USA blocco oggetti S3 con ILM

StorageGRID

NetApp
October 03, 2025

Sommario

USA blocco oggetti S3 con ILM

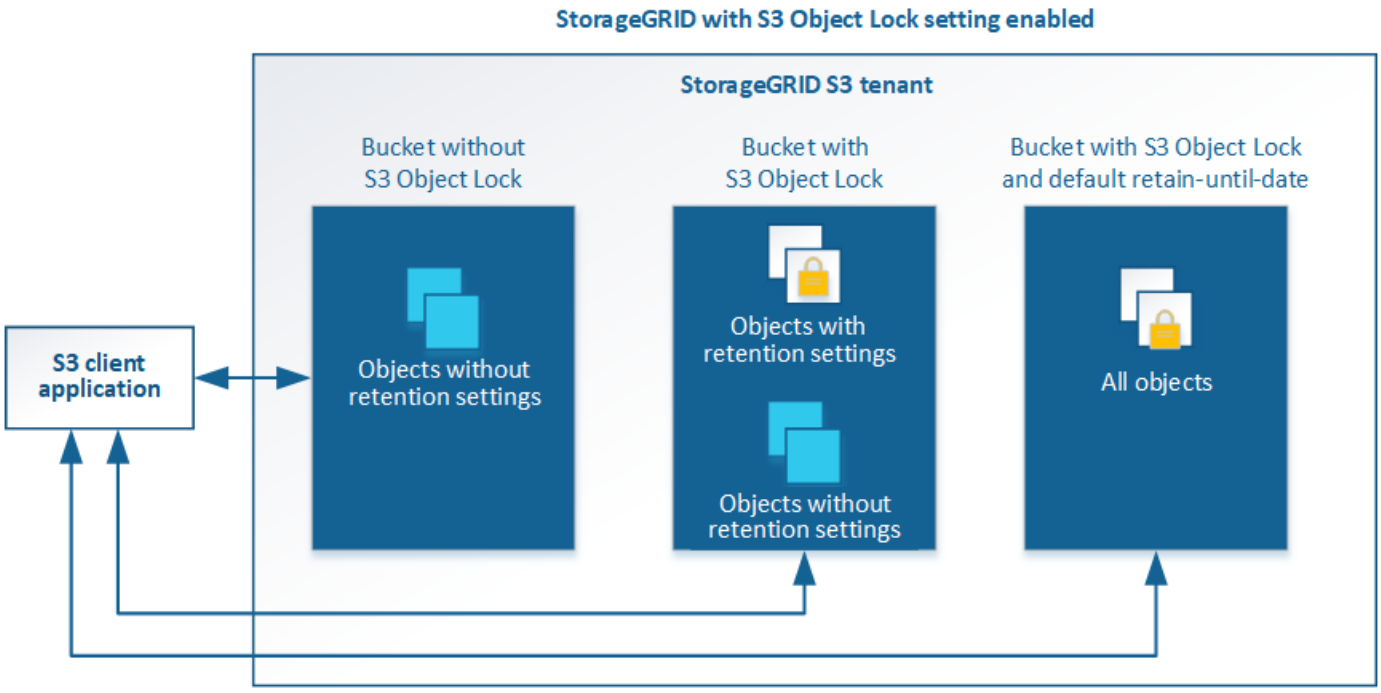
Gestire gli oggetti con S3 Object Lock

In qualità di amministratore di rete, è possibile attivare il blocco oggetti S3 per il sistema StorageGRID e implementare un criterio ILM conforme per garantire che gli oggetti in specifici bucket S3 non vengano cancellati o sovrascritti per un determinato periodo di tempo.

Che cos'è il blocco oggetti S3?

La funzione blocco oggetti StorageGRID S3 è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon Simple Storage Service (Amazon S3).

Come mostrato nella figura, quando l'impostazione globale S3 Object Lock è attivata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock attivato, le applicazioni client S3 possono specificare le impostazioni di conservazione per qualsiasi versione di oggetto in quel bucket. Una versione dell'oggetto deve avere le impostazioni di conservazione specificate per essere protetta da S3 Object Lock. Inoltre, ogni bucket con S3 Object Lock abilitato può disporre di una modalità di conservazione e di un periodo di conservazione predefiniti, che si applicano se gli oggetti vengono aggiunti al bucket senza le proprie impostazioni di conservazione.



La funzione blocco oggetto StorageGRID S3 offre una singola modalità di conservazione equivalente alla modalità di conformità Amazon S3. Per impostazione predefinita, una versione dell'oggetto protetto non può essere sovrascritta o eliminata da alcun utente. La funzione blocco oggetti di StorageGRID S3 non supporta una modalità di governance e non consente agli utenti con autorizzazioni speciali di ignorare le impostazioni di conservazione o di eliminare gli oggetti protetti.

