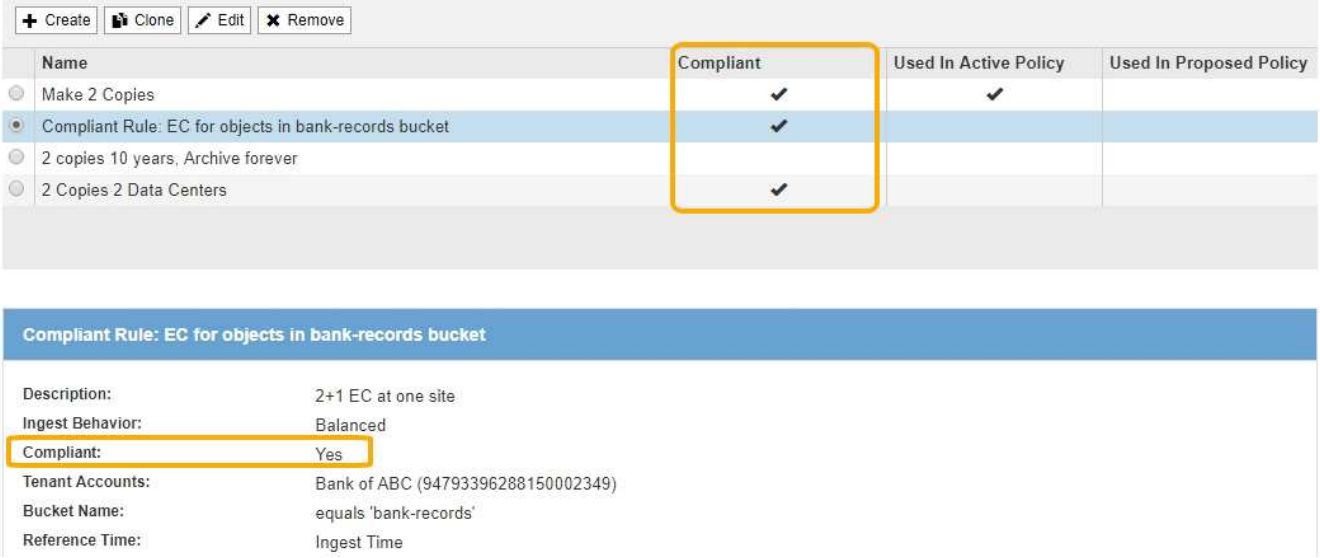
S3物件鎖定需求

您必須檢閱啟用全域S3物件鎖定設定的需求、建立相容ILM規則和ILM原則的需求、StorageGRID 以及使用S3物件鎖定之貯體和物件的限制等資訊。

使用全域S3物件鎖定設定的需求

- 您必須先使用Grid Manager或Grid Management API啟用全域S3物件鎖定設定、任何S3租戶才能建立啟用S3物件鎖定的儲存區。
- 啟用全域S3物件鎖定設定可讓所有S3租戶帳戶建立啟用S3物件鎖定的儲存區。
- 啟用全域S3物件鎖定設定之後、就無法停用此設定。
- 除非作用中ILM原則中的預設規則為_Compliance（也就是、預設規則必須符合啟用S3物件鎖定的儲存區需求）、否則您無法啟用全域S3物件鎖定。
- 啟用全域S3物件鎖定設定時、除非原則中的預設規則相容、否則您無法建立新的建議ILM原則或啟動現有的建議ILM原則。啟用全域S3物件鎖定設定之後、「ILM規則」和「ILM原則」頁面會指出哪些ILM規則符合規定。

