Gestire gli oggetti con ILM

StorageGRID

NetApp
October 03, 2025

Sommario

Gestire gli oggetti con ILM

Scopri come gestire gli oggetti con le regole e le policy del ciclo di vita delle informazioni e come utilizzare S3 Object Lock per rispettare le normative per la conservazione degli oggetti.

- "Gestione degli oggetti con la gestione del ciclo di vita delle informazioni"
- "Gestione degli oggetti con S3 Object Lock"
- "Esempio di regole e policy ILM"

Gestione degli oggetti con la gestione del ciclo di vita delle informazioni

È possibile gestire gli oggetti in un sistema StorageGRID configurando le regole e le policy di Information Lifecycle Management (ILM). Le regole e i criteri ILM spiegano a StorageGRID come creare e distribuire copie di dati a oggetti e come gestirle nel tempo.

La progettazione e l'implementazione delle regole ILM e della policy ILM richiede un'attenta pianificazione. È necessario comprendere i requisiti operativi, la topologia del sistema StorageGRID, le esigenze di protezione degli oggetti e i tipi di storage disponibili. Quindi, è necessario determinare come si desidera copiare, distribuire e memorizzare diversi tipi di oggetti.

- "Come ILM opera per tutta la vita di un oggetto"
- "Che cos'è una policy ILM"
- "Che cos'è una regola ILM"
- "Creazione di livelli di storage, pool di storage, profili EC e regioni"
- "Creazione di una regola ILM"
- "Creazione di un criterio ILM"
- "Utilizzo delle regole ILM e delle policy ILM"

Come ILM opera per tutta la vita di un oggetto

Comprendere come StorageGRID utilizza ILM per gestire gli oggetti in ogni fase della loro vita può aiutarti a progettare una policy più efficace.

- **Ingest**: L'acquisizione inizia quando un'applicazione client S3 o Swift stabilisce una connessione per salvare un oggetto nel sistema StorageGRID e viene completata quando StorageGRID restituisce un messaggio "Engest Successful" al client. I dati degli oggetti vengono protetti durante l'acquisizione applicando immediatamente le istruzioni ILM (posizionamento sincrono) o creando copie interinali e applicando ILM successivamente (doppio commit), a seconda di come sono stati specificati i requisiti ILM.
- **Gestione delle copie**: Dopo aver creato il numero e il tipo di copie degli oggetti specificati nelle istruzioni di posizionamento di ILM, StorageGRID gestisce le posizioni degli oggetti e protegge gli oggetti dalla perdita.
  - Scansione e valutazione ILM: StorageGRID esegue una scansione continua dell'elenco di oggetti memorizzati nella griglia e verifica se le copie correnti soddisfano i requisiti ILM. Quando sono richiesti tipi, numeri o posizioni diversi di copie di oggetti, StorageGRID crea, elimina o sposta le copie in base

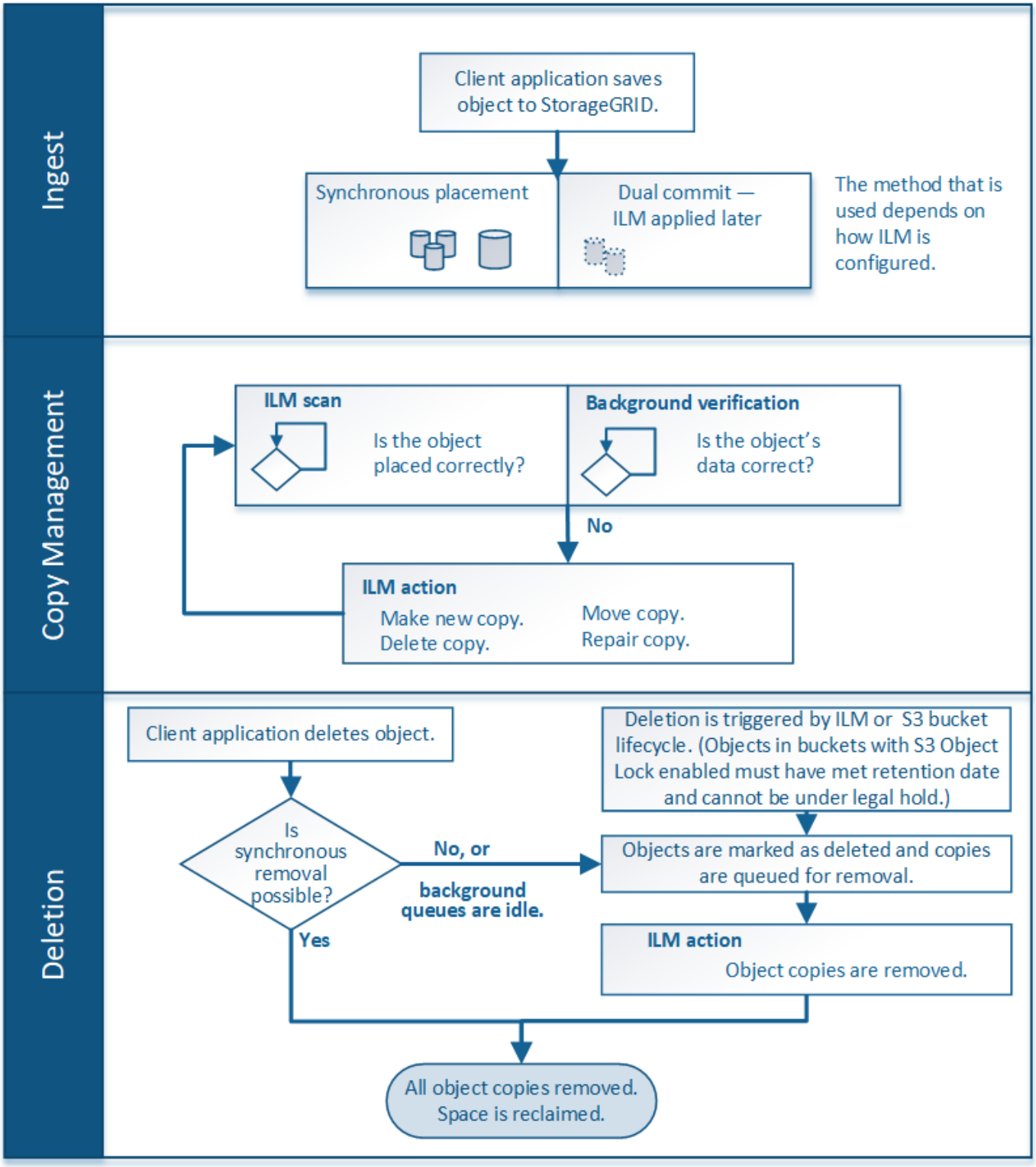
alle necessità.

    - Verifica in background: StorageGRID esegue continuamente la verifica in background per verificare l'integrità dei dati dell'oggetto. Se viene rilevato un problema, StorageGRID crea automaticamente una nuova copia dell'oggetto o un frammento di oggetto erasure-coded sostitutivo in una posizione che soddisfa i requisiti ILM correnti. Consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

- **Eliminazione oggetto**: La gestione di un oggetto termina quando tutte le copie vengono rimosse dal sistema StorageGRID. Gli oggetti possono essere rimossi in seguito a una richiesta di eliminazione da parte di un client o in seguito all'eliminazione da parte di ILM o all'eliminazione causata dalla scadenza di un ciclo di vita del bucket S3.

  > Gli oggetti in un bucket con S3 Object Lock abilitato non possono essere cancellati se sono in stato di conservazione legale o se è stata specificata una data di conservazione fino alla data, ma non ancora soddisfatta.

Il diagramma riassume il funzionamento di ILM durante l'intero ciclo di vita di un oggetto.



Informazioni correlate

"Monitor risoluzione dei problemi"

Modalità di acquisizione degli oggetti

StorageGRID protegge gli oggetti durante l'acquisizione eseguendo il posizionamento sincrono o eseguendo il commit doppio, come specificato nella regola ILM che corrisponde agli oggetti.

Quando un client S3 o Swift memorizza un oggetto nella griglia, StorageGRID acquisisce l'oggetto utilizzando uno dei due metodi seguenti:

- **Posizionamento sincrono**: StorageGRID crea immediatamente tutte le copie degli oggetti necessarie per soddisfare i requisiti ILM. StorageGRID invia un messaggio "ingest Successful" al client al momento della creazione di tutte le copie.

  Se StorageGRID non riesce a creare immediatamente tutte le copie degli oggetti (ad esempio, perché una posizione richiesta non è temporaneamente disponibile), invia un messaggio "ingest failed" al client, In alternativa, è possibile creare copie temporanee degli oggetti e valutare ILM in un secondo momento, a seconda della scelta effettuata al momento della creazione della regola ILM.

- **Doppio commit**: StorageGRID crea immediatamente due copie temporanee dell'oggetto, ciascuna su un nodo di storage diverso, e invia un messaggio "acquisizione riuscita" al client. StorageGRID inserisce quindi in coda l'oggetto per la valutazione ILM.

  Quando StorageGRID esegue la valutazione ILM, verifica innanzitutto se le copie intermedie soddisfano le istruzioni di posizionamento della regola ILM. Ad esempio, le due copie intermedie potrebbero soddisfare le istruzioni di una regola ILM a due copie, ma non soddisferebbero le istruzioni di una regola di erasure coding. Se le copie intermedie non soddisfano le istruzioni ILM, StorageGRID crea nuove copie a oggetti ed elimina le copie temporanee non necessarie.

  Se StorageGRID non riesce a creare due copie intermedie (ad esempio, se un problema di rete impedisce la creazione della seconda copia), StorageGRID non riprova. L'acquisizione non riesce.

> I client S3 o Swift possono specificare che StorageGRID crea una singola copia provvisoria al momento dell'acquisizione specificando `REDUCED_REDUNDANCY` per la classe di storage. Per ulteriori informazioni, consultare le istruzioni per l'implementazione di un client S3 o Swift.

Per impostazione predefinita, StorageGRID utilizza il posizionamento sincrono per proteggere gli oggetti durante l'acquisizione.

Informazioni correlate

"Opzioni di protezione dei dati per l'acquisizione"

"Utilizzare S3"

"USA Swift"

Opzioni di protezione dei dati per l'acquisizione

Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Dual commit, balanced o strict. A seconda della scelta, StorageGRID esegue copie temporanee e mette in coda gli oggetti per la valutazione ILM in un secondo momento, oppure utilizza il posizionamento sincrono e crea immediatamente copie per soddisfare i requisiti ILM.

Commit doppio

Quando si seleziona l'opzione doppio commit, StorageGRID esegue immediatamente copie temporanee degli oggetti su due nodi di storage diversi e restituisce un messaggio "ingest Successful" al client. L'oggetto viene messo in coda per la valutazione ILM e le copie che soddisfano le istruzioni di posizionamento della regola

vengono eseguite in un secondo momento.

Quando utilizzare l'opzione Dual Commit

Utilizzare l'opzione Dual Commit in uno dei seguenti casi:

- Stai utilizzando regole ILM multi-sito e la latenza di acquisizione client è la tua principale considerazione. Quando si utilizza il doppio commit, è necessario assicurarsi che la griglia possa eseguire il lavoro aggiuntivo di creazione e rimozione delle copie a doppio commit se non soddisfano ILM. In particolare:
  - Il carico sulla griglia deve essere sufficientemente basso da impedire un backlog ILM.
  - La griglia deve avere risorse hardware in eccesso (IOPS, CPU, memoria, larghezza di banda della rete e così via).
- Si stanno utilizzando regole ILM multi-sito e la connessione WAN tra i siti in genere ha una latenza elevata o una larghezza di banda limitata. In questo scenario, l'utilizzo dell'opzione di commit doppio può contribuire a prevenire i timeout del client. Prima di scegliere l'opzione Dual Commit, è necessario testare l'applicazione client con carichi di lavoro realistici.

Rigoroso

Quando si seleziona l'opzione Strict, StorageGRID utilizza il posizionamento sincrono all'acquisizione e crea immediatamente tutte le copie degli oggetti specificate nelle istruzioni di posizionamento della regola. L'acquisizione non riesce se StorageGRID non riesce a creare tutte le copie, ad esempio perché una posizione di storage richiesta non è temporaneamente disponibile. Il client deve riprovare l'operazione.

Quando utilizzare l'opzione Strict

Utilizzare l'opzione Strict se si dispone di un requisito operativo o normativo per memorizzare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potrebbe essere necessario utilizzare l'opzione Strict e un filtro avanzato Location Constraint per garantire che gli oggetti non vengano mai memorizzati in un determinato data center.

"Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"

Bilanciato

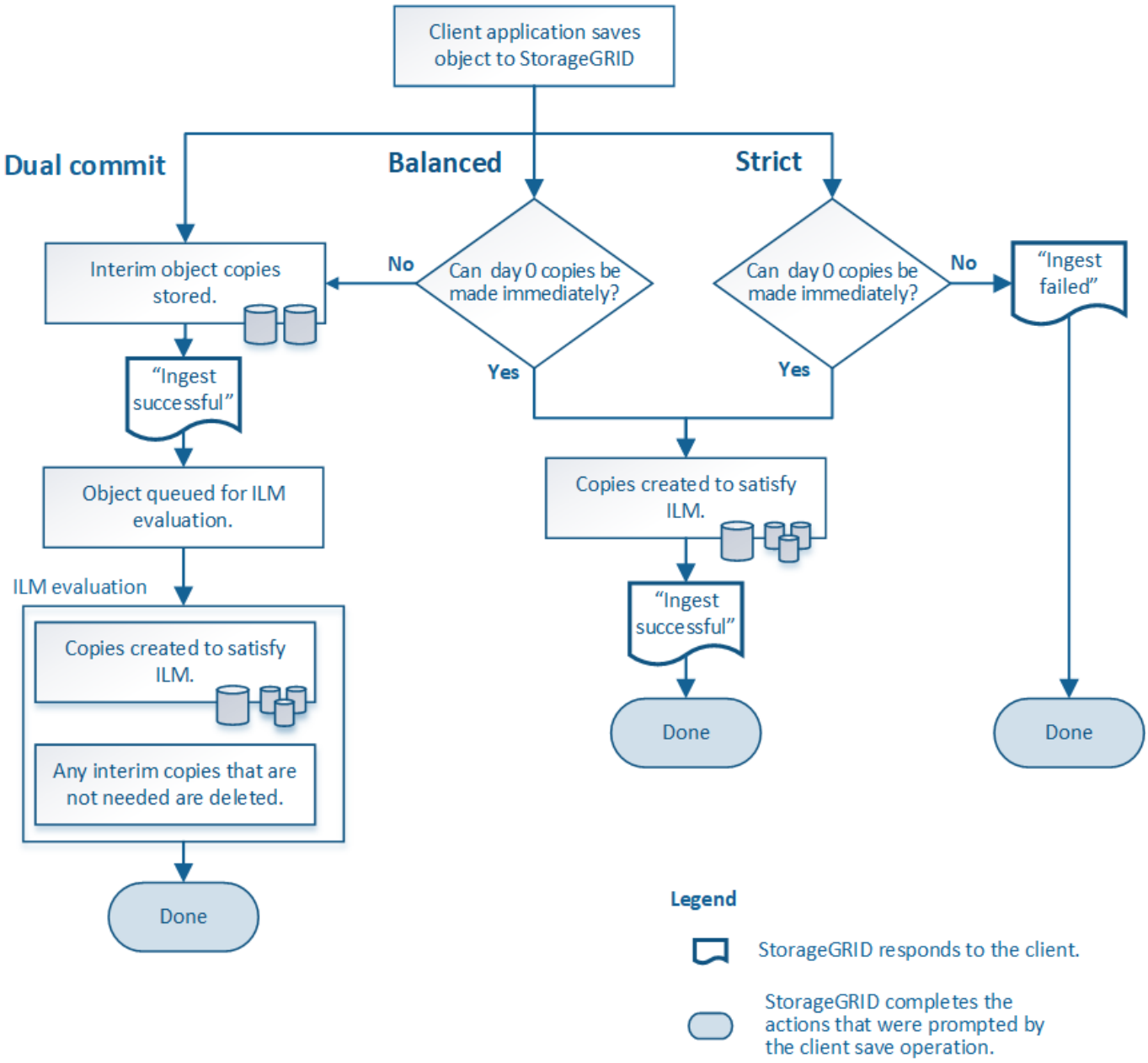
Quando si seleziona l'opzione Balanced (bilanciamento), StorageGRID utilizza anche il posizionamento sincrono all'acquisizione e crea immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. In contrasto con l'opzione rigorosa, se StorageGRID non riesce a eseguire immediatamente tutte le copie, utilizza invece il doppio commit.

Quando utilizzare l'opzione Balanced (bilanciamento)

Utilizza l'opzione Balanced per ottenere la migliore combinazione di protezione dei dati, performance di grid e successo di acquisizione. Balanced (bilanciamento) è l'opzione predefinita nella creazione guidata regole ILM.

Diagramma di flusso di tre opzioni di acquisizione

Il diagramma di flusso mostra cosa accade quando gli oggetti vengono associati da una regola ILM che utilizza una di queste opzioni di acquisizione.



Informazioni correlate

"Modalità di acquisizione degli oggetti"

Vantaggi, svantaggi e limitazioni delle opzioni di protezione dei dati

Comprendere i vantaggi e gli svantaggi di ciascuna delle tre opzioni per la protezione dei dati in fase di acquisizione (Balanced, Strict o Dual Commit) può aiutare a decidere quale scegliere per una regola ILM.

Vantaggi delle opzioni bilanciate e rigorose

Rispetto al doppio commit, che crea copie intermedie durante l'acquisizione, le due opzioni di posizionamento sincrono possono offrire i seguenti vantaggi:

- **Maggiore sicurezza dei dati**: I dati degli oggetti sono immediatamente protetti come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per la protezione da

un'ampia varietà di condizioni di guasto, incluso il guasto di più di una posizione di storage. Il doppio commit può proteggere solo dalla perdita di una singola copia locale.

- **Operazione grid più efficiente**: Ogni oggetto viene elaborato una sola volta, man mano che viene acquisito. Poiché il sistema StorageGRID non deve tenere traccia o eliminare le copie temporanee, il carico di elaborazione è inferiore e lo spazio del database viene consumato meno.
- **(Balanced) Recommended** (consigliato): L'opzione Balanced (bilanciato) offre un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Balanced (bilanciato) a meno che non sia richiesto un comportamento rigoroso di acquisizione o che la griglia soddisfi tutti i criteri per l'utilizzo di Dual Commit.
- **(Strict) certezze circa le posizioni degli oggetti**: L'opzione Strict garantisce che gli oggetti siano memorizzati immediatamente in base alle istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni bilanciate e rigide

Rispetto al doppio commit, le opzioni bilanciate e rigide presentano alcuni svantaggi:

- **Ingest dei client più lunghi**: Le latenze di acquisizione dei client potrebbero essere più lunghe. Quando si utilizzano le opzioni bilanciate e rigorose, un messaggio "ingest Successful" (acquisizione riuscita) non viene restituito al client fino a quando non vengono creati e memorizzati tutti i frammenti con codifica di cancellazione o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano il posizionamento finale molto più rapidamente.
- **(Strict) tassi più elevati di errore di acquisizione**: Con l'opzione Strict, l'acquisizione non riesce ogni volta che StorageGRID non è in grado di eseguire immediatamente tutte le copie specificate nella regola ILM. Se una posizione di storage richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia di oggetti tra siti, potrebbero verificarsi elevati tassi di errore di acquisizione.
- **(Strict) le posizioni di caricamento multiparte S3 potrebbero non essere quelle previste in alcune circostanze**: Con Strict, si prevede che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'acquisizione non funzioni. Tuttavia, con un caricamento S3 multiparte, ILM viene valutato per ogni parte dell'oggetto così come è stato acquisito e per l'oggetto nel suo complesso al termine del caricamento multiparte. Nei seguenti casi, ciò potrebbe comportare posizionamenti diversi da quelli previsti:
  - **Se ILM cambia mentre è in corso un caricamento di più parti S3**: Poiché ogni parte viene posizionata in base alla regola attiva quando la parte viene inserita, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento di più parti. In questi casi, l'acquisizione dell'oggetto non ha esito negativo. Al contrario, qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.
  - **Quando le regole ILM filtrano sulla dimensione**: Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o superiori sono memorizzati in DC1 mentre tutti gli oggetti più piccoli sono memorizzati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene memorizzata in DC2. Quando ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Strict) Ingest non ha esito negativo quando i tag degli oggetti o i metadati vengono aggiornati e non è possibile eseguire le nuove posizioni richieste**: Con Strict, si prevede che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'acquisizione non riesca. Tuttavia, quando si aggiornano metadati o tag per un oggetto già memorizzato nella griglia, l'oggetto non viene reinserito. Ciò significa che le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento non vengono apportate immediatamente. Le modifiche al posizionamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Se non è possibile apportare modifiche al posizionamento richieste (ad esempio, perché non è disponibile una nuova posizione richiesta), l'oggetto aggiornato mantiene la posizione corrente fino a quando non sono possibili modifiche al posizionamento.

Limitazioni al posizionamento degli oggetti con opzioni bilanciate o rigide

Le opzioni bilanciate o rigide non possono essere utilizzate per le regole ILM che hanno una delle seguenti istruzioni di posizionamento:

- Posizionamento in un pool di storage cloud al giorno 0.
- Posizionamento in un nodo di archivio al giorno 0.
- Posizionamenti in un pool di storage cloud o in un nodo di archivio quando la regola ha un tempo di creazione definito dall'utente come tempo di riferimento.

Queste restrizioni esistono perché StorageGRID non può eseguire copie in modo sincrono a un pool di storage cloud o a un nodo di archivio e un tempo di creazione definito dall'utente potrebbe risolversi fino al momento attuale.

Come interagiscono le regole ILM e i controlli di coerenza per influire sulla protezione dei dati

Sia la regola ILM che la scelta del controllo di coerenza influiscono sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il comportamento di acquisizione selezionato per una regola ILM influisce sul posizionamento iniziale delle copie degli oggetti, mentre il controllo di coerenza utilizzato quando viene memorizzato un oggetto influisce sul posizionamento iniziale dei metadati degli oggetti. Poiché StorageGRID richiede l'accesso sia ai metadati di un oggetto che ai suoi dati per soddisfare le richieste dei client, la selezione dei livelli di protezione corrispondenti per il livello di coerenza e il comportamento di acquisizione può fornire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Ecco un breve riepilogo dei controlli di coerenza disponibili in StorageGRID:

- **All**: Tutti i nodi ricevono immediatamente i metadati dell'oggetto o la richiesta non riesce.
- **Strong-Global**: I metadati degli oggetti vengono distribuiti immediatamente a tutti i siti. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-Site**: I metadati degli oggetti vengono distribuiti immediatamente ad altri nodi del sito. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write**: Fornisce coerenza di lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati.
- **Available** (eventuale coerenza per le operazioni HEAD): Si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD.

> Prima di selezionare un livello di coerenza, leggere la descrizione completa di queste impostazioni nelle istruzioni per la creazione di un'applicazione client S3 o Swift. Prima di modificare il valore predefinito, è necessario comprendere i vantaggi e le limitazioni.

Esempio di come il controllo di coerenza e la regola ILM possono interagire

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente impostazione del livello di coerenza:

- **ILM rule**: Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.
- **Livello di coerenza**: "strong-Global" (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie degli oggetti e distribuisce i metadati a entrambi i siti prima di restituire il risultato al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione del messaggio di successo. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, le copie dei dati dell'oggetto e dei metadati dell'oggetto rimangono nel sito remoto. L'oggetto è completamente recuperabile.

Se invece sono state utilizzate la stessa regola ILM e il livello di coerenza "strong-site", il client potrebbe ricevere un messaggio di successo dopo la replica dei dati dell'oggetto nel sito remoto, ma prima della distribuzione dei metadati dell'oggetto. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso poco dopo l'acquisizione, i metadati dell'oggetto andranno persi. Impossibile recuperare l'oggetto.

L'interconnessione tra i livelli di coerenza e le regole ILM può essere complessa. Contattare NetApp per assistenza.

Informazioni correlate

"Che cos'è la replica"

"Che cos'è la cancellazione dei codici"

"Quali sono gli schemi di erasure coding"

"Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"

"Utilizzare S3"

"USA Swift"

Modalità di archiviazione degli oggetti (replica o erasure coding)

StorageGRID è in grado di proteggere gli oggetti dalla perdita memorizzando copie replicate o copie codificate per la cancellazione. Specificare il tipo di copie da creare nelle istruzioni di posizionamento delle regole ILM.

- "Che cos'è la replica"
- "Perché non utilizzare la replica a copia singola"
- "Che cos'è la cancellazione dei codici"
- "Quali sono gli schemi di erasure coding"
- "Vantaggi, svantaggi e requisiti per l'erasure coding"

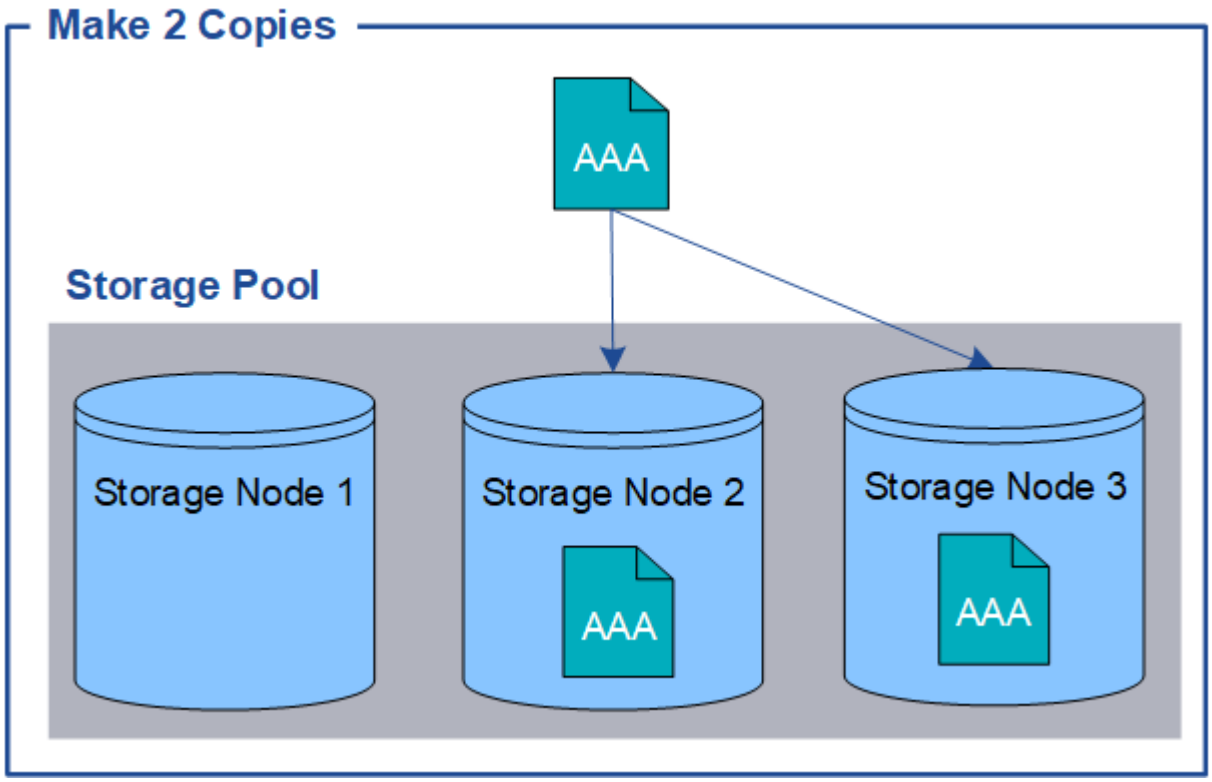
Che cos'è la replica

La replica è uno dei due metodi utilizzati da StorageGRID per memorizzare i dati degli oggetti. Quando gli oggetti corrispondono a una regola ILM che utilizza la replica, il sistema crea copie esatte dei dati dell'oggetto e le memorizza nei nodi di storage o nei nodi di archivio.

Quando si configura una regola ILM per la creazione di copie replicate, specificare il numero di copie da creare, la posizione delle copie e la durata della memorizzazione delle copie in ciascuna posizione.

Nell'esempio seguente, la regola ILM specifica che due copie replicate di ciascun oggetto devono essere

collocate in un pool di storage che contiene tre nodi di storage.



Quando StorageGRID associa gli oggetti a questa regola, crea due copie dell'oggetto, collocando ciascuna copia su un nodo di storage diverso nel pool di storage. Le due copie possono essere collocate su due dei tre nodi di storage disponibili. In questo caso, la regola ha posizionato le copie degli oggetti sui nodi di storage 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato in caso di guasto di uno qualsiasi dei nodi del pool di storage.

> StorageGRID può memorizzare solo una copia replicata di un oggetto su un dato nodo di storage. Se la griglia include tre nodi di storage e si crea una regola ILM di 4 copie, verranno eseguite solo tre copie, una copia per ciascun nodo di storage. Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

Informazioni correlate

"Che cos'è un pool di storage"

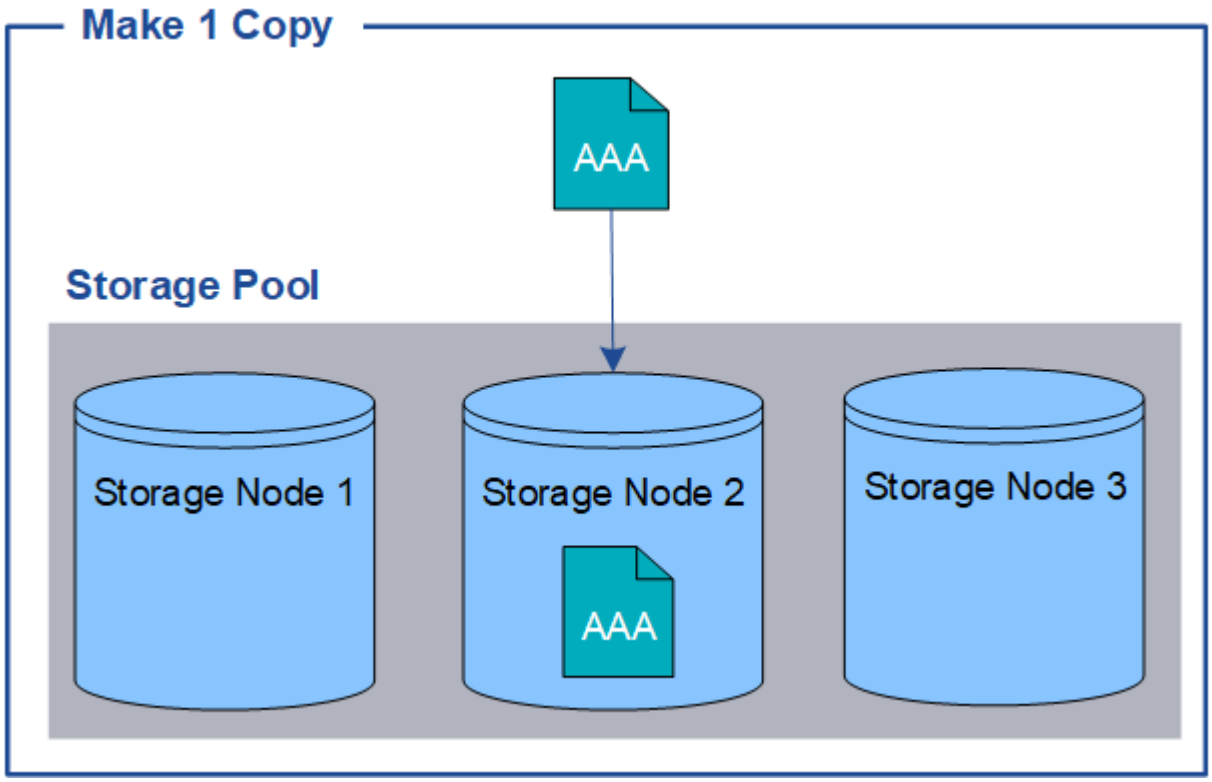
"Utilizzo di più pool di storage per la replica tra siti"

Perché non utilizzare la replica a copia singola

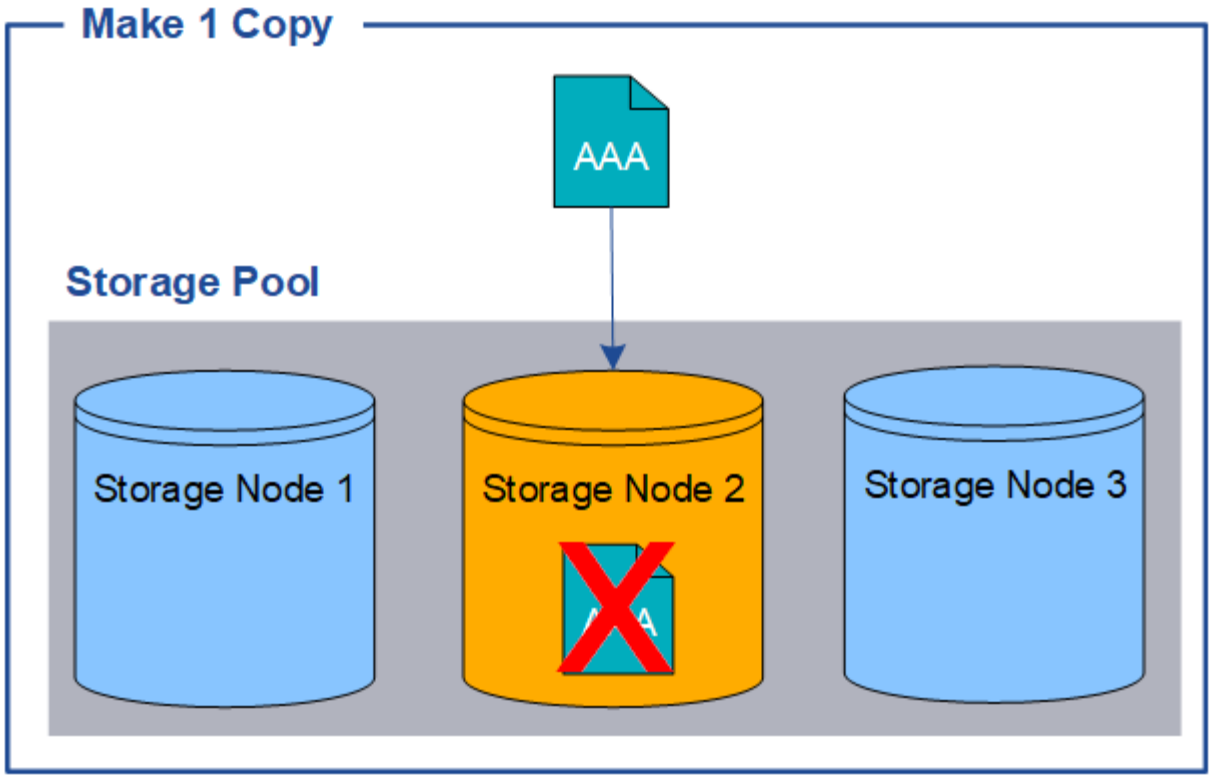
Quando si crea una regola ILM per creare copie replicate, è necessario specificare almeno due copie per un periodo di tempo qualsiasi nelle istruzioni di posizionamento.

> Non utilizzare una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

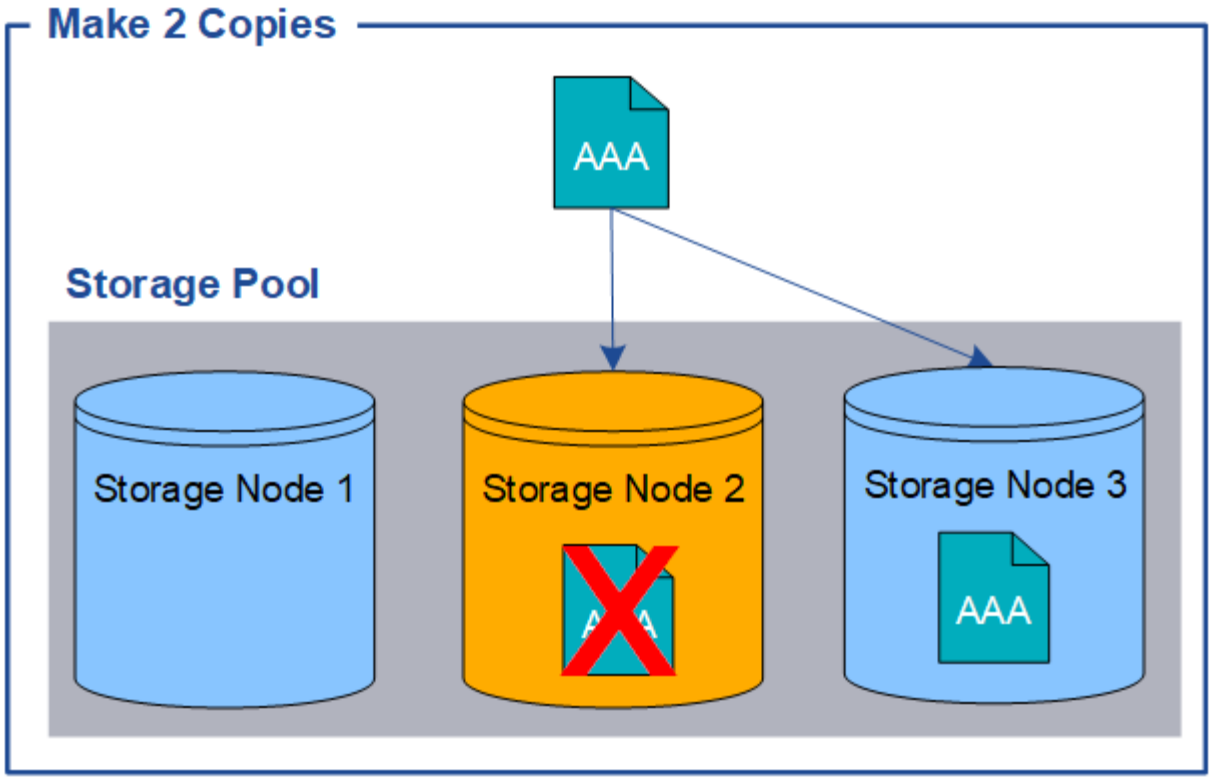
Nell'esempio seguente, la regola Make 1 Copy ILM specifica che una copia replicata di un oggetto deve essere inserita in un pool di storage che contiene tre nodi di storage. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID inserisce una singola copia su un solo nodo di storage.