Se in un bucket è attivato il blocco oggetti S3, l'applicazione client S3 può specificare una o entrambe le seguenti impostazioni di conservazione a livello di oggetto durante la creazione o l'aggiornamento di un oggetto:

- **Mantieni-fino-data**: Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. Come richiesto, è possibile aumentare la data di conservazione di un oggetto fino alla data odierna, ma non è possibile diminuarla.
- **Conservazione legale**: L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa. Le conservazioni legali sono indipendenti dalla conservazione fino alla data odierna.

Per ulteriori informazioni sulle impostazioni di conservazione degli oggetti, visitare il sito Web all'indirizzo USA blocco oggetti S3.

Per ulteriori informazioni sulle impostazioni predefinite di conservazione dei bucket, visitare il sito Web all'indirizzo USA la conservazione predefinita del bucket S3 Object Lock.

Confronto tra blocco oggetti S3 e conformità legacy

Il blocco oggetti S3 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Poiché la funzione blocco oggetti S3 è conforme ai requisiti di Amazon S3, la funzionalità proprietaria di conformità StorageGRID, ora denominata "conformità legacy".

Se in precedenza è stata attivata l'impostazione di conformità globale, l'impostazione di blocco oggetti S3 globale è stata attivata automaticamente. Gli utenti del tenant non sono più in grado di creare nuovi bucket con la conformità abilitata; tuttavia, secondo necessità, gli utenti del tenant possono continuare a utilizzare e gestire qualsiasi bucket compatibile esistente, che include l'esecuzione delle seguenti attività:

- Acquisizione di nuovi oggetti in un bucket esistente che ha abilitato la conformità legacy.
- Aumento del periodo di conservazione di un bucket esistente che ha abilitato la conformità legacy.
- Modifica dell'impostazione di eliminazione automatica per un bucket esistente che ha abilitato la compliance legacy.
- Mettere un blocco legale su un bucket esistente che ha abilitato la compliance legacy.
- Sollevare un blocco legale.

Vedere "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5" per istruzioni.

Se è stata utilizzata la funzionalità di conformità legacy in una versione precedente di StorageGRID, fare riferimento alla tabella seguente per informazioni sul confronto con la funzione blocco oggetti S3 di StorageGRID.