  在下列範例中、「ILM規則」頁面列出三個規則、這些規則均符合啟用S3物件鎖定的儲存區。

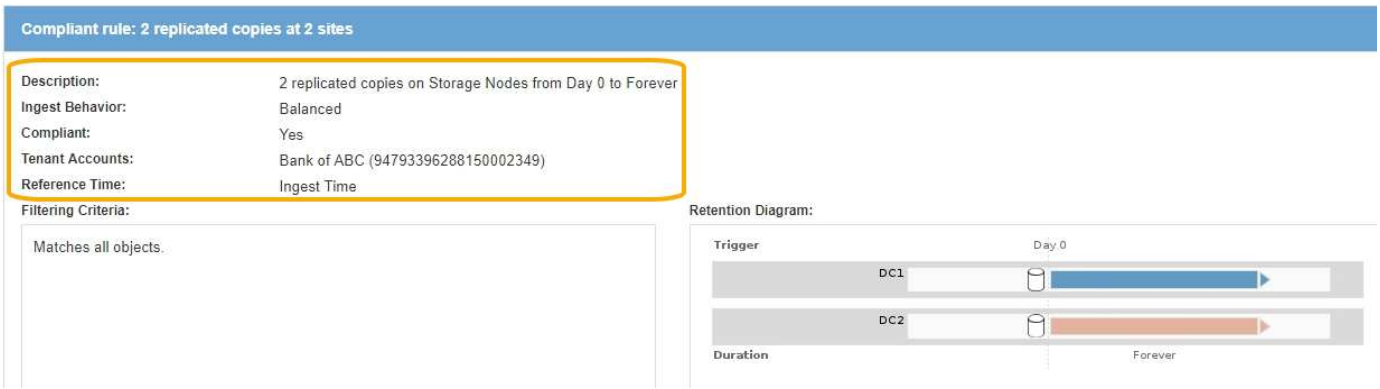


符合ILM規則的要求

如果您要啟用全域S3物件鎖定設定、必須確保使用中ILM原則中的預設規則符合規定。相容的規則可同時滿足啟用S3物件鎖定的兩個儲存區需求、以及啟用舊版法規遵循的任何現有儲存區：

- 它必須建立至少兩個複寫的物件複本、或一個銷毀編碼複本。
- 這些複本必須存在於儲存節點上、且必須在放置說明中的每一行的整個期間內存在。
- 物件複本無法儲存在雲端儲存資源池中。
- 物件複本無法儲存在歸檔節點上。
- 至少一行的放置說明必須從第0天開始、使用*擷取時間*作為參考時間。
- 至少一行的放置說明必須是「永遠」。

例如、此規則可滿足啟用S3物件鎖定的儲存區需求。它儲存兩個複寫的物件複本、從擷取時間（第0天）到「永遠」。 物件將儲存在兩個資料中心的儲存節點上。



主動式與建議的ILM原則需求

當全域S3物件鎖定設定已啟用時、作用中和建議的ILM原則可以同時包含相容和不相容的規則。

- 作用中或任何建議的ILM原則中的預設規則必須符合規定。

- 不符合規定的規則僅適用於未啟用S3物件鎖定或未啟用舊版符合性功能的儲存區中的物件。
- 符合法規的規則可套用至任何儲存區中的物件；不需要為儲存區啟用S3物件鎖定或舊版符合法規。