Quando una regola ILM crea una sola copia replicata di un oggetto, l'oggetto diventa inaccessibile quando il nodo di storage non è disponibile. In questo esempio, l'accesso all'oggetto AAA viene temporaneamente perso ogni volta che il nodo di storage 2 non è in linea, ad esempio durante un aggiornamento o un'altra procedura di manutenzione. In caso di guasto del nodo di storage 2, l'oggetto AAA andrà perso completamente.



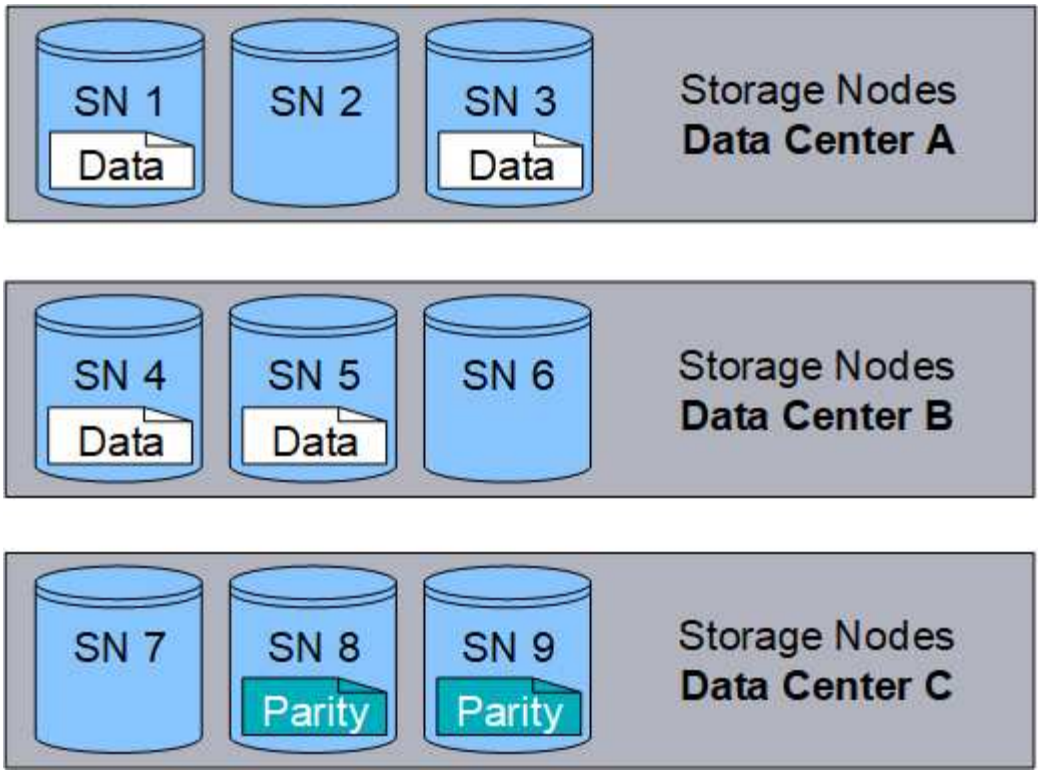
Per evitare di perdere i dati degli oggetti, è necessario eseguire almeno due copie di tutti gli oggetti che si desidera proteggere con la replica. Se esistono due o più copie, è comunque possibile accedere all'oggetto se un nodo di storage si guasta o non è in linea.



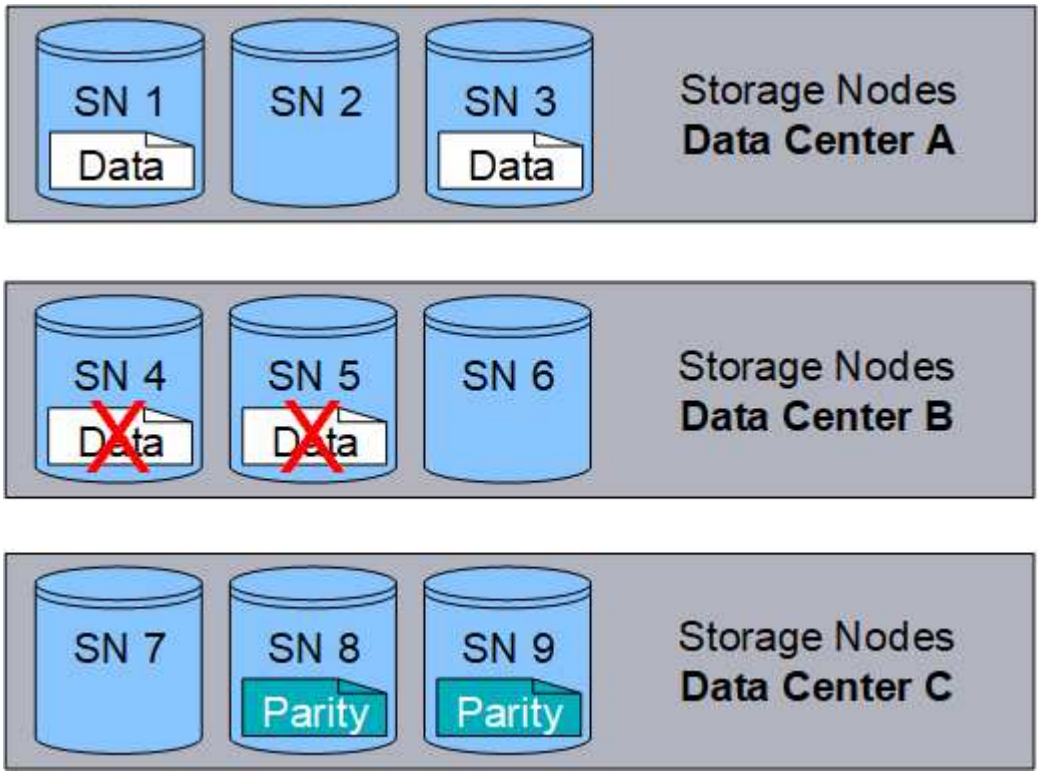
Che cos'è la cancellazione dei codici

Erasure coding è il secondo metodo utilizzato da StorageGRID per memorizzare i dati degli oggetti. Quando StorageGRID associa oggetti a una regola ILM configurata per creare copie con codifica di cancellazione, slice i dati degli oggetti in frammenti di dati, calcola ulteriori frammenti di parità e memorizza ogni frammento su un nodo di storage diverso. Quando si accede a un oggetto, questo viene riassemblato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità viene corrotto o perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei dati rimanenti e dei frammenti di parità.

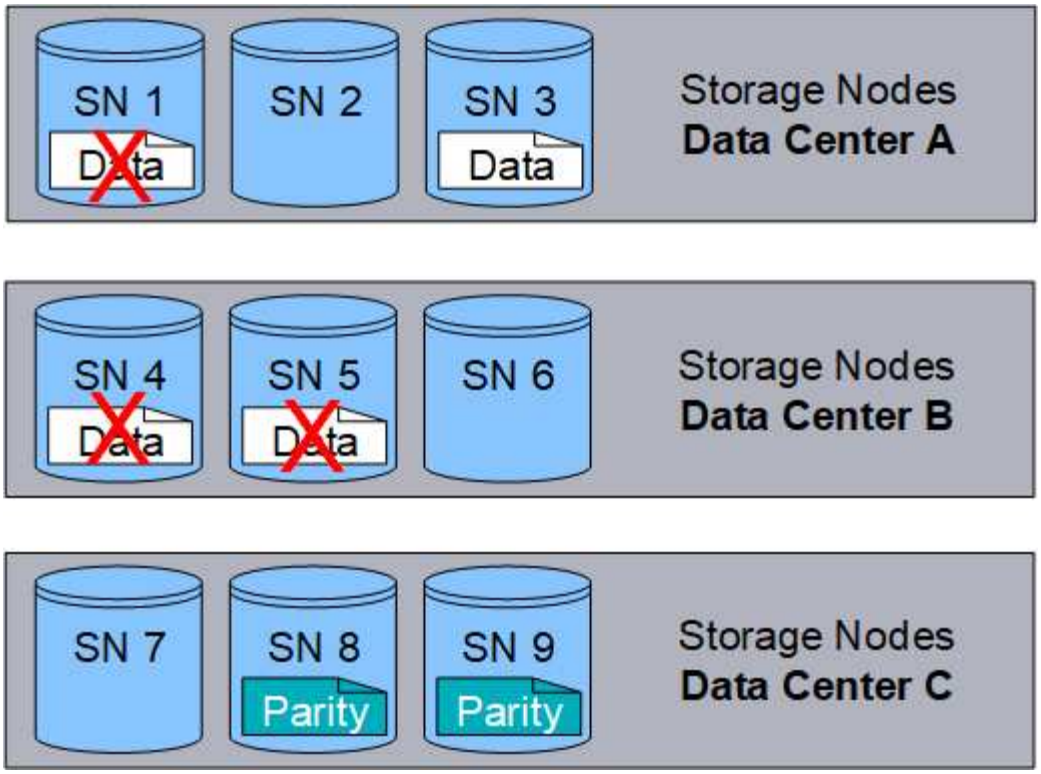
Nell'esempio seguente viene illustrato l'utilizzo di un algoritmo di erasure coding sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di erasure coding 4+2. Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati dell'oggetto. Ciascuno dei sei frammenti viene memorizzato su un nodo diverso in tre siti del data center per fornire protezione dei dati in caso di guasti al nodo o perdita del sito.



Lo schema di erasure coding 4+2 richiede un minimo di nove nodi di storage, con tre nodi di storage in ciascuno dei tre siti diversi. Un oggetto può essere recuperato finché quattro dei sei frammenti (dati o parità) rimangono disponibili. È possibile perdere fino a due frammenti senza perdita dei dati dell'oggetto. In caso di perdita di un intero sito del data center, l'oggetto può comunque essere recuperato o riparato, purché tutti gli altri frammenti rimangano accessibili.



In caso di perdita di più di due nodi di storage, l'oggetto non può essere recuperato.



Informazioni correlate

"Che cos'è un pool di storage"

"Quali sono gli schemi di erasure coding"

"Configurazione dei profili di codifica Erasure"

Quali sono gli schemi di erasure coding

Quando si configura il profilo Erasure coding per una regola ILM, si seleziona uno schema di erasure coding disponibile in base al numero di nodi e siti di storage che si intende utilizzare nel pool di storage. Gli schemi di erasure coding controllano il numero di frammenti di dati e il numero di frammenti di parità creati per ciascun oggetto.

Il sistema StorageGRID utilizza l'algoritmo di erasure coding Reed-Solomon. L'algoritmo suddivide un oggetto in k frammenti di dati e calcola m frammenti di parità. I frammenti k + m = n sono distribuiti su n nodi di storage per fornire protezione dei dati. Un oggetto può sostenere fino a m frammenti persi o corrotti. k frammenti sono necessari per recuperare o riparare un oggetto.

Quando si configura un profilo di codifica Erasure, attenersi alle seguenti linee guida per i pool di storage:

- Il pool di storage deve includere tre o più siti, o esattamente un sito.

  > Non è possibile configurare un profilo di codifica Erasure se il pool di storage include due siti.

  - Schemi di erasure coding per pool di storage contenenti tre o più siti
  - Schemi di erasure coding per pool di storage a sito singolo
- Non utilizzare il pool di storage predefinito, tutti i nodi di storage o un pool di storage che include il sito

predefinito, tutti i siti.

- Il pool di storage deve includere almeno *k*+*m* +1 nodi di storage.

  Il numero minimo di nodi di storage richiesto è *k*+*m*. Tuttavia, disporre di almeno un nodo di storage aggiuntivo può contribuire a prevenire gli errori di acquisizione o i backlog ILM se un nodo di storage richiesto non è temporaneamente disponibile.

L'overhead dello storage di uno schema di erasure coding viene calcolato dividendo il numero di frammenti di parità (*m*) per il numero di frammenti di dati (*k*). È possibile utilizzare l'overhead dello storage per calcolare la quantità di spazio su disco richiesta da ciascun oggetto con codifica di cancellazione:

```
disk space = object size + (object size * storage overhead)
```

Ad esempio, se si memorizza un oggetto da 10 MB utilizzando lo schema 4+2 (con un overhead dello storage del 50%), l'oggetto consuma 15 MB di storage grid. Se si memorizza lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (con un overhead dello storage del 33%), l'oggetto consuma circa 13.3 MB.

Seleziona lo schema di erasure coding con il valore totale più basso di *k*+*m* che soddisfi le tue esigenze. gli schemi di erasure coding con un numero inferiore di frammenti sono in generale più efficienti dal punto di vista computazionale, in quanto vengono creati e distribuiti (o recuperati) meno frammenti per oggetto, possono mostrare performance migliori grazie alle maggiori dimensioni dei frammenti e possono richiedere l'aggiunta di un numero inferiore di nodi in un'espansione quando è necessario più storage. (Per informazioni sulla pianificazione di un'espansione dello storage, consultare le istruzioni relative all'espansione di StorageGRID).

Schemi di erasure coding per pool di storage contenenti tre o più siti

La seguente tabella descrive gli schemi di erasure coding attualmente supportati da StorageGRID per i pool di storage che includono tre o più siti. Tutti questi schemi offrono la protezione contro le perdite di sito. È possibile perdere un sito e l'oggetto sarà ancora accessibile.

Per gli schemi di erasure coding che forniscono la protezione contro la perdita di sito, il numero consigliato di nodi di storage nel pool di storage supera *k*+*m*+1 perché ogni sito richiede un minimo di tre nodi di storage.

Schema di erasure coding (*k*+*m*)	Numero minimo di siti implementati	Numero consigliato di nodi di storage in ogni sito	Numero totale consigliato di nodi di storage	Protezione contro le perdite di sito?	Overhead dello storage
4+2	3	3	9	Sì	50%
6+2	4	3	12	Sì	33%
8+2	5	3	15	Sì	25%
6+3	3	4	12	Sì	50%
9+3	4	4	16	Sì	33%
2+1	3	3	9	Sì	50%
4+1	5	3	15	Sì	25%

Schema di erasure coding (*k*+*m*)	Numero minimo di siti implementati	Numero consigliato di nodi di storage in ogni sito	Numero totale consigliato di nodi di storage	Protezione contro le perdite di sito?	Overhead dello storage
6+1	7	3	21	Sì	17%
7+5	3	5	15	Sì	71%

> StorageGRID richiede un minimo di tre nodi di storage per sito. Per utilizzare lo schema 7+5, ogni sito richiede almeno quattro nodi di storage. Si consiglia di utilizzare cinque nodi di storage per sito.

Quando si seleziona uno schema di erasure coding che fornisce la protezione del sito, bilanciare l'importanza relativa dei seguenti fattori:

- **Numero di frammenti**: Le prestazioni e la flessibilità di espansione sono generalmente migliori quando il numero totale di frammenti è inferiore.
- **Fault tolerance**: La tolleranza di errore viene aumentata con più segmenti di parità (ovvero, quando *m* ha un valore più elevato).
- **Traffico di rete**: Durante il ripristino da errori, l'utilizzo di uno schema con più frammenti (ovvero, un totale maggiore per *k*+*m*) crea più traffico di rete.
- **Overhead dello storage**: Gli schemi con overhead più elevato richiedono più spazio di storage per oggetto.

Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3 (entrambi con un overhead dello storage del 50%), selezionare lo schema 6+3 se è richiesta una fault tolerance aggiuntiva. Selezionare lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, selezionare 4+2 perché il numero totale di frammenti è inferiore.

> In caso di dubbi sul programma da utilizzare, selezionare 4+2 o 6+3 oppure contattare il supporto tecnico.

Schemi di erasure coding per pool di storage a sito singolo

Un pool di storage a sito singolo supporta tutti gli schemi di erasure coding definiti per tre o più siti, a condizione che il sito disponga di un numero sufficiente di nodi di storage.

Il numero minimo di nodi di storage richiesto è *k*+*m*, ma si consiglia un pool di storage con *k*+*m*+1 nodi di storage. Ad esempio, lo schema di erasure coding 2+1 richiede un pool di storage con almeno tre nodi di storage, ma si consiglia di utilizzare quattro nodi di storage.

Schema di erasure coding (*k*+*m*)	Numero minimo di nodi di storage	Numero consigliato di nodi di storage	Overhead dello storage
4+2	6	7	50%
6+2	8	9	33%

Schema di erasure coding (*k+m*)	Numero minimo di nodi di storage	Numero consigliato di nodi di storage	Overhead dello storage
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Informazioni correlate

"Espandi il tuo grid"

Vantaggi, svantaggi e requisiti per l'erasure coding

Prima di decidere se utilizzare la replica o la cancellazione del codice per proteggere i dati degli oggetti dalla perdita, è necessario comprendere i vantaggi, gli svantaggi e i requisiti per la cancellazione del codice.

Vantaggi dell'erasure coding

Rispetto alla replica, l'erasure coding offre maggiore affidabilità, disponibilità ed efficienza dello storage.

- **Affidabilità**: L'affidabilità viene misurata in termini di tolleranza agli errori, ovvero il numero di guasti simultanei che possono essere sostenuti senza perdita di dati. Con la replica, più copie identiche vengono memorizzate su nodi diversi e tra siti diversi. Con la codifica erasure, un oggetto viene codificato in dati e frammenti di parità e distribuito su molti nodi e siti. Questa dispersione fornisce protezione da guasti sia a livello di sito che di nodo. Rispetto alla replica, l'erasure coding offre una maggiore affidabilità a costi di storage comparabili.
- **Disponibilità**: La disponibilità può essere definita come la capacità di recuperare oggetti se i nodi di storage si guastano o diventano inaccessibili. Rispetto alla replica, l'erasure coding offre una maggiore disponibilità a costi di storage comparabili.
- **Efficienza dello storage**: Per livelli simili di disponibilità e affidabilità, gli oggetti protetti tramite erasure coding consumano meno spazio su disco rispetto agli stessi oggetti se protetti tramite replica. Ad esempio, un oggetto da 10 MB replicato in due siti consuma 20 MB di spazio su disco (due copie), mentre un oggetto con codifica di cancellazione su tre siti con uno schema di codifica di cancellazione 6+3 consuma solo 15 MB di spazio su disco.

> Lo spazio su disco per gli oggetti con codifica in cancellazione viene calcolato come dimensione dell'oggetto più l'overhead dello storage. La percentuale di overhead dello storage è il numero di frammenti di parità diviso per il numero di frammenti di dati.

Svantaggi della codifica erasure

Rispetto alla replica, l'erasure coding presenta i seguenti svantaggi:

- È necessario un maggior numero di nodi e siti di storage. Ad esempio, se si utilizza uno schema di erasure coding di 6+3, è necessario disporre di almeno tre nodi di storage in tre siti diversi. Al contrario, se si replicano semplicemente i dati degli oggetti, è necessario un solo nodo di storage per ogni copia.
- Aumento dei costi e della complessità delle espansioni dello storage. Per espandere un'implementazione che utilizza la replica, è sufficiente aggiungere capacità di storage in ogni posizione in cui vengono eseguite le copie a oggetti. Per espandere un'implementazione che utilizza il erasure coding, è necessario prendere in considerazione sia lo schema di erasure coding in uso sia la capacità dei nodi di storage esistenti. Ad esempio, se si attende che i nodi esistenti siano pieni al 100%, è necessario aggiungere almeno *k+m* nodi di storage, ma se si espandono quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e massimizzare la capacità di storage utilizzabile. Per ulteriori informazioni, consulta le istruzioni per espandere StorageGRID.
- L'utilizzo di erasure coding in siti distribuiti geograficamente aumenta le latenze di recupero. I frammenti di oggetti per un oggetto che viene erasure coded e distribuito tra siti remoti richiedono più tempo per il recupero su connessioni WAN rispetto a un oggetto che viene replicato e disponibile localmente (lo stesso sito a cui si connette il client).
- Quando si utilizza il erasure coding in siti distribuiti geograficamente, il traffico di rete WAN è più elevato per recuperi e riparazioni, in particolare per oggetti recuperati di frequente o per riparazioni di oggetti su connessioni di rete WAN.
- Quando si utilizza l'erasure coding tra siti, il throughput massimo degli oggetti diminuisce drasticamente con l'aumentare della latenza di rete tra siti. Questa diminuzione è dovuta alla corrispondente diminuzione del throughput di rete TCP, che influisce sulla velocità con cui il sistema StorageGRID può memorizzare e recuperare frammenti di oggetti.
- Maggiore utilizzo delle risorse di calcolo.

Quando utilizzare la codifica di cancellazione

L'erasure coding è più adatto ai seguenti requisiti:

- Oggetti di dimensioni superiori a 1 MB.

> A causa dell'overhead di gestione del numero di frammenti associati a una copia con codice erasure, non utilizzare la codifica erasure per oggetti di dimensioni pari o inferiori a 200 KB.

- Storage a lungo termine o a freddo per contenuti recuperati raramente.
- Elevata disponibilità e affidabilità dei dati.
- Protezione contro guasti completi del sito e dei nodi.
- Efficienza dello storage.
- Implementazioni a singolo sito che richiedono una protezione dei dati efficiente con una sola copia codificata in cancellazione anziché più copie replicate.
- Implementazioni multi-sito in cui la latenza tra siti è inferiore a 100 ms.

Informazioni correlate

"Espandi il tuo grid"

Come viene determinata la conservazione degli oggetti

StorageGRID offre agli amministratori di grid e ai singoli utenti tenant opzioni per specificare la durata della memorizzazione degli oggetti. In generale, tutte le istruzioni di conservazione fornite da un utente tenant hanno la precedenza sulle istruzioni di conservazione fornite dall'amministratore della griglia.

Come gli utenti tenant controllano la conservazione degli oggetti

Gli utenti del tenant possono controllare per quanto tempo i propri oggetti vengono memorizzati in StorageGRID in tre modi principali:

- Se l'impostazione globale S3 Object Lock è attivata per la griglia, gli utenti del tenant S3 possono creare bucket con S3 Object Lock abilitato e quindi utilizzare l'API REST S3 per specificare le impostazioni di conservazione fino alla data e conservazione legale per ciascuna versione dell'oggetto aggiunta a quel bucket.
  - Una versione dell'oggetto sottoposta a blocco legale non può essere eliminata con alcun metodo.
  - Prima che venga raggiunta la data di conservazione di una versione a oggetti, tale versione non può essere eliminata da alcun metodo.
  - Gli oggetti nei bucket con S3 Object Lock abilitato vengono conservati da ILM "forever". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta del client o dalla scadenza del ciclo di vita del bucket.

    "Gestione degli oggetti con S3 Object Lock"

- Gli utenti del tenant S3 possono aggiungere una configurazione del ciclo di vita ai bucket che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID memorizza un oggetto fino a quando non viene soddisfatta la data o il numero di giorni specificati nell'azione di scadenza, a meno che il client non elimini prima l'oggetto.
- Un client S3 o Swift può emettere una richiesta di eliminazione degli oggetti. StorageGRID assegna sempre la priorità alle richieste di eliminazione dei client sul ciclo di vita del bucket S3 o ILM quando si determina se eliminare o conservare un oggetto.

Come gli amministratori della griglia controllano la conservazione degli oggetti

Gli amministratori della griglia utilizzano le istruzioni di posizionamento ILM per controllare la durata della memorizzazione degli oggetti. Quando un oggetto viene associato da una regola ILM, StorageGRID memorizza tali oggetti fino allo scadere dell'ultimo periodo di tempo della regola ILM. Gli oggetti vengono conservati a tempo indeterminato se viene specificato "forever" per le istruzioni di posizionamento.

Indipendentemente da chi controlla la durata della conservazione degli oggetti, le impostazioni ILM controllano i tipi di copie degli oggetti (replicate o codificate per la cancellazione) che vengono memorizzate e la posizione delle copie (nodi di storage, pool di storage cloud o nodi di archiviazione).

Come interagiscono il ciclo di vita del bucket S3 e ILM

L'azione Expiration (scadenza) in un ciclo di vita del bucket S3 sovrascrive sempre le impostazioni ILM. Di conseguenza, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni ILM per il posizionamento dell'oggetto.

Esempi di conservazione degli oggetti

Per comprendere meglio le interazioni tra blocco oggetti S3, impostazioni del ciclo di vita del bucket, richieste di eliminazione client e ILM, considerare gli esempi seguenti.

Esempio 1: Il ciclo di vita del bucket S3 mantiene gli oggetti più a lungo di ILM

ILM

Memorizzazione di due copie per 1 anno (365 giorni)

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Risultato

StorageGRID memorizza l'oggetto per 730 giorni. StorageGRID utilizza le impostazioni del ciclo di vita del bucket per determinare se eliminare o conservare un oggetto.

> Se il ciclo di vita del bucket specifica che gli oggetti devono essere mantenuti più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento ILM per determinare il numero e il tipo di copie da memorizzare. In questo esempio, due copie dell'oggetto continueranno ad essere memorizzate in StorageGRID dai giorni 366 al 730.

Esempio 2: Il ciclo di vita del bucket S3 scade gli oggetti prima di ILM

ILM

Memorizzazione di due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Scadenza oggetti in 1 anno (365 giorni)

Risultato

StorageGRID elimina entrambe le copie dell'oggetto dopo il giorno 365.

Esempio 3: L'eliminazione del client sovrascrive il ciclo di vita del bucket e ILM

ILM

Memorizzazione di due copie sui nodi di storage "forever"

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Richiesta di eliminazione del client

Emesso il giorno 400

Risultato

StorageGRID elimina entrambe le copie dell'oggetto il giorno 400 in risposta alla richiesta di eliminazione del client.

Esempio 4: S3 Object Lock sovrascrive la richiesta di eliminazione del client

Blocco oggetti S3

Retain-until-date per una versione a oggetti è 2026-03-31. Non è in vigore una conservazione a fini giudiziari.

Regola ILM conforme

Memorizzazione di due copie sui nodi di storage “forever”.

Richiesta di eliminazione del client

Pubblicato il 2024-03-31.

Risultato

StorageGRID non eliminerà la versione dell’oggetto perché la data di conservazione è ancora a 2 anni di distanza.

Informazioni correlate

"Gestione degli oggetti con S3 Object Lock"

"Utilizzare S3"

"Quali sono le istruzioni per il posizionamento delle regole ILM"

Modalità di eliminazione degli oggetti

StorageGRID può eliminare gli oggetti in risposta diretta a una richiesta del client o automaticamente in conseguenza della scadenza di un ciclo di vita del bucket S3 o dei requisiti della policy ILM. La comprensione dei diversi modi in cui è possibile eliminare gli oggetti e del modo in cui StorageGRID gestisce le richieste di eliminazione può aiutare a gestire gli oggetti in modo più efficace.

StorageGRID può utilizzare uno dei due metodi per eliminare gli oggetti:

- Eliminazione sincrona: Quando StorageGRID riceve una richiesta di eliminazione del client, tutte le copie degli oggetti vengono rimosse immediatamente. Il client viene informato che l’eliminazione è stata eseguita correttamente dopo la rimozione delle copie.
- Gli oggetti vengono messi in coda per l’eliminazione: Quando StorageGRID riceve una richiesta di eliminazione, l’oggetto viene messo in coda per l’eliminazione e il client viene immediatamente informato dell’avvenuta eliminazione. Le copie degli oggetti vengono rimosse in seguito dall’elaborazione ILM in background.

Quando si eliminano gli oggetti, StorageGRID utilizza il metodo che ottimizza le performance di eliminazione, riduce al minimo i potenziali backlog di eliminazione e libera lo spazio più rapidamente.

La tabella riassume quando StorageGRID utilizza ciascun metodo.

Metodo di eliminazione	Se utilizzato
Gli oggetti vengono messi in coda per l'eliminazione	Quando **una delle seguenti condizioni** è vera: • L'eliminazione automatica degli oggetti è stata attivata da uno dei seguenti eventi: ◦ Viene raggiunta la data di scadenza o il numero di giorni nella configurazione del ciclo di vita di un bucket S3. ◦ È trascorso l'ultimo periodo di tempo specificato in una regola ILM. **Nota:** gli oggetti in un bucket che ha attivato il blocco oggetti S3 non possono essere cancellati se sono in stato di conservazione legale o se è stato specificato un periodo di conservazione fino alla data, ma non ancora soddisfatto. • Un client S3 o Swift richiede l'eliminazione e una o più di queste condizioni sono vere: ◦ Impossibile eliminare le copie entro 30 secondi, ad esempio perché una posizione dell'oggetto non è temporaneamente disponibile. ◦ Le code di eliminazione in background sono inattive.
Gli oggetti vengono rimossi immediatamente (eliminazione sincrona)	Quando un client S3 o Swift effettua una richiesta di eliminazione e **tutte** le seguenti condizioni sono soddisfatte: • Tutte le copie possono essere rimosse entro 30 secondi. • Le code di eliminazione in background contengono oggetti da elaborare.

Quando i client S3 o Swift effettuano richieste di eliminazione, StorageGRID inizia aggiungendo una serie di oggetti alla coda di eliminazione. Passa quindi all'eliminazione sincrona. Assicurarsi che la coda di eliminazione in background disponga di oggetti da elaborare consente a StorageGRID di elaborare le eliminazioni in modo più efficiente, in particolare per i client con bassa concorrenza, evitando al contempo i backlog di eliminazione dei client.

Comprendere l'impatto del modo in cui StorageGRID elimina gli oggetti

Il modo in cui StorageGRID elimina gli oggetti può influire sulle prestazioni del sistema:

- Quando StorageGRID esegue l'eliminazione sincrona, StorageGRID può impiegare fino a 30 secondi per restituire un risultato al client. Ciò significa che l'eliminazione può sembrare più lenta, anche se le copie vengono effettivamente rimosse più rapidamente di quanto non lo siano quando StorageGRID mette in coda gli oggetti per l'eliminazione.
- Se si stanno monitorando attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, si potrebbe notare che la velocità di eliminazione sembra rallentare dopo l'eliminazione di un certo numero di oggetti. Questa modifica si verifica quando StorageGRID passa dall'accodamento di oggetti per l'eliminazione all'eliminazione sincrona. La riduzione apparente del tasso di eliminazione non significa che le copie degli oggetti vengano rimosse più lentamente. Al contrario, indica che, in media, lo spazio viene liberato più rapidamente.

Se si eliminano grandi quantità di oggetti e la priorità è liberare spazio rapidamente, considerare l'utilizzo di una richiesta client per eliminare gli oggetti piuttosto che eliminarli utilizzando ILM o altri metodi. In generale, lo spazio viene liberato più rapidamente quando l'eliminazione viene eseguita dai client perché StorageGRID può utilizzare l'eliminazione sincrona.

Tenere presente che il tempo necessario per liberare spazio dopo l'eliminazione di un oggetto dipende da diversi fattori:

- Se le copie degli oggetti vengono rimosse in modo sincrono o messe in coda per la rimozione in un secondo momento (per le richieste di eliminazione del client).
- Altri fattori, come il numero di oggetti nella griglia o la disponibilità di risorse della griglia quando le copie degli oggetti vengono messe in coda per la rimozione (sia per le eliminazioni dei client che per altri metodi).

Modalità di eliminazione degli oggetti con versione S3

Quando il controllo delle versioni è attivato per un bucket S3, StorageGRID segue il comportamento di Amazon S3 quando risponde alle richieste di eliminazione, sia che provengano da un client S3, dalla scadenza di un ciclo di vita del bucket S3 o dai requisiti della policy ILM.

Quando gli oggetti sono sottoposti a versione, le richieste di eliminazione degli oggetti non eliminano la versione corrente dell'oggetto e non liberano spazio. Invece, una richiesta di eliminazione di un oggetto crea semplicemente un indicatore di eliminazione come versione corrente dell'oggetto, rendendo la versione precedente dell'oggetto "non aggiornata".

Anche se l'oggetto non è stato rimosso, StorageGRID si comporta come se la versione corrente dell'oggetto non fosse più disponibile. Le richieste a quell'oggetto restituiscono 404 non trovato. Tuttavia, poiché i dati dell'oggetto non correnti non sono stati rimossi, le richieste che specificano una versione non corrente dell'oggetto possono avere successo.

Per liberare spazio durante l'eliminazione degli oggetti con versione, è necessario effettuare una delle seguenti operazioni:

- **S3 client request**: Specificare il numero di versione dell'oggetto nella richiesta S3 DELETE Object (`DELETE /object?versionId=ID`). Tenere presente che questa richiesta rimuove solo le copie degli oggetti per la versione specificata (le altre versioni occupano ancora spazio).
- **Ciclo di vita del bucket**: Utilizzare `NoncurrentVersionExpiration` azione nella configurazione del ciclo di vita del bucket. Quando viene raggiunto il numero di giorni non correnti specificato, StorageGRID rimuove in modo permanente tutte le copie delle versioni degli oggetti non correnti. Queste versioni degli oggetti non possono essere ripristinate.
- **ILM**: Aggiungi due regole ILM al tuo criterio ILM. Utilizzare **tempo non corrente** come tempo di riferimento nella prima regola per far corrispondere le versioni non correnti dell'oggetto. Utilizzare **Ingest Time** nella seconda regola per corrispondere alla versione corrente. La regola **ora non corrente** deve essere visualizzata nel criterio sopra la regola **ora di acquisizione**.

Informazioni correlate

"Utilizzare S3"

"Esempio 4: Regole ILM e policy per gli oggetti con versione S3"

Che cos'è una policy ILM

Un criterio ILM (Information Lifecycle Management) è un insieme ordinato di regole ILM che determina il modo in cui il sistema StorageGRID gestisce i dati degli oggetti nel tempo.

Come un criterio ILM valuta gli oggetti

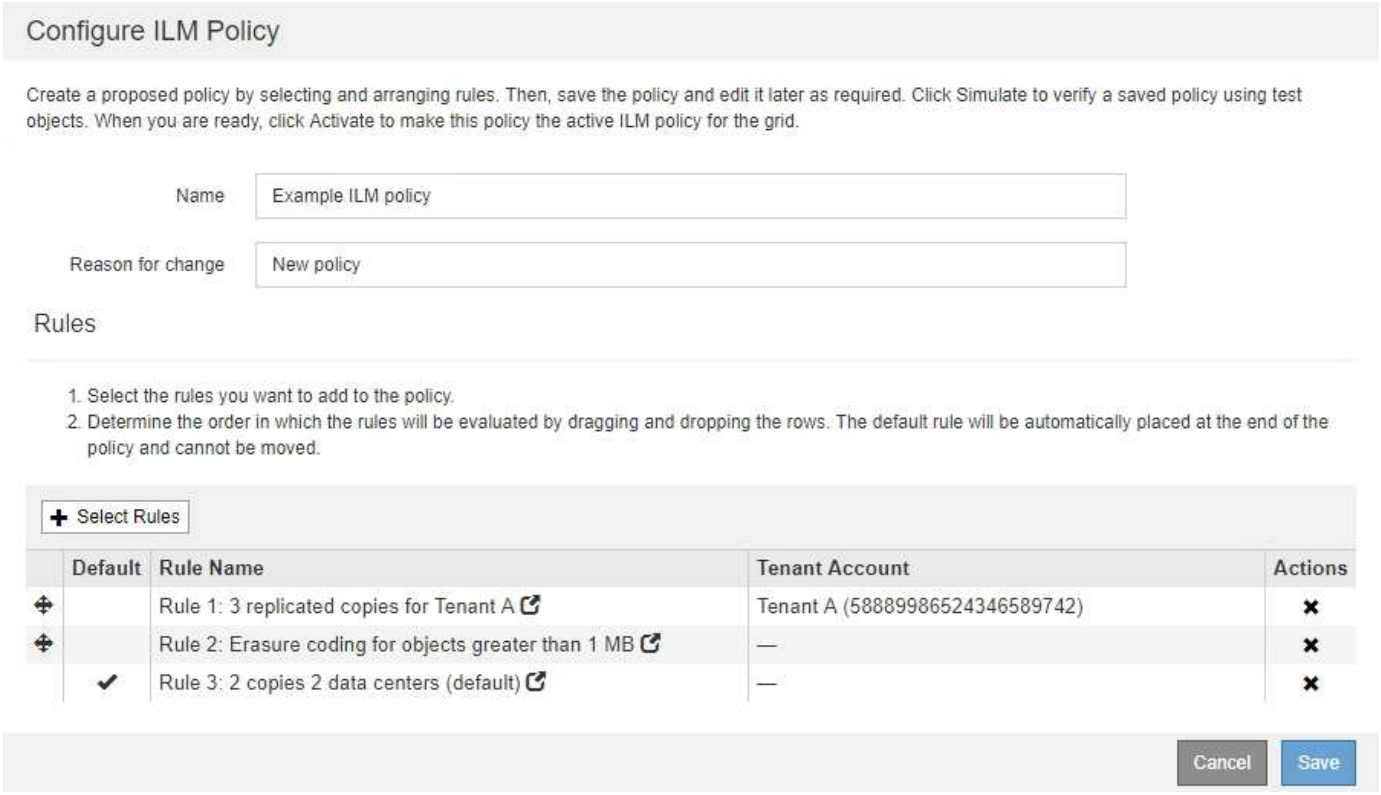
Il criterio ILM attivo per il sistema StorageGRID controlla il posizionamento, la durata e la protezione dei dati di tutti gli oggetti.