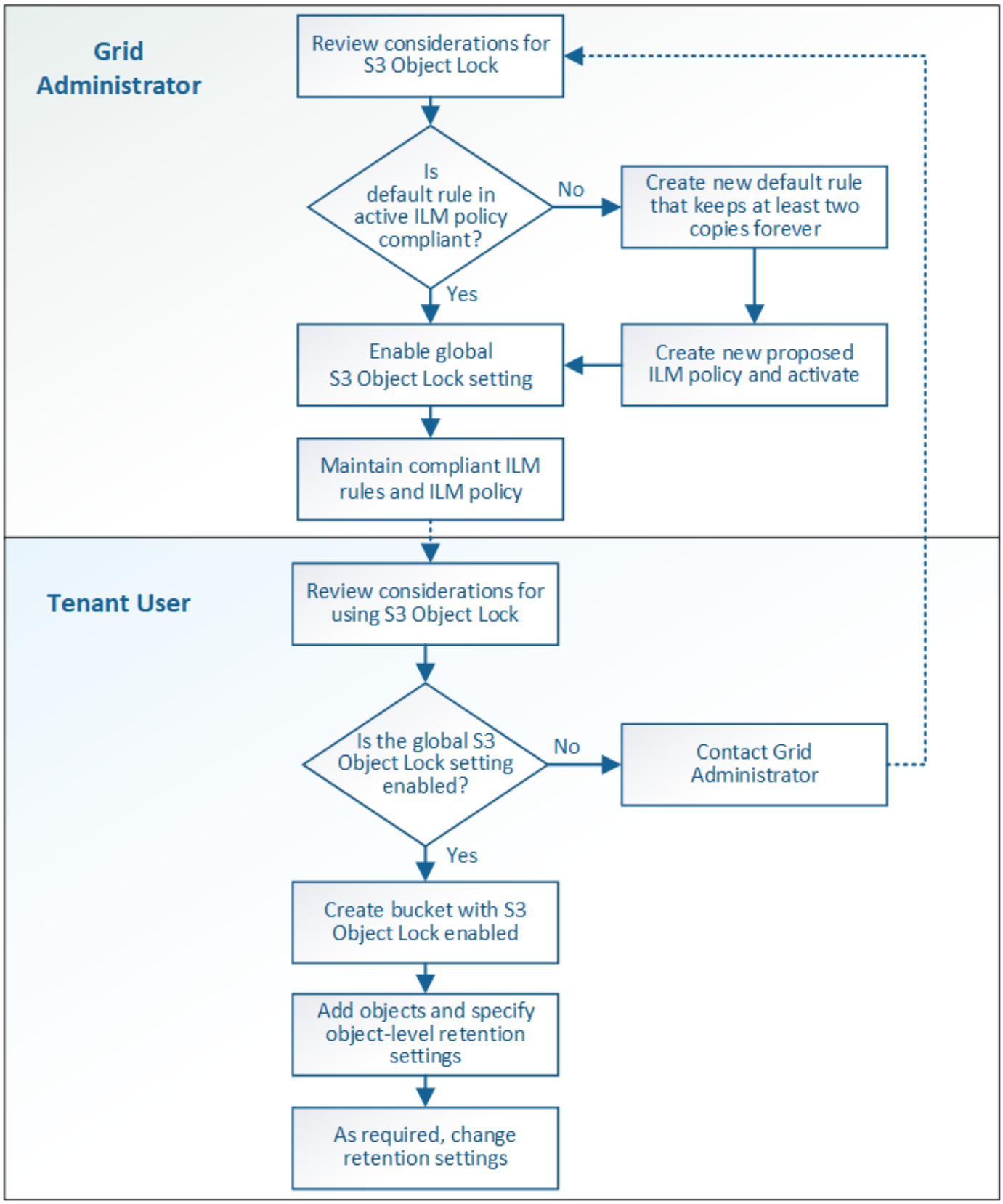
	Blocco oggetti S3 (nuovo)	Compliance (legacy)
In che modo la funzionalità è abilitata a livello globale?	Da Grid Manager, selezionare **CONFIGURATION** > **System** > **S3 Object Lock**.	Non più supportato. **Nota:** se è stata attivata l'impostazione di conformità globale utilizzando una versione precedente di StorageGRID, l'impostazione blocco oggetti S3 viene attivata in StorageGRID 11.6. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi.
In che modo è abilitata la funzione per un bucket?	Gli utenti devono attivare il blocco oggetti S3 quando creano un nuovo bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3.	Gli utenti non possono più creare nuovi bucket con la funzione Compliance abilitata; tuttavia, possono continuare ad aggiungere nuovi oggetti ai bucket Compliance esistenti.
La versione del bucket è supportata?	Sì. La versione del bucket è obbligatoria e viene attivata automaticamente quando il blocco oggetti S3 è attivato per il bucket.	No La funzionalità Compliance legacy non consente il controllo delle versioni del bucket.
Come viene impostata la conservazione degli oggetti?	Gli utenti possono impostare un periodo di conservazione fino alla data di scadenza per ciascuna versione dell'oggetto.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
Un bucket può avere impostazioni predefinite per la conservazione e la conservazione legale?	Sì. I bucket StorageGRID con blocco oggetti S3 attivato possono avere un periodo di conservazione predefinito che viene applicato alle versioni di oggetti che non hanno le proprie impostazioni di conservazione specificate durante l'acquisizione.	Sì
È possibile modificare il periodo di conservazione?	Il periodo di conservazione fino alla data di una versione a oggetti può essere aumentato ma non ridotto.	Il periodo di conservazione del bucket può essere aumentato ma non ridotto.
Dove viene controllata la conservazione legale?	Gli utenti possono porre un blocco legale o revocare un blocco legale per qualsiasi versione di oggetto nel bucket.	Un blocco legale viene posizionato sul bucket e influisce su tutti gli oggetti nel bucket.

	Blocco oggetti S3 (nuovo)	Compliance (legacy)
Quando è possibile eliminare gli oggetti?	Una versione dell'oggetto può essere eliminata dopo aver raggiunto la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale.	È possibile eliminare un oggetto dopo la scadenza del periodo di conservazione, presupponendo che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere cancellati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	No

Workflow per blocco oggetti S3

In qualità di amministratore della griglia, è necessario coordinare strettamente gli utenti tenant per garantire che gli oggetti siano protetti in modo da soddisfare i requisiti di conservazione.

Il diagramma del flusso di lavoro mostra i passaggi di alto livello per l'utilizzo di S3 Object Lock. Questi passaggi vengono eseguiti dall'amministratore della griglia e dagli utenti del tenant.



Task di amministrazione della griglia

Come mostra il diagramma del flusso di lavoro, un amministratore della griglia deve eseguire due attività di alto livello prima che gli utenti del tenant S3 possano utilizzare il blocco oggetti S3:

1. Creare almeno una regola ILM conforme e impostarla come regola predefinita nel criterio ILM attivo.
2. Attivare l'impostazione globale S3 Object Lock per l'intero sistema StorageGRID.

Attività utente tenant

Una volta attivata l'impostazione globale S3 Object Lock, i tenant possono eseguire le seguenti attività:

1. Creare bucket con S3 Object Lock attivato.
2. Specificare le impostazioni di conservazione predefinite per il bucket, che vengono applicate agli oggetti aggiunti al bucket che non specificano le proprie impostazioni di conservazione.
3. Aggiungere oggetti a tali bucket e specificare i periodi di conservazione a livello di oggetto e le impostazioni di conservazione a livello legale.
4. Se necessario, aggiornare un periodo di conservazione o modificare l'impostazione di conservazione legale per un singolo oggetto.