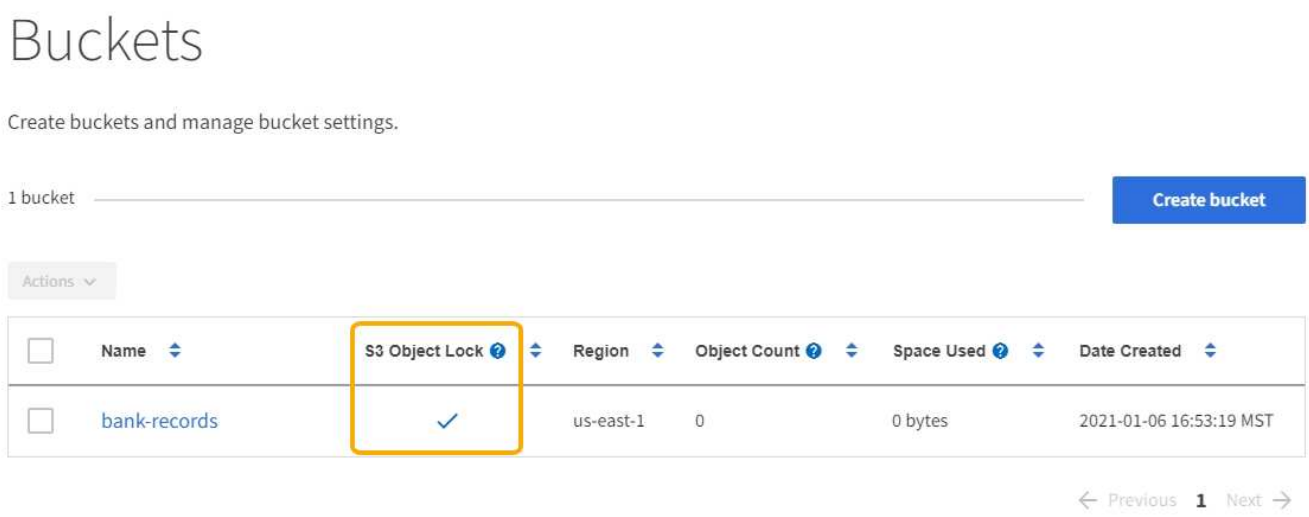
符合法規的ILM原則可能包括下列三項規則：

1. 一種相容規則、可在啟用S3物件鎖定的情況下、在特定儲存區中建立物件的銷毀編碼複本。EC複本會從第0天儲存在儲存節點上、直到永遠儲存在儲存節點上。
2. 不符合規定的規則、會在儲存節點上建立一年的兩個複寫物件複本、然後將一個物件複本移至「歸檔節點」、並永久儲存該複本。此規則僅適用於未啟用S3物件鎖定或舊版法規遵循的儲存區、因為它只會永久儲存一個物件複本、而且會使用歸檔節點。
3. 這是一種預設且符合法規的規則、可在儲存節點上建立兩個複寫的物件複本、從第0天到永遠。此規則適用於前兩個規則未篩選的任何儲存區中的任何物件。

啟用S3物件鎖定的儲存區需求

- 如果StorageGRID 已針對整個S3物件鎖定設定啟用for the S廳 系統、您可以使用租戶管理程式、租戶管理API或S3 REST API來建立啟用S3物件鎖定的儲存區。

  此租戶管理程式範例顯示已啟用S3物件鎖定的儲存區。



- 如果您打算使用S3物件鎖定、則必須在建立儲存區時啟用S3物件鎖定。您無法為現有的儲存區啟用S3物件鎖定。
- S3物件鎖定需要庫位版本管理。當「S3物件鎖定」已啟用時、StorageGRID 即可自動啟用該儲存區的版本管理功能。
- 在建立啟用S3物件鎖定的儲存區之後、您無法停用該儲存區的S3物件鎖定或暫停版本管理。
- 您也可以設定儲存區的預設保留。上傳物件版本時、預設保留會套用至物件版本。您可以指定保留模式來覆寫儲存區預設值、並在上傳物件版本的要求中保留截止日期。
- S3物件生命週期儲存區支援儲存區生命週期組態。
- 啟用S3物件鎖定的儲存區不支援CloudMirror複寫。

啟用S3物件鎖定之儲存區中的物件需求

- 為了保護物件版本、S3用戶端應用程式必須設定儲存區預設保留、或在每個上傳要求中指定保留設定。
- 您可以增加物件版本的保留截止日期、但絕不能減少此值。
- 如果您收到尚待處理的法律行動或法規調查通知、您可以在物件版本上保留合法資訊、以保留相關資訊。當物件版本處於合法持有狀態時、即使StorageGRID 物件已達到保留日期、也無法從該物件刪除。一旦取消合法持有、如果已達到保留截止日期、就可以刪除物件版本。
- S3物件鎖定需要使用版本控制的儲存區。保留設定適用於個別物件版本。物件版本可以同時具有「保留直到日期」和「合法保留」設定、但不能有另一個設定、或兩者都沒有。指定物件的保留截止日期或合法保留設定、只會保護要求中指定的版本。您可以建立物件的新版本、而舊版物件仍會保持鎖定狀態。