Quando i client salvano gli oggetti in StorageGRID, gli oggetti vengono valutati in base all'insieme ordinato di regole ILM nel criterio attivo, come segue:

1. Se i filtri per la prima regola del criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di tale regola e memorizzato in base alle istruzioni di posizionamento di tale regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato in base a ogni regola successiva nel criterio fino a quando non viene effettuata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di inserimento e posizionamento della regola predefinita nel criterio. La regola predefinita è l'ultima regola di un criterio e non può utilizzare alcun filtro.

Esempio di policy ILM

Questo esempio di policy ILM utilizza tre regole ILM.

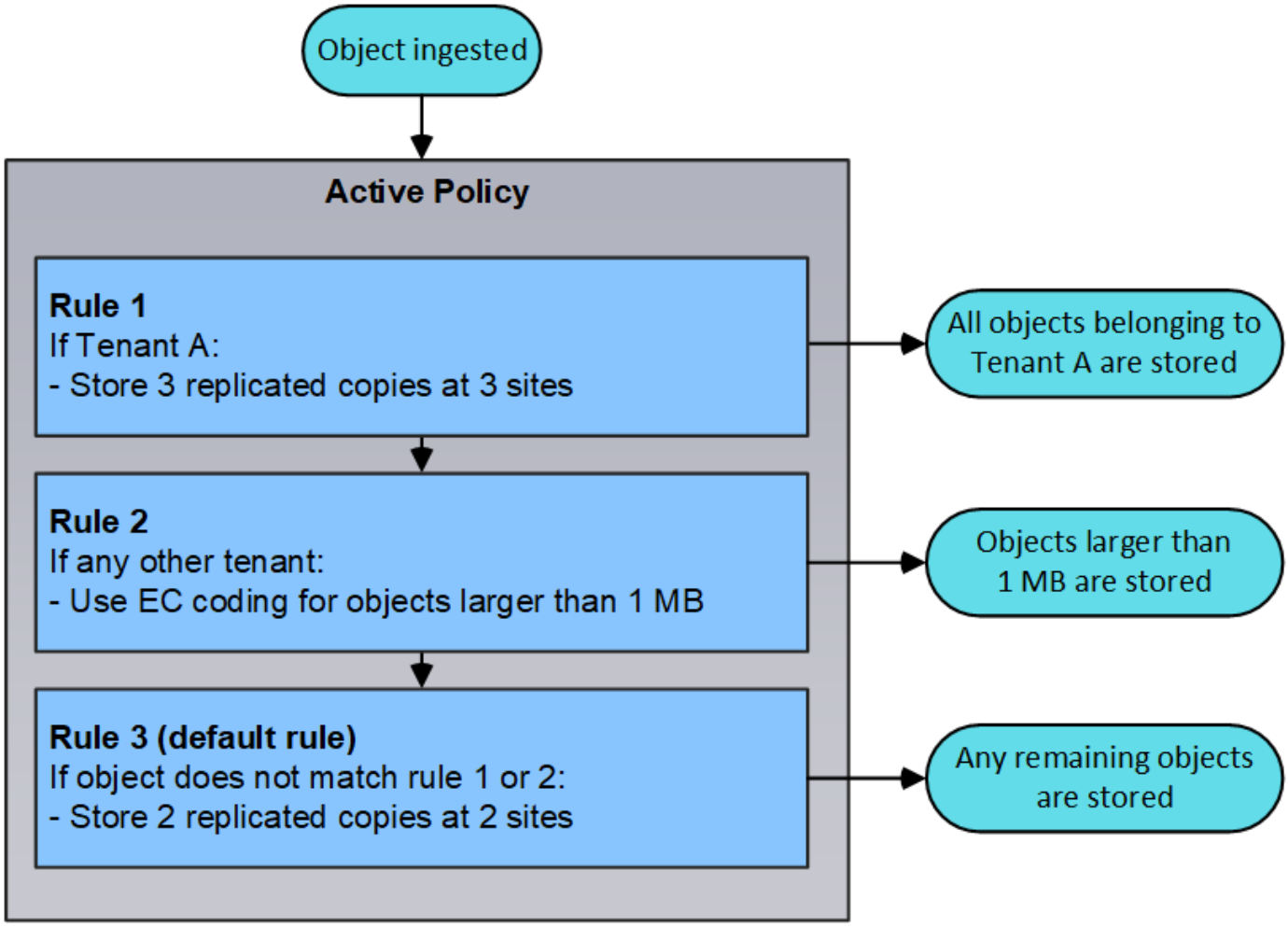


In questo esempio, la regola 1 corrisponde a tutti gli oggetti appartenenti al tenant A. Questi oggetti vengono memorizzati come tre copie replicate in tre siti. Gli oggetti appartenenti ad altri tenant non corrispondono alla

regola 1, quindi vengono valutati in base alla regola 2.

La regola 2 corrisponde a tutti gli oggetti degli altri tenant, ma solo se sono più grandi di 1 MB. Questi oggetti più grandi vengono memorizzati utilizzando la codifica di cancellazione 6+3 in tre siti. La regola 2 non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati in base alla regola 3.

La regola 3 è l'ultima regola predefinita del criterio e non utilizza filtri. La regola 3 crea due copie replicate di tutti gli oggetti non corrispondenti alla regola 1 o alla regola 2 (oggetti non appartenenti al tenant A di dimensioni pari o inferiori a 1 MB).



Quali sono le politiche proposte, attive e storiche

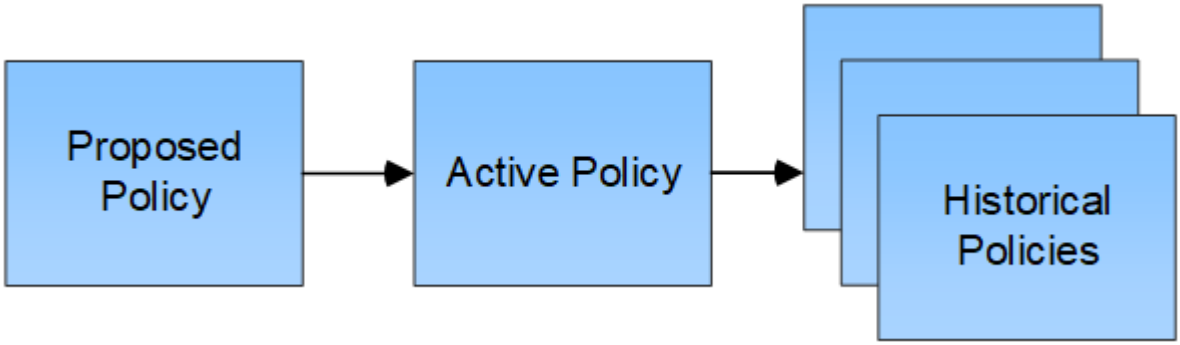
Ogni sistema StorageGRID deve disporre di un criterio ILM attivo. Un sistema StorageGRID potrebbe anche disporre di una policy ILM proposta e di un numero qualsiasi di policy storiche.

Quando si crea per la prima volta un criterio ILM, si crea un criterio proposto selezionando una o più regole ILM e ordinandole in un ordine specifico. Una volta simulata la policy proposta per confermarne il comportamento, attivarla per creare la policy attiva.

Quando si attiva un nuovo criterio ILM, StorageGRID utilizza tale criterio per gestire tutti gli oggetti, inclusi quelli esistenti e quelli appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando vengono implementate le regole ILM nel nuovo criterio.

L'attivazione della policy proposta fa sì che la policy precedentemente attiva diventi una policy storica.

Impossibile eliminare i criteri ILM storici.



Informazioni correlate

"Creazione di un criterio ILM"

Che cos'è una regola ILM

Per gestire gli oggetti, creare un set di regole ILM (Information Lifecycle Management) e organizzarle in un criterio ILM. Ogni oggetto acquisito nel sistema viene valutato in base al criterio attivo. Quando una regola del criterio corrisponde ai metadati di un oggetto, le istruzioni della regola determinano le azioni eseguite da StorageGRID per copiare e memorizzare tale oggetto.

Le regole ILM definiscono:

- Quali oggetti devono essere memorizzati. Una regola può essere applicata a tutti gli oggetti oppure è possibile specificare filtri per identificare gli oggetti a cui si applica una regola. Ad esempio, una regola può essere applicata solo agli oggetti associati a determinati account tenant, a specifici bucket S3 o a contenitori Swift o a specifici valori di metadati.
- Il tipo e la posizione di storage. Gli oggetti possono essere memorizzati nei nodi di storage, nei pool di storage cloud o nei nodi di archiviazione.
- Il tipo di copie a oggetti eseguite. Le copie possono essere replicate o codificate per la cancellazione.
- Per le copie replicate, il numero di copie eseguite.
- Per le copie codificate erasure, viene utilizzato lo schema di erasure coding.
- Il cambia nel tempo nella posizione di storage di un oggetto e nel tipo di copie.
- Modalità di protezione dei dati degli oggetti durante l'acquisizione degli oggetti nella griglia (posizionamento sincrono o doppio commit).

Si noti che i metadati degli oggetti non sono gestiti dalle regole ILM. I metadati degli oggetti vengono invece memorizzati in un database Cassandra in un archivio di metadati. Tre copie dei metadati degli oggetti vengono gestite automaticamente in ogni sito per proteggere i dati dalla perdita. Le copie sono distribuite uniformemente in tutti i nodi di storage.

Elementi di una regola ILM

Una regola ILM ha tre elementi:

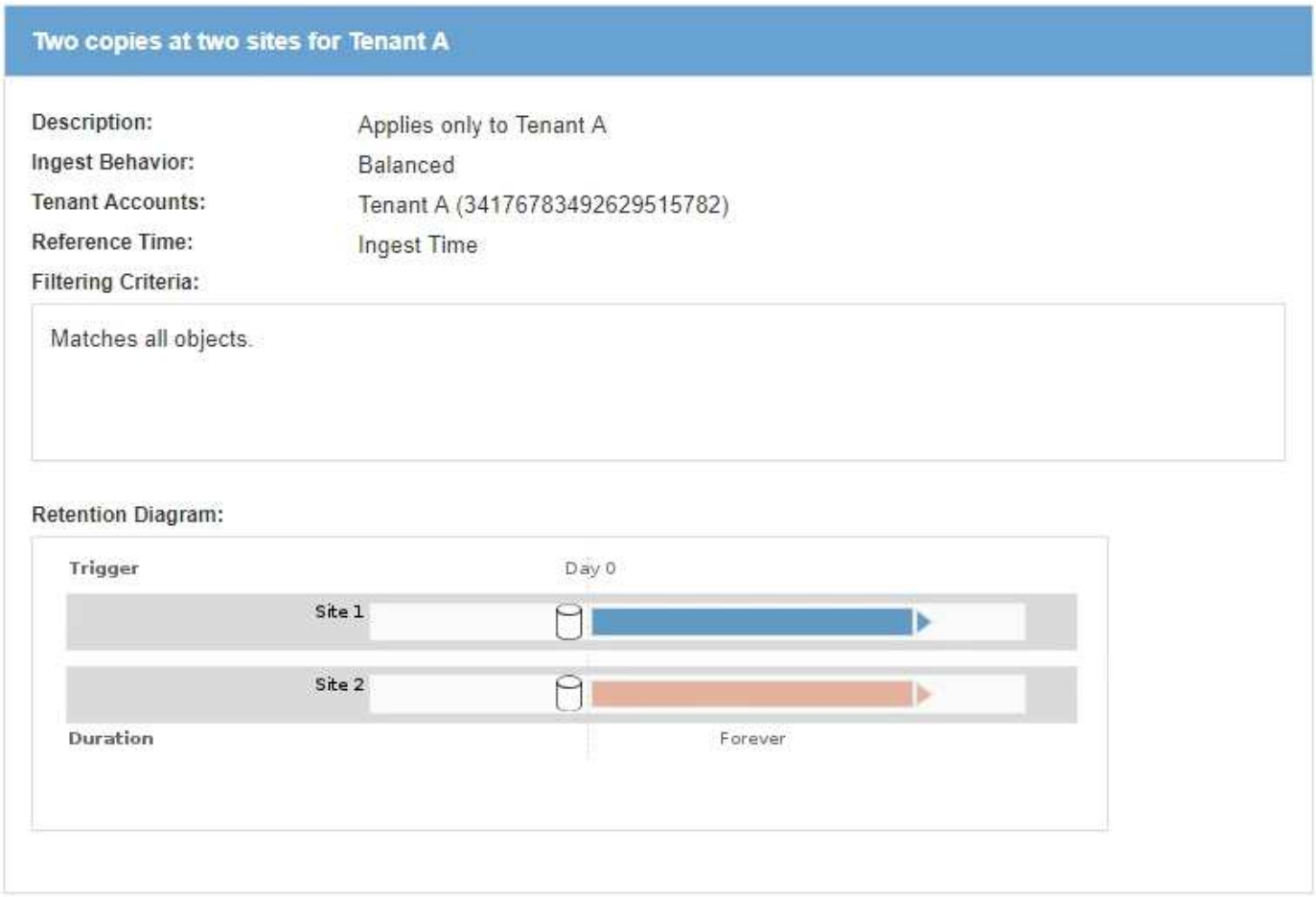
- **Filtering Criteria**: I filtri di base e avanzati di una regola definiscono a quali oggetti si applica la regola. Se un oggetto corrisponde a tutti i filtri, StorageGRID applica la regola e crea le copie dell'oggetto specificate nelle istruzioni di posizionamento della regola.

- **Istruzioni di posizionamento**: Le istruzioni di posizionamento di una regola definiscono il numero, il tipo e la posizione delle copie degli oggetti. Ciascuna regola può includere una sequenza di istruzioni di posizionamento per modificare il numero, il tipo e la posizione delle copie degli oggetti nel tempo. Quando scade il periodo di tempo per un posizionamento, le istruzioni nel posizionamento successivo vengono applicate automaticamente dalla valutazione ILM successiva.
- **Ingest Behavior**: Il comportamento di acquisizione di una regola definisce ciò che accade quando un client S3 o Swift salva un oggetto nella griglia. Il comportamento di acquisizione controlla se le copie degli oggetti vengono posizionate immediatamente in base alle istruzioni della regola o se vengono eseguite copie temporanee e le istruzioni di posizionamento vengono applicate in un secondo momento.

Esempio di regola ILM

Questo esempio di regola ILM si applica agli oggetti appartenenti al tenant A. Esegue due copie replicate di tali oggetti e memorizza ciascuna copia in un sito diverso. Le due copie vengono conservate “forever,”, il che significa che StorageGRID non le eliminerà automaticamente. Al contrario, StorageGRID conserverà questi oggetti fino a quando non saranno cancellati da una richiesta di eliminazione del client o dalla scadenza di un ciclo di vita del bucket.

Questa regola utilizza l’opzione bilanciata per il comportamento di acquisizione: L’istruzione di posizionamento a due siti viene applicata non appena il tenant A salva un oggetto in StorageGRID, a meno che non sia possibile eseguire immediatamente entrambe le copie richieste. Ad esempio, se il sito 2 non è raggiungibile quando il tenant A salva un oggetto, StorageGRID eseguirà due copie intermedie sui nodi di storage nel sito 1. Non appena il sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta presso il sito.



Informazioni correlate

"Opzioni di protezione dei dati per l’acquisizione"

"Che cos'è un pool di storage"

"Cos'è un pool di storage cloud"

"Modalità di archiviazione degli oggetti (replica o erasure coding)"

"Che cos'è il filtraggio delle regole ILM"

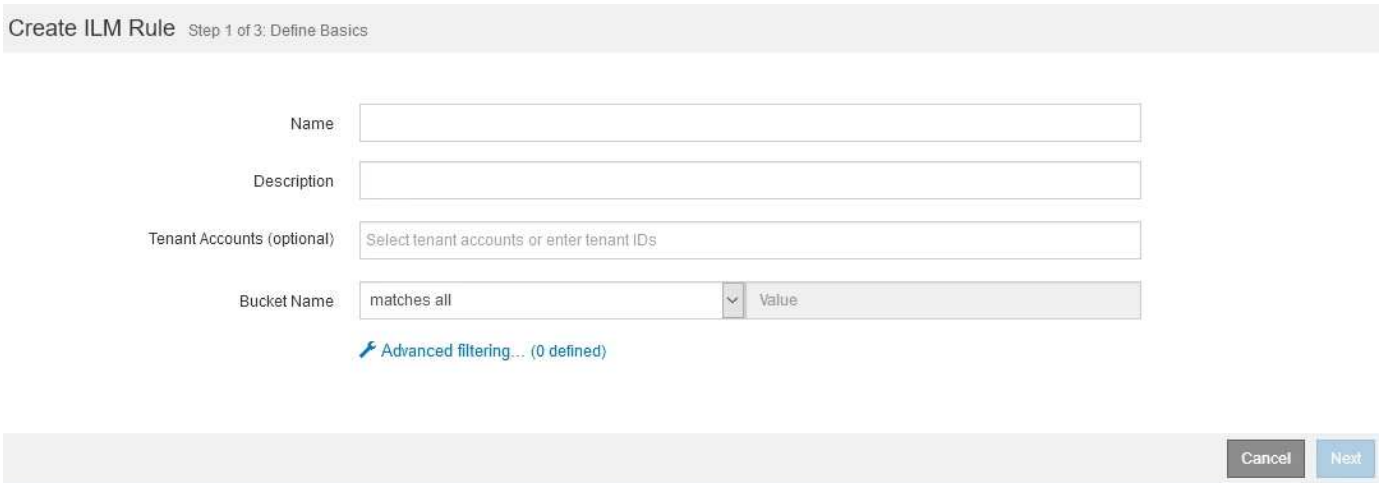
"Quali sono le istruzioni per il posizionamento delle regole ILM"

Che cos'è il filtraggio delle regole ILM

Quando si crea una regola ILM, si specificano i filtri per identificare gli oggetti a cui si applica la regola.

Nel caso più semplice, una regola potrebbe non utilizzare alcun filtro. Qualsiasi regola che non utilizza filtri si applica a tutti gli oggetti, quindi deve essere l'ultima regola (predefinita) in un criterio ILM. La regola predefinita fornisce istruzioni di archiviazione per gli oggetti che non corrispondono ai filtri di un'altra regola.

I filtri di base consentono di applicare regole diverse a gruppi di oggetti distinti e di grandi dimensioni. I filtri di base nella pagina Define Basics della procedura guidata Create ILM Rule consentono di applicare una regola a specifici account tenant, bucket S3 specifici o container Swift o entrambi.



Questi filtri di base offrono un modo semplice per applicare regole diverse a un numero elevato di oggetti. Ad esempio, potrebbe essere necessario memorizzare i record finanziari della tua azienda per soddisfare i requisiti normativi, mentre potrebbe essere necessario memorizzare i dati del reparto di marketing per facilitare le operazioni quotidiane. Dopo aver creato account tenant separati per ciascun reparto o aver separato i dati dai diversi reparti in bucket S3 separati, è possibile creare facilmente una regola che si applica a tutti i record finanziari e una seconda regola che si applica a tutti i dati di marketing.

La pagina **Advanced Filtering** della procedura guidata Create ILM Rule offre un controllo granulare. È possibile creare filtri per selezionare gli oggetti in base alle seguenti proprietà dell'oggetto:

- Tempo di acquisizione
- Ora dell'ultimo accesso
- Nome completo o parziale dell'oggetto (Key)
- Regione bucket S3 (vincolo di posizione)
- Dimensione dell'oggetto

- Metadati dell'utente
- Tag oggetti S3

È possibile filtrare gli oggetti in base a criteri molto specifici. Ad esempio, gli oggetti memorizzati dal reparto di imaging di un ospedale potrebbero essere utilizzati frequentemente quando hanno meno di 30 giorni e poco tempo dopo, mentre gli oggetti che contengono informazioni sulle visite dei pazienti potrebbero dover essere copiati nel reparto di fatturazione della sede centrale della rete sanitaria. È possibile creare filtri che identifichino ciascun tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag di oggetto S3 o a qualsiasi altro criterio pertinente, quindi creare regole separate per memorizzare ciascun set di oggetti in modo appropriato.

È inoltre possibile combinare filtri di base e avanzati in base alle esigenze in una singola regola. Ad esempio, il reparto marketing potrebbe voler memorizzare file di immagini di grandi dimensioni in modo diverso dai record dei vendor, mentre il reparto risorse umane potrebbe dover memorizzare i record del personale in un'area geografica specifica e le informazioni sulle policy a livello centrale. In questo caso, è possibile creare regole che filtrino in base all'account tenant per separare i record da ciascun reparto, utilizzando filtri avanzati in ciascuna regola per identificare il tipo specifico di oggetti a cui si applica la regola.

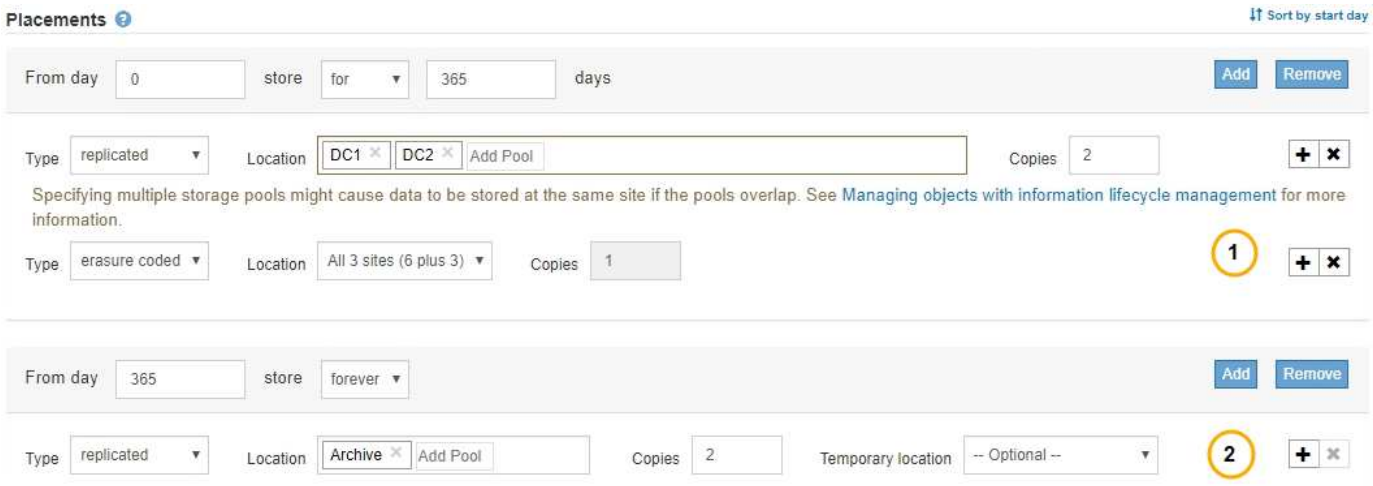
Quali sono le istruzioni per il posizionamento delle regole ILM

Le istruzioni di posizionamento determinano dove, quando e come vengono memorizzati i dati degli oggetti. Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo.

Quando si crea un'istruzione di posizionamento, si specifica quando si applica il posizionamento (il periodo di tempo), quale tipo di copie creare (replicate o codificate per la cancellazione) e dove memorizzare le copie (una o più posizioni di archiviazione). All'interno di una singola regola è possibile specificare più posizioni per un periodo di tempo e le istruzioni di posizionamento per più di un periodo di tempo:

- Per specificare più di un posizionamento degli oggetti durante un singolo periodo di tempo, fare clic sull'icona con il segno più ➕ per aggiungere più di una riga per quel periodo di tempo.
- Per specificare il posizionamento degli oggetti per più di un periodo di tempo, fare clic sul pulsante **Add** (Aggiungi) per aggiungere il periodo di tempo successivo. Quindi, specificare una o più righe entro il periodo di tempo.

L'esempio mostra la pagina Definisci posizioni della procedura guidata Crea regola ILM.



1	La prima istruzione di posizionamento ha due righe per il primo anno: 1. La prima riga crea due copie di oggetti replicate in due siti del data center. 2. La seconda riga crea una copia 6+3 con codifica di cancellazione utilizzando tre siti del data center.
2	La seconda istruzione di posizionamento crea due copie archiviate dopo un anno e le conserva per sempre.

Quando si definisce il set di istruzioni di posizionamento per una regola, è necessario assicurarsi che almeno un'istruzione di posizionamento inizi al giorno 0, che non vi siano intervalli tra i periodi di tempo definiti, e che l'istruzione finale di posizionamento continui per sempre o fino a quando non si richiede più alcuna copia oggetto.

Alla scadenza di ogni periodo di tempo previsto dalla regola, vengono applicate le istruzioni per il posizionamento dei contenuti per il periodo di tempo successivo. Vengono create nuove copie di oggetti e tutte le copie non necessarie vengono eliminate.

Creazione di livelli di storage, pool di storage, profili EC e regioni

Prima di poter creare le regole ILM per il sistema StorageGRID, è necessario definire le posizioni di archiviazione degli oggetti, determinare i tipi di copie desiderati e, facoltativamente, configurare le aree S3.

- "Creazione e assegnazione dei gradi di storage"
- "Configurazione dei pool di storage"
- "Utilizzo dei Cloud Storage Pools"
- "Configurazione dei profili di codifica Erasure"
- "Configurazione delle regioni (opzionale e solo S3)"

Creazione e assegnazione dei gradi di storage

I gradi di storage identificano il tipo di storage utilizzato da un nodo di storage. È possibile creare gradi di storage se si desidera che le regole ILM posizionino determinati oggetti su determinati nodi di storage, invece che su tutti i nodi del sito. Ad esempio, è possibile che alcuni oggetti vengano memorizzati nei nodi di storage più veloci, ad esempio le appliance di storage all-flash StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Se si utilizzano più tipi di storage, è possibile creare un livello di storage per identificare ciascun tipo. La creazione dei gradi di storage consente di selezionare un tipo specifico di nodo di storage durante la configurazione dei pool di storage.

Se il livello di storage non è un problema (ad esempio, tutti i nodi di storage sono identici), è possibile saltare questa procedura e utilizzare il livello di storage predefinito di tutti i nodi di storage durante la configurazione dei pool di storage.

Quando si aggiunge un nuovo nodo di storage in un'espansione, tale nodo viene aggiunto al livello di storage predefinito di tutti i nodi di storage. Di conseguenza:

- Se una regola ILM utilizza un pool di storage con il grado All Storage Node, il nuovo nodo può essere utilizzato immediatamente dopo il completamento dell'espansione.
- Se una regola ILM utilizza un pool di storage con un livello di storage personalizzato, il nuovo nodo non verrà utilizzato fino a quando non si assegna manualmente il livello di storage personalizzato al nodo, come descritto di seguito.

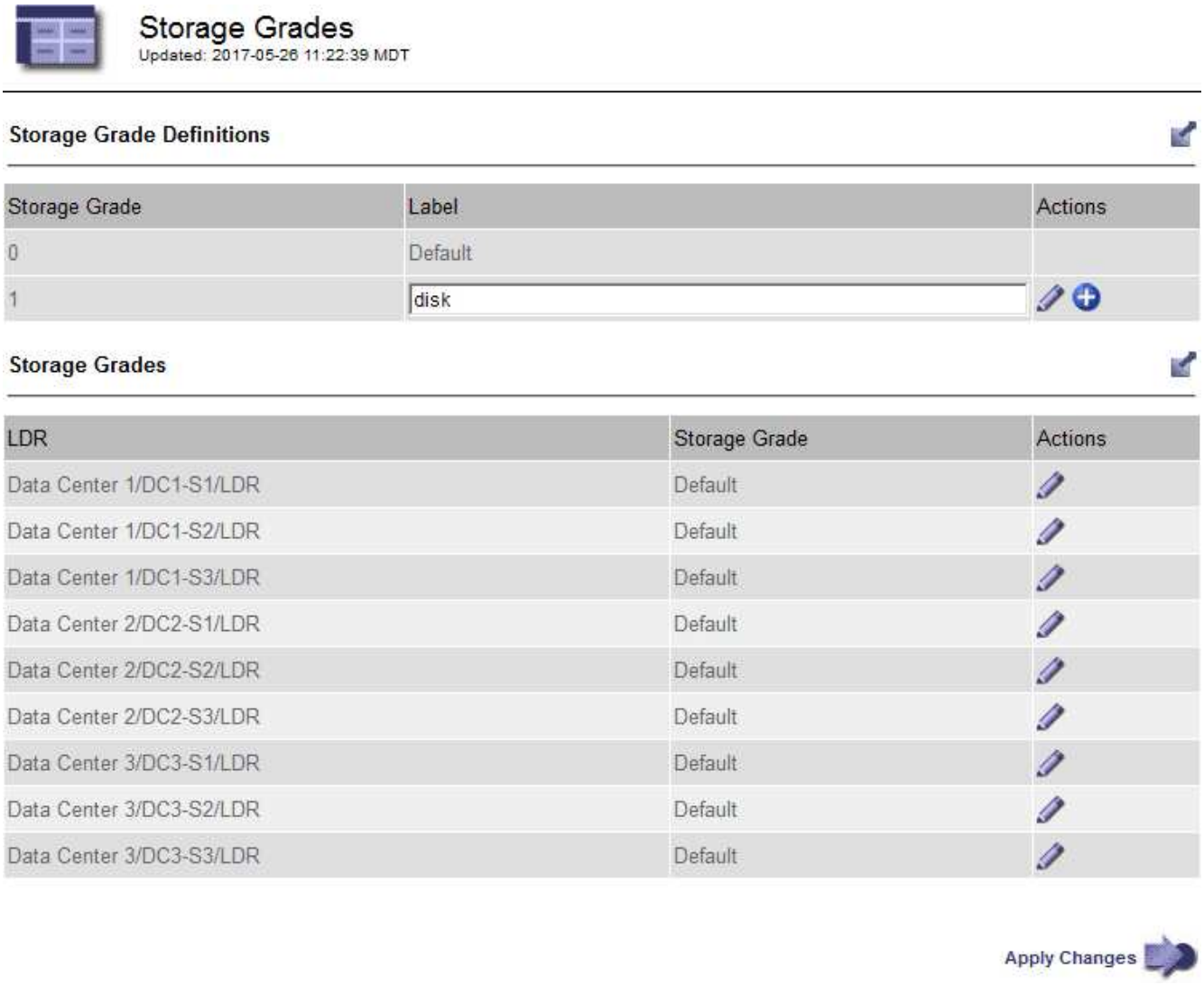
> Durante la creazione dei livelli di storage, non creare più livelli di storage del necessario. Ad esempio, non creare un livello di storage per ciascun nodo di storage. Assegnare invece ogni livello di storage a due o più nodi. I gradi di storage assegnati a un solo nodo possono causare backlog ILM se tale nodo non è più disponibile.

Fasi

1. Selezionare **ILM** > **Storage Grades**.
2. Creare un livello di storage:

   a. Per ogni livello di storage da definire, fare clic su **Inserisci** per aggiungere una riga e inserire un'etichetta per il livello di storage.

      Impossibile modificare il livello di storage predefinito. È riservato ai nuovi nodi di storage aggiunti durante l'espansione del sistema StorageGRID.



a. Per modificare un livello di storage esistente, fare clic su **Edit** (Modifica) e modificare l'etichetta secondo necessità.

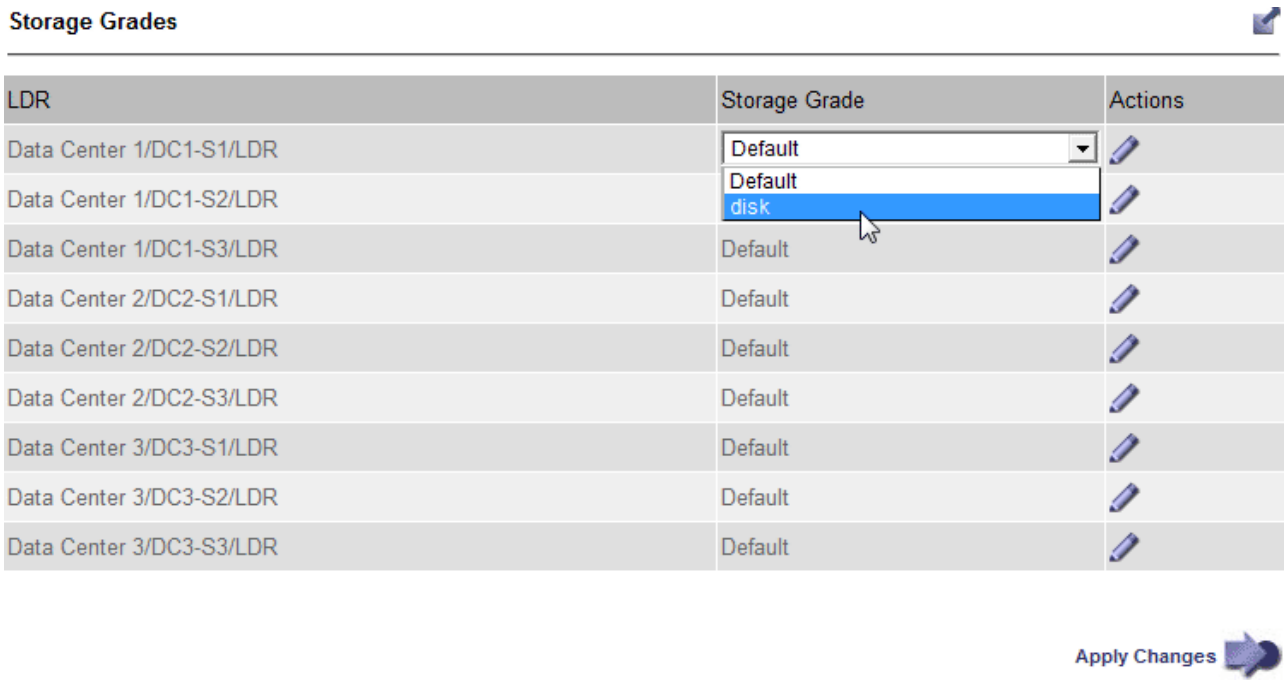
> Non è possibile eliminare i gradi di storage.

b. Fare clic su **Applica modifiche**.

   Questi livelli di storage sono ora disponibili per l'assegnazione ai nodi di storage.

3. Assegnare un livello di storage a un nodo di storage:

   a. Per il servizio LDR di ciascun nodo di storage, fare clic su **Edit** (Modifica) e selezionare un livello di storage dall'elenco.



Assegnare un grado di storage a un nodo di storage specifico una sola volta. Un nodo di storage recuperato dal guasto mantiene il livello di storage assegnato in precedenza. Non modificare questa assegnazione dopo l'attivazione del criterio ILM. Se l'assegnazione viene modificata, i dati vengono memorizzati in base al nuovo livello di storage.

a. Fare clic su **Applica modifiche**.

Configurazione dei pool di storage

Quando si definisce una regola ILM, si utilizzano i pool di storage per specificare dove memorizzare gli oggetti . Prima di creare un pool di storage, è necessario rivedere le linee guida del pool di storage.

- "Che cos'è un pool di storage"
- "Linee guida per la creazione di pool di storage"
- "Utilizzo di più pool di storage per la replica tra siti"
- "Utilizzo di un pool di storage come posizione temporanea (obsoleto)"
- "Creazione di un pool di storage"
- "Visualizzazione dei dettagli del pool di storage"
- "Modifica di un pool di storage"
- "Rimozione di un pool di storage"

Che cos'è un pool di storage

Un pool di storage è un raggruppamento logico di nodi di storage o nodi di archivio. I pool di storage vengono configurati per determinare dove il sistema StorageGRID memorizza i dati a oggetti e il tipo di storage utilizzato.

I pool di storage hanno due attributi:

- **Storage grade**: Per i nodi di storage, le performance relative dello storage di backup.
- **Sito**: Il data center in cui verranno memorizzati gli oggetti.

I pool di storage vengono utilizzati nelle regole ILM per determinare dove sono memorizzati i dati degli oggetti. Quando si configurano le regole ILM per la replica, si selezionano uno o più pool di storage che includono nodi di storage o nodi di archivio. Quando si creano profili di codifica Erasure, si seleziona un pool di storage che include i nodi di storage.

Linee guida per la creazione di pool di storage

Per la configurazione e l'utilizzo dei pool di storage, attenersi alle seguenti linee guida.

Linee guida per tutti i pool di storage

- StorageGRID include un pool di storage predefinito, tutti i nodi di storage, che utilizza il sito predefinito, tutti i siti e il livello di storage predefinito, tutti i nodi di storage. Il pool di storage All Storage Node viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti del data center.

