



USA blocco oggetti S3

StorageGRID 11.8

NetApp
March 19, 2024

Sommario

- USA blocco oggetti S3 1
 - Gestire gli oggetti con S3 Object Lock 1
 - Workflow per blocco oggetti S3 4
 - Requisiti per il blocco oggetti S3 6
 - Attiva il blocco oggetti S3 a livello globale 8
 - Risolvi gli errori di coerenza durante l'aggiornamento della configurazione blocco oggetti S3 o Compliance legacy 9

USA blocco oggetti S3

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 periodo di tempo specificato.

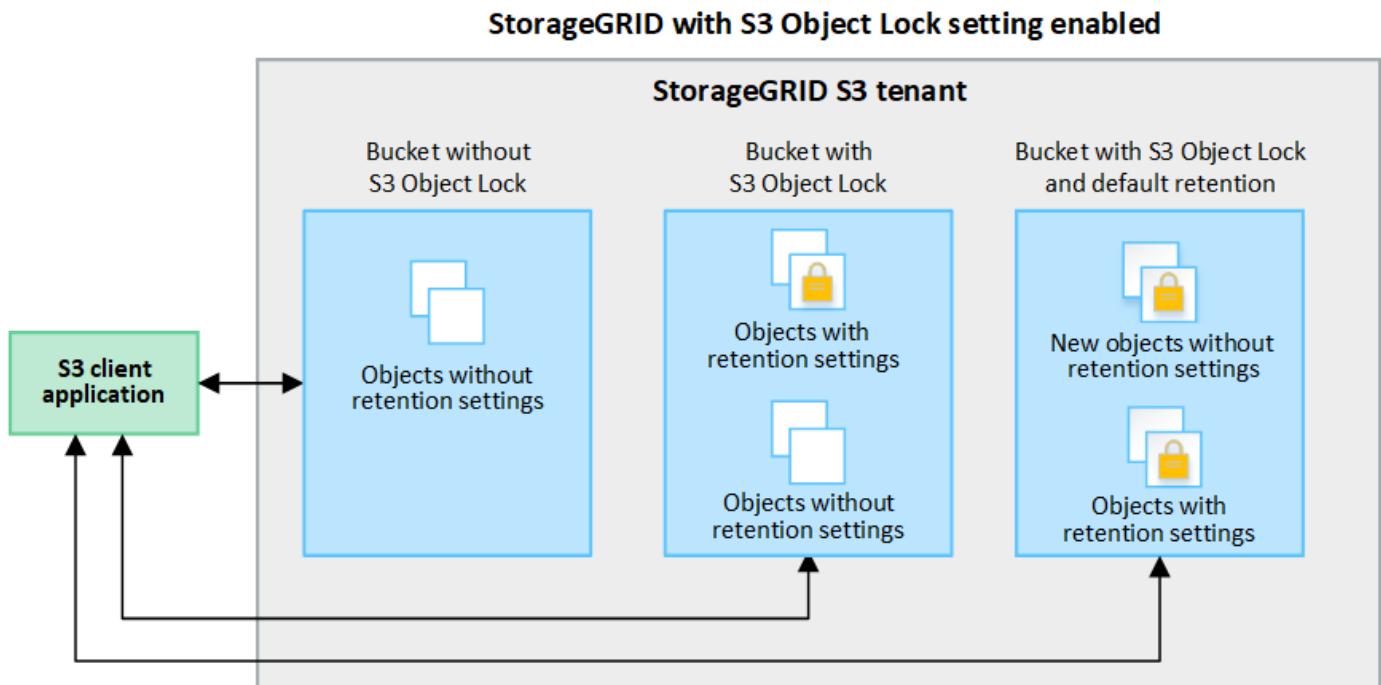
Che cos'è il blocco oggetti S3?

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, è necessario il controllo della versione del bucket e viene attivato automaticamente.

Se un bucket ha attivato il blocco oggetti S3, le applicazioni client S3 possono specificare le impostazioni di conservazione per qualsiasi versione di oggetto salvata in quel bucket.

Inoltre, un bucket con S3 Object Lock attivato può avere una modalità di conservazione e un periodo di conservazione predefiniti. Le impostazioni predefinite si applicano solo agli oggetti aggiunti al bucket senza le proprie impostazioni di conservazione.



Modalità di conservazione

La funzione blocco oggetti di StorageGRID S3 supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità equivalgono alle modalità di conservazione Amazon S3.

- In modalità compliance:

- L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
- La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
- La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità governance:
 - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare alcune impostazioni di conservazione.
 - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione:** Conformità o governance.
- **Mantieni-fino-data:** Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere cancellato.
- **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.



Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Per ulteriori informazioni sulle impostazioni dell'oggetto, vedere ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#).