啟用S3物件鎖定的儲存區物件生命週期

儲存在已啟用S3物件鎖定的儲存區中的每個物件都會經過三個階段：

1. 物件擷取
   - 在啟用S3物件鎖定的情況下、將物件版本新增至儲存區時、S3用戶端應用程式可以使用預設的儲存區保留設定、或是選擇性地指定物件的保留設定（保留至日期、合法保留或兩者皆保留）。接著、將產生該物件的中繼資料、其中包括唯一的物件識別碼（UUID）和擷取日期與時間。StorageGRID
   - 擷取具有保留設定的物件版本之後、就無法修改其資料和S3使用者定義的中繼資料。
   - 不受物件資料限制、可獨立儲存物件中繼資料。StorageGRID它會在每個站台維護三份所有物件中繼資料複本。
2. 物件保留
   - 物件的多個複本是StorageGRID 由NetApp儲存的。複本的確切數量和類型、以及儲存位置、取決於使用中ILM原則中的相容規則。
3. 物件刪除
   - 物件到達保留截止日期時、即可刪除。
   - 無法刪除合法持有的物件。

相關資訊

- 使用租戶帳戶
- 使用S3
- 比較S3物件鎖定與舊版法規遵循
- 範例7：S3物件鎖定的符合ILM原則
- 檢閱稽核記錄
- 使用S3物件鎖定預設儲存區保留。

全域啟用S3物件鎖定

如果S3租戶帳戶在儲存物件資料時需要遵守法規要求、您必須為整個StorageGRID 整個整個系統啟用S3物件鎖定。啟用全域S3物件鎖定設定、可讓任何S3租戶使用者使用S3物件鎖定來建立及管理儲存區和物件。

您需要的產品

- 您擁有root存取權限。
- 您將使用登入Grid Manager 支援的網頁瀏覽器。
- 您已檢閱S3物件鎖定工作流程、而且必須瞭解考量事項。
- 作用中ILM原則中的預設規則相容。
  - 建立預設ILM規則
  - 建立ILM原則

關於這項工作

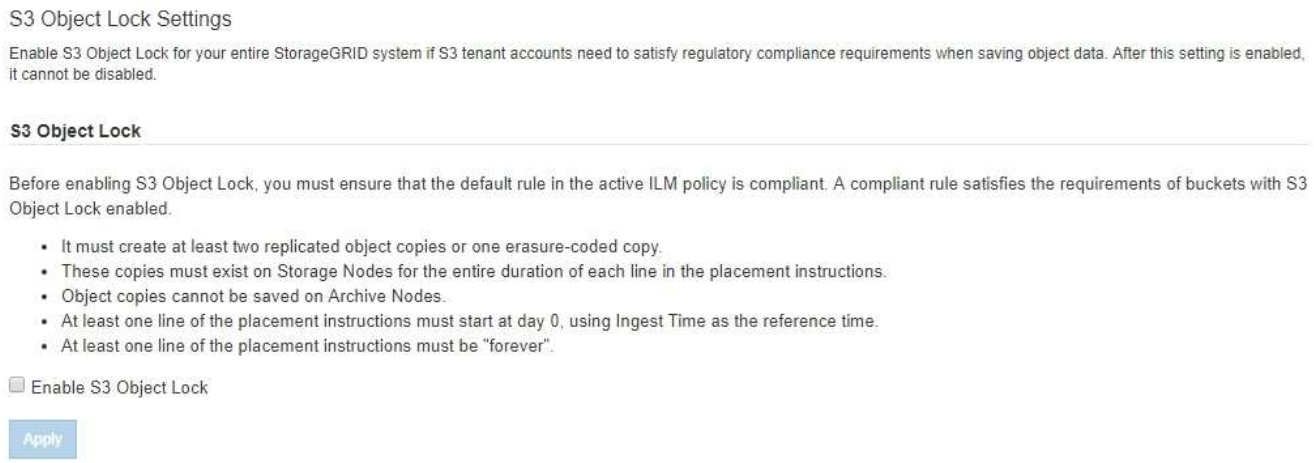
網格管理員必須啟用全域S3物件鎖定設定、才能讓租戶使用者建立啟用S3物件鎖定的新儲存區。啟用此設定之後、就無法停用。