> Si sconsiglia di utilizzare il pool di storage All Storage Node o il sito All Sites perché questi elementi vengono aggiornati automaticamente per includere i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato. Prima di utilizzare il pool di storage All Storage Node o il sito predefinito, rivedere attentamente le linee guida per le copie replicate e codificate per l'erasure.

- Le configurazioni del pool di storage sono il più semplici possibile. Non creare più pool di storage del necessario.
- Creare pool di storage con il maggior numero possibile di nodi. Ogni pool di storage deve contenere due o più nodi. Un pool di storage con nodi insufficienti può causare backlog ILM se un nodo diventa non disponibile.
- Evitare di creare o utilizzare pool di storage che si sovrappongono (contenenti uno o più degli stessi nodi). Se i pool di storage si sovrappongono, è possibile che più di una copia dei dati dell'oggetto venga salvata sullo stesso nodo.

Linee guida per i pool di storage utilizzati per le copie replicate

- Creare un pool di storage diverso per ciascun sito. Quindi, specificare uno o più pool di storage specifici del sito nelle istruzioni di posizionamento per ciascuna regola. L'utilizzo di un pool di storage per ciascun sito garantisce che le copie degli oggetti replicate vengano posizionate esattamente dove ci si aspetta (ad esempio, una copia di ogni oggetto in ogni sito per la protezione dalla perdita di sito).
- Se si aggiunge un sito in un'espansione, creare un nuovo pool di storage per il nuovo sito. Quindi, aggiornare le regole ILM per controllare quali oggetti sono memorizzati nel nuovo sito.
- In generale, non utilizzare il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti.

Linee guida per i pool di storage utilizzati per le copie erasure-coded

- Non è possibile utilizzare i nodi di archiviazione per i dati con codifica erasure.
- Il numero di nodi e siti di storage contenuti nel pool di storage determina quali schemi di erasure coding sono disponibili.
- Se un pool di storage include solo due siti, non è possibile utilizzare tale pool di storage per la cancellazione del codice. Non sono disponibili schemi di erasure coding per un pool di storage con due siti.

- In generale, non utilizzare il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti in qualsiasi profilo di codifica Erasure.

> Se la griglia include un solo sito, non è possibile utilizzare il pool di storage All Storage Node o il sito predefinito All Sites in un profilo di codifica Erasure. Questo comportamento impedisce che il profilo di codifica Erasure diventi non valido se viene aggiunto un secondo sito.

- Se si hanno requisiti di throughput elevati, la creazione di un pool di storage che include più siti non è consigliata se la latenza di rete tra siti è superiore a 100 ms. Con l'aumentare della latenza, la velocità con cui StorageGRID può creare, posizionare e recuperare frammenti di oggetti diminuisce drasticamente a causa della diminuzione del throughput di rete TCP. La diminuzione del throughput influisce sui tassi massimi raggiungibili di acquisizione e recupero degli oggetti (quando si seleziona Strict o Balanced come comportamento Ingest) o può portare a backlog della coda ILM (quando viene selezionato Dual Commit come comportamento Ingest).
- Se possibile, un pool di storage deve includere un numero superiore al numero minimo di nodi di storage richiesto per lo schema di erasure coding selezionato. Ad esempio, se si utilizza uno schema di erasure coding 6+3, è necessario disporre di almeno nove nodi di storage. Tuttavia, si consiglia di disporre di almeno un nodo di storage aggiuntivo per sito.
- Distribuire i nodi di storage tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di erasure coding 6+3, configurare un pool di storage che includa almeno tre nodi di storage in tre siti.

Linee guida per i pool di storage utilizzati per le copie archiviate

- Non è possibile creare un pool di storage che includa nodi di storage e nodi di archiviazione. Le copie archiviate richiedono un pool di storage che includa solo i nodi di archiviazione.
- Quando si utilizza un pool di storage che include nodi di archiviazione, è necessario mantenere almeno una copia replicata o codificata in cancellazione su un pool di storage che include nodi di storage.
- Se l'impostazione blocco oggetti S3 globale è attivata e si sta creando una regola ILM conforme, non è possibile utilizzare un pool di storage che include nodi di archiviazione. Vedere le istruzioni per la gestione degli oggetti con S3 Object Lock.
- Se il tipo di destinazione di un nodo di archiviazione è Cloud Tiering - Simple Storage Service (S3), il nodo di archiviazione deve trovarsi nel proprio pool di storage. Consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

"Che cos'è la replica"

"Che cos'è la cancellazione dei codici"

"Quali sono gli schemi di erasure coding"

"Utilizzo di più pool di storage per la replica tra siti"

"Utilizzo di un pool di storage come posizione temporanea (obsoleto)"

"Gestione degli oggetti con S3 Object Lock"

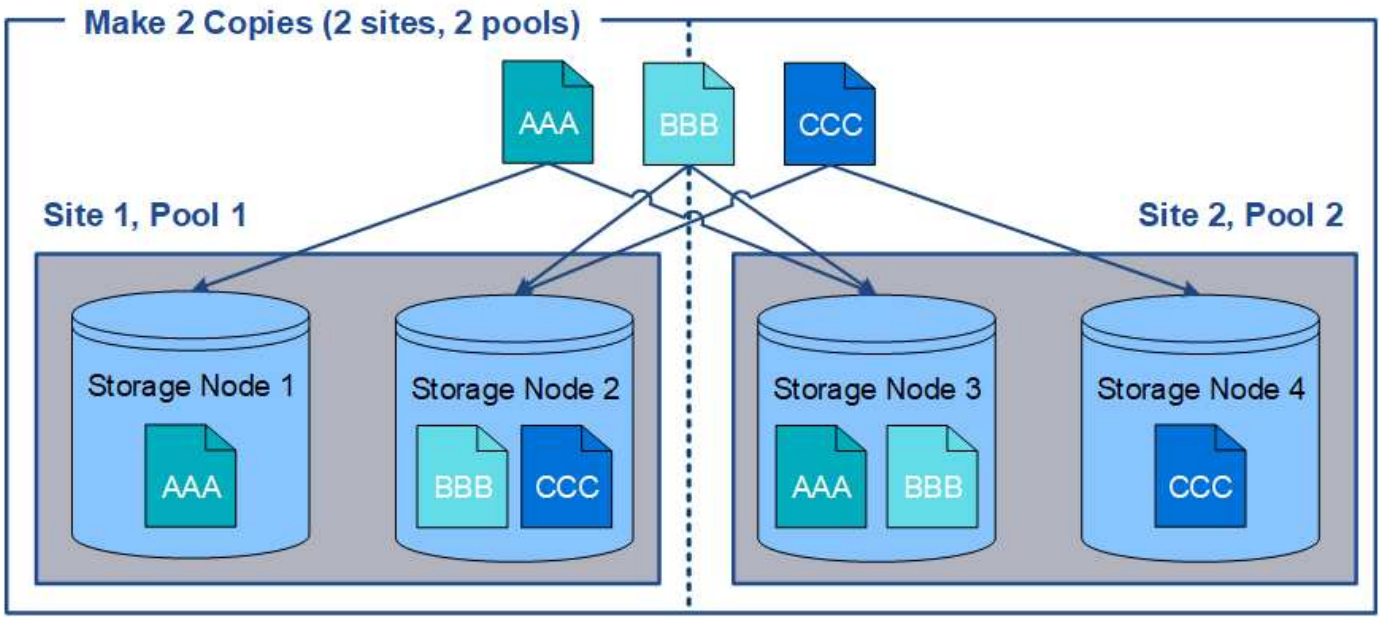
"Amministrare StorageGRID"

Utilizzo di più pool di storage per la replica tra siti

Se l'implementazione di StorageGRID include più siti, è possibile attivare la protezione dalla perdita di sito creando un pool di storage per ciascun sito e specificando entrambi i pool di storage nelle istruzioni di posizionamento della regola. Ad esempio, se si configura una regola ILM per eseguire due copie replicate e specificare pool di storage in due siti, una copia di ciascun oggetto verrà posizionata in ciascun sito. Se si configura una regola per eseguire due copie e si specificano tre pool di storage, le copie vengono distribuite in modo da bilanciare l'utilizzo del disco tra i pool di storage, garantendo al contempo che le due copie vengano memorizzate in siti diversi.

Nell'esempio seguente viene illustrato cosa può accadere se una regola ILM inserisce copie di oggetti replicate in un singolo pool di storage contenente nodi di storage da due siti. Poiché il sistema utilizza i nodi disponibili nel pool di storage quando inserisce le copie replicate, potrebbe posizionare tutte le copie di alcuni oggetti all'interno di uno solo dei siti. In questo esempio, il sistema ha memorizzato due copie di Object AAA sui nodi di storage nel sito 1 e due copie di Object CCC sui nodi di storage nel sito 2. Solo il BBB oggetto è protetto se uno dei siti si guasta o diventa inaccessibile.

Al contrario, questo esempio illustra come vengono memorizzati gli oggetti quando si utilizzano più pool di storage. Nell'esempio, la regola ILM specifica che devono essere create due copie replicate di ciascun oggetto e che le copie devono essere distribuite in due pool di storage. Ogni pool di storage contiene tutti i nodi di storage in un sito. Poiché una copia di ciascun oggetto viene memorizzata in ogni sito, i dati dell'oggetto sono protetti da guasti o inaccessibilità del sito.



Quando si utilizzano più pool di storage, tenere presenti le seguenti regole:

- Se si creano n copie, è necessario aggiungere n o più pool di storage. Ad esempio, se una regola è configurata per eseguire tre copie, è necessario specificare tre o più pool di storage.
- Se il numero di copie corrisponde al numero di pool di storage, viene memorizzata una copia dell'oggetto in ciascun pool di storage.
- Se il numero di copie è inferiore al numero di pool di storage, il sistema distribuisce le copie per mantenere bilanciato l'utilizzo del disco tra i pool e garantire che due o più copie non vengano memorizzate nello

stesso pool di storage.

- Se i pool di storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. È necessario assicurarsi che i pool di storage selezionati non contengano gli stessi nodi di storage.

Utilizzo di un pool di storage come posizione temporanea (obsoleto)

Quando si crea una regola ILM con un posizionamento degli oggetti che include un singolo pool di storage, viene richiesto di specificare un secondo pool di storage da utilizzare come posizione temporanea.

Le posizioni temporanee sono state deprecate e verranno rimosse in una release futura. Non selezionare un pool di storage come posizione temporanea per una nuova regola ILM.

> Se si seleziona il comportamento di acquisizione rigorosa (fase 3 della procedura guidata Crea regola ILM), la posizione temporanea viene ignorata.

Informazioni correlate

"Opzioni di protezione dei dati per l'acquisizione"

Creazione di un pool di storage

Si creano pool di storage per determinare dove il sistema StorageGRID memorizza i dati a oggetti e il tipo di storage utilizzato. Ogni pool di storage include uno o più siti e uno o più tipi di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver esaminato le linee guida per la creazione di pool di storage.

A proposito di questa attività

I pool di storage determinano la posizione in cui vengono memorizzati i dati degli oggetti. Il numero di pool di storage necessari dipende dal numero di siti nella griglia e dal tipo di copie desiderato: Replicate o con codifica di cancellazione.

- Per la replica e l'erasure coding a sito singolo, creare un pool di storage per ciascun sito. Ad esempio, se si desidera memorizzare copie di oggetti replicate in tre siti, creare tre pool di storage.
- Per la cancellazione del codice in tre o più siti, creare un pool di storage che includa una voce per ciascun sito. Ad esempio, se si desidera erasure gli oggetti del codice in tre siti, creare un pool di storage. Selezionare l'icona più ➕ per aggiungere una voce per ciascun sito.

> Non includere il sito All Sites predefinito in un pool di storage che verrà utilizzato in un profilo di codifica Erasure. Al contrario, aggiungere una voce separata al pool di storage per ogni sito che memorizzerà i dati codificati in cancellazione. Vedere questo passo ad esempio.

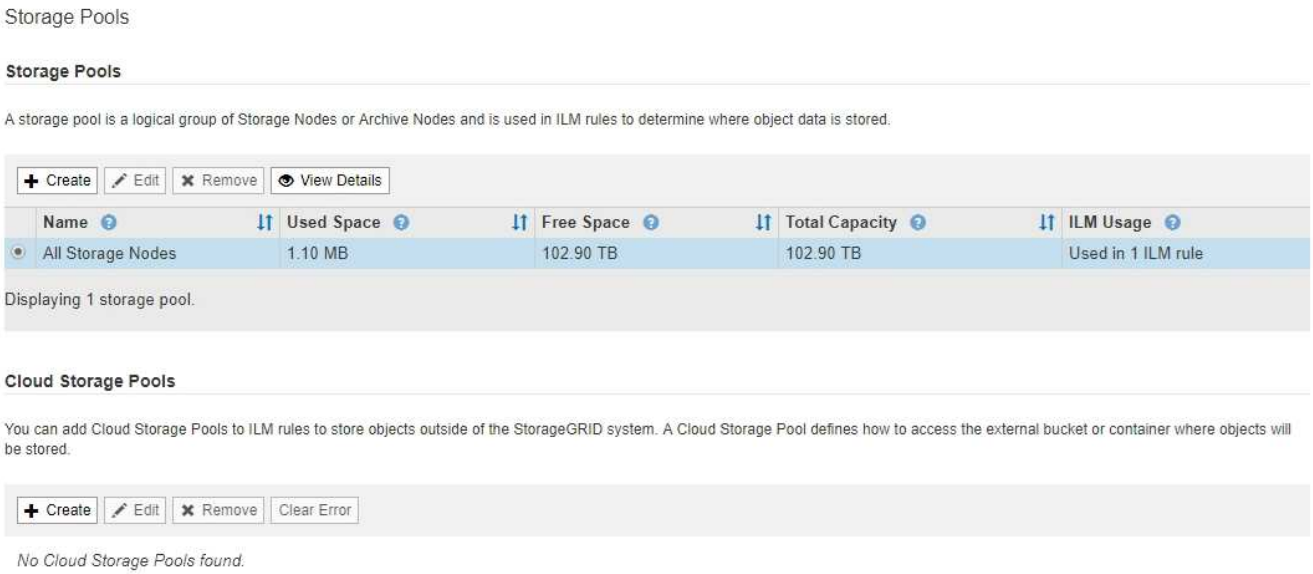
- Se si dispone di più storage di livello, non creare un pool di storage che includa diversi tipi di storage in un singolo sito.

"Linee guida per la creazione di pool di storage"

Fasi

1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools (Pool di storage) che elenca tutti i pool di storage definiti.

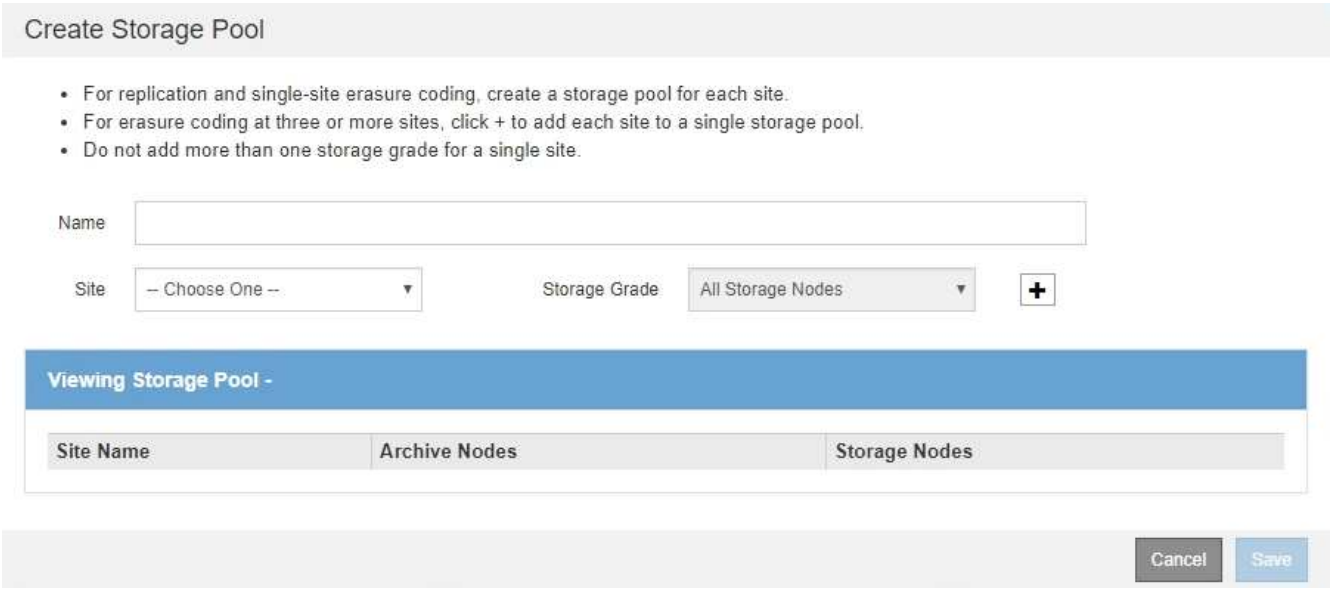


   L'elenco include il pool di storage predefinito del sistema, tutti i nodi di storage, che utilizza il sito predefinito del sistema, tutti i siti e il livello di storage predefinito, tutti i nodi di storage.

   > Poiché il pool di storage All Storage Node viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti del data center, si sconsiglia di utilizzare questo pool di storage nelle regole ILM.

2. Per creare un nuovo pool di storage, selezionare **Crea**.

   Viene visualizzata la finestra di dialogo Create Storage Pool (Crea pool di storage).



3. Immettere un nome univoco per il pool di storage.

Utilizzare un nome facilmente identificabile quando si configurano i profili di codifica Erasure e le regole ILM.

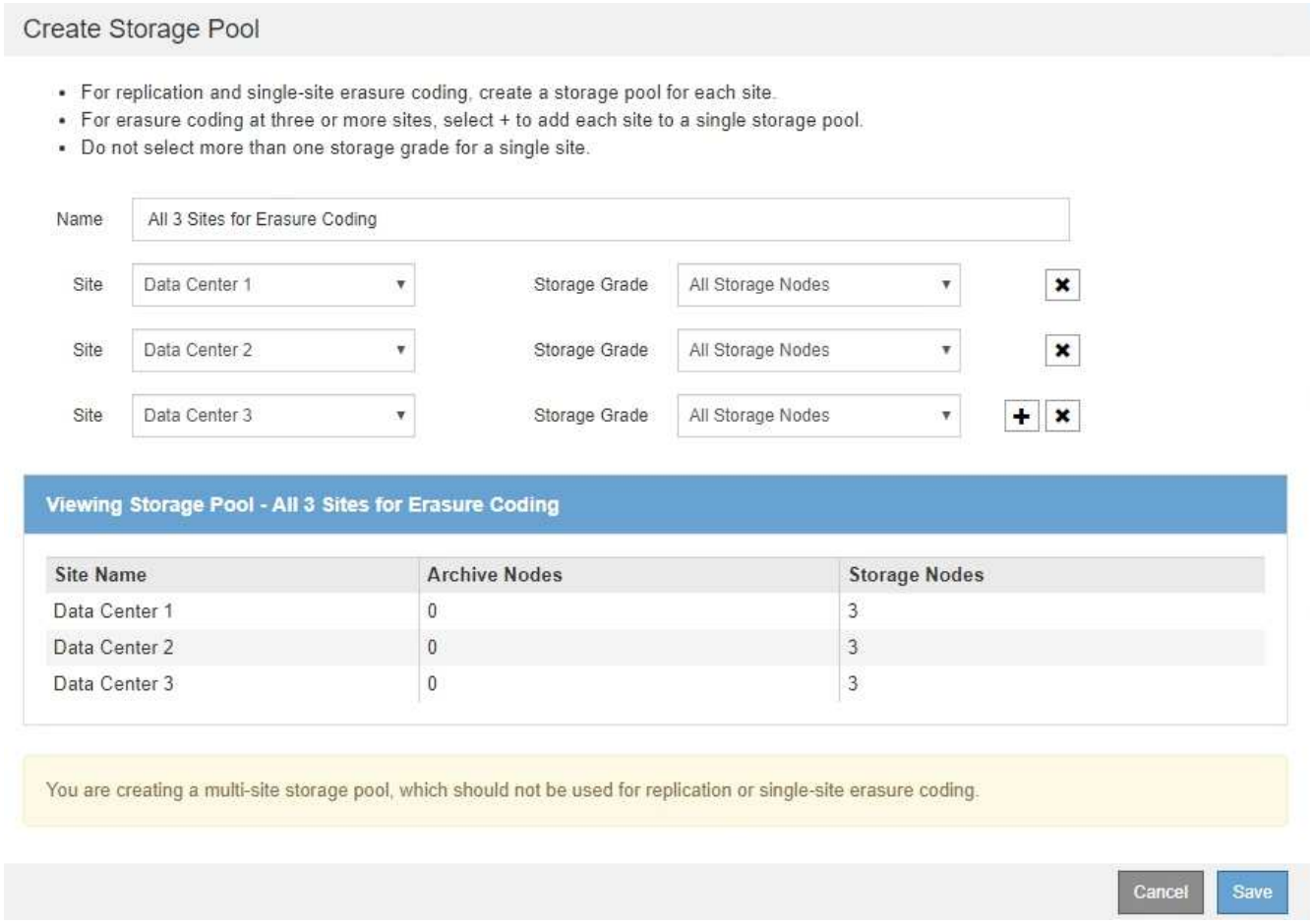
4. Dall'elenco a discesa **Sito**, selezionare un sito per questo pool di storage.

   Quando si seleziona un sito, il numero di nodi di storage e di nodi di archiviazione nella tabella viene aggiornato automaticamente.

5. Dall'elenco a discesa **Storage Grade**, selezionare il tipo di storage da utilizzare se una regola ILM utilizza questo pool di storage.

   Il livello di storage predefinito di All Storage Node include tutti i nodi di storage nel sito selezionato. Il livello di storage dei nodi di archiviazione predefinito include tutti i nodi di archiviazione nel sito selezionato. Se sono stati creati altri gradi di storage per i nodi di storage nel grid, questi vengono elencati nell'elenco a discesa.

6. se si desidera utilizzare il pool di storage in un profilo di codifica Erasure multi-sito, selezionare ➕ per aggiungere una voce per ciascun sito al pool di storage.



Non è possibile creare voci duplicate o creare un pool di storage che includa sia il livello di storage **Archive Node** che qualsiasi livello di storage che contenga i nodi di storage.

Viene visualizzato un avviso se si aggiungono più voci per un sito ma con diversi gradi di storage.

Per rimuovere una voce, selezionare ✖.

7. Quando si è soddisfatti delle selezioni effettuate, selezionare **Save** (Salva).

   Il nuovo pool di storage viene aggiunto all'elenco.

Informazioni correlate

"Linee guida per la creazione di pool di storage"

Visualizzazione dei dettagli del pool di storage

È possibile visualizzare i dettagli di un pool di storage per determinare dove viene utilizzato il pool di storage e per vedere quali nodi e gradi di storage sono inclusi.

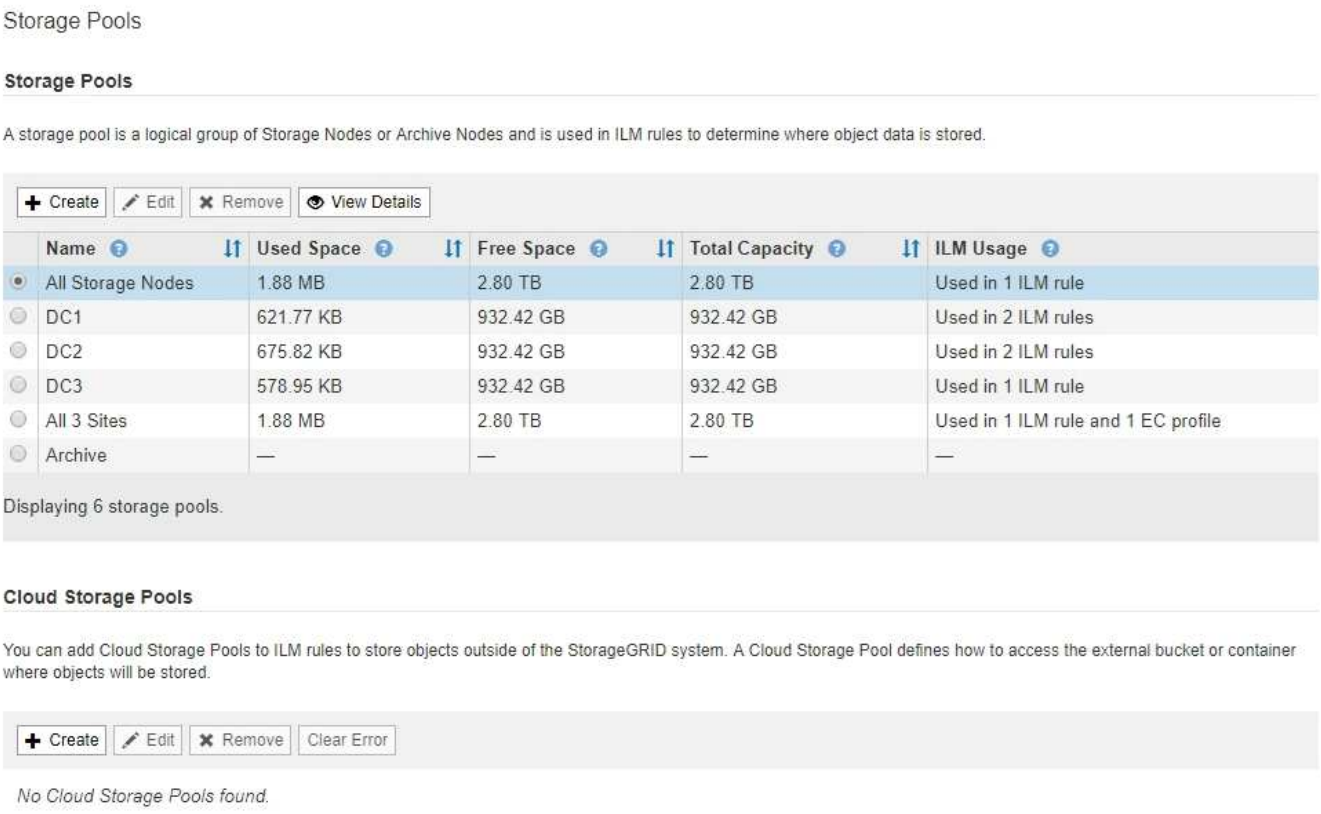
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools. In questa pagina sono elencati tutti i pool di storage definiti.



   La tabella include le seguenti informazioni per ogni pool di storage che include i nodi di storage:

   - **Name**: Il nome univoco del pool di storage.
   - **Spazio utilizzato**: La quantità di spazio attualmente utilizzata per memorizzare gli oggetti nel pool di storage.
   - **Spazio libero**: La quantità di spazio disponibile per memorizzare gli oggetti nel pool di storage.

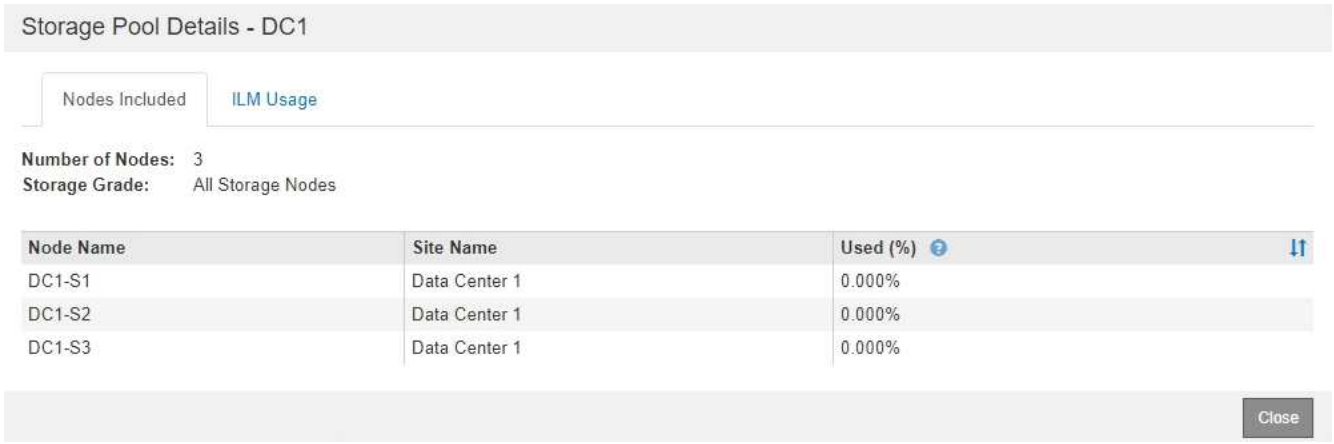
- **Capacità totale**: La dimensione del pool di storage, che equivale alla quantità totale di spazio utilizzabile per i dati oggetto per tutti i nodi nel pool di storage .
- **ILM Usage**: Modalità di utilizzo del pool di storage. Un pool di storage potrebbe essere inutilizzato o utilizzato in una o più regole ILM, profili di codifica Erasure o entrambi.

> Non è possibile rimuovere un pool di storage se è in uso.

2. Per visualizzare i dettagli relativi a uno specifico pool di storage, selezionare il relativo pulsante di opzione e selezionare **Visualizza dettagli**.

   Viene visualizzato il modale Storage Pool Details (Dettagli pool di storage

3. Visualizzare la scheda **nodi inclusi** per informazioni sui nodi di storage o di archivio inclusi nel pool di storage.



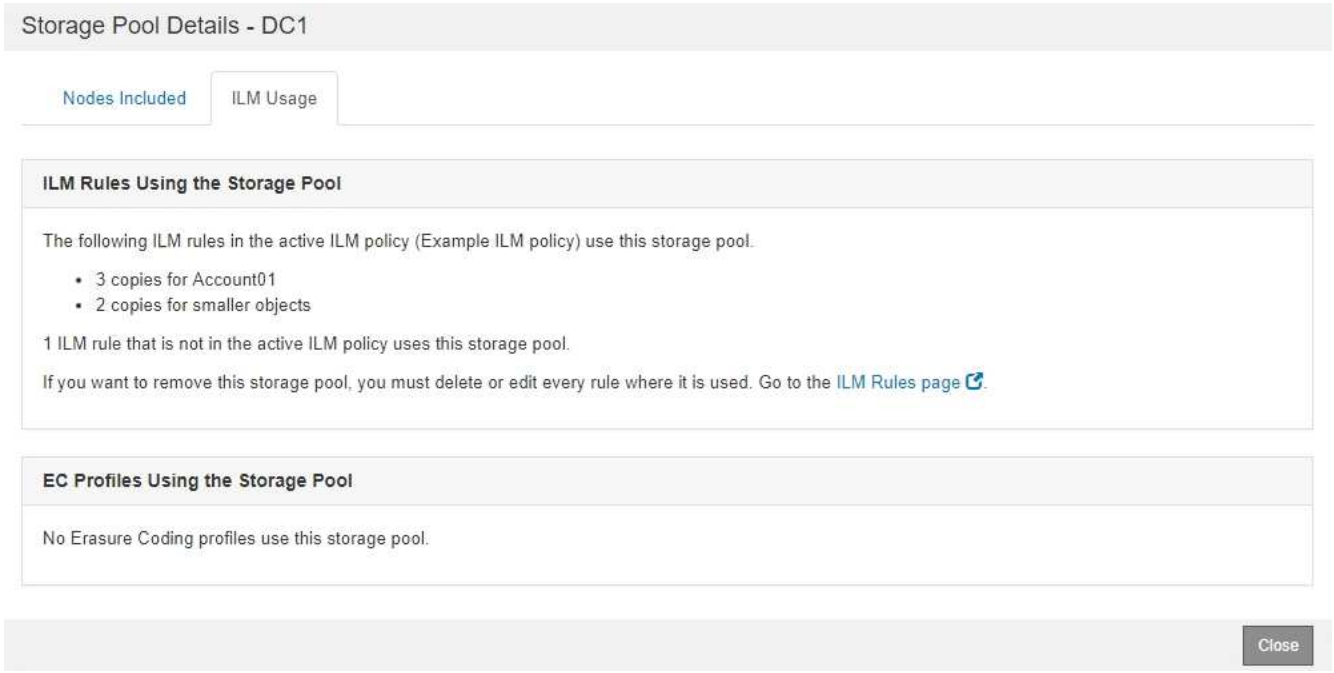
   La tabella include le seguenti informazioni per ciascun nodo:

   - Nome del nodo
   - Nome del sito
   - Utilizzato (%): Per i nodi di storage, la percentuale dello spazio utilizzabile totale per i dati dell'oggetto che è stato utilizzato. Questo valore non include i metadati degli oggetti.

> Lo stesso valore utilizzato (%) viene mostrato anche nel grafico Storage Used - Object Data per ciascun nodo di storage (selezionare **Nodes** > ***Storage Node*** > **Storage**).

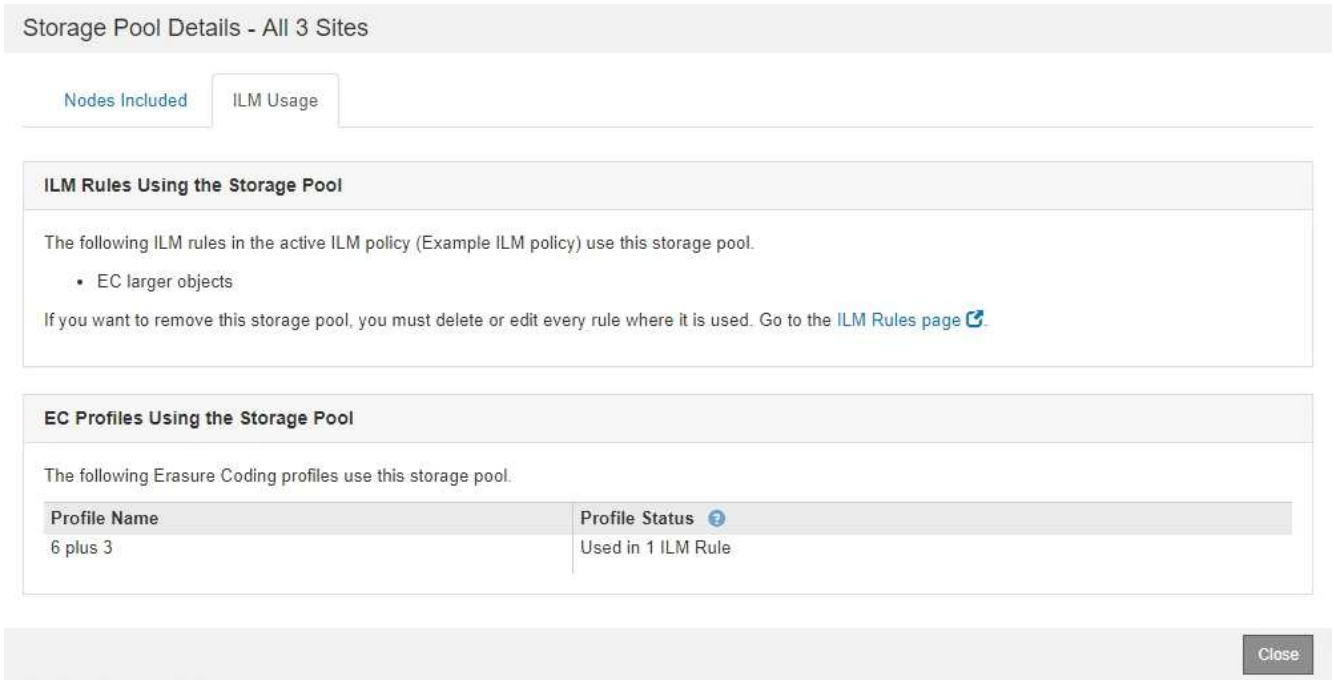
4. Selezionare la scheda **utilizzo ILM** per determinare se il pool di storage è attualmente utilizzato in qualsiasi regola ILM o profilo di codifica Erasure.

   In questo esempio, il pool di storage DC1 viene utilizzato in tre regole ILM: Due regole che si trovano nel criterio ILM attivo e una regola che non si trova nel criterio attivo.



Non è possibile rimuovere un pool di storage se utilizzato in una regola ILM.

In questo esempio, il pool di storage di tutti e 3 i siti viene utilizzato in un profilo di codifica Erasure. A sua volta, il profilo di codifica Erasure viene utilizzato da una regola ILM nel criterio ILM attivo.



Non è possibile rimuovere un pool di storage se utilizzato in un profilo di codifica Erasure.

5. Se si desidera, accedere alla pagina **ILM Rules** per informazioni e gestione delle regole che utilizzano il pool di storage.

   Consultare le istruzioni per l'utilizzo delle regole ILM.

6. Una volta visualizzati i dettagli del pool di storage, selezionare **Chiudi**.

Informazioni correlate

"Utilizzo delle regole ILM e delle policy ILM"

Modifica di un pool di storage

È possibile modificare un pool di storage per modificarne il nome o per aggiornare siti e gradi di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver esaminato le linee guida per la creazione di pool di storage.
- Se si intende modificare un pool di storage utilizzato da una regola nel criterio ILM attivo, è necessario considerare come le modifiche influiranno sul posizionamento dei dati degli oggetti.

A proposito di questa attività

Se si aggiunge un nuovo livello di storage a un pool di storage utilizzato nel criterio ILM attivo, tenere presente che i nodi di storage nel nuovo livello di storage non verranno utilizzati automaticamente. Per forzare StorageGRID a utilizzare un nuovo livello di storage, è necessario attivare un nuovo criterio ILM dopo aver salvato il pool di storage modificato.