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita:** Conformità o governance.
- **Default Retention Period** (periodo di conservazione predefinito): Per quanto tempo le nuove versioni degli oggetti aggiunte a questo bucket devono essere conservate, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di proprie impostazioni di conservazione. Gli oggetti bucket esistenti non vengono influenzati quando si aggiungono o si modificano queste impostazioni predefinite.

Vedere ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).

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 oggetto S3 è conforme ai requisiti Amazon S3, depreca la funzione di conformità proprietaria di StorageGRID, che ora viene chiamata "conformità legacy".



L'impostazione di conformità globale è obsoleta. Se questa impostazione è stata attivata utilizzando una versione precedente di StorageGRID, l'impostazione blocco oggetti S3 viene attivata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per ulteriori informazioni, vedere ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#).

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.

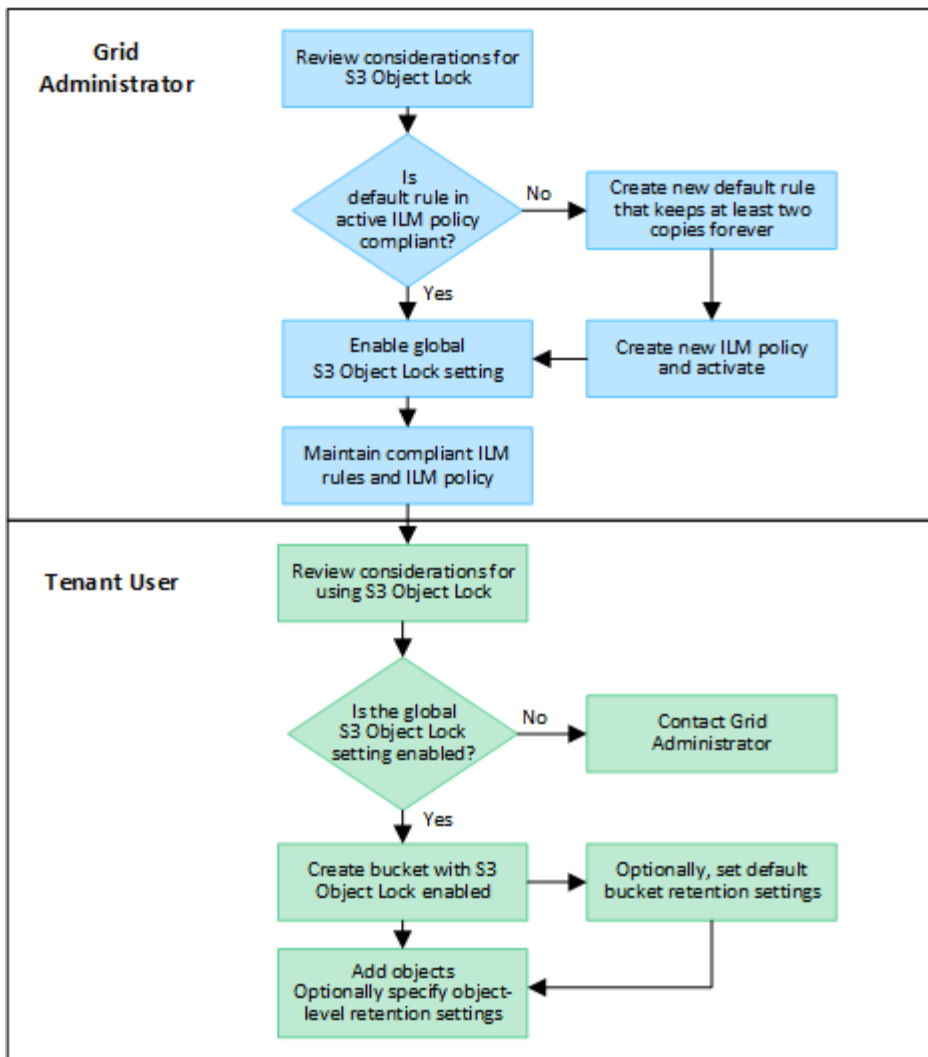
	Blocco oggetti S3	Compliance (legacy)
In che modo la funzionalità è abilitata a livello globale?	Da Grid Manager, selezionare CONFIGURATION > System > S3 Object Lock .	Non più supportato.
In che modo è abilitata la funzione per un bucket?	Gli utenti devono attivare il blocco oggetti S3 quando creano un nuovo bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3.	Non più supportato.
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
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 oppure impostare un periodo di conservazione predefinito per ciascun bucket.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
È possibile modificare il periodo di conservazione?	<ul style="list-style-type: none"> In modalità compliance, è possibile aumentare il periodo di conservazione fino alla data di una versione a oggetti, ma non ridurlo mai. In modalità governance, gli utenti con autorizzazioni speciali possono ridurre o persino rimuovere le impostazioni di conservazione di un oggetto. 	Il periodo di conservazione di un bucket può essere aumentato ma non ridotto.