> 如果您使用舊版StorageGRID 的支援功能啟用全域規範設定、StorageGRID 則S3物件鎖定設定會在支援功能11.6.您可以繼續使用StorageGRID 效益管理功能來管理現有的相容庫位設定、但您無法建立新的相容庫位。請參閱 "NetApp知識庫：如何管理StorageGRID 支援老舊的知識庫、請參閱《知識庫文章"。

步驟

1. 選擇*組態*>*系統*>* S3物件鎖定*。

   「S3物件鎖定設定」頁面隨即出現。

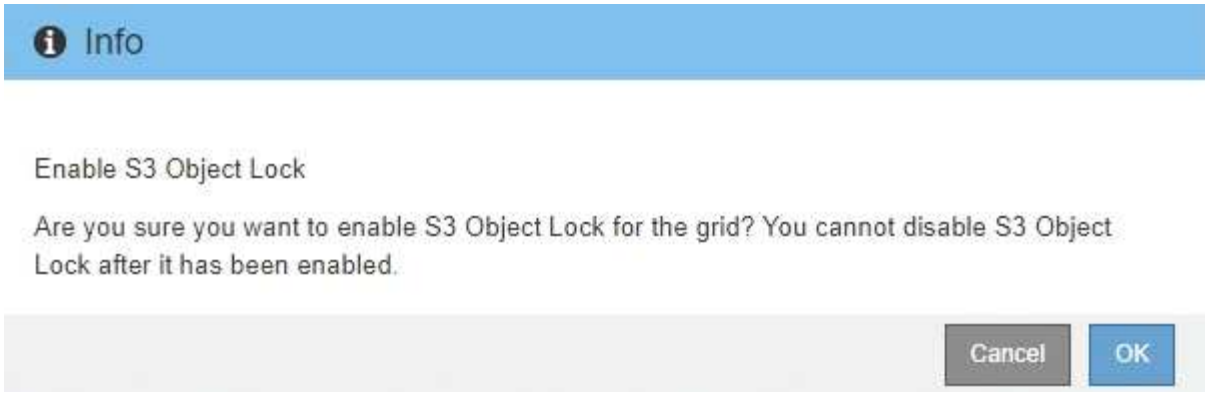
   

   如果您已使用舊版StorageGRID 的支援功能啟用「全球法規遵循」設定、則頁面會包含下列附註：

   > 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. 選取*啟用S3物件鎖定*。
3. 選擇*應用*。

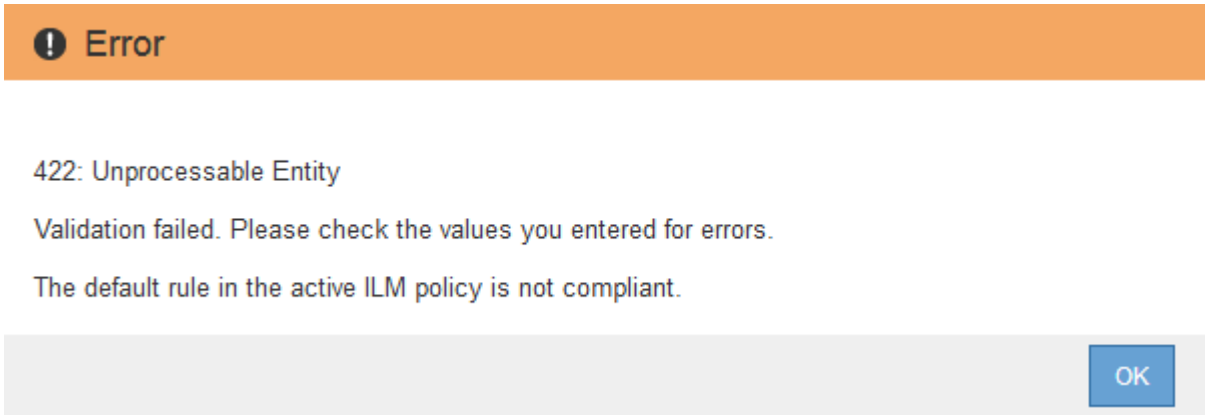
   此時會出現確認對話方塊、提醒您啟用S3物件鎖定後、將無法停用該對話方塊。



4. 如果確定要為整個系統永久啟用S3物件鎖定、請選取*確定*。

   當您選取*確定*時：

   - 如果作用中ILM原則中的預設規則相容、則「S3物件鎖定」現在會針對整個網格啟用、而且無法停用。
   - 如果預設規則不相容、則會出現錯誤、表示您必須建立並啟動新的ILM原則、其中包含以相容規則為預設規則的新ILM原則。選取*確定*、然後建立新的建議原則、加以模擬並加以啟動。