Fasi

1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools.

2. Selezionare il pulsante di opzione per il pool di storage che si desidera modificare.

   Non è possibile modificare il pool di storage di tutti i nodi di storage.

3. Selezionare **Modifica**.
4. Se necessario, modificare il nome del pool di storage.
5. Se necessario, selezionare altri siti e livelli di storage.

   > Se il pool di storage viene utilizzato in un profilo di codifica Erasure e la modifica causerebbe l'invalidità dello schema di erasure coding, non sarà possibile modificare il livello di sito o storage. Ad esempio, se un pool di storage utilizzato in un profilo di codifica Erasure include attualmente un livello di storage con un solo sito, non è possibile utilizzare un livello di storage con due siti, poiché la modifica renderebbe lo schema di erasure-coding non valido.

6. Selezionare **Salva**.

Al termine

Se è stato aggiunto un nuovo livello di storage a un pool di storage utilizzato nel criterio ILM attivo, attivare un nuovo criterio ILM per forzare StorageGRID a utilizzare il nuovo livello di storage. Ad esempio, clonare il criterio ILM esistente e attivare il clone.

Rimozione di un pool di storage

È possibile rimuovere un pool di storage che non viene utilizzato.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools.

2. Esaminare la colonna ILM Usage nella tabella per determinare se è possibile rimuovere il pool di storage.

   Non è possibile rimuovere un pool di storage se utilizzato in una regola ILM o in un profilo di codifica Erasure. Se necessario, selezionare **View Details** > **ILM Usage** (Visualizza dettagli* > **ILM Usage**) per determinare dove viene utilizzato un pool di storage.

3. Se il pool di storage che si desidera rimuovere non viene utilizzato, selezionare il pulsante di opzione.
4. Selezionare **Rimuovi**.
5. Selezionare **OK**.

Utilizzo dei Cloud Storage Pools

È possibile utilizzare i pool di storage cloud per spostare gli oggetti StorageGRID in una posizione di storage esterna, ad esempio lo storage S3 Glacier o Microsoft Azure Blob. Lo spostamento di oggetti all'esterno della griglia consente di sfruttare un Tier di storage a basso costo per l'archiviazione a lungo termine.

- "Cos'è un pool di storage cloud"
- "Ciclo di vita di un oggetto Cloud Storage Pool"
- "Quando utilizzare i Cloud Storage Pools"
- "Considerazioni per i Cloud Storage Pools"
- "Confronto tra Cloud Storage Pools e la replica CloudMirror"
- "Creazione di un pool di storage cloud"
- "Modifica di un pool di storage cloud"
- "Rimozione di un pool di storage cloud"
- "Risoluzione dei problemi relativi ai pool di storage cloud"

Cos'è un pool di storage cloud

Un pool di storage cloud consente di utilizzare ILM per spostare i dati degli oggetti all'esterno del sistema StorageGRID. Ad esempio, è possibile spostare gli oggetti con accesso non frequente in uno storage cloud a basso costo, ad esempio Amazon S3 Glacier, S3 Glacier Deep Archive o il Tier di accesso all'archivio nello storage Microsoft Azure Blob. In alternativa, è possibile mantenere un backup cloud degli oggetti

StorageGRID per migliorare il disaster recovery.

Dal punto di vista di ILM, un pool di storage cloud è simile a un pool di storage. Per memorizzare gli oggetti in entrambe le posizioni, selezionare il pool quando si creano le istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di storage sono costituiti da nodi di storage o nodi di archiviazione all'interno del sistema StorageGRID, un pool di storage cloud è costituito da un bucket esterno (S3) o da un container (storage blob Azure).

La seguente tabella confronta i pool di storage con i pool di storage cloud e mostra le analogie e le differenze di alto livello.

	Pool di storage	**Pool di cloud storage**
Come viene creato?	Utilizzando l'opzione **ILM** > **Storage Pools** in Grid Manager. È necessario impostare i gradi di storage prima di poter creare il pool di storage.	Utilizzando l'opzione **ILM** > **Storage Pools** in Grid Manager. È necessario configurare il bucket o il container esterno prima di poter creare il Cloud Storage Pool.
Quanti pool è possibile creare?	Senza limiti.	Fino a 10.

	Pool di storage	Pool di cloud storage
Dove sono memorizzati gli oggetti?	Su uno o più nodi di storage o nodi di archiviazione all'interno di StorageGRID.	In un bucket Amazon S3 o in un container di storage Azure Blob esterno al sistema StorageGRID. Se il Cloud Storage Pool è un bucket Amazon S3: • È possibile configurare un ciclo di vita del bucket per la transizione di oggetti a storage a lungo termine e a basso costo, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema di storage esterno deve supportare la classe di storage Glacier e l'API di ripristino degli oggetti S3 POST. • È possibile creare pool di storage cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta l'AWS Secret Region. Se il pool di storage cloud è un container di storage Azure Blob, StorageGRID passa l'oggetto al Tier di archiviazione. **Nota:** in generale, non configurare la gestione del ciclo di vita dello storage Azure Blob per il container utilizzato per un pool di storage cloud. Le operazioni DI ripristino POST-oggetto sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nel criterio ILM attivo.	Una regola ILM nel criterio ILM attivo.
Quale metodo di protezione dei dati viene utilizzato?	Replica o erasure coding.	Replica.
Quante copie di ciascun oggetto sono consentite?	Multiplo.	Una copia nel pool di storage cloud e, facoltativamente, una o più copie in StorageGRID. **Nota:** non è possibile memorizzare un oggetto in più di un Cloud Storage Pool alla volta.
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Storage a basso costo.

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti memorizzati in ciascun tipo di Cloud Storage Pool.

Informazioni correlate

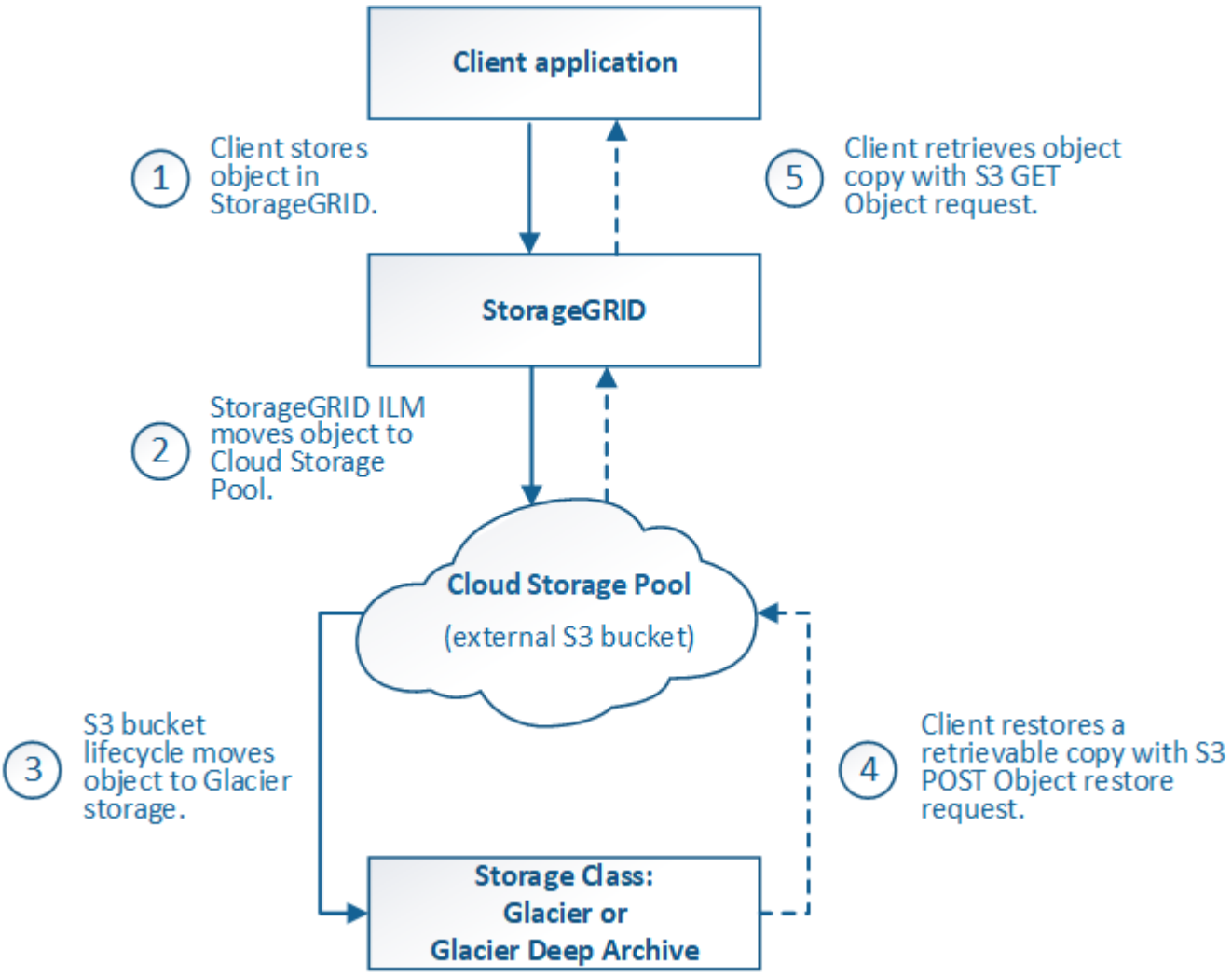
S3: Ciclo di vita di un oggetto Cloud Storage Pool

Azure: Ciclo di vita di un oggetto Cloud Storage Pool]

S3: Ciclo di vita di un oggetto Cloud Storage Pool

La figura mostra le fasi del ciclo di vita di un oggetto memorizzato in un pool di storage cloud S3.

> Nella figura e nelle spiegazioni, “Glacier” si riferisce sia alla classe di storage Glacier che alla classe di storage Glacier Deep Archive, con un’eccezione: La classe di storage Glacier Deep Archive non supporta il Tier di ripristino accelerato. È supportato solo il recupero in blocco o standard.



1. **Oggetto memorizzato in StorageGRID**

   Per avviare il ciclo di vita, un’applicazione client memorizza un oggetto in StorageGRID.

2. **Oggetto spostato in S3 Cloud Storage Pool**
   - Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di storage cloud.
   - Quando l'oggetto è stato spostato nel pool di storage cloud S3, l'applicazione client può recuperarlo utilizzando una richiesta di oggetti Get S3 da StorageGRID, a meno che l'oggetto non sia stato trasferito allo storage Glacier.
3. **Oggetto in transizione a Glacier (stato non recuperabile)**
   - Facoltativamente, l'oggetto può essere passato allo storage Glacier. Ad esempio, il bucket S3 esterno potrebbe utilizzare la configurazione del ciclo di vita per trasferire un oggetto allo storage Glacier immediatamente o dopo un certo numero di giorni.

> Se si desidera eseguire la transizione degli oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione di storage che implementi la classe di storage Glacier e supporti l'API di ripristino degli oggetti S3 POST.

> Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino DEGLI oggetti POST, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti allo storage S3 Glacier. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

   - Durante la transizione, l'applicazione client può utilizzare una richiesta di oggetto S3 HEAD per monitorare lo stato dell'oggetto.
4. **Oggetto ripristinato dallo storage Glacier**

   Se un oggetto è stato passato allo storage Glacier, l'applicazione client può emettere una richiesta di ripristino dell'oggetto S3 POST per ripristinare una copia recuperabile nel Cloud Storage Pool S3. La richiesta specifica il numero di giorni in cui la copia deve essere disponibile nel Cloud Storage Pool e il Tier di accesso ai dati da utilizzare per l'operazione di ripristino (accelerato, Standard o in blocco). Una volta raggiunta la data di scadenza della copia recuperabile, la copia viene automaticamente riportata in uno stato non recuperabile.

> Se una o più copie dell'oggetto esistono anche nei nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier inviando una richiesta DI ripristino DELL'oggetto POST. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

5. **Oggetto recuperato**

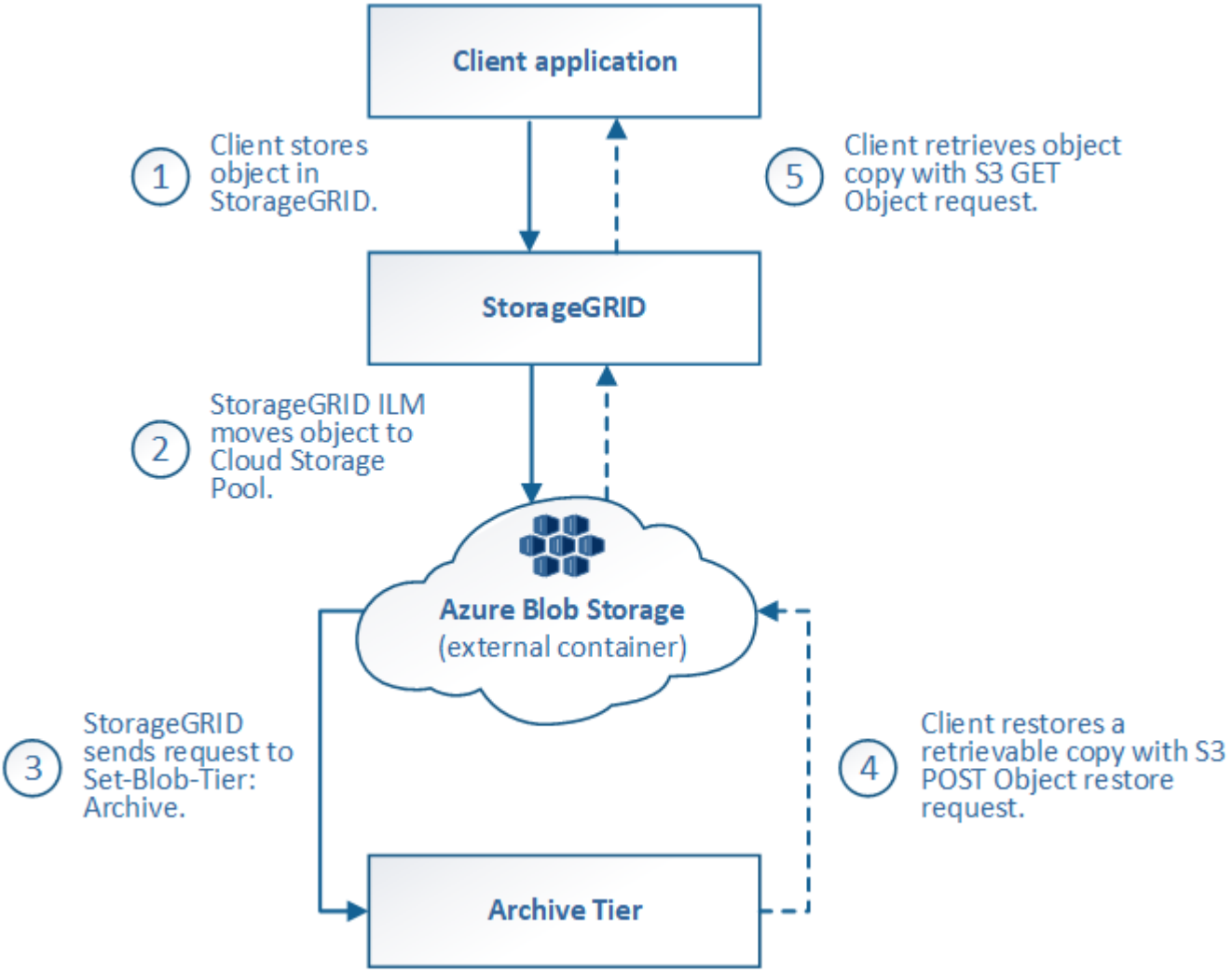
   Una volta ripristinato un oggetto, l'applicazione client può inviare una richiesta DI RECUPERO dell'oggetto ripristinato.

Informazioni correlate

"Utilizzare S3"

Azure: Ciclo di vita di un oggetto Cloud Storage Pool

La figura mostra le fasi del ciclo di vita di un oggetto memorizzato in un pool di storage Azure Cloud.



1. **Oggetto memorizzato in StorageGRID**

   Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. **Oggetto spostato in Azure Cloud Storage Pool**

   Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud Azure come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di storage blob Azure esterno specificato dal pool di storage cloud

   > Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino POST-oggetto, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti al Tier di archiviazione dello storage di Azure Blob. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

3. **Oggetto sottoposto a transizione al Tier di archiviazione (stato non recuperabile)**

   Subito dopo aver spostato l'oggetto nel pool di storage cloud di Azure, StorageGRID passa

automaticamente l'oggetto al livello di archiviazione dello storage Blob di Azure.

4. **Oggetto ripristinato dal Tier di archiviazione**

   Se un oggetto è stato passato al Tier Archive, l'applicazione client può emettere una richiesta di ripristino dell'oggetto S3 POST per ripristinare una copia recuperabile nel pool di storage di Azure Cloud.

   Quando StorageGRID riceve IL ripristino dell'oggetto POST, passa temporaneamente l'oggetto al livello di raffreddamento dello storage di Azure Blob. Non appena viene raggiunta la data di scadenza nella richiesta DI ripristino DELL'oggetto POST, StorageGRID riconsegna l'oggetto al livello di archiviazione.

   > Se una o più copie dell'oggetto esistono anche nei nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso di archiviazione inviando una richiesta DI ripristino POST-oggetto. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

5. **Oggetto recuperato**

   Una volta ripristinato un oggetto in Azure Cloud Storage Pool, l'applicazione client può inviare una richiesta DI RECUPERO dell'oggetto ripristinato.

Quando utilizzare i Cloud Storage Pools

I pool di cloud storage possono offrire vantaggi significativi in diversi casi di utilizzo.

Backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un pool di storage cloud per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati dell'oggetto nel pool di storage cloud possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario emettere una richiesta di ripristino S3 POST Object per accedere alla copia dell'oggetto di backup nel Cloud Storage Pool.

I dati dell'oggetto in un pool di storage cloud possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un guasto di un volume di storage o di un nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

Per implementare una soluzione di backup:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che memorizzi simultaneamente le copie degli oggetti sui nodi di storage (come copie replicate o codificate in cancellazione) e una singola copia degli oggetti nel Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Tiering dei dati da StorageGRID a una posizione esterna

È possibile utilizzare un pool di storage cloud per memorizzare oggetti all'esterno del sistema StorageGRID. Si supponga, ad esempio, di disporre di un elevato numero di oggetti da conservare, ma si prevede di accedervi raramente, se mai. È possibile utilizzare un pool di storage cloud per tierare gli oggetti in modo da ridurre il costo dello storage e liberare spazio in StorageGRID.

Per implementare una soluzione di tiering:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che sposti gli oggetti utilizzati raramente dai nodi di storage al Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Mantenere più endpoint cloud

Puoi configurare più Cloud Storage Pool se desideri eseguire il tiering o il backup dei dati degli oggetti in più di un cloud. I filtri nelle regole ILM consentono di specificare quali oggetti sono memorizzati in ciascun Cloud Storage Pool. Ad esempio, è possibile memorizzare oggetti di alcuni tenant o bucket in Amazon S3 Glacier e oggetti di altri tenant o bucket nello storage Azure Blob. In alternativa, puoi spostare i dati tra lo storage Amazon S3 Glacier e Azure Blob. Quando si utilizzano più Cloud Storage Pool, tenere presente che un oggetto può essere memorizzato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 pool di cloud storage.
2. Configurare le regole ILM in modo che memorizzino i dati dell'oggetto appropriati all'ora appropriata in ciascun Cloud Storage Pool. Ad esempio, memorizzare oggetti dal bucket A nel Cloud Storage Pool A e memorizzare oggetti dal bucket B nel Cloud Storage Pool B. Oppure, memorizzare gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e spostarli nel Cloud Storage Pool B.
3. Aggiungere le regole alla policy ILM. Quindi, simulare e attivare la policy.

Considerazioni per i Cloud Storage Pools

Se si prevede di utilizzare un pool di storage cloud per spostare oggetti fuori dal sistema StorageGRID, è necessario esaminare le considerazioni relative alla configurazione e all'utilizzo dei pool di storage cloud.

Considerazioni generali

- In generale, lo storage di archiviazione cloud, come Amazon S3 Glacier o Azure Blob, è un luogo conveniente per memorizzare i dati degli oggetti. Tuttavia, i costi per recuperare i dati dallo storage di archiviazione cloud sono relativamente elevati. Per ottenere il costo complessivo più basso, è necessario considerare quando e con quale frequenza accedere agli oggetti nel Cloud Storage Pool. L'utilizzo di un Cloud Storage Pool è consigliato solo per i contenuti ai quali si prevede di accedere con frequenza limitata.
- Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino POST-oggetto, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti allo storage S3 Glacier o al Tier di archiviazione dello storage Blob Azure. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).
- L'utilizzo dei pool di storage cloud con FabricPool non è supportato a causa della latenza aggiunta per recuperare un oggetto dalla destinazione del pool di storage cloud.

Informazioni necessarie per creare un pool di storage cloud

Prima di creare un Cloud Storage Pool, è necessario creare il bucket S3 esterno o il container di storage Azure Blob esterno da utilizzare per il Cloud Storage Pool. Quindi, quando si crea il pool di storage cloud in StorageGRID, è necessario specificare le seguenti informazioni:

- Il tipo di provider: Storage Amazon S3 o Azure Blob.
- Se si seleziona Amazon S3, specificare se il Cloud Storage Pool deve essere utilizzato con l'AWS Secret Region (**CAP (C2S Access Portal)**).
- Il nome esatto del bucket o del container.
- L'endpoint del servizio doveva accedere al bucket o al container.
- L'autenticazione necessaria per accedere al bucket o al container:
  - **S3**: Facoltativamente, un ID della chiave di accesso e una chiave di accesso segreta.
  - **C2S**: L'URL completo per ottenere le credenziali temporanee dal server CAP; un certificato CA del server, un certificato client, una chiave privata per il certificato client e, se la chiave privata è crittografata, la passphrase per la decrittografia.
  - **Azure Blob storage**: Un nome account e una chiave account. Queste credenziali devono disporre dell'autorizzazione completa per il container.
- Facoltativamente, un certificato CA personalizzato per verificare le connessioni TLS al bucket o al container.

Considerazioni sulle porte utilizzate per i pool di cloud storage

Per garantire che le regole ILM possano spostare oggetti da e verso il Cloud Storage Pool specificato, è necessario configurare la rete o le reti che contengono i nodi di storage del sistema. È necessario assicurarsi che le seguenti porte possano comunicare con il Cloud Storage Pool.

Per impostazione predefinita, i Cloud Storage Pool utilizzano le seguenti porte:

- **80**: Per gli URI endpoint che iniziano con http
- **443**: Per gli URI endpoint che iniziano con https

È possibile specificare una porta diversa quando si crea o si modifica un Cloud Storage Pool.

Se si utilizza un server proxy non trasparente, è necessario configurare anche un proxy di storage per consentire l'invio dei messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Considerazioni sui costi

L'accesso allo storage nel cloud utilizzando un Cloud Storage Pool richiede la connettività di rete al cloud. Devi considerare il costo dell'infrastruttura di rete che utilizzerai per accedere al cloud e fornirlo in modo appropriato, in base alla quantità di dati che prevederai di spostare tra StorageGRID e il cloud utilizzando il pool di storage cloud.

Quando StorageGRID si connette all'endpoint esterno del pool di storage nel cloud, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Anche se a queste richieste saranno associati costi aggiuntivi, il costo del monitoraggio di un pool di storage cloud dovrebbe essere solo una piccola frazione del costo complessivo di storage degli oggetti in S3 o Azure.

Se si devono spostare gli oggetti da un endpoint esterno del pool di cloud storage a StorageGRID, potrebbero verificarsi costi più significativi. Gli oggetti possono essere spostati di nuovo in StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un pool di storage cloud e si decide di memorizzare l'oggetto in StorageGRID. In questo caso, è sufficiente riconfigurare le regole e le policy ILM. Quando si verifica la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal pool di storage cloud. StorageGRID crea quindi localmente il numero specificato di copie replicate o codificate per la

cancellazione. Una volta spostato di nuovo l'oggetto in StorageGRID, la copia nel pool di storage cloud viene eliminata.

- Gli oggetti vengono persi a causa di un guasto al nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

> Quando gli oggetti vengono spostati di nuovo in StorageGRID da un pool di storage cloud, StorageGRID invia più richieste all'endpoint del pool di storage cloud per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

La policy del bucket per il bucket S3 esterno utilizzato per un pool di storage cloud deve concedere l'autorizzazione StorageGRID per spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando richiesto e molto altro ancora. Idealmente, StorageGRID dovrebbe avere un accesso completo al bucket (`s3:*`); tuttavia, se ciò non è possibile, il criterio bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Considerazioni sul ciclo di vita del bucket esterno

Lo spostamento degli oggetti tra StorageGRID e il bucket S3 esterno specificato nel pool di storage cloud è controllato dalle regole ILM e dalla policy ILM attiva in StorageGRID. Al contrario, la transizione degli oggetti dal bucket S3 esterno specificato nel Cloud Storage Pool ad Amazon S3 Glacier o S3 Glacier Deep Archive (o a una soluzione di storage che implementa la classe di storage Glacier) è controllata dalla configurazione del ciclo di vita di tale bucket.

Se si desidera eseguire la transizione di oggetti dal Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e utilizzare una soluzione di storage che implementa la classe di storage Glacier e supporta l'API S3 POST Object Restore.

Ad esempio, supponiamo che tutti gli oggetti spostati da StorageGRID al pool di storage cloud debbano essere trasferiti immediatamente allo storage Amazon S3 Glacier. Creare una configurazione del ciclo di vita sul bucket S3 esterno che specifica una singola azione (**transizione**) come segue:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Questa regola trasferirebbe tutti gli oggetti bucket al Glacier Amazon S3 il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al pool di storage cloud).

> Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai le azioni **Expiration** per definire quando gli oggetti scadono. Le azioni di scadenza fanno sì che il sistema di storage esterno elimini gli oggetti scaduti. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non viene trovato.

Se si desidera trasferire oggetti nel Cloud Storage Pool in S3 Glacier Deep Archive (invece di Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tenere presente che non è possibile utilizzare `Expedited` tier per ripristinare gli oggetti da S3 Glacier Deep Archive.

Azure: Considerazioni per il Tier di accesso

Quando si configura un account di storage Azure, è possibile impostare il Tier di accesso predefinito su Hot o Cool. Quando si crea un account storage da utilizzare con un Cloud Storage Pool, è necessario utilizzare l'hot Tier come Tier predefinito. Anche se StorageGRID imposta immediatamente il Tier per l'archiviazione quando sposta gli oggetti nel pool di storage cloud, l'utilizzo dell'impostazione predefinita di Hot garantisce che non venga addebitata una tariffa per l'eliminazione anticipata degli oggetti rimossi dal Tier Cool prima del minimo di 30 giorni.

Azure: Gestione del ciclo di vita non supportata

Non utilizzare la gestione del ciclo di vita dello storage Azure Blob per il container utilizzato con un pool di storage cloud. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

"Creazione di un pool di storage cloud"

"S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"

"C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"

"Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud"

"Amministrare StorageGRID"

Confronto tra Cloud Storage Pools e la replica CloudMirror

Quando si inizia a utilizzare i pool di storage cloud, potrebbe essere utile comprendere le analogie e le differenze tra i pool di storage cloud e il servizio di replica di StorageGRID CloudMirror.

	Pool di cloud storage	Servizio di replica di CloudMirror
Qual è lo scopo principale?	Un Cloud Storage Pool agisce come destinazione di archiviazione. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure può essere una copia aggiuntiva. Ovvero, invece di mantenere due copie on-premise, puoi conservare una sola copia all'interno di StorageGRID e inviarne una copia al pool di storage cloud.	Il servizio di replica CloudMirror consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). La replica di CloudMirror crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come viene configurato?	I pool di cloud storage vengono definiti allo stesso modo dei pool di storage, utilizzando Grid Manager o l'API Grid Management. È possibile selezionare un Cloud Storage Pool come posizione di posizionamento in una regola ILM. Mentre un pool di storage è costituito da un gruppo di nodi di storage, un pool di storage cloud viene definito utilizzando un endpoint remoto S3 o Azure (indirizzo IP, credenziali e così via).	Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. Una volta configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.
Chi è responsabile della sua configurazione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Tier Azure Blob Archive	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3)
Qual è la causa dello spostamento degli oggetti nella destinazione?	Una o più regole ILM nel criterio ILM attivo. Le regole ILM definiscono gli oggetti che StorageGRID sposta nel pool di storage cloud e quando gli oggetti vengono spostati.	L'atto di inserire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror.gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.

	Pool di cloud storage	Servizio di replica di CloudMirror
Come vengono recuperati gli oggetti?	Le applicazioni devono effettuare richieste a StorageGRID per recuperare gli oggetti spostati in un pool di storage cloud. Se l'unica copia di un oggetto è stata trasferita allo storage di archiviazione, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia mirrorata nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.
Puoi leggere direttamente dalla destinazione?	No Gli oggetti spostati in un pool di storage cloud vengono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero dal pool di storage cloud).	Sì, perché la copia mirrorata è una copia indipendente.
Cosa succede se un oggetto viene cancellato dall'origine?	L'oggetto viene eliminato anche nel Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto cancellato non esiste più nel bucket StorageGRID, ma continua ad esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.
Come si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID guasti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, pertanto è possibile accedervi direttamente prima del ripristino dei nodi StorageGRID.

Informazioni correlate

"Amministrare StorageGRID"

Creazione di un pool di storage cloud

Quando crei un pool di storage cloud, specifica il nome e la posizione del bucket o del container esterno che StorageGRID utilizzerà per memorizzare gli oggetti, il tipo di provider cloud (Amazon S3 o Azure Blob Storage) e le informazioni necessarie per accedere al bucket o al container esterno da parte di StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

- Devi aver esaminato le linee guida per la configurazione dei Cloud Storage Pools.
- Il bucket o il container esterno a cui fa riferimento il Cloud Storage Pool deve esistere.
- È necessario disporre di tutte le informazioni di autenticazione necessarie per accedere al bucket o al container.

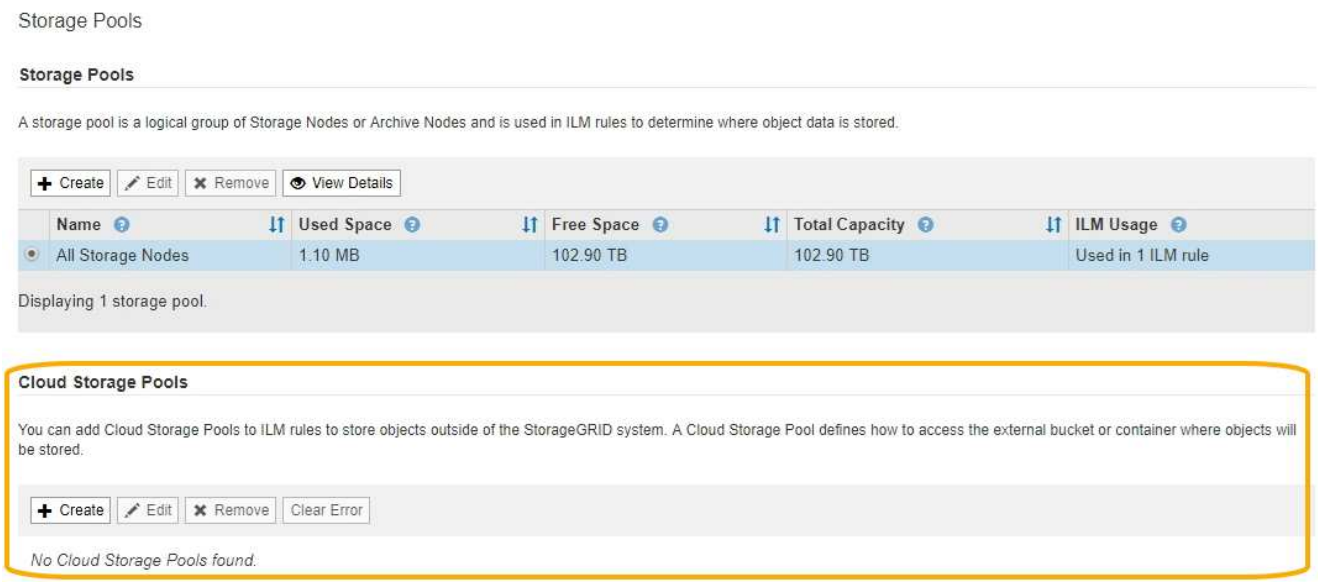
A proposito di questa attività

Un Cloud Storage Pool specifica un singolo bucket S3 esterno o un container di storage Azure Blob. StorageGRID convalida il pool di storage cloud non appena viene salvato, quindi devi assicurarti che il bucket o il container specificato nel pool di storage cloud esista e sia raggiungibile.

Fasi

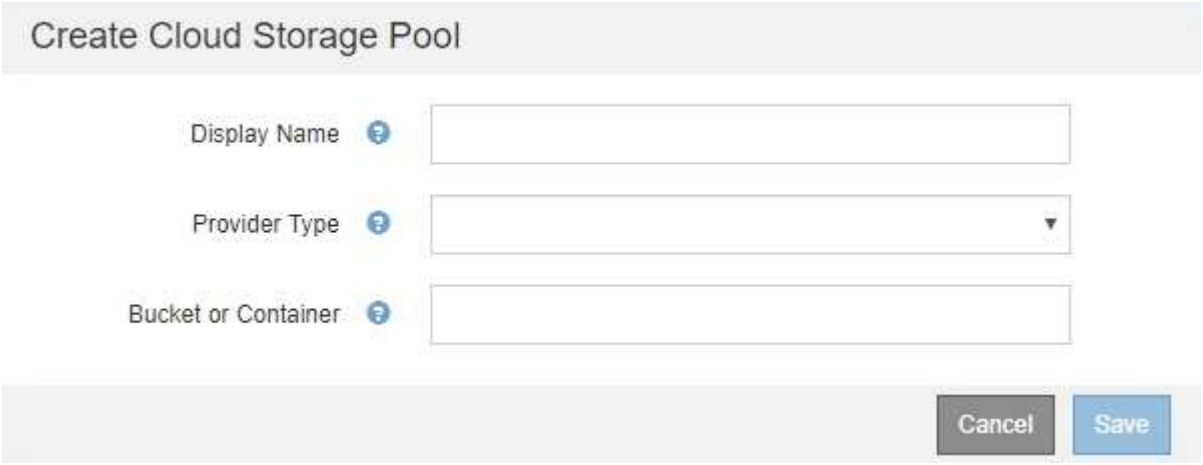
1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools. Questa pagina include due sezioni: Pool di storage e pool di storage cloud.



2. Nella sezione Cloud Storage Pools della pagina, fare clic su **Create** (Crea).

   Viene visualizzata la finestra di dialogo Create Cloud Storage Pool (Crea pool di storage cloud).