Informazioni correlate

- Utilizzare un account tenant
- Utilizzare S3
- USA la conservazione predefinita del bucket S3 Object Lock

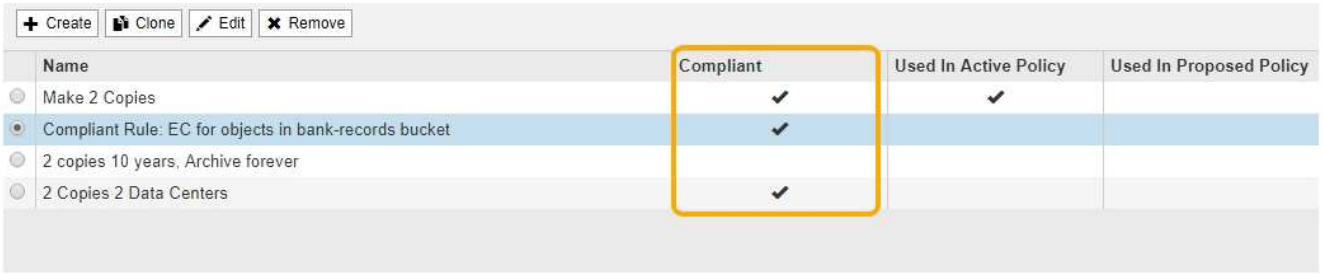
Requisiti per il blocco oggetti S3

È necessario esaminare i requisiti per l'attivazione dell'impostazione globale di blocco oggetti S3, i requisiti per la creazione di regole ILM e criteri ILM conformi e le restrizioni applicate da StorageGRID ai bucket e agli oggetti che utilizzano il blocco oggetti S3.

Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock

- È necessario attivare l'impostazione globale S3 Object Lock utilizzando Grid Manager o l'API Grid Management prima che qualsiasi tenant S3 possa creare un bucket con S3 Object Lock attivato.
- L'attivazione dell'impostazione globale S3 Object Lock consente a tutti gli account tenant S3 di creare bucket con S3 Object Lock attivato.
- Dopo aver attivato l'impostazione globale S3 Object Lock (blocco oggetto S3), non è possibile disattivare l'impostazione.
- Non è possibile attivare il blocco oggetti S3 globale a meno che la regola predefinita nel criterio ILM attivo non sia *compliant* (ovvero, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetti S3 attivato).
- Quando l'impostazione blocco oggetto S3 globale è attivata, non è possibile creare un nuovo criterio ILM proposto o attivare un criterio ILM proposto esistente a meno che la regola predefinita del criterio non sia conforme. Una volta attivata l'impostazione globale S3 Object Lock, le pagine ILM Rules (regole ILM) e ILM Policies (Criteri ILM) indicano quali regole ILM sono conformi.

  Nell'esempio seguente, la pagina ILM Rules (regole ILM) elenca tre regole che sono conformi ai bucket con S3 Object Lock abilitato.

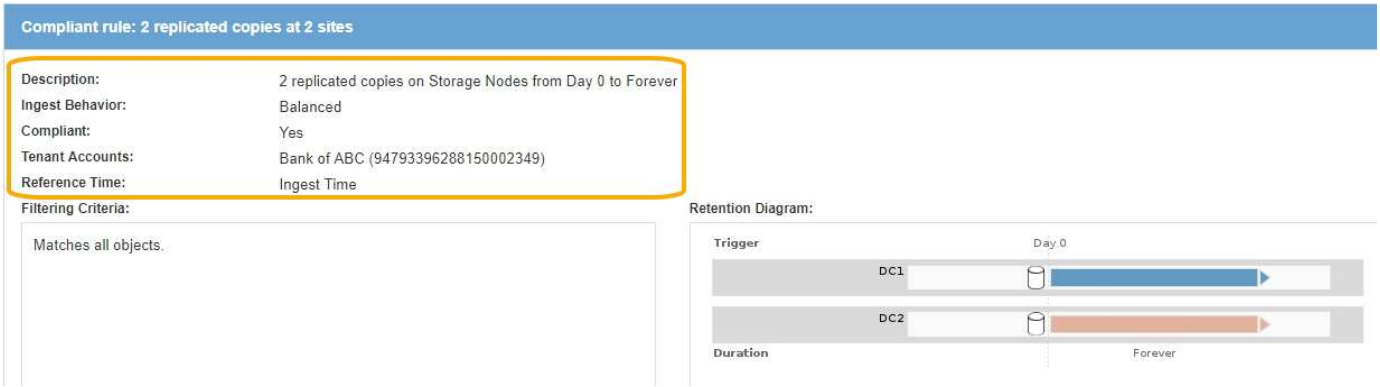


Requisiti per le regole ILM conformi

Se si desidera attivare l'impostazione blocco oggetti S3 globale, assicurarsi che la regola predefinita nel criterio ILM attivo sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con blocco oggetti S3 attivato e di tutti i bucket esistenti con conformità legacy attivata:

- Deve creare almeno due copie di oggetti replicate o una copia con codice di cancellazione.
- Queste copie devono esistere nei nodi di storage per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
- Impossibile salvare le copie degli oggetti in un pool di storage cloud.
- Impossibile salvare le copie degli oggetti nei nodi di archiviazione.
- Almeno una riga delle istruzioni di posizionamento deve iniziare al giorno 0, utilizzando **Ingest Time** come ora di riferimento.
- Almeno una riga delle istruzioni di posizionamento deve essere "forever".

Ad esempio, questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato. Memorizza due copie di oggetti replicate dall'ora di inizio (giorno 0) a "forever". Gli oggetti verranno memorizzati nei nodi di storage di due data center.



Requisiti per le policy ILM attive e proposte

Quando l'impostazione blocco oggetto S3 globale è attivata, i criteri ILM attivi e proposti possono includere

regole conformi e non conformi.

- La regola predefinita del criterio ILM attivo o proposto deve essere conforme.
- Le regole non conformi si applicano solo agli oggetti nei bucket che non hanno attivato il blocco oggetti S3 o che non hanno la funzione Compliance legacy attivata.
- Le regole conformi possono essere applicate agli oggetti in qualsiasi bucket; non è necessario attivare il blocco oggetti S3 o la conformità legacy per il bucket.

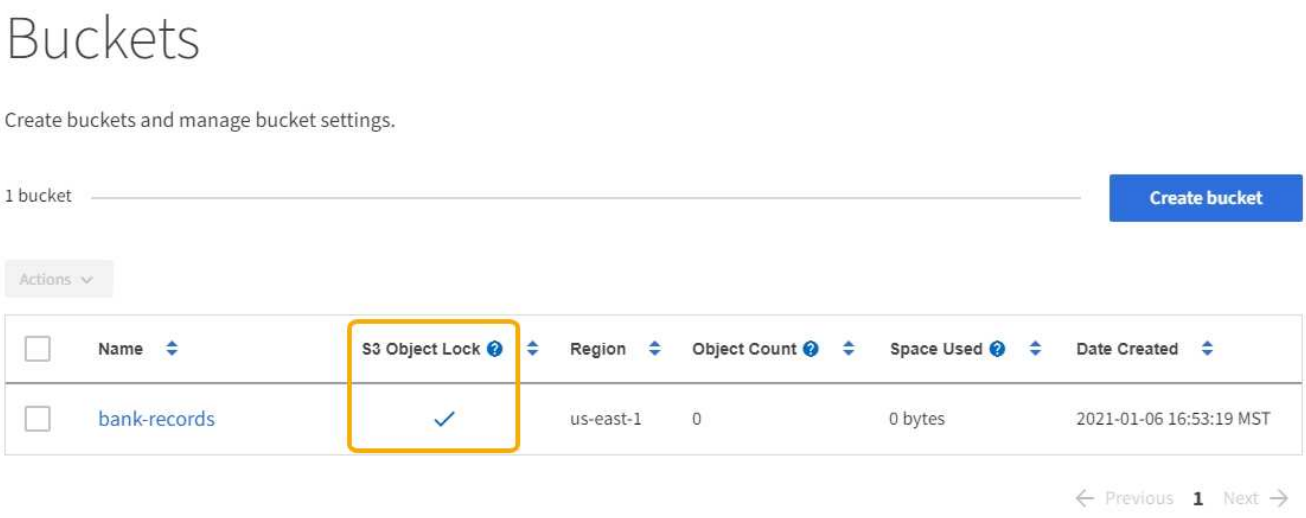
Un criterio ILM conforme potrebbe includere le seguenti tre regole:

1. Regola conforme che crea copie con codifica in cancellazione degli oggetti in un bucket specifico con blocco oggetti S3 attivato. Le copie EC vengono memorizzate nei nodi di storage dal giorno 0 a sempre.
2. Una regola non conforme che crea due copie di oggetti replicate sui nodi di storage per un anno, quindi sposta una copia di oggetti nei nodi di archivio e memorizza la copia per sempre. Questa regola si applica solo ai bucket che non hanno attivato il blocco oggetti S3 o la compliance legacy perché memorizza una sola copia dell'oggetto per sempre e utilizza i nodi di archiviazione.
3. Una regola predefinita e conforme che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a sempre. Questa regola si applica a qualsiasi oggetto in qualsiasi bucket che non è stato filtrato dalle prime due regole.

Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.

  Questo esempio di Tenant Manager mostra un bucket con blocco oggetti S3 attivato.



- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Non è possibile attivare il blocco oggetti S3 per un bucket esistente.
- La versione del bucket è richiesta con S3 Object Lock. Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket.
- Dopo aver creato un bucket con S3 Object Lock attivato, non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per quel bucket.
- Facoltativamente, è possibile configurare la conservazione predefinita per un bucket. Quando viene caricata una versione dell'oggetto, la conservazione predefinita viene applicata alla versione dell'oggetto. È possibile eseguire l'override del valore predefinito del bucket specificando una modalità di conservazione e

conservarla fino a data nella richiesta di caricare una versione dell'oggetto.