完成後

啟用全域S3物件鎖定設定之後、您可能需要 建立預設規則 這是符合法規的且 建立ILM原則 這是符合法規的。啟用此設定之後、ILM原則可以選擇性地同時包含相容的預設規則和不相容的預設規則。例如、您可能想要使用不符合規定的規則、該規則不具備未啟用S3物件鎖定之儲存區中物件的篩選條件。

相關資訊

- 比較S3物件鎖定與舊版法規遵循

更新S3物件鎖定或舊版法規遵循組態時、可解決一致性錯誤

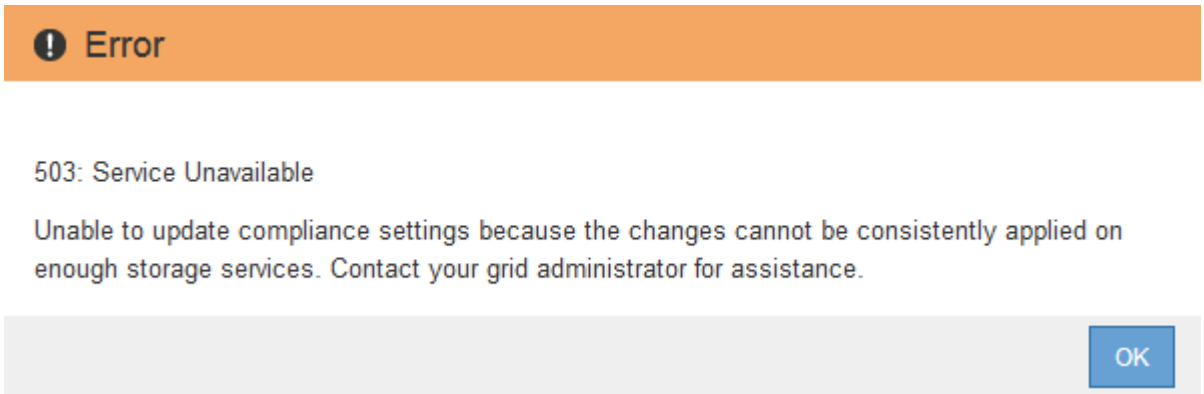
如果站台上的資料中心站台或多個儲存節點無法使用、您可能需要協助S3租戶使用者將變更套用至S3物件鎖定或舊版法規遵循組態。

已啟用S3物件鎖定（或舊版法規遵循）的租戶使用者、可以變更某些設定。例如、使用S3物件鎖定的租戶使用者可能需要將物件版本置於合法持有之下。

當租戶使用者更新S3儲存區或物件版本的設定時StorageGRID 、BIOS會嘗試立即更新整個網格的儲存區或物件中繼資料。如果系統因為資料中心站台或多個儲存節點無法使用而無法更新中繼資料、則會顯示錯誤訊息。具體

而言：

- 租戶管理程式使用者會看到下列錯誤訊息：



- 租戶管理API使用者和S3 API使用者會收到類似訊息文字的回應代碼「503 Service Unavailable」（503服務無法使用）。

若要解決此錯誤、請依照下列步驟操作：

1. 請儘快讓所有儲存節點或站台再次可用。
2. 如果您無法在每個站台上提供足夠的儲存節點、請聯絡技術支援部門、他們可以協助您恢復節點、並確保在整個網格中一致地套用變更。
3. 解決基礎問題之後、請提醒租戶使用者重試其組態變更。

相關資訊

- 使用租戶帳戶
- 使用S3
- 恢復與維護

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。