3. Inserire le seguenti informazioni:

Campo	Descrizione
Nome visualizzato	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Utilizzare un nome che sia facile da identificare quando si configurano le regole ILM.
Tipo di provider	Quale cloud provider utilizzerai per questo Cloud Storage Pool: • Amazon S3 (selezionare questa opzione per un pool di storage cloud S3 o C2S S3) • Azure Blob Storage **Nota:** quando si seleziona un tipo di provider, nella parte inferiore della pagina vengono visualizzate le sezioni Service Endpoint, Authentication e Server Verification.
Bucket o container	Il nome del bucket S3 esterno o del container Azure creato per il Cloud Storage Pool. Il nome specificato qui deve corrispondere esattamente al nome del bucket o del container, altrimenti la creazione del Cloud Storage Pool non avrà esito positivo. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

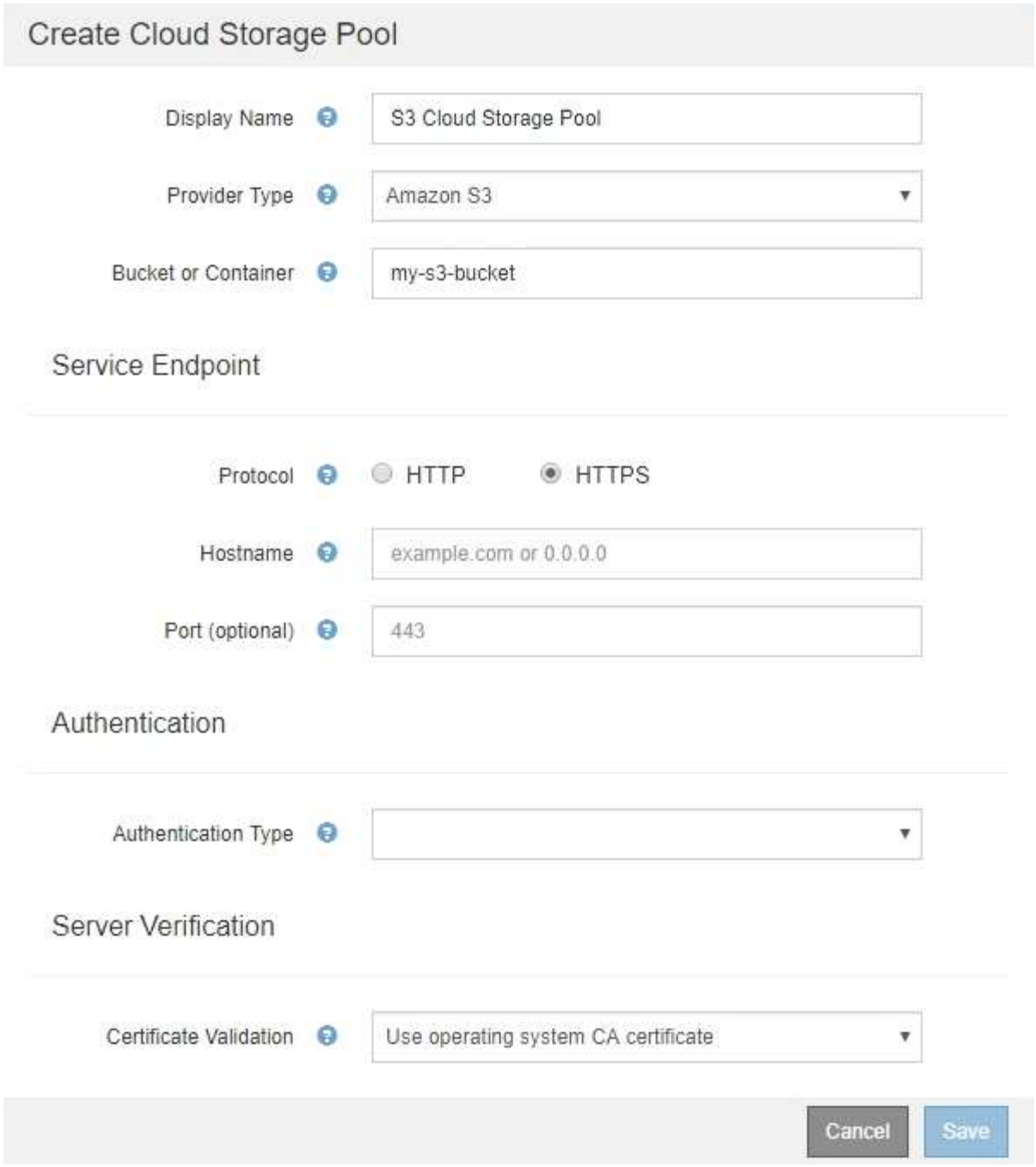
4. Completare le sezioni Service Endpoint, Authentication e Server Verification della pagina, in base al tipo di provider selezionato.
   - "S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"
   - "C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"
   - "Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud"

S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool

Quando si crea un Cloud Storage Pool per S3, è necessario selezionare il tipo di autenticazione richiesto per l'endpoint del Cloud Storage Pool. È possibile specificare Anonymous o immettere un ID della chiave di accesso e una chiave di accesso segreta.

Di cosa hai bisogno

- Devi aver inserito le informazioni di base per il Cloud Storage Pool e specificato **Amazon S3** come tipo di provider.



- Se si utilizza l'autenticazione della chiave di accesso, è necessario conoscere l'ID della chiave di accesso e la chiave di accesso segreta per il bucket S3 esterno.

Fasi

1. Nella sezione **Service Endpoint**, fornire le seguenti informazioni:

   a. Selezionare il protocollo da utilizzare per la connessione al Cloud Storage Pool.

      Il protocollo predefinito è HTTPS.

   b. Inserire il nome host del server o l'indirizzo IP del Cloud Storage Pool.

      Ad esempio:

`s3-aws-region.amazonaws.com`

> Non includere il nome del bucket in questo campo. Il nome del bucket viene incluso nel campo **bucket o container**.

a. Facoltativamente, specificare la porta da utilizzare per la connessione al Cloud Storage Pool.

   Lasciare vuoto questo campo per utilizzare la porta predefinita: Porta 443 per HTTPS o porta 80 per HTTP.

2. Nella sezione **Authentication**, selezionare il tipo di autenticazione richiesto per l'endpoint Cloud Storage Pool.

Opzione	Descrizione
Chiave di accesso	Per accedere al bucket Cloud Storage Pool sono necessari un ID della chiave di accesso e una chiave di accesso segreta.
Anonimo	Tutti hanno accesso al bucket Cloud Storage Pool. Non sono richiesti un ID della chiave di accesso e una chiave di accesso segreta.
CAP (portale di accesso C2S)	Utilizzato solo per C2S S3. Passare a. "C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool".

3. Se si seleziona Access Key (chiave di accesso), immettere le seguenti informazioni:

Opzione	Descrizione
ID chiave di accesso	L'ID della chiave di accesso per l'account proprietario del bucket esterno.
Chiave di accesso segreta	La chiave di accesso segreta associata.

4. Nella sezione verifica server, selezionare il metodo da utilizzare per convalidare il certificato per le connessioni TLS al Cloud Storage Pool:

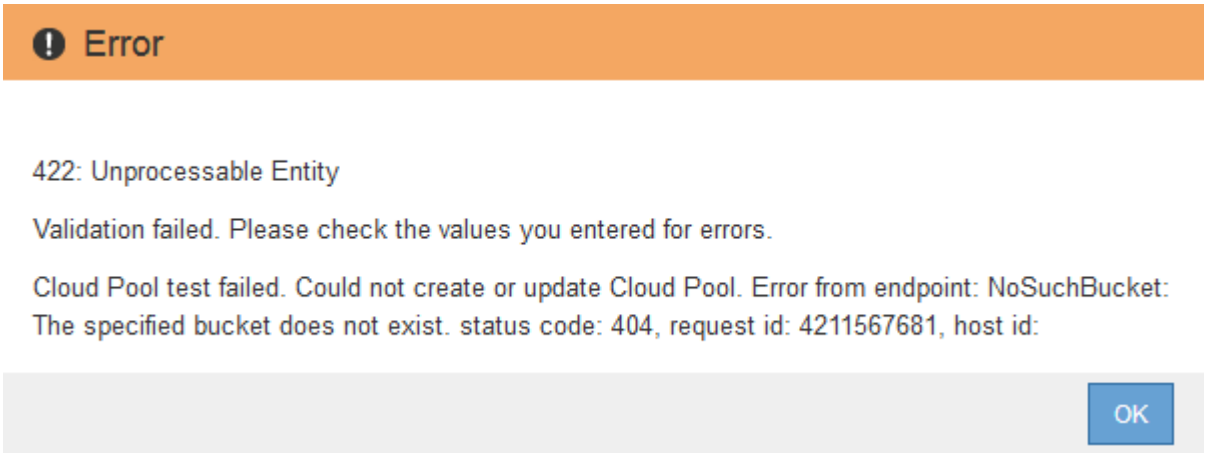
Opzione	Descrizione
Utilizzare il certificato CA del sistema operativo	Utilizzare i certificati CA predefiniti installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Fare clic su **Select New** (Seleziona nuovo) e caricare il certificato CA con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

5. Fare clic su **Save** (Salva).

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del bucket e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file di marker nel bucket per identificare il bucket come un Cloud Storage Pool. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket specificato non esiste già, potrebbe essere visualizzato un errore.



Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

"Risoluzione dei problemi relativi ai pool di storage cloud"

C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool

Per utilizzare il servizio servizi cloud commerciali (C2S) S3 come pool di storage cloud, è necessario configurare il portale di accesso C2S (CAP) come tipo di autenticazione, in modo che StorageGRID possa richiedere credenziali temporanee per accedere al bucket S3 nel proprio account C2S.

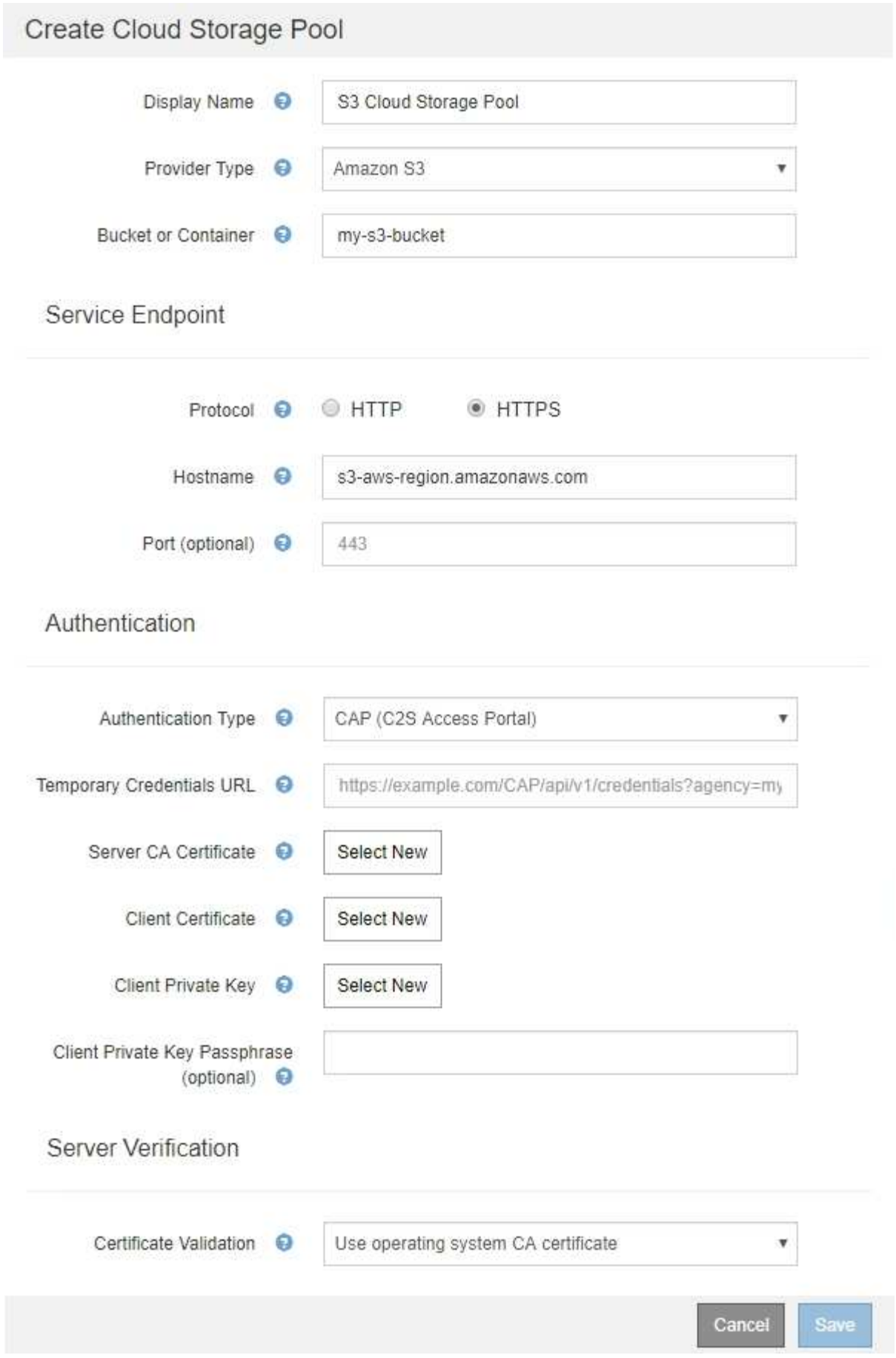
Di cosa hai bisogno

- Devi aver inserito le informazioni di base per un pool di storage cloud Amazon S3, incluso l'endpoint del servizio.
- È necessario conoscere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati all'account C2S.
- È necessario disporre di un certificato CA del server emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per verificare l'identità del server CAP. Il certificato CA del server deve utilizzare la codifica PEM.
- È necessario disporre di un certificato client emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per identificare se stesso nel server CAP. Il certificato client deve utilizzare la codifica PEM e deve avere ottenuto l'accesso all'account C2S.
- È necessario disporre di una chiave privata con codifica PEM per il certificato client.
- Se la chiave privata per il certificato client è crittografata, è necessario disporre della passphrase per decrittografare il certificato.

Fasi

1. Nella sezione **Authentication**, selezionare **CAP (C2S Access Portal)** dall'elenco a discesa **Authentication Type** (tipo di autenticazione).

   Vengono visualizzati i campi DI autenticazione CAP C2S.


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. Fornire le seguenti informazioni:
   a. Per **URL credenziali temporanee**, immettere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati all'account C2S.
   b. Per **certificato CA server**, fare clic su **Seleziona nuovo** e caricare il certificato CA con codifica PEM che StorageGRID utilizzerà per verificare il server CAP.
   c. Per **certificato client**, fare clic su **Seleziona nuovo** e caricare il certificato con codifica PEM che StorageGRID utilizzerà per identificarsi nel server CAP.
   d. Per **Client Private Key**, fare clic su **Select New** (Seleziona nuovo) e caricare la chiave privata con codifica PEM per il certificato del client.

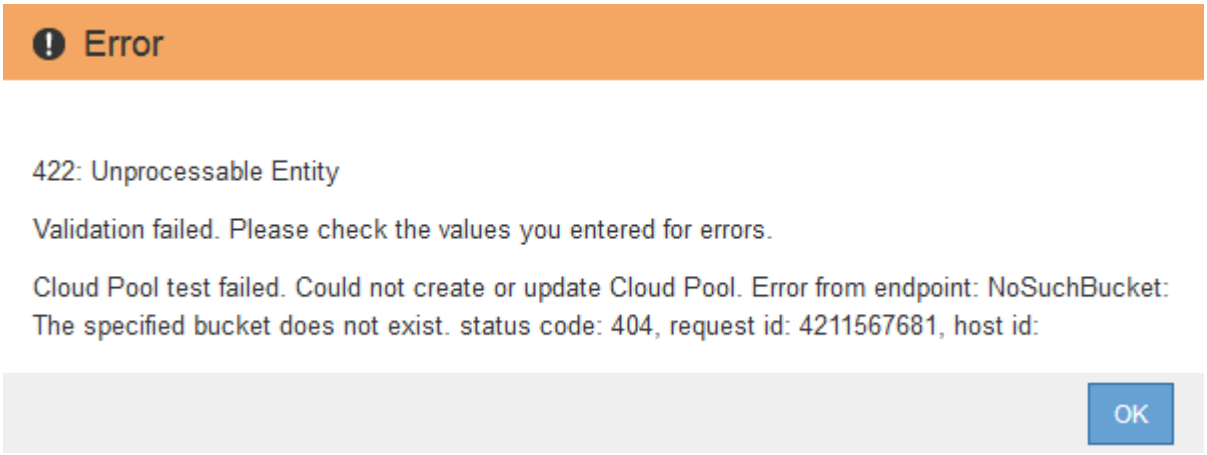
      Se la chiave privata è crittografata, è necessario utilizzare il formato tradizionale. (Il formato crittografato PKCS n. 8 non è supportato).

   e. Se la chiave privata del client è crittografata, immettere la passphrase per la decrittografia della chiave privata del client. In caso contrario, lasciare vuoto il campo **Client Private Key Passphrase** (Password chiave privata client).
3. Nella sezione verifica server, fornire le seguenti informazioni:
   a. Per **convalida certificato**, selezionare **Usa certificato CA personalizzato**.
   b. Fare clic su **Select New** (Seleziona nuovo) e caricare il certificato CA con codifica PEM.
4. Fare clic su **Save** (Salva).

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del bucket e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file di marker nel bucket per identificare il bucket come un Cloud Storage Pool. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket specificato non esiste già, potrebbe essere visualizzato un errore.



Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

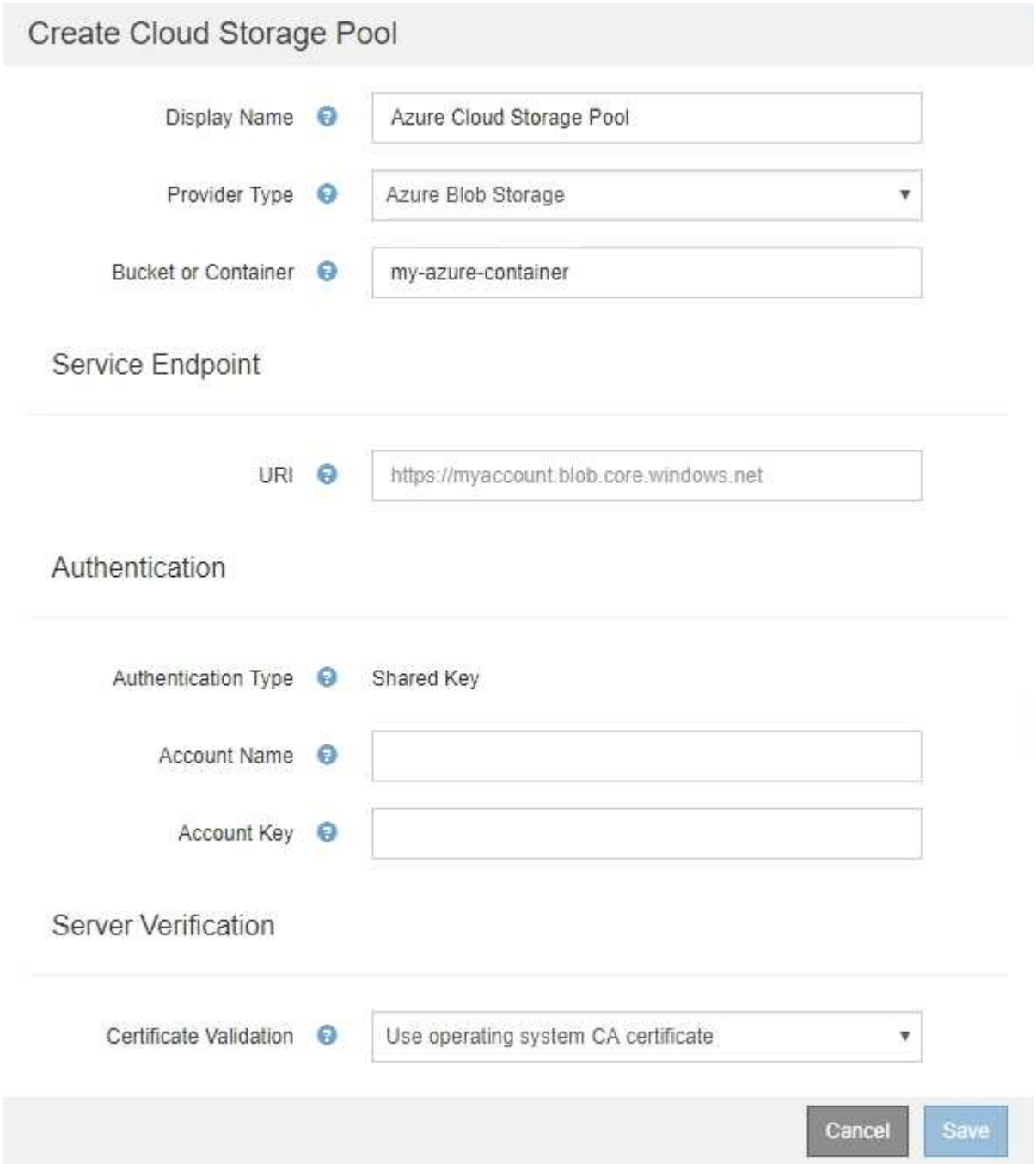
"Risoluzione dei problemi relativi ai pool di storage cloud"

Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud

Quando si crea un pool di storage cloud per lo storage Azure Blob, è necessario specificare un nome account e una chiave account per il container esterno che StorageGRID utilizzerà per memorizzare gli oggetti.

Di cosa hai bisogno

- È necessario aver inserito le informazioni di base per il Cloud Storage Pool e specificato **Azure Blob Storage** come tipo di provider. Nel campo **Authentication Type** (tipo di autenticazione) viene visualizzato **Shared Key** (chiave condivisa).



- È necessario conoscere l'URI (Uniform Resource Identifier) utilizzato per accedere al container di storage Blob utilizzato per il Cloud Storage Pool.
- È necessario conoscere il nome dell'account di storage e la chiave segreta. È possibile utilizzare il portale Azure per trovare questi valori.

Fasi

1. Nella sezione **Service Endpoint**, immettere l'URI (Uniform Resource Identifier) utilizzato per accedere al container di storage Blob utilizzato per il Cloud Storage Pool.

   Specificare l'URI in uno dei seguenti formati:

   - `https://host:port`
   - `http://host:port`

   Se non si specifica una porta, per impostazione predefinita viene utilizzata la porta 443 per gli URI HTTPS e la porta 80 per gli URI HTTP. + + + **URI di esempio per Azure Blob Storage Container**: `https://myaccount.blob.core.windows.net`

2. Nella sezione **Authentication**, fornire le seguenti informazioni:

   a. Per **Nome account**, immettere il nome dell'account di storage Blob proprietario del container di servizi esterno.

   b. Per **account Key**, immettere la chiave segreta per l'account di storage Blob.

   Per gli endpoint Azure, è necessario utilizzare l'autenticazione con chiave condivisa.

3. Nella sezione **verifica server**, selezionare il metodo da utilizzare per validare il certificato per le connessioni TLS al Cloud Storage Pool:

Opzione	Descrizione
Utilizzare il certificato CA del sistema operativo	Utilizzare i certificati CA predefiniti installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Fare clic su **Select New** (Seleziona nuovo) e caricare il certificato con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

4. Fare clic su **Save** (Salva).

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del container e dell'URI e ne consente l'accesso utilizzando le credenziali specificate.
- Scrive un file marker nel container per identificarlo come pool di storage cloud. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il contenitore specificato non esiste già, potrebbe essere visualizzato un errore.

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

"Risoluzione dei problemi relativi ai pool di storage cloud"

Modifica di un pool di storage cloud

È possibile modificare un Cloud Storage Pool per modificarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non è possibile modificare il bucket S3 o il container Azure per un Cloud Storage Pool.

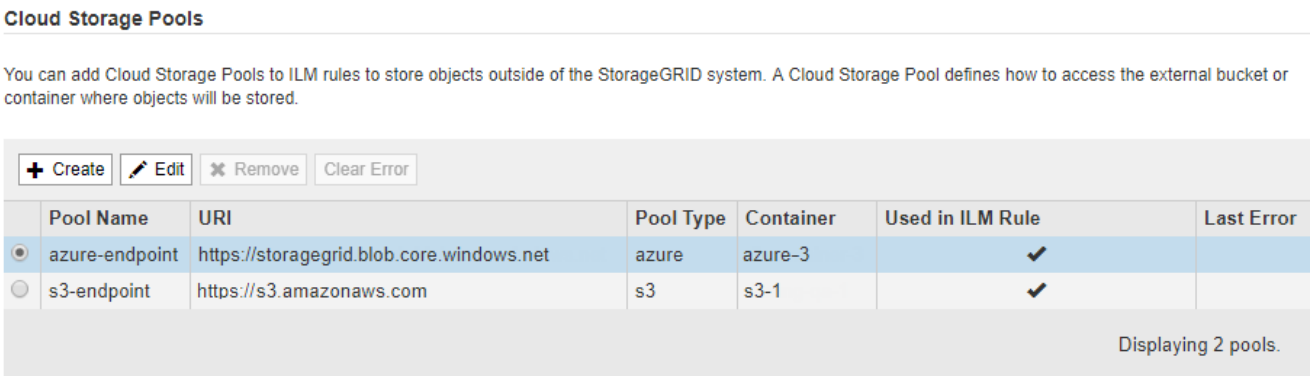
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Devi aver esaminato le linee guida per la configurazione dei Cloud Storage Pools.

Fasi

1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools. La tabella Cloud Storage Pools elenca i Cloud Storage Pools esistenti.



2. Selezionare il pulsante di opzione per il Cloud Storage Pool che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Se necessario, modificare il nome visualizzato, l'endpoint del servizio, le credenziali di autenticazione o il metodo di convalida del certificato.

   > Non è possibile modificare il tipo di provider, il bucket S3 o il container Azure per un Cloud Storage Pool.

   Se in precedenza è stato caricato un certificato server o client, è possibile selezionare **Visualizza attuale** per rivedere il certificato attualmente in uso.

5. Fare clic su **Save** (Salva).

   Quando si salva un pool di storage cloud, StorageGRID convalida l'esistenza del bucket o del container e dell'endpoint del servizio e che è possibile raggiungerli utilizzando le credenziali specificate.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore. Ad esempio, se si verifica un errore del certificato, potrebbe essere visualizzato un errore.

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

"Considerazioni per i Cloud Storage Pools"

"Risoluzione dei problemi relativi ai pool di storage cloud"

Rimozione di un pool di storage cloud

È possibile rimuovere un Cloud Storage Pool che non viene utilizzato in una regola ILM e che non contiene dati oggetto.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Hai confermato che il bucket S3 o il container Azure non contiene oggetti. Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool se contiene oggetti. Consulta “risoluzione dei problemi relativi ai pool di storage cloud”.

> Quando crei un pool di storage cloud, StorageGRID scrive un file di marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

- Sono già state rimosse le regole ILM che potrebbero aver utilizzato il pool.

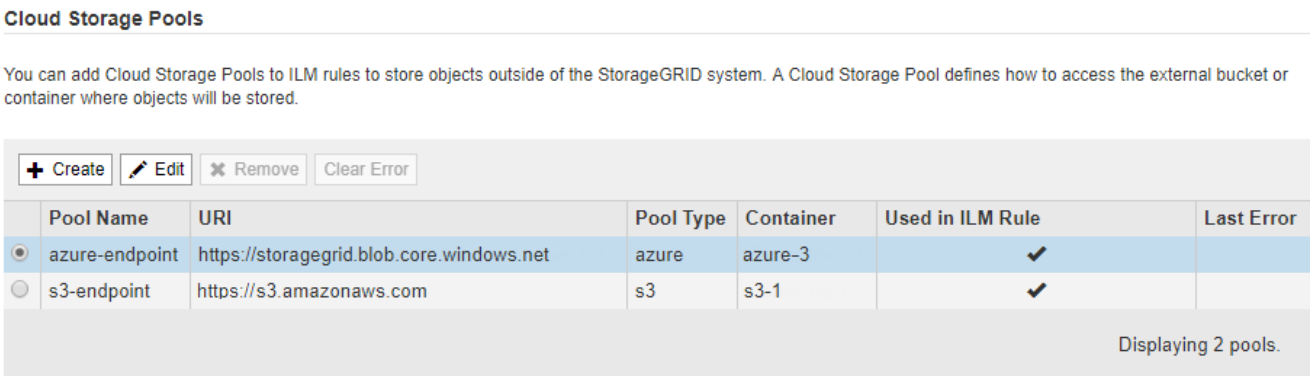
Fasi

1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools.

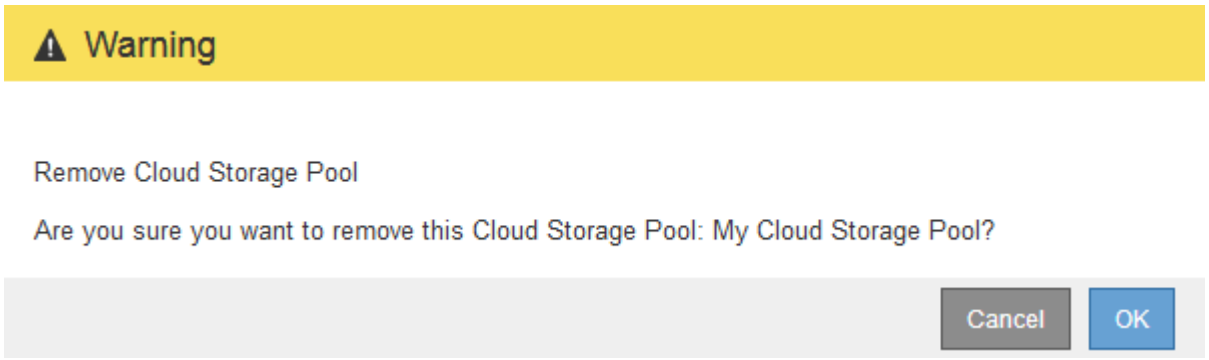
2. Selezionare il pulsante di opzione per un Cloud Storage Pool che non è attualmente utilizzato in una regola ILM.

   Non è possibile rimuovere un pool di storage cloud se utilizzato in una regola ILM. Il pulsante **Remove** (Rimuovi) è disattivato.



3. Fare clic su **Rimuovi**.

   Viene visualizzato un avviso di conferma.



4. Fare clic su **OK**.

   Il Cloud Storage Pool viene rimosso.

Informazioni correlate

"Risoluzione dei problemi relativi ai pool di storage cloud"

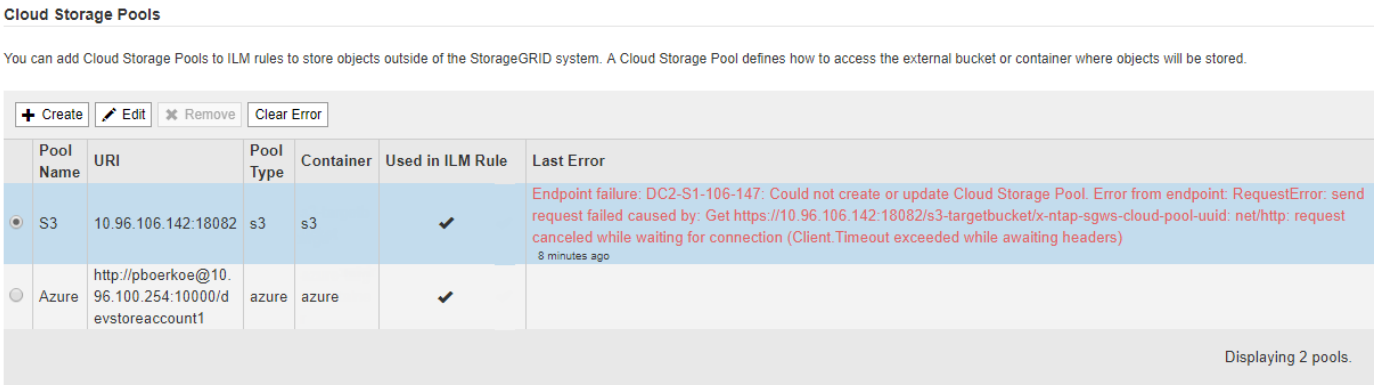
Risoluzione dei problemi relativi ai pool di storage cloud

Se si verificano errori durante la creazione, la modifica o l'eliminazione di un pool di storage cloud, attenersi alla procedura di risoluzione dei problemi riportata di seguito per risolvere il problema.

Determinare se si è verificato un errore

StorageGRID esegue una semplice verifica dello stato di salute di ogni pool di storage cloud una volta al minuto per garantire che sia possibile accedere al pool di storage cloud e che funzioni correttamente. Se il controllo dello stato di salute rileva un problema, viene visualizzato un messaggio nella colonna Last Error (ultimo errore) della tabella Cloud Storage Pools (pool di storage cloud) della pagina Storage Pools (pool di storage).

La tabella mostra l'errore più recente rilevato per ciascun Cloud Storage Pool e indica quanto tempo fa si è verificato l'errore.

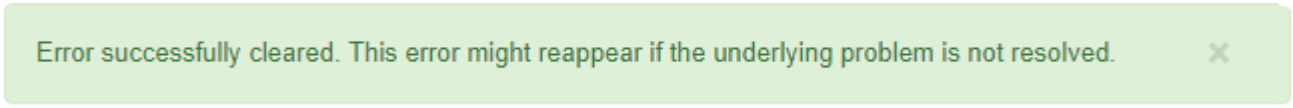


Inoltre, un avviso di **errore di connettività del Cloud Storage Pool** viene attivato se il controllo dello stato di salute rileva che uno o più nuovi errori del Cloud Storage Pool si sono verificati negli ultimi 5 minuti. Se si

riceve una notifica via email per questo avviso, accedere alla pagina Storage Pool (selezionare **ILM** > **Storage Pools**), esaminare i messaggi di errore nella colonna Last Error (ultimo errore) e consultare le linee guida per la risoluzione dei problemi riportate di seguito.

Verifica della risoluzione di un errore

Dopo aver risolto eventuali problemi sottostanti, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, selezionare il pulsante di opzione per l'endpoint e fare clic su **Clear Error**. Un messaggio di conferma indica che StorageGRID ha eliminato l'errore per il pool di storage cloud.



Se il problema sottostante è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema sottostante non è stato risolto (o se si verifica un errore diverso), il messaggio di errore viene visualizzato nella colonna Last Error (ultimo errore) entro pochi minuti.

Errore: Questo Cloud Storage Pool contiene contenuti imprevisti

Questo errore potrebbe verificarsi quando si tenta di creare, modificare o eliminare un pool di storage cloud. Questo errore si verifica se il bucket o il container include `x-ntap-sgws-cloud-pool-uuid` Il file marker, ma non ha l'UUID previsto.

In genere, questo errore viene visualizzato solo se si crea un nuovo pool di storage cloud e un'altra istanza di StorageGRID sta già utilizzando lo stesso pool di storage cloud.

Per risolvere il problema, attenersi alla seguente procedura:

- Assicurati che nessuno nella tua organizzazione stia utilizzando questo Cloud Storage Pool.
- Eliminare `x-ntap-sgws-cloud-pool-uuid` E provare a configurare nuovamente il Cloud Storage Pool.

Errore: Impossibile creare o aggiornare il Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. Questo errore indica che alcuni problemi di connettività o configurazione impediscono a StorageGRID di scrivere nel pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

- Se il messaggio di errore contiene `Get *url*: EOF`, Verificare che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi il protocollo HTTP per un container o bucket che richiede HTTPS.
- Se il messaggio di errore contiene `Get *url*: net/http: request canceled while waiting for connection`, Verificare che la configurazione di rete consenta ai nodi di storage di accedere all'endpoint del servizio utilizzato per il Cloud Storage Pool.
- Per tutti gli altri messaggi di errore degli endpoint, provare una o più delle seguenti soluzioni:
  - Creare un container o bucket esterno con lo stesso nome immesso per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.
  - Correggere il nome del container o bucket specificato per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.

Errore: Impossibile analizzare il certificato CA

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. L'errore si verifica se StorageGRID non ha potuto analizzare il certificato inserito durante la configurazione del pool di storage cloud.

Per correggere il problema, controllare il certificato CA fornito per eventuali problemi.

Errore: Impossibile trovare un pool di storage cloud con questo ID

Questo errore potrebbe verificarsi quando si tenta di modificare o eliminare un pool di storage cloud. Questo errore si verifica se l'endpoint restituisce una risposta 404, il che può significare una delle seguenti:

- Le credenziali utilizzate per il Cloud Storage Pool non dispongono dell'autorizzazione di lettura per il bucket.
- Il bucket utilizzato per il Cloud Storage Pool non include `x-ntap-sgws-cloud-pool-uuid` file marker.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare che l'utente associato alla chiave di accesso configurata disponga delle autorizzazioni necessarie.
- Modificare il Cloud Storage Pool con le credenziali che dispongono delle autorizzazioni necessarie.
- Se le autorizzazioni sono corrette, contattare l'assistenza.

Errore: Impossibile controllare il contenuto del Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore indica che un problema di connettività o configurazione impedisce a StorageGRID di leggere il contenuto del bucket del pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

Errore: Gli oggetti sono già stati posizionati in questo bucket

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati da ILM, dati presenti nel bucket prima della configurazione del Cloud Storage Pool o dati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Seguire le istruzioni per lo spostamento degli oggetti in StorageGRID in "ciclo di vita di un oggetto pool di storage cloud".
- Se si è certi che ILM non abbia inserito gli oggetti rimanenti nel Cloud Storage Pool, eliminarli manualmente dal bucket.

> Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbe essere stato collocato in tale posizione da ILM. Se in un secondo momento si tenta di accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non viene trovato.

Errore: Il proxy ha rilevato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool

Questo errore potrebbe verificarsi se è stato configurato un proxy dello storage non trasparente tra i nodi di storage e l'endpoint S3 esterno utilizzato per il Cloud Storage Pool. Questo errore si verifica se il server proxy esterno non riesce a raggiungere l'endpoint del Cloud Storage Pool. Ad esempio, il server DNS potrebbe non essere in grado di risolvere il nome host o potrebbe esserci un problema di rete esterno.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare le impostazioni del Cloud Storage Pool (**ILM** > **Storage Pools**).
- Controllare la configurazione di rete del server proxy dello storage.

Informazioni correlate

"Ciclo di vita di un oggetto Cloud Storage Pool"

Configurazione dei profili di codifica Erasure

È possibile configurare i profili di codifica Erasure associando un pool di storage a uno schema di codifica erasure, ad esempio 6+3. Quindi, quando si configurano le istruzioni di posizionamento per una regola ILM, è possibile selezionare il profilo di codifica Erasure. Se un oggetto corrisponde alla regola, i frammenti di dati e parità vengono creati e distribuiti nelle posizioni di storage nel pool di storage in base allo schema di erasure coding.

- "Creazione di un profilo di codifica Erasure"
- "Ridenominazione di un profilo di codifica Erasure"
- "Disattivazione di un profilo di codifica Erasure"

Creazione di un profilo di codifica Erasure

Per creare un profilo di codifica Erasure, associare un pool di storage contenente nodi di storage a uno schema di codifica erasure. Questa associazione determina il numero di dati e di frammenti di parità creati e la posizione in cui il sistema distribuisce tali frammenti.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver creato un pool di storage che includa esattamente un sito o un pool di storage che includa tre o più siti. Non sono disponibili schemi di erasure coding per un pool di storage con solo due siti.

A proposito di questa attività

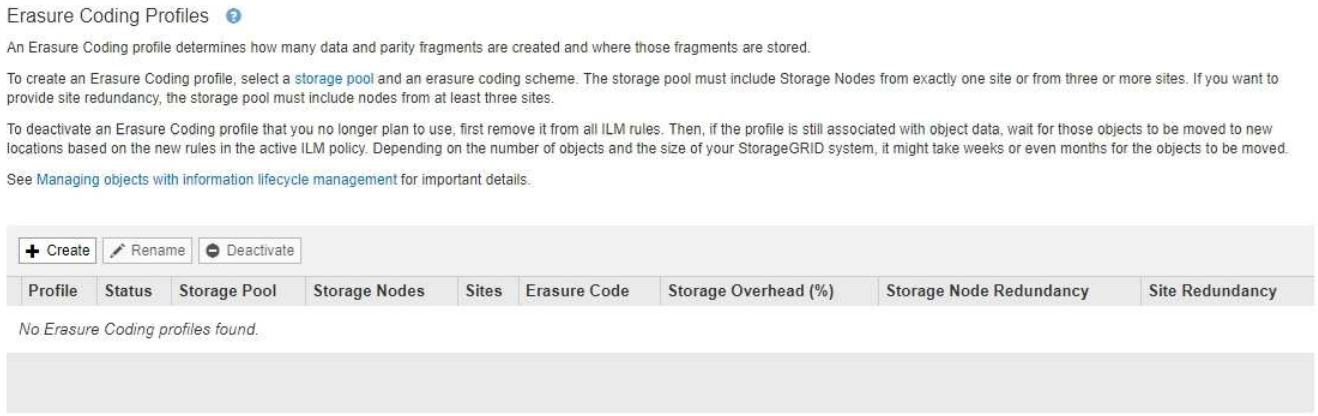
I pool di storage utilizzati nei profili di codifica Erasure devono includere esattamente un sito o tre o più siti. Se si desidera fornire la ridondanza del sito, il pool di storage deve avere almeno tre siti.

> È necessario selezionare un pool di storage che contiene nodi di storage. Non è possibile utilizzare i nodi di archiviazione per i dati con codifica erasure.

Fasi

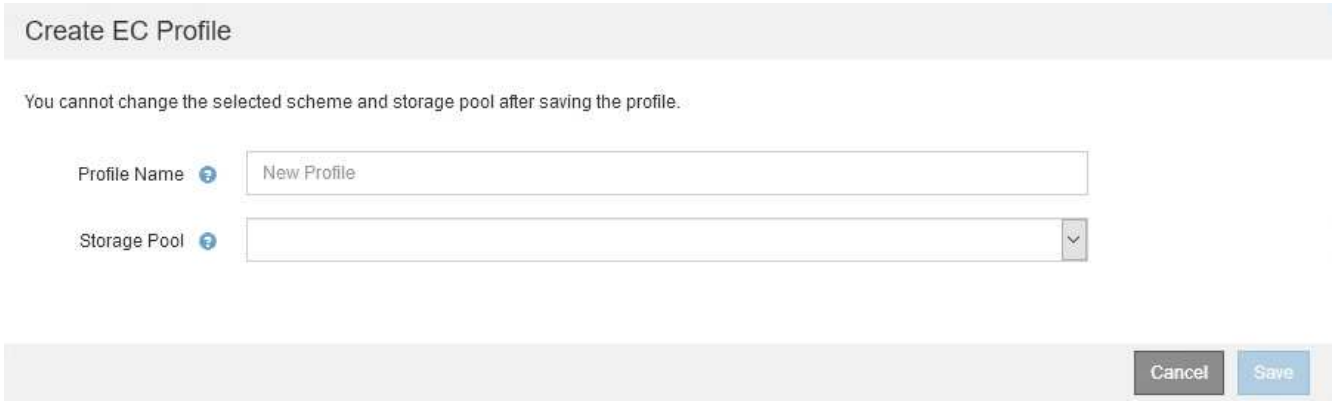
1. Selezionare **ILM** > **Erasure coding**.

   Viene visualizzata la pagina Erasure Coding Profiles.



2. Fare clic su **Create** (Crea).

   Viene visualizzata la finestra di dialogo Create EC Profile (Crea profilo EC).



3. Immettere un nome univoco per il profilo di codifica Erasure.

   I nomi dei profili di erasure coding devono essere univoci. Si verifica un errore di convalida se si utilizza il nome di un profilo esistente, anche se tale profilo è stato disattivato.

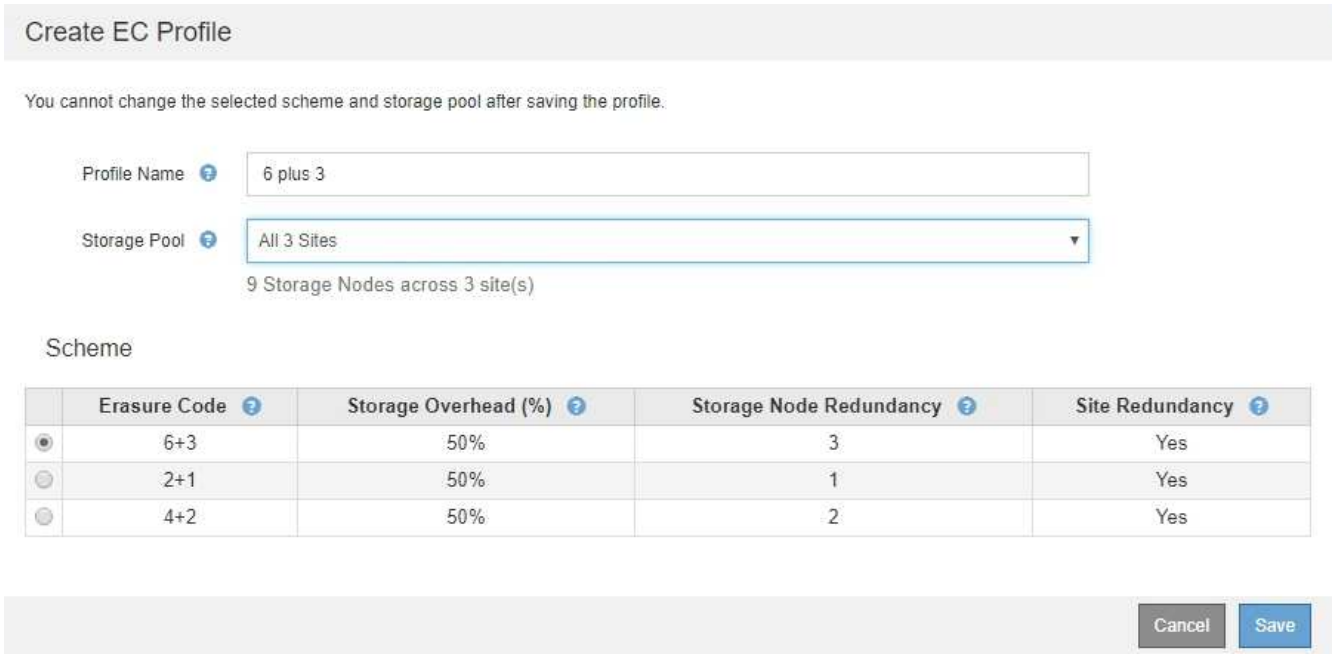
   Il nome del profilo di codifica Erasure viene aggiunto al nome del pool di storage nelle istruzioni di posizionamento per una regola ILM.

4. Selezionare il pool di storage creato per questo profilo di codifica Erasure.

Se il grid attualmente include un solo sito, non è possibile utilizzare il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti. Questo comportamento impedisce che il profilo di codifica Erasure diventi non valido se viene aggiunto un secondo sito.

Se un pool di storage include esattamente due siti, non è possibile utilizzare tale pool di storage per la cancellazione del codice. Non sono disponibili schemi di erasure coding per un pool di storage con due siti.

Quando si seleziona un pool di storage, viene visualizzato l'elenco degli schemi di erasure coding disponibili, in base al numero di nodi e siti di storage nel pool.



Per ogni schema di erasure coding disponibile sono elencate le seguenti informazioni:

- **Erasure Code**: Il nome dello schema di erasure coding nel seguente formato: Frammenti di dati + frammenti di parità.
- **Overhead dello storage (%)**: Lo storage aggiuntivo richiesto per i frammenti di parità in relazione alle dimensioni dei dati dell'oggetto. Overhead dello storage = numero totale di frammenti di parità / numero totale di frammenti di dati.
- **Ridondanza dei nodi di storage**: Il numero di nodi di storage che possono essere persi pur mantenendo la capacità di recuperare i dati degli oggetti.
- **Ridondanza del sito**: Se il codice di cancellazione selezionato consente di recuperare i dati dell'oggetto in caso di perdita di un sito.

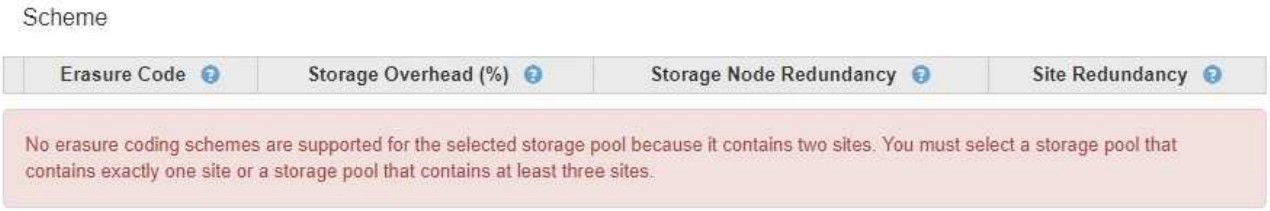
  Per supportare la ridondanza del sito, il pool di storage selezionato deve includere più siti, ciascuno con un numero sufficiente di nodi di storage per consentire la perdita di qualsiasi sito. Ad esempio, per supportare la ridondanza del sito utilizzando uno schema di erasure coding 6+3, il pool di storage selezionato deve includere almeno tre siti con almeno tre nodi di storage in ciascun sito.

  I messaggi vengono visualizzati nei seguenti casi:

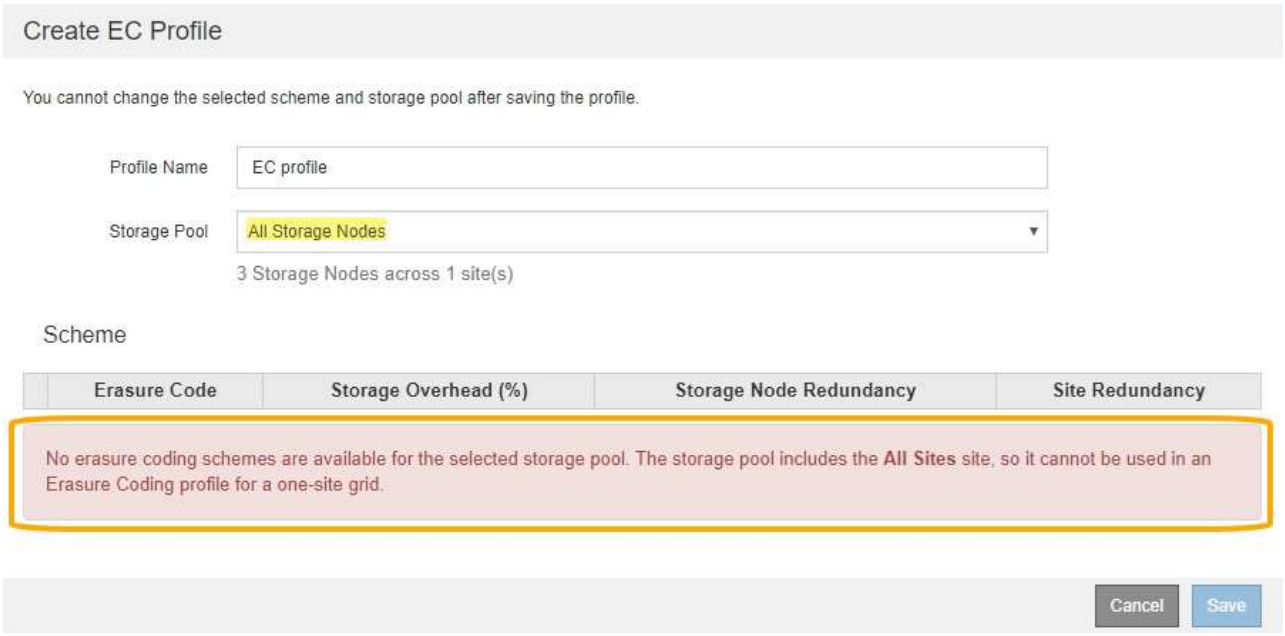
- Il pool di storage selezionato non fornisce ridondanza del sito. Il seguente messaggio è previsto

quando il pool di storage selezionato include un solo sito. È possibile utilizzare questo profilo di codifica Erasure nelle regole ILM per la protezione dai guasti dei nodi.

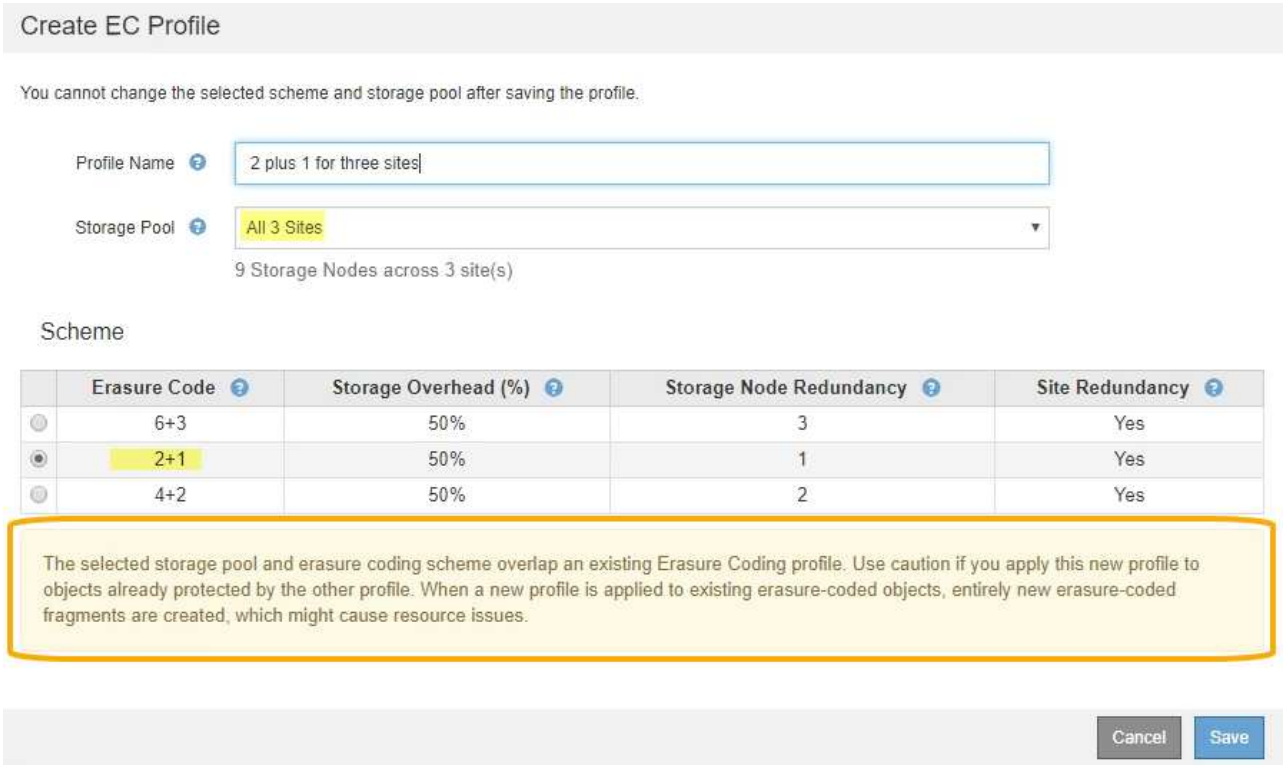
- Il pool di storage selezionato non soddisfa i requisiti per qualsiasi schema di erasure coding. Ad esempio, il seguente messaggio è previsto quando il pool di storage selezionato include esattamente due siti. Se si desidera utilizzare la codifica erasure per proteggere i dati degli oggetti, è necessario selezionare un pool di storage con esattamente un sito o un pool di storage con tre o più siti.



- Il grid include un solo sito ed è stato selezionato il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti.



- Lo schema di erasure coding e il pool di storage selezionati si sovrappongono a un altro profilo di codifica Erasure.



In questo esempio, viene visualizzato un messaggio di avviso perché un altro profilo di codifica Erasure sta utilizzando lo schema 2+1 e il pool di storage per l'altro profilo utilizza anche uno dei siti nel pool di storage All 3 Sites.

Anche se non è possibile creare questo nuovo profilo, è necessario prestare molta attenzione quando si inizia a utilizzarlo nel criterio ILM. Se questo nuovo profilo viene applicato a oggetti con codifica in cancellazione già protetti dall'altro profilo, StorageGRID creerà un set completamente nuovo di frammenti di oggetti. Non riutilizza i frammenti 2+1 esistenti. I problemi relativi alle risorse potrebbero verificarsi quando si esegue la migrazione da un profilo di codifica Erasure all'altro, anche se gli schemi di codifica erasure sono gli stessi.

5. Se sono elencati più schemi di erasure coding, selezionare quello che si desidera utilizzare.

   Quando si decide quale schema di erasure coding utilizzare, è necessario bilanciare la tolleranza agli errori (ottenuta con più segmenti di parità) con i requisiti di traffico di rete per le riparazioni (più frammenti equivalgono a più traffico di rete). Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3, selezionare lo schema 6+3 se sono richieste ulteriori parità e tolleranza di errore. Selezionare lo schema 4+2 se le risorse di rete sono limitate per ridurre l'utilizzo della rete durante le riparazioni dei nodi.

6. Fare clic su **Save** (Salva).

Ridenominazione di un profilo di codifica Erasure

È possibile rinominare un profilo di codifica Erasure per rendere più evidente la funzione del profilo.

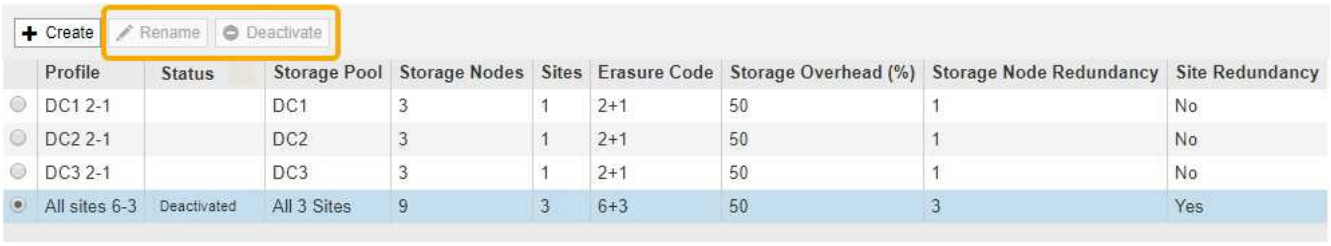
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **ILM** > **Erasure coding**.

   Viene visualizzata la pagina Erasure Coding Profiles. I pulsanti **Rinomina** e **Disattiva** sono entrambi disattivati.



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. Selezionare il profilo che si desidera rinominare.

   I pulsanti **Rinomina** e **Disattiva** diventano abilitati.

3. Fare clic su **Rinomina**.

   Viene visualizzata la finestra di dialogo Rename EC Profile (Rinomina profilo EC).

4. Immettere un nome univoco per il profilo di codifica Erasure.

   Il nome del profilo di codifica Erasure viene aggiunto al nome del pool di storage nelle istruzioni di posizionamento per una regola ILM.

   I nomi dei profili di erasure coding devono essere univoci. Si verifica un errore di convalida se si utilizza il nome di un profilo esistente, anche se tale profilo è stato disattivato.

5. Fare clic su **Save** (Salva).

Disattivazione di un profilo di codifica Erasure

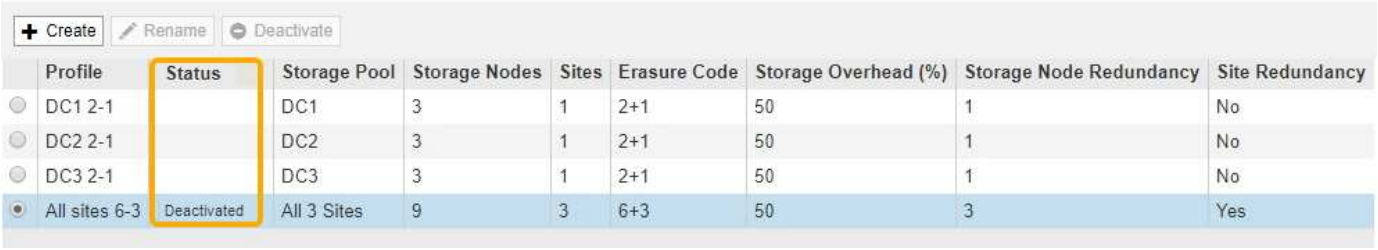
Puoi disattivare un profilo di codifica Erasure se non intendi utilizzarlo e se il profilo non è attualmente utilizzato in nessuna regola ILM.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Devi aver confermato che non sono in corso operazioni di riparazione dei dati codificati per la cancellazione o procedure di decommissionamento. Se si tenta di disattivare un profilo di codifica Erasure mentre è in corso una di queste operazioni, viene visualizzato un messaggio di errore.

A proposito di questa attività

Quando si disattiva un profilo di codifica Erasure, il profilo continua a essere visualizzato nella pagina Erasure Coding Profiles, ma il suo stato è **Disattivato**.



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

Non è più possibile utilizzare un profilo di codifica Erasure disattivato. Un profilo disattivato non viene visualizzato quando si creano le istruzioni di posizionamento per una regola ILM. Non è possibile riattivare un profilo disattivato.

StorageGRID impedisce di disattivare un profilo di codifica Erasure se si verifica una delle seguenti condizioni:

- Il profilo di codifica Erasure è attualmente utilizzato in una regola ILM.
- Il profilo di codifica Erasure non viene più utilizzato in alcuna regola ILM, ma i dati degli oggetti e i frammenti di parità per il profilo esistono ancora.

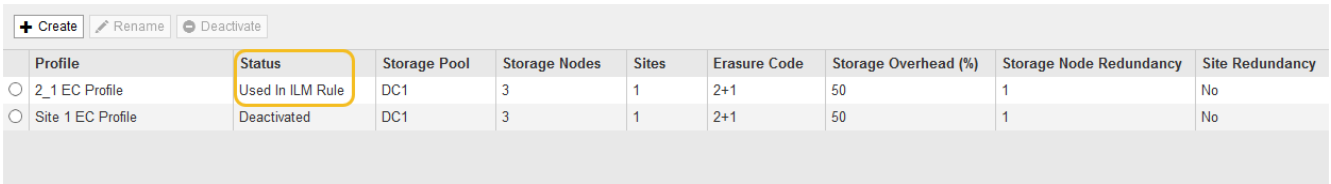
Fasi

1. Selezionare **ILM** > **Erasure coding**.

   Viene visualizzata la pagina Erasure Coding Profiles. I pulsanti **Rinomina** e **Disattiva** sono entrambi disattivati.

2. Controllare la colonna **Status** per verificare che il profilo di codifica Erasure che si desidera disattivare non sia utilizzato in alcuna regola ILM.

   Non è possibile disattivare un profilo di codifica Erasure se utilizzato in qualsiasi regola ILM. Nell'esempio, il profilo **2_1 EC** viene utilizzato in almeno una regola ILM.



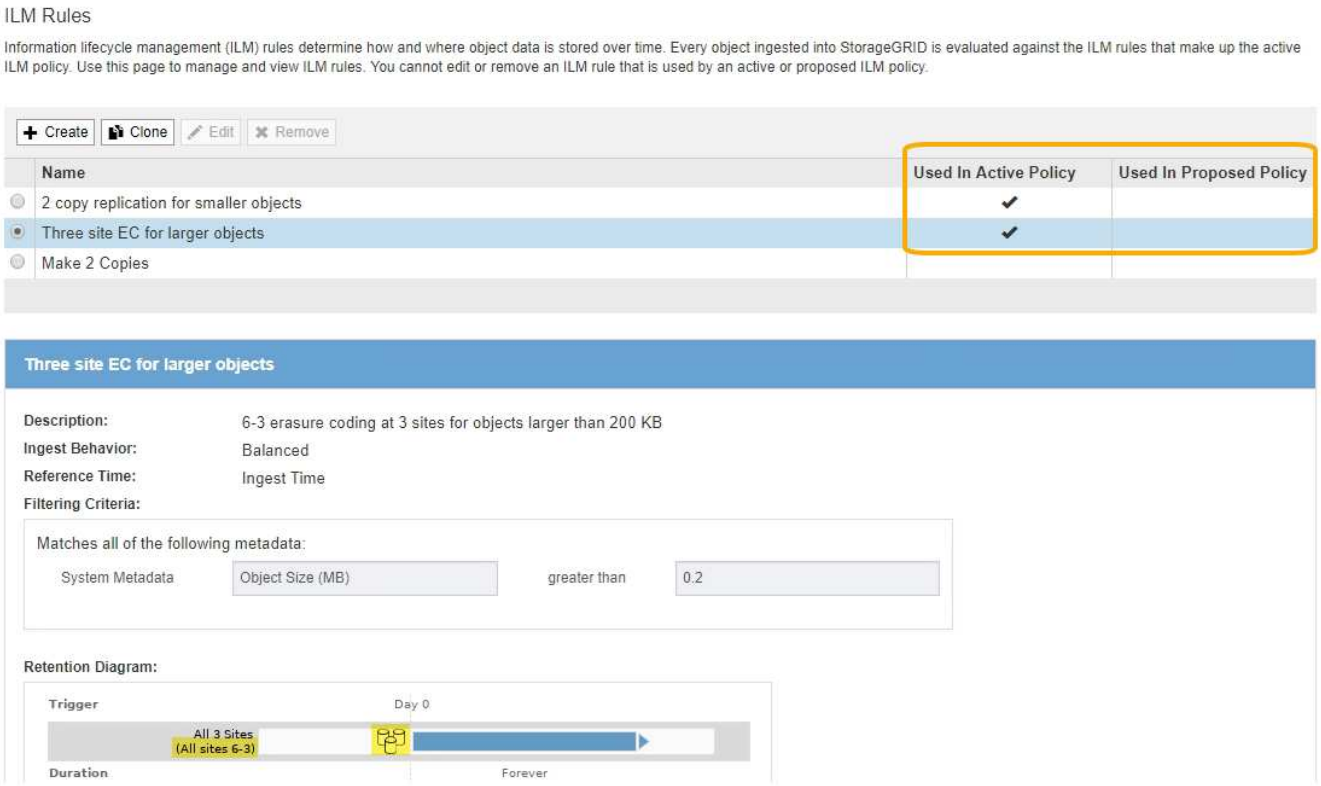
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

3. Se il profilo viene utilizzato in una regola ILM, attenersi alla seguente procedura:

   a. Selezionare **ILM** > **regole**.

   b. Per ciascuna regola elencata, selezionare il pulsante di opzione e consultare il diagramma di conservazione per determinare se la regola utilizza il profilo di codifica Erasure che si desidera disattivare.

Nell'esempio, la regola EC **tre siti per oggetti più grandi** utilizza un pool di storage denominato **tutti e 3 i siti** e il profilo di codifica Erasure **tutti i siti 6-3**. I profili di erasure coding sono rappresentati da questa icona:



a. Se la regola ILM utilizza il profilo di codifica Erasure che si desidera disattivare, determinare se la regola viene utilizzata nel criterio ILM attivo o in un criterio proposto.

   Nell'esempio, la regola EC **tre siti per oggetti più grandi** viene utilizzata nel criterio ILM attivo.

b. Completare i passaggi aggiuntivi della tabella, in base alla posizione in cui viene utilizzato il profilo di codifica Erasure.

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
Mai utilizzato in nessuna regola ILM	Non sono necessari passaggi aggiuntivi. Continuare con questa procedura.	*nessuno*
In una regola ILM che non è mai stata utilizzata in alcun criterio ILM	i. Modificare o eliminare tutte le regole ILM interessate. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure. ii. Continuare con questa procedura.	"Utilizzo delle regole ILM e delle policy ILM"

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
In una regola ILM attualmente nel criterio ILM attivo	i. Clonare il criterio attivo. ii. Rimuovere la regola ILM che utilizza il profilo di codifica Erasure. iii. Aggiungere una o più nuove regole ILM per garantire la protezione degli oggetti. iv. Salvare, simulare e attivare la nuova policy. v. Attendere che il nuovo criterio venga applicato e che gli oggetti esistenti vengano spostati in nuove posizioni in base alle nuove regole aggiunte. **Nota:** a seconda del numero di oggetti e delle dimensioni del sistema StorageGRID, potrebbero essere necessarie settimane o addirittura mesi per le operazioni ILM per spostare gli oggetti in nuove posizioni, in base alle nuove regole ILM. Sebbene sia possibile disattivare in modo sicuro un profilo di codifica Erasure mentre è ancora associato ai dati, l'operazione di disattivazione non riesce. Se il profilo non è ancora pronto per la disattivazione, viene visualizzato un messaggio di errore. vi. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure. vii. Continuare con questa procedura.	• "Creazione di un criterio ILM" • "Utilizzo delle regole ILM e delle policy ILM"
In una regola ILM attualmente in un criterio ILM proposto	i. Modificare la policy proposta. ii. Rimuovere la regola ILM che utilizza il profilo di codifica Erasure. iii. Aggiungere una o più nuove regole ILM per garantire la protezione di tutti gli oggetti. iv. Salvare la policy proposta. v. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure. vi. Continuare con questa procedura.	• "Creazione di un criterio ILM" • "Utilizzo delle regole ILM e delle policy ILM"

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
In una regola ILM che si trova in una policy ILM storica	i. Modificare o eliminare la regola. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure. (La regola verrà ora visualizzata come regola storica nella policy storica). ii. Continuare con questa procedura.	• "Utilizzo delle regole ILM e delle policy ILM"

c. Aggiornare la pagina Erasure Coding Profiles per assicurarsi che il profilo non venga utilizzato in una regola ILM.

4. Se il profilo non viene utilizzato in una regola ILM, selezionare il pulsante di opzione e selezionare **Disattiva**.

   Viene visualizzata la finestra di dialogo Disattiva profilo EC.

5. Se sei sicuro di voler disattivare il profilo, seleziona **Disattiva**.
   - Se StorageGRID è in grado di disattivare il profilo di codifica di cancellazione, il suo stato è **Disattivato**. Non è più possibile selezionare questo profilo per nessuna regola ILM.
   - Se StorageGRID non è in grado di disattivare il profilo, viene visualizzato un messaggio di errore. Ad esempio, se i dati dell'oggetto sono ancora associati a questo profilo, viene visualizzato un messaggio di errore. Potrebbe essere necessario attendere alcune settimane prima di provare di nuovo il processo di disattivazione.

Configurazione delle regioni (opzionale e solo S3)

Le regole ILM possono filtrare gli oggetti in base alle aree in cui vengono creati i bucket S3, consentendo di memorizzare oggetti da diverse aree in diverse posizioni di storage. Se si desidera utilizzare un'area del bucket S3 come filtro in una regola, è necessario innanzitutto creare le regioni che possono essere utilizzate dai bucket nel sistema.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Quando si crea un bucket S3, è possibile specificare che il bucket venga creato in un'area specifica. La specifica di una regione consente al bucket di essere geograficamente vicino ai propri utenti, in modo da ottimizzare la latenza, ridurre al minimo i costi e soddisfare i requisiti normativi.

Quando si crea una regola ILM, è possibile utilizzare la regione associata a un bucket S3 come filtro avanzato. Ad esempio, è possibile progettare una regola che si applica solo agli oggetti nei bucket S3 creati nella regione US-West-2. È quindi possibile specificare che le copie di tali oggetti vengano collocate sui nodi di storage in un sito del data center all'interno di tale regione per ottimizzare la latenza.

Durante la configurazione delle regioni, attenersi alle seguenti linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati come appartenenti alla regione US-East-1.
- È necessario creare le regioni utilizzando Grid Manager prima di poter specificare un'area non predefinita quando si creano i bucket utilizzando l'API Tenant Manager o Tenant Management o con l'elemento di richiesta LocationConstraint per le richieste API S3 PUT bucket. Si verifica un errore se una richiesta PUT bucket utilizza un'area non definita in StorageGRID.
- Quando si crea il bucket S3, è necessario utilizzare il nome esatto della regione. I nomi delle regioni distinguono tra maiuscole e minuscole e devono contenere almeno 2 e non più di 32 caratteri. I caratteri validi sono numeri, lettere e trattini.

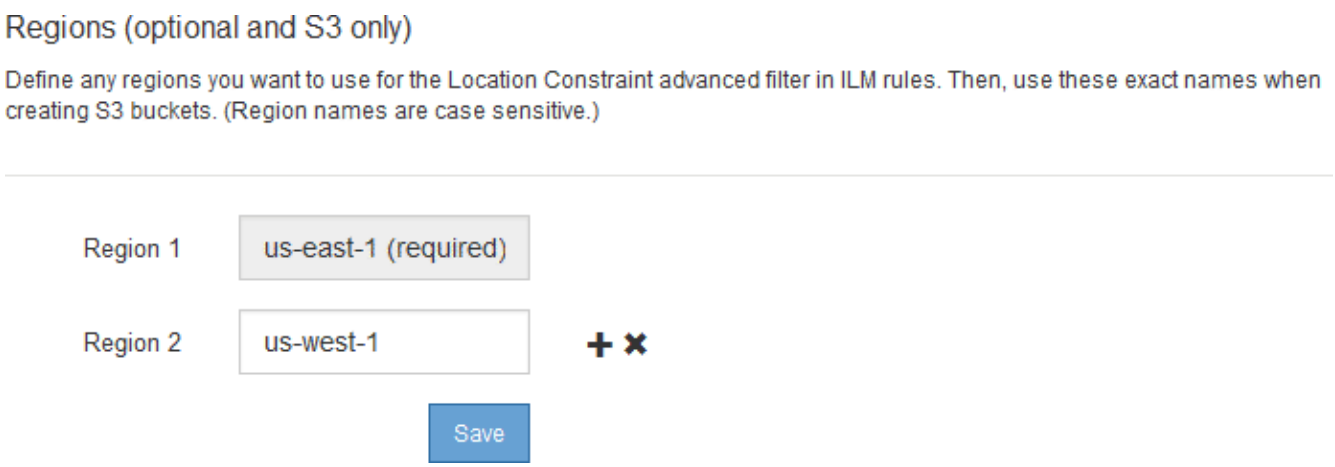
> EU non è considerato un alias per eu-West-1. Se si desidera utilizzare la regione EU o eu-West-1, è necessario utilizzare il nome esatto.

- Non è possibile eliminare o modificare una regione se è attualmente utilizzata nel criterio ILM attivo o nel criterio ILM proposto.
- Se la regione utilizzata come filtro avanzato in una regola ILM non è valida, è comunque possibile aggiungere tale regola al criterio proposto. Tuttavia, si verifica un errore se si tenta di salvare o attivare la policy proposta. (Se si utilizza una regione come filtro avanzato in una regola ILM ma si elimina tale regione in un secondo momento o se si utilizza l'API Grid Management per creare una regola e specificare una regione non definita), potrebbe verificarsi un'area non valida.
- Se si elimina una regione dopo averla utilizzata per creare un bucket S3, sarà necessario aggiungerla nuovamente se si desidera utilizzare il filtro avanzato Location Constraint per trovare gli oggetti in tale bucket.

Fasi

1. Selezionare **ILM** > **regioni**.

   Viene visualizzata la pagina regioni, con le regioni attualmente definite. **Regione 1** mostra la regione predefinita, `us-east-1`, che non può essere modificato o rimosso.

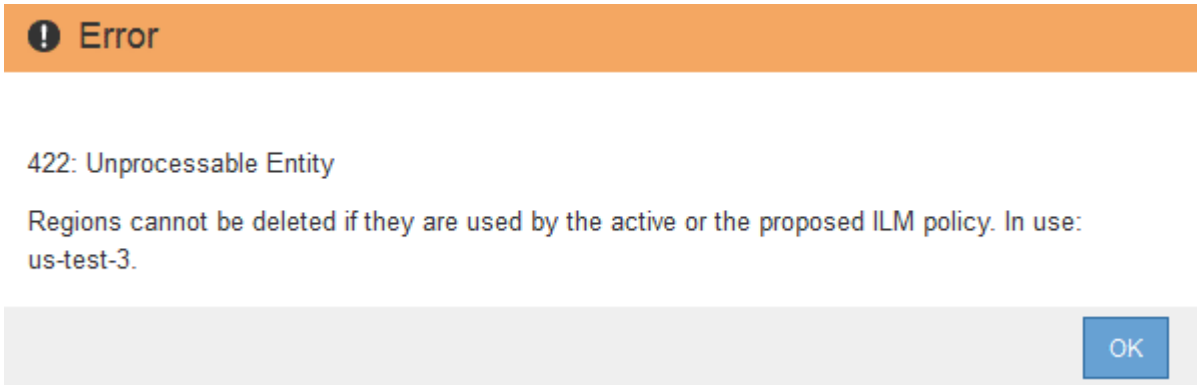


2. Per aggiungere una regione:
   a. Fare clic sull'icona di inserimento ✚ a destra dell'ultima voce.
   b. Immettere il nome di una regione che si desidera utilizzare durante la creazione dei bucket S3.

      Quando si crea il bucket S3 corrispondente, è necessario utilizzare il nome esatto della regione come elemento di richiesta LocationConstraint.

3. Per rimuovere una regione non utilizzata, fare clic sull'icona di eliminazione ✖.

   Se si tenta di rimuovere una regione attualmente utilizzata nel criterio attivo o nel criterio proposto, viene visualizzato un messaggio di errore.



4. Una volta apportate le modifiche, fare clic su **Save** (Salva).

   È ora possibile selezionare queste regioni dall'elenco **Location Constraint** nella pagina Advanced Filtering della creazione guidata regole ILM.

Informazioni correlate

"Utilizzo di filtri avanzati nelle regole ILM"

Creazione di una regola ILM

Le regole ILM consentono di gestire il posizionamento dei dati degli oggetti nel tempo. Per creare una regola ILM, utilizzare la procedura guidata Crea regola ILM.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si desidera specificare a quali account tenant si applica questa regola, è necessario disporre dell'autorizzazione account tenant o conoscere l'ID account per ciascun account.
- Se si desidera che la regola filtri gli oggetti sui metadati dell'ultimo accesso, gli ultimi aggiornamenti dell'ora di accesso devono essere attivati dal bucket per S3 o dal container per Swift.
- Se si creano copie replicate, è necessario aver configurato qualsiasi pool di storage o pool di cloud storage che si intende utilizzare.
- Se si stanno creando copie con codice erasure, è necessario aver configurato un profilo di codifica Erasure.
- È necessario avere familiarità con "opzioni di protezione dei dati per l'acquisizione".
- Se è necessario creare una regola conforme per l'utilizzo con il blocco oggetti S3, è necessario avere familiarità con "Requisiti per il blocco oggetti S3".

> Per creare la regola ILM predefinita per un criterio, utilizzare questa procedura: "Creazione di una regola ILM predefinita".

A proposito di questa attività

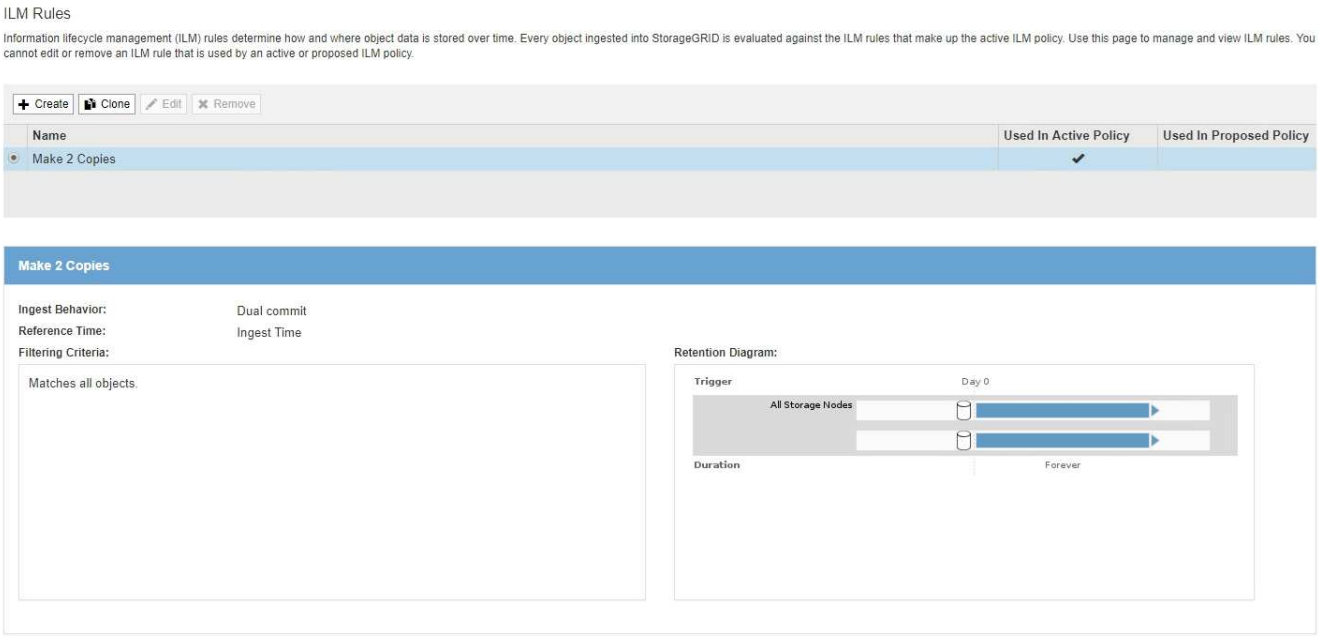
Quando si creano regole ILM:

- Prendere in considerazione la topologia e le configurazioni dello storage del sistema StorageGRID.
- Considerare i tipi di copie di oggetti che si desidera eseguire (replicate o codificate per la cancellazione) e il numero di copie di ciascun oggetto richieste.
- Determinare i tipi di metadati degli oggetti utilizzati nelle applicazioni che si connettono al sistema StorageGRID. Le regole ILM filtrano gli oggetti in base ai metadati.
- Considerare dove si desidera che le copie a oggetti vengano collocate nel tempo.
- Decidere quale opzione utilizzare per l'opzione di protezione dei dati al momento dell'acquisizione (Balanced, Strict o Dual Commit)

Fasi

1. Selezionare **ILM** > **regole**.

   Viene visualizzata la pagina ILM Rules (regole ILM), con la regola stock, fare 2 copie, selezionata.



La pagina regole ILM appare leggermente diversa se l'impostazione globale di blocco oggetti S3 è stata attivata per il sistema StorageGRID. La tabella di riepilogo include una colonna **conforme** e i dettagli della regola selezionata includono un campo **conforme**.

2. Selezionare **Crea**.

   Viene visualizzata la fase 1 (Definisci le basi) della procedura guidata Crea regola ILM. La pagina Definisci le basi consente di definire gli oggetti a cui si applica la regola.

Informazioni correlate

"Utilizzare S3"

"USA Swift"

"Configurazione dei profili di codifica Erasure"

"Configurazione dei pool di storage"

"Utilizzo dei Cloud Storage Pools"

"Opzioni di protezione dei dati per l'acquisizione"

"Gestione degli oggetti con S3 Object Lock"

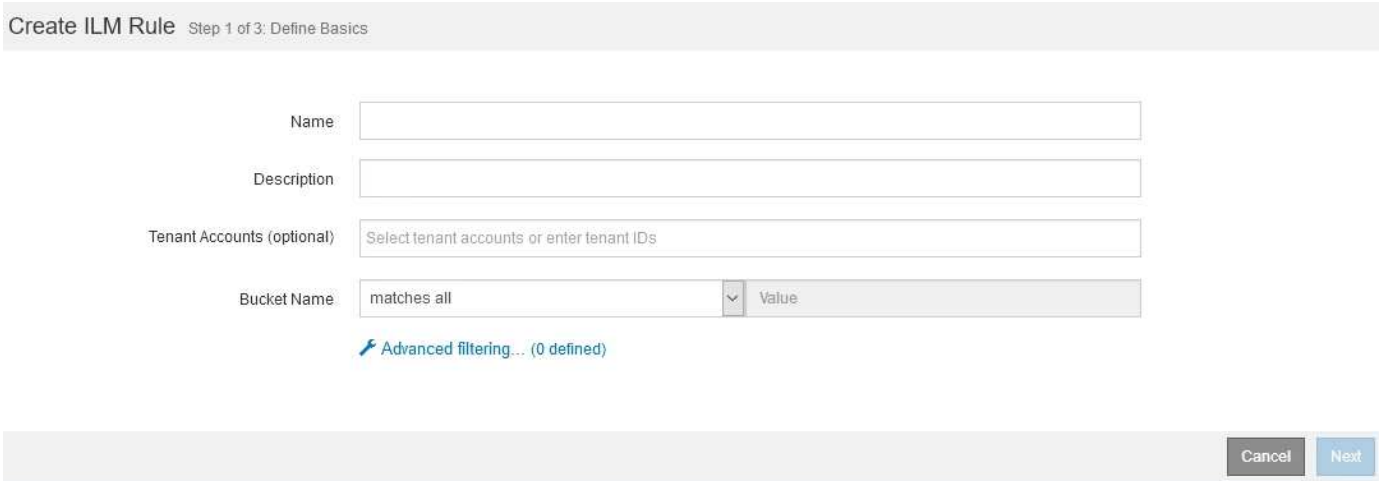
Fase 1 di 3: Definizione delle nozioni di base

Il passaggio 1 (Definisci le basi) della procedura guidata Crea regola ILM consente di definire i filtri di base e avanzati della regola.

A proposito di questa attività

Quando si valuta un oggetto rispetto a una regola ILM, StorageGRID confronta i metadati dell'oggetto con i filtri della regola. Se i metadati dell'oggetto corrispondono a tutti i filtri, StorageGRID utilizza la regola per posizionare l'oggetto. È possibile progettare una regola da applicare a tutti gli oggetti, oppure specificare filtri di base, come uno o più account tenant o nomi bucket, o filtri avanzati, come la dimensione dell'oggetto o i

metadati dell'utente.



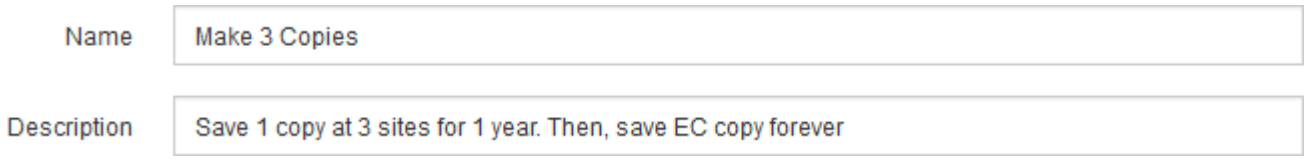
Fasi

1. Immettere un nome univoco per la regola nel campo **Nome**.

   È necessario immettere da 1 a 64 caratteri.

2. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.

   È necessario descrivere lo scopo o la funzione della regola in modo da poterne riconoscere in un secondo momento.



3. Facoltativamente, selezionare uno o più account tenant S3 o Swift a cui si applica questa regola. Se questa regola è applicabile a tutti i tenant, lasciare vuoto questo campo.

   Se non si dispone dell'autorizzazione Root Access o dell'autorizzazione Tenant Accounts, non è possibile selezionare i tenant dall'elenco. Immettere invece l'ID tenant o più ID come stringa delimitata da virgole.

4. Facoltativamente, specificare i bucket S3 o i container Swift a cui si applica questa regola.

   Se l'opzione **Match All** (corrispondenza totale) è selezionata (impostazione predefinita), la regola si applica a tutti i bucket S3 o a tutti i container Swift.

5. Se si desidera, selezionare **Advanced Filtering** (filtraggio avanzato) per specificare filtri aggiuntivi.

   Se non si configura il filtraggio avanzato, la regola si applica a tutti gli oggetti che corrispondono ai filtri di base.

   > Se questa regola consente di creare copie con codifica in cancellazione, selezionare **Advanced Filtering** (filtraggio avanzato). Quindi, aggiungere il filtro avanzato **Object Size (MB)** e impostarlo su **maggiore di 0.2**. Il filtro delle dimensioni garantisce che gli oggetti di dimensioni pari o inferiori a 2 MB non vengano sottoposti a erasure coding.

6. Selezionare **Avanti**.

Viene visualizzato il punto 2 (definizione delle posizioni).

Informazioni correlate

"Che cos'è il filtraggio delle regole ILM"

"Utilizzo di filtri avanzati nelle regole ILM"

"Fase 2 di 3: Definizione delle posizioni"

Utilizzo di filtri avanzati nelle regole ILM

Il filtraggio avanzato consente di creare regole ILM applicabili solo a oggetti specifici in base ai metadati. Quando si imposta il filtraggio avanzato per una regola, si seleziona il tipo di metadati che si desidera associare, si seleziona un operatore e si specifica un valore di metadati. Quando si valutano gli oggetti, la regola ILM viene applicata solo agli oggetti che hanno metadati corrispondenti al filtro avanzato.

La tabella mostra i tipi di metadati che è possibile specificare nei filtri avanzati, gli operatori che è possibile utilizzare per ogni tipo di metadati e i valori di metadati previsti.

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di acquisizione (microsecondi)	• uguale a • non uguale • inferiore a. • inferiore o uguale a. • maggiore di • maggiore di o uguale a.	Ora e data di acquisizione dell'oggetto. **Nota:** per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui il nuovo criterio verrà applicato per garantire che gli oggetti esistenti non vengano spostati inutilmente.
Chiave	• uguale a • non uguale • contiene • non contiene • inizia con • non inizia con • termina con • non finisce con	Tutto o parte di una chiave oggetti S3 o Swift univoca. Ad esempio, è possibile associare gli oggetti che terminano con `.txt` oppure inizia con `test-object/`.

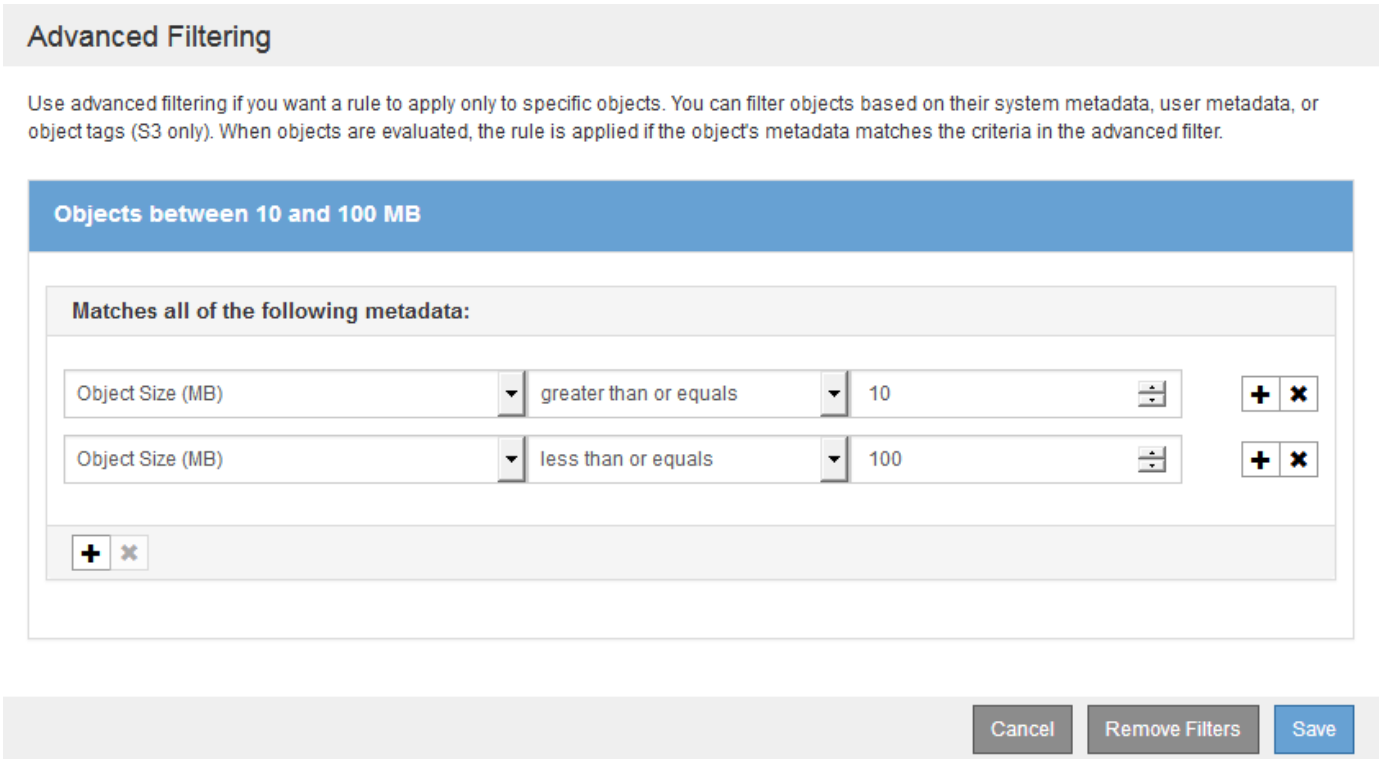
Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di ultimo accesso (microsecondi)	• uguale a • non uguale • inferiore a. • inferiore o uguale a. • maggiore di • maggiore di o uguale a. • esiste • non esiste	Ora e data dell'ultimo recupero dell'oggetto (letto o visualizzato). **Nota:** se si prevede di utilizzare l'ultimo tempo di accesso come filtro avanzato, è necessario abilitare gli ultimi aggiornamenti dell'ora di accesso per il bucket S3 o il container Swift. "Utilizzo dell'ultimo tempo di accesso nelle regole ILM"
Vincolo di posizione (solo S3)	• uguale a • non uguale	La regione in cui è stato creato un bucket S3. Utilizzare **ILM** > **regioni** per definire le regioni visualizzate. **Nota:** Un valore di US-East-1 corrisponde agli oggetti nei bucket creati nella regione US-East-1 e agli oggetti nei bucket che non hanno alcuna regione specificata. "Configurazione delle regioni (opzionale e solo S3)"
Dimensione oggetto (MB)	• uguale a • non uguale • inferiore a. • inferiore o uguale a. • maggiore di • maggiore di o uguale a.	Dimensione dell'oggetto in MB. Per filtrare le dimensioni degli oggetti inferiori a 1 MB, digitare un valore decimale. Ad esempio, impostare il filtro avanzato **dimensione oggetto (MB)** su **maggiore di 0.2** per qualsiasi regola che crea copie con codifica di cancellazione. Questa impostazione garantisce che l'erasure coding non venga utilizzato per oggetti di dimensioni inferiori o pari a 200 KB. **Nota:** il tipo di browser e le impostazioni internazionali controllano se è necessario utilizzare un punto o una virgola come separatore decimale.

Tipo di metadati	Operatori supportati	Valore dei metadati
Metadati dell'utente	• contiene • termina con • uguale a • esiste • non contiene • non finisce con • non uguale • non esiste • non inizia con • inizia con	Coppia key-value, dove **User Metadata Name** è la chiave e **User Metadata Value** è il valore. Ad esempio, per filtrare gli oggetti con metadati utente di `color=blue`, specificare `color` Per **User Metadata Name**, `equals` per l'operatore, e. `blue` Per **valore metadati utente**. **Nota:** i nomi dei metadati utente non distinguono tra maiuscole e minuscole; i valori dei metadati utente distinguono tra maiuscole e minuscole.
Tag oggetto (solo S3)	• contiene • termina con • uguale a • esiste • non contiene • non finisce con • non uguale • non esiste • non inizia con • inizia con	Coppia Key-value, dove **Object Tag Name** è la chiave e **Object Tag Value** è il valore. Ad esempio, per filtrare gli oggetti che hanno un tag Object di `Image=True`, specificare `Image` Per **Nome tag oggetto**, `equals` per l'operatore, e. `True` Per **valore tag oggetto**. **Nota:** i nomi dei tag degli oggetti e i valori dei tag degli oggetti fanno distinzione tra maiuscole e minuscole. È necessario inserire questi elementi esattamente come sono stati definiti per l'oggetto.

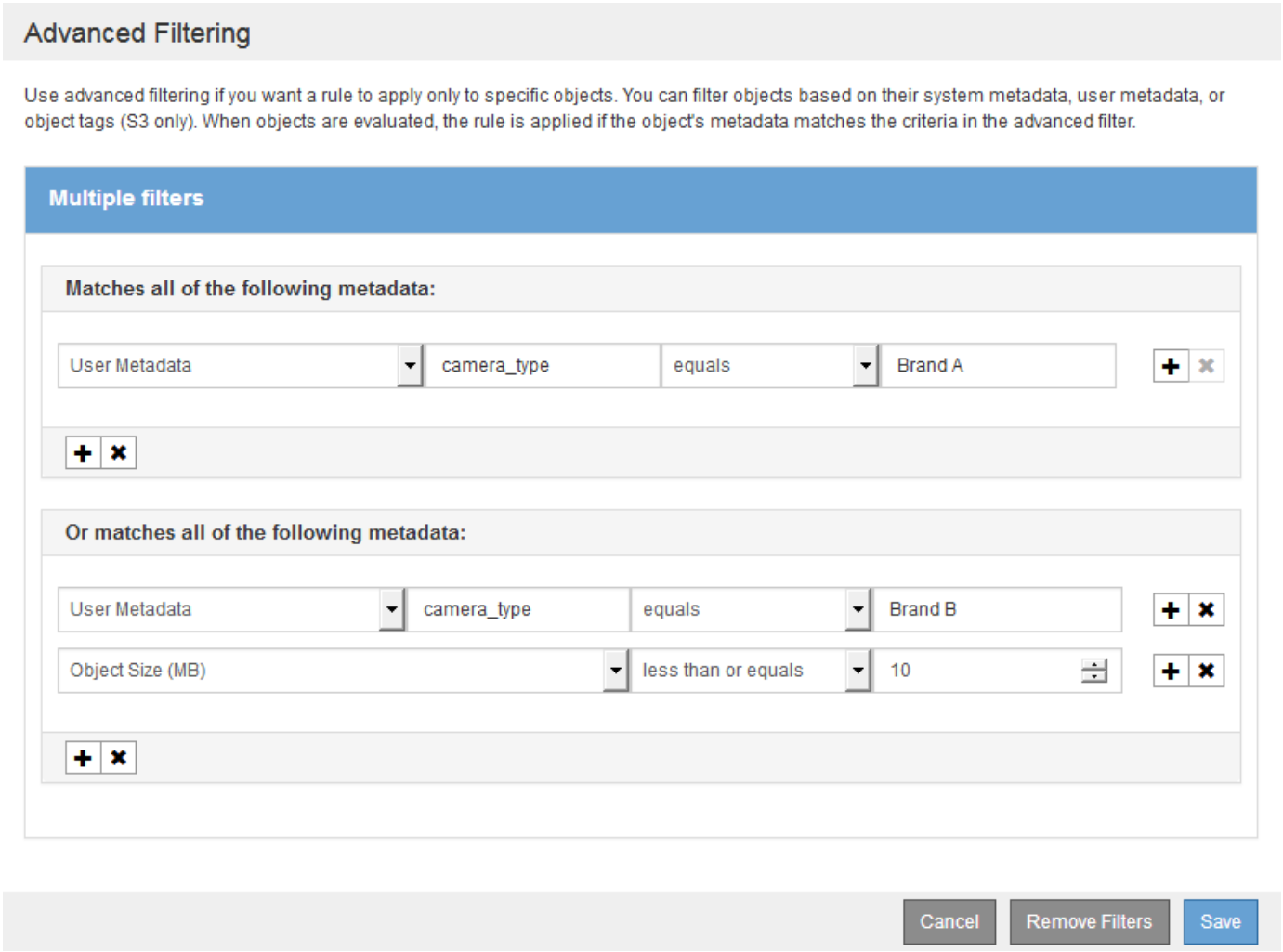
Specifica di più tipi di metadati e valori

Quando si definisce il filtraggio avanzato, è possibile specificare più tipi di metadati e più valori di metadati. Ad esempio, se si desidera che una regola corrisponda a oggetti di dimensioni comprese tra 10 MB e 100 MB, selezionare il tipo di metadati **Object Size** e specificare due valori di metadati.

- Il primo valore di metadati specifica oggetti superiori o uguali a 10 MB.
- Il secondo valore di metadati specifica gli oggetti inferiori o uguali a 100 MB.



L'utilizzo di più voci consente di avere un controllo preciso su quali oggetti vengono associati. Nell'esempio seguente, la regola si applica agli oggetti che hanno un marchio A o un marchio B come valore dei metadati dell'utente camera_TYPE. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.



Informazioni correlate

"Utilizzo dell'ultimo tempo di accesso nelle regole ILM"

"Configurazione delle regioni (opzionale e solo S3)"

Fase 2 di 3: Definizione delle posizioni

Il passaggio 2 (definizione delle posizioni) della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano la durata della memorizzazione degli oggetti, il tipo di copie (replicate o codificate per la cancellazione), la posizione di archiviazione e il numero di copie.

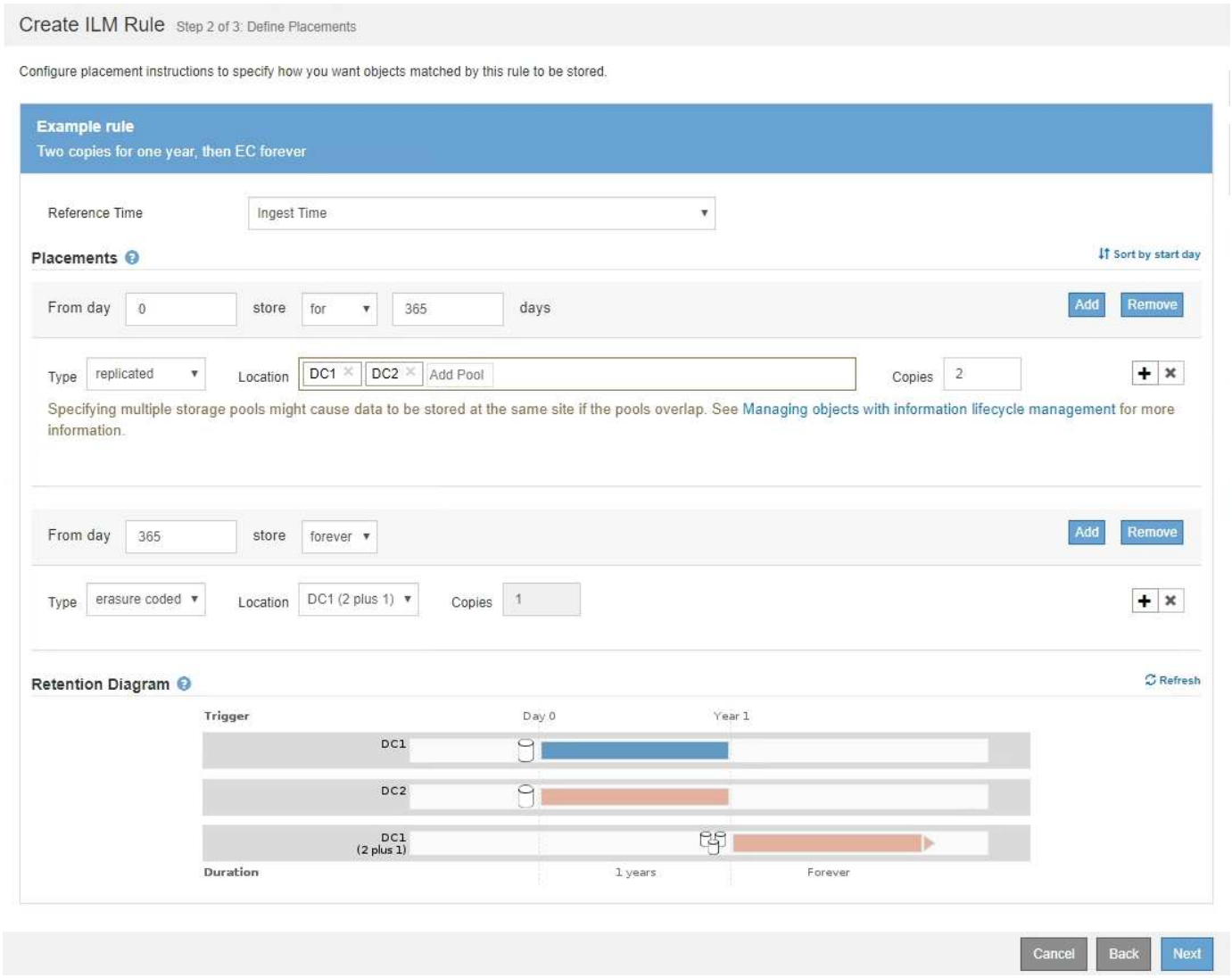
A proposito di questa attività

Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo. Quando si utilizzano più istruzioni, i periodi di tempo devono essere contigui e almeno un'istruzione deve iniziare il giorno 0. Le istruzioni possono continuare per sempre o fino a quando non sono più necessarie copie di oggetti.

Ogni istruzione di posizionamento può avere più righe se si desidera creare diversi tipi di copie o utilizzare posizioni diverse durante tale periodo di tempo.

Questa regola ILM di esempio crea due copie replicate per il primo anno. Ogni copia viene salvata in un pool di storage in un sito diverso. Dopo un anno, viene creata una copia 2+1 con codice di cancellazione e salvata in

un solo sito.



Fasi

1. Per **Reference Time** (tempo di riferimento), selezionare il tipo di tempo da utilizzare per il calcolo dell'ora di inizio di un'istruzione di posizionamento.

Opzione	Descrizione
Tempo di acquisizione	L'ora in cui l'oggetto è stato acquisito.
Ora ultimo accesso	L'ora in cui l'oggetto è stato recuperato per l'ultima volta (letto o visualizzato). **Nota:** per utilizzare questa opzione, è necessario attivare gli aggiornamenti dell'ultimo tempo di accesso per il bucket S3 o il container Swift. "Utilizzo dell'ultimo tempo di accesso nelle regole ILM"

Opzione	Descrizione
Ora non corrente	Il tempo in cui una versione dell'oggetto è diventata non aggiornata a causa dell'acquisizione di una nuova versione e della sua sostituzione come versione corrente. **Nota:** l'ora non corrente si applica solo agli oggetti S3 nei bucket abilitati per il controllo delle versioni. È possibile utilizzare questa opzione per ridurre l'impatto dello storage degli oggetti con versione filtrando le versioni degli oggetti non correnti. Vedere "esempio 4: Regole ILM e policy per gli oggetti con versione S3".
Tempo di creazione definito dall'utente	Tempo specificato nei metadati definiti dall'utente.

Se si desidera creare una regola conforme, selezionare **Ingest Time**.

2. Nella sezione **posizionamenti**, selezionare un'ora di inizio e una durata per il primo periodo di tempo.

   Ad esempio, è possibile specificare dove memorizzare gli oggetti per il primo anno ("Ay 0 for 365 days `d`"). Almeno un'istruzione deve iniziare al giorno 0.

3. Se si desidera creare copie replicate:
   a. Dall'elenco a discesa **tipo**, selezionare **replicato**.
   b. Nel campo **Location**, selezionare **Add Pool** per ciascun pool di storage che si desidera aggiungere.

      Se si specifica un solo pool di storage, tenere presente che StorageGRID può memorizzare solo una copia replicata di un oggetto su un nodo di storage specifico. Se la griglia include tre nodi di storage e si seleziona 4 come numero di copie, verranno eseguite solo tre copie: Una copia per ciascun nodo di storage.

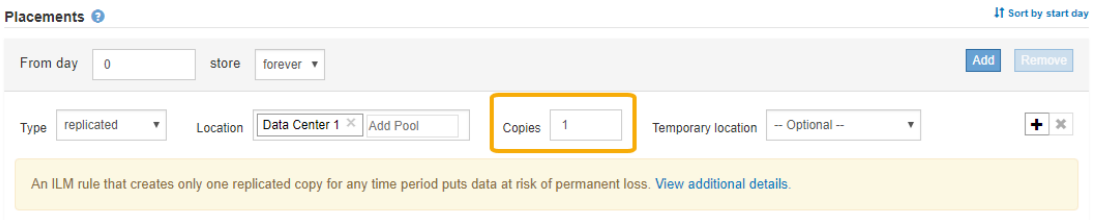
      Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

      Se si specificano più pool di storage, tenere presenti le seguenti regole:

      - Il numero di copie non può essere superiore al numero di pool di storage.
      - Se il numero di copie corrisponde al numero di pool di storage, viene memorizzata una copia dell'oggetto in ciascun pool di storage.
      - Se il numero di copie è inferiore al numero di pool di storage, il sistema distribuisce le copie per mantenere bilanciato l'utilizzo del disco tra i pool, garantendo al contempo che nessun sito riceva più di una copia di un oggetto.
      - Se i pool di storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di storage predefinito di tutti i nodi di storage e di un altro pool di storage.

c. Selezionare il numero di copie che si desidera eseguire.

Se si modifica il numero di copie in 1, viene visualizzato un avviso. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto durante un periodo di tempo, tale oggetto viene perso se un nodo di storage si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.



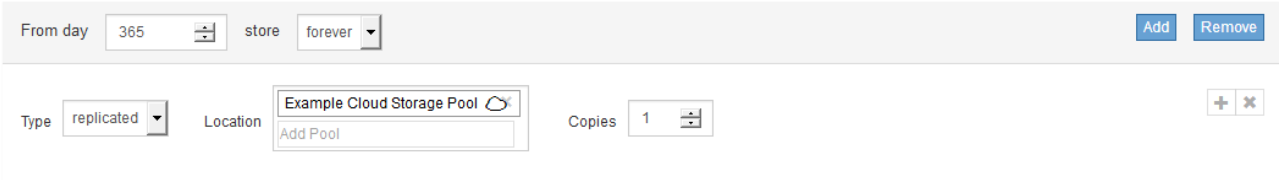
Per evitare questi rischi, effettuare una o più delle seguenti operazioni:

- Aumentare il numero di copie per il periodo di tempo.
- Fare clic sull'icona con il segno più ➕ per creare copie aggiuntive durante il periodo di tempo. Quindi, selezionare un pool di storage diverso o un pool di storage cloud.
- Selezionare **erasure coded** per tipo, invece di **Replicated**. È possibile ignorare questo avviso se questa regola crea già più copie per tutti i periodi di tempo.

d. Se è stato specificato un solo pool di storage, ignorare il campo **posizione temporanea**.

Le posizioni temporanee sono obsolete e verranno rimosse in una release futura.

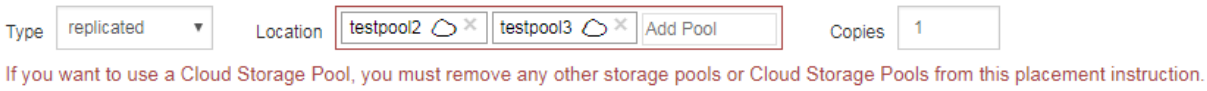
4. Se si desidera memorizzare oggetti in un pool di storage cloud:
   a. Dall'elenco a discesa **tipo**, selezionare **replicato**.
   b. Nel campo **Location**, selezionare **Add Pool** (Aggiungi pool). Quindi, selezionare un pool di storage cloud.



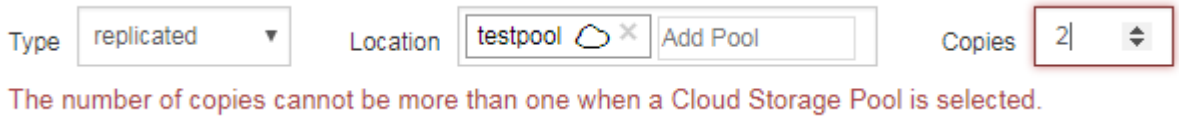
Quando si utilizzano i Cloud Storage Pool, tenere presenti le seguenti regole:

- Non è possibile selezionare più di un Cloud Storage Pool in una singola istruzione di posizionamento. Allo stesso modo, non è possibile selezionare un Cloud Storage Pool e un pool di

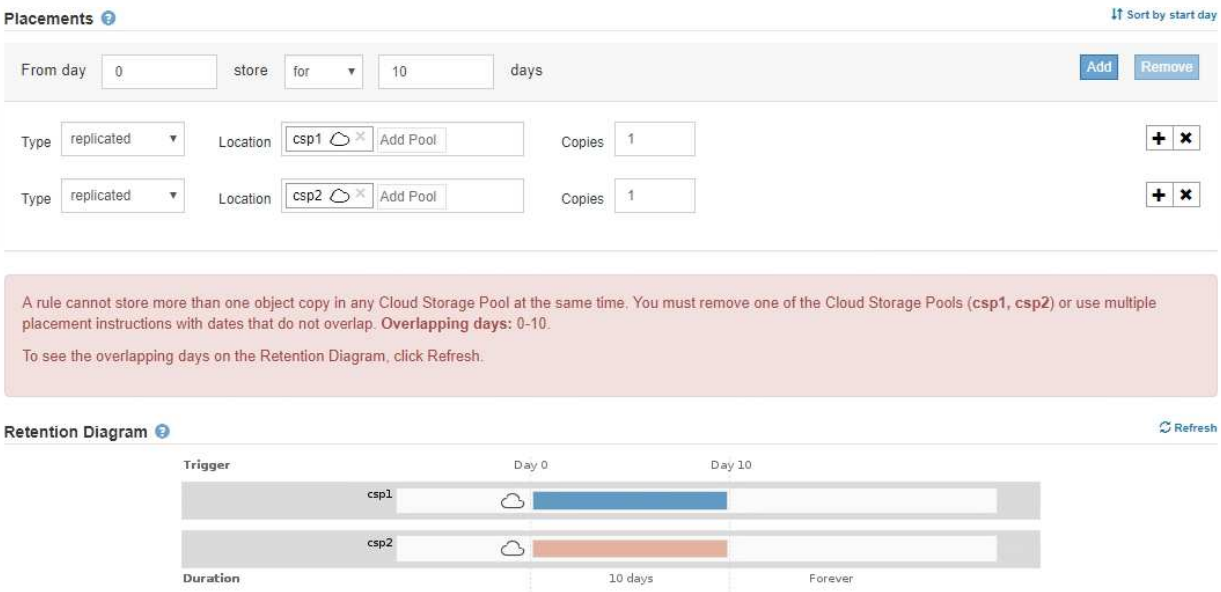
storage nelle stesse istruzioni di posizionamento.