- La configurazione del ciclo di vita del bucket è supportata per i bucket S3 Object Lifecycle.
- La replica di CloudMirror non è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- Per proteggere una versione a oggetti, l'applicazione client S3 deve configurare la conservazione predefinita del bucket o specificare le impostazioni di conservazione in ogni richiesta di caricamento.
- È possibile aumentare la data di conservazione per una versione a oggetti, ma non è mai possibile diminuire questo valore.
- Se si riceve la notifica di un'azione legale o di un'indagine normativa in sospeso, è possibile conservare le informazioni pertinenti ponendo un blocco legale su una versione dell'oggetto. Quando una versione dell'oggetto è sottoposta a un blocco legale, non è possibile eliminare tale oggetto da StorageGRID, anche se ha raggiunto la data di conservazione. Non appena la conservazione legale viene revocata, la versione dell'oggetto può essere eliminata se è stata raggiunta la data di conservazione.
- S3 Object Lock richiede l'utilizzo di bucket con versione. Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock attivato

Ogni oggetto salvato in un bucket con S3 Object Lock attivato passa attraverso tre fasi:

1. **Acquisizione oggetto**
   - Quando si aggiunge una versione dell'oggetto a un bucket con S3 Object Lock attivato, l'applicazione client S3 può utilizzare le impostazioni predefinite di conservazione del bucket o, facoltativamente, specificare le impostazioni di conservazione per l'oggetto (conservazione fino alla data, conservazione legale o entrambe). StorageGRID genera quindi metadati per l'oggetto, che includono un UUID (Unique Object Identifier) e la data e l'ora di acquisizione.
   - Dopo l'acquisizione di una versione a oggetti con impostazioni di conservazione, i relativi dati e i metadati S3 definiti dall'utente non possono essere modificati.
   - StorageGRID memorizza i metadati dell'oggetto indipendentemente dai dati dell'oggetto. Conserva tre copie di tutti i metadati degli oggetti in ogni sito.
2. **Conservazione degli oggetti**
   - StorageGRID memorizza più copie dell'oggetto. Il numero e il tipo esatti di copie e le posizioni di storage sono determinati dalle regole conformi nel criterio ILM attivo.
3. **Eliminazione di oggetti**
   - È possibile eliminare un oggetto una volta raggiunta la data di conservazione.
   - Non è possibile eliminare un oggetto sottoposto a conservazione a fini giudiziari.

Informazioni correlate

- Utilizzare un account tenant
- Utilizzare S3
- Confronto tra blocco oggetti S3 e conformità legacy

- Esempio 7: Policy ILM conforme per il blocco oggetti S3
- Esaminare i registri di audit
- USA la conservazione predefinita del bucket S3 Object Lock.

Attiva il blocco oggetti S3 a livello globale

Se un account tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, è necessario attivare il blocco oggetti S3 per l'intero sistema StorageGRID. L'attivazione dell'impostazione globale S3 Object Lock consente a qualsiasi utente del tenant S3 di creare e gestire bucket e oggetti con S3 Object Lock.

Di cosa hai bisogno

- Si dispone dell'autorizzazione di accesso root.
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Hai esaminato il flusso di lavoro S3 Object Lock ed è necessario comprenderne le considerazioni.
- La regola predefinita nel criterio ILM attivo è conforme.
  - Creare una regola ILM predefinita
  - Creare un criterio ILM

A proposito di questa attività

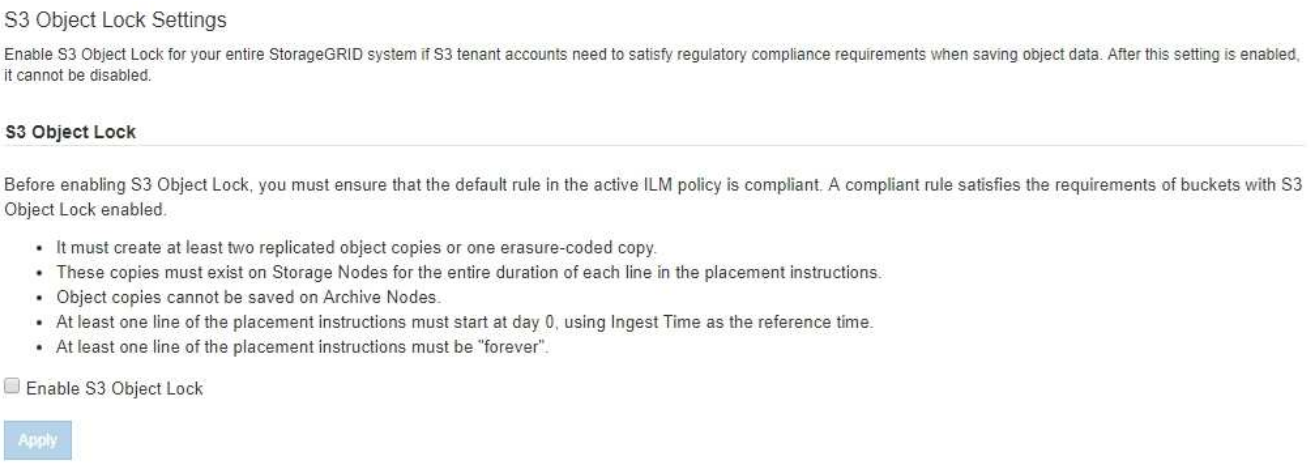
Un amministratore della griglia deve attivare l'impostazione globale S3 Object Lock per consentire agli utenti tenant di creare nuovi bucket con S3 Object Lock attivato. Una volta attivata, questa impostazione non può essere disattivata.

> Se l'impostazione di conformità globale è stata attivata utilizzando una versione precedente di StorageGRID, l'impostazione blocco oggetto S3 viene attivata in StorageGRID 11.6. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Vedere "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5".

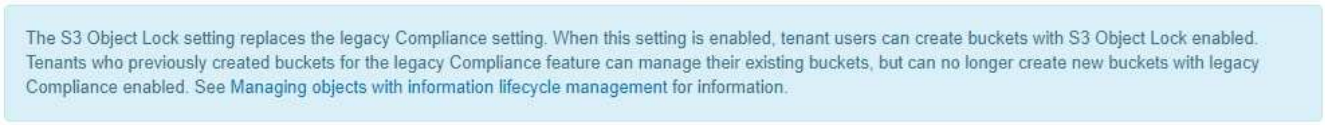
Fasi

1. Selezionare **CONFIGURATION** > **System** > **S3 Object Lock**.

   Viene visualizzata la pagina S3 Object Lock Settings (Impostazioni blocco oggetti S3).

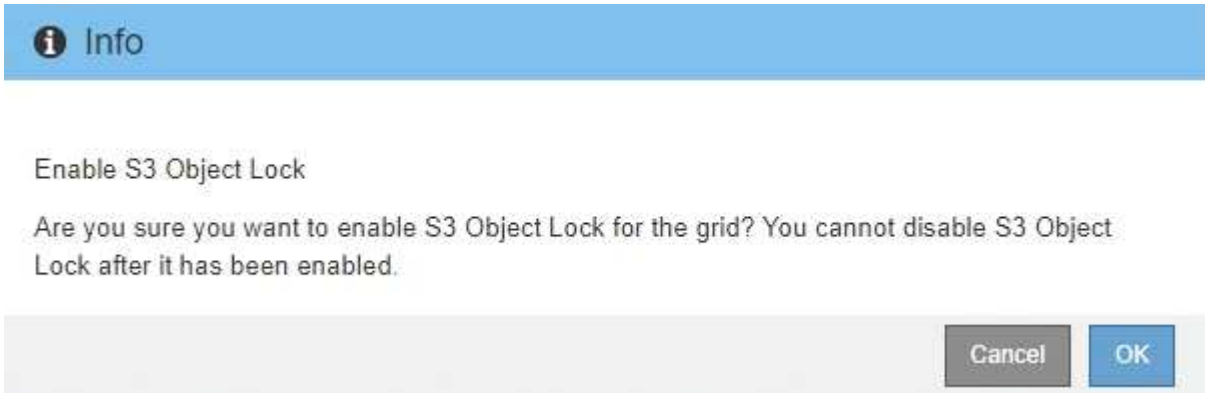


Se l'impostazione di conformità globale era stata attivata utilizzando una versione precedente di StorageGRID, la pagina contiene la seguente nota:



2. Selezionare **Enable S3 Object Lock** (attiva blocco oggetti S3).
3. Selezionare **Applica**.

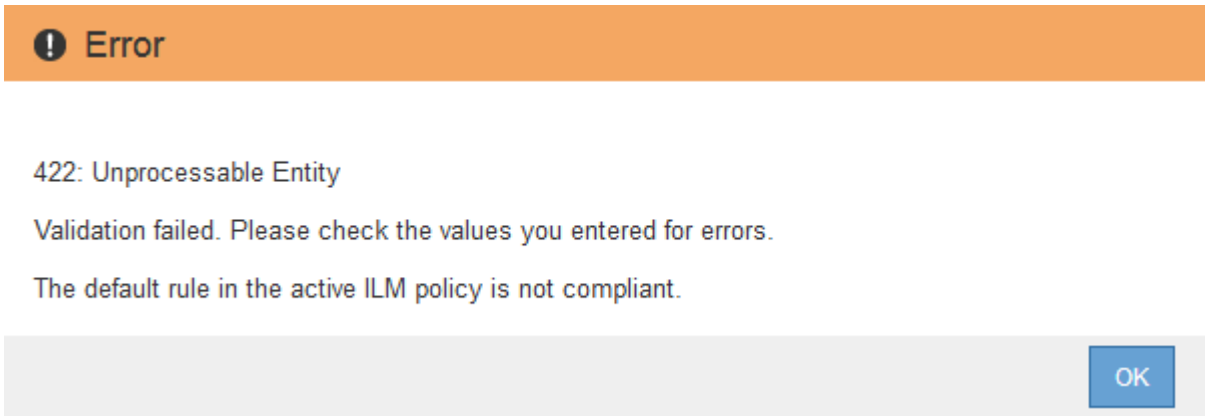
   Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare il blocco oggetti S3 dopo averlo attivato.



4. Se si è certi di voler abilitare in modo permanente il blocco oggetti S3 per l'intero sistema, selezionare **OK**.

   Quando si seleziona **OK**:

   - Se la regola predefinita nel criterio ILM attivo è conforme, il blocco oggetti S3 è ora attivato per l'intera griglia e non può essere disattivato.
   - Se la regola predefinita non è conforme, viene visualizzato un errore che indica che è necessario creare e attivare un nuovo criterio ILM che include una regola conforme come regola predefinita. Selezionare **OK** e creare una nuova policy proposta, simularla e attivarla.



Al termine

Dopo aver attivato l'impostazione globale S3 Object Lock, potrebbe essere necessario creare una regola predefinita conforme e. Creare un criterio ILM conforme. Una volta attivata l'impostazione, il criterio ILM può includere facoltativamente una regola predefinita conforme e una regola predefinita non conforme. Ad

esempio, è possibile utilizzare una regola non conforme che non dispone di filtri per gli oggetti nei bucket che non hanno attivato il blocco oggetti S3.

Informazioni correlate

- Confronta il blocco oggetti S3 con la conformità legacy

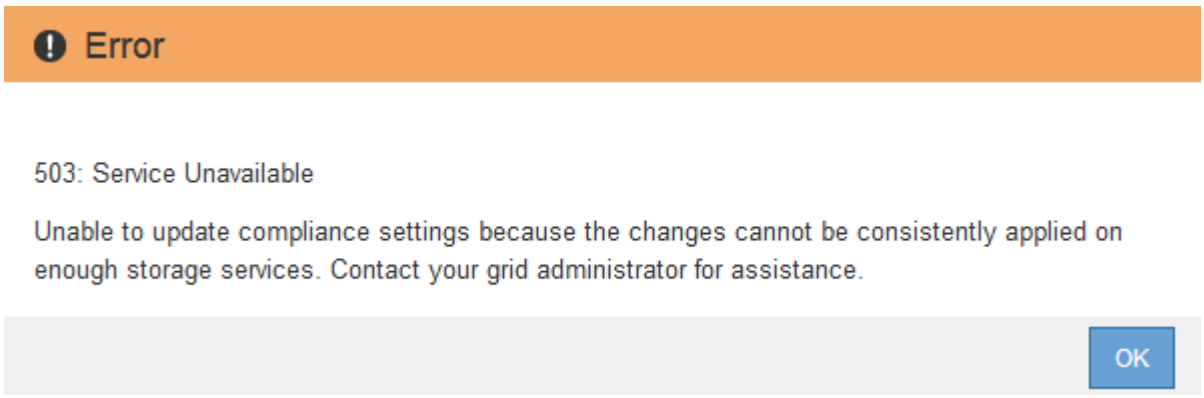
Risolvi gli errori di coerenza durante l'aggiornamento della configurazione blocco oggetti S3 o Compliance legacy

Se un sito del data center o più nodi di storage in un sito non sono più disponibili, potrebbe essere necessario aiutare gli utenti del tenant S3 ad applicare le modifiche alla configurazione S3 Object Lock o legacy Compliance.

Gli utenti tenant che hanno bucket con S3 Object Lock (o Compliance legacy) abilitato possono modificare alcune impostazioni. Ad esempio, un utente tenant che utilizza il blocco oggetti S3 potrebbe dover mettere una versione dell'oggetto sotto il blocco legale.

Quando un utente tenant aggiorna le impostazioni di un bucket S3 o di una versione a oggetti, StorageGRID tenta di aggiornare immediatamente il bucket o i metadati dell'oggetto nella griglia. Se il sistema non è in grado di aggiornare i metadati perché un sito del data center o più nodi di storage non sono disponibili, viene visualizzato un messaggio di errore. In particolare:

- Gli utenti di tenant Manager visualizzano il seguente messaggio di errore:



- Gli utenti delle API di gestione tenant e gli utenti delle API S3 ricevono un codice di risposta di `503 Service Unavailable` con testo simile.

Per risolvere questo errore, attenersi alla seguente procedura:

1. Tentare di rendere nuovamente disponibili tutti i nodi o i siti di storage il prima possibile.
2. Se non si riesce a rendere disponibile una quantità sufficiente di nodi di storage in ogni sito, contattare il supporto tecnico, che può aiutare a ripristinare i nodi e garantire che le modifiche vengano applicate in modo coerente in tutta la griglia.
3. Una volta risolto il problema sottostante, ricordare all'utente tenant di ripetere le modifiche alla configurazione.

Informazioni correlate

- Utilizzare un account tenant
- Utilizzare S3

- Ripristino e manutenzione

Informazioni sul copyright

Informazioni sul marchio commerciale