	Blocco oggetti S3	Compliance (legacy)
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.
Quando è possibile eliminare gli oggetti?	<ul style="list-style-type: none"> • In modalità compliance, è possibile eliminare una versione dell'oggetto dopo aver raggiunto la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale. • In modalità governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta 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.



Attività dell'amministratore di rete

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 in un 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. Facoltativamente, specificare le impostazioni di conservazione predefinite per il bucket. Tutte le impostazioni predefinite del bucket vengono applicate solo a nuovi oggetti che non dispongono di impostazioni di conservazione personalizzate.
3. Aggiungere oggetti a tali bucket e specificare facoltativamente i periodi di conservazione a livello di oggetto e le impostazioni di conservazione a livello legale.
4. Come richiesto, aggiornare la conservazione predefinita per il bucket o aggiornare il periodo di conservazione o l'impostazione di conservazione legale per un singolo oggetto.

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 di blocco oggetti S3 globale, non è possibile disattivare l'impostazione.
- Non è possibile attivare il blocco oggetto S3 globale a meno che la regola predefinita in tutti i criteri ILM attivi non sia *conforme* (vale a dire, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetto S3 abilitato).
- Quando l'impostazione blocco oggetti S3 globale è attivata, non è possibile creare un nuovo criterio ILM o attivare un criterio ILM esistente a meno che la regola predefinita nel criterio non sia conforme. Una volta attivata l'impostazione globale S3 Object Lock, le pagine delle regole ILM e dei criteri ILM indicano quali regole ILM sono conformi.

Requisiti per le regole ILM conformi

Se si desidera attivare l'impostazione blocco oggetto S3 globale, è necessario verificare che la regola predefinita in tutti i criteri ILM attivi 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 Cloud Storage Pool.
- 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 "per sempre".

Requisiti per le policy ILM

Quando l'impostazione blocco oggetto S3 globale è attivata, i criteri ILM attivi e inattivi possono includere regole conformi e non conformi.

- La regola predefinita in un criterio ILM attivo o inattivo 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 funzionalità 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.
- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Impossibile attivare il blocco oggetti S3 per un bucket esistente.
- Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket. Non puoi disattivare il blocco oggetti S3 o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione e un periodo di conservazione predefiniti per ciascun bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di proprie impostazioni di conservazione. È possibile eseguire l'override di queste impostazioni predefinite specificando una modalità di conservazione e conservarla fino alla data per ogni versione dell'oggetto al momento del caricamento.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con blocco oggetti S3 attivato.
- 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 dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure le impostazioni di conservazione per ciascuna versione dell'oggetto. È possibile specificare le impostazioni di conservazione a livello di oggetto utilizzando l'applicazione client S3 o l'API REST S3.
- 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 le seguenti fasi:

1. Acquisizione oggetto

Quando una versione dell'oggetto viene aggiunta al bucket con S3 Object Lock attivato, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate le impostazioni di conservazione, vengono applicate le impostazioni a

livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.

- Se non sono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
- Se non sono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

Se vengono applicate le impostazioni di conservazione, vengono protetti sia l'oggetto che i metadati S3 definiti dall'utente.

2. Conservazione ed eliminazione degli oggetti

StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti delle copie degli oggetti e le posizioni dello storage sono determinati dalle regole di conformità nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla modalità di conservazione.

- Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Informazioni correlate

- ["Creare un bucket S3"](#)
- ["Aggiornare la conservazione predefinita del blocco degli oggetti S3"](#)
- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Esempio 7: Policy ILM conforme per il blocco oggetti S3"](#)

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.

Prima di iniziare

- Hai il ["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 e hai compreso le considerazioni.
- La regola predefinita nel criterio ILM attivo è conforme. Vedere ["Creare una regola ILM predefinita"](#) per ulteriori informazioni.

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.



L'impostazione di conformità globale è obsoleta. Se questa impostazione è stata attivata utilizzando una versione precedente di StorageGRID, l'impostazione blocco oggetti S3 viene attivata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per ulteriori informazioni, 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).

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 che è stato 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. È necessario creare e attivare un nuovo criterio ILM che includa una regola conforme come regola predefinita. Selezionare **OK**. Quindi, creare una nuova policy, simularla e attivarla. Vedere ["Creare un criterio ILM"](#) per istruzioni.

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 errore:

```
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.
```

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 L'API REST S3"](#)
- ["Ripristino e manutenzione"](#)

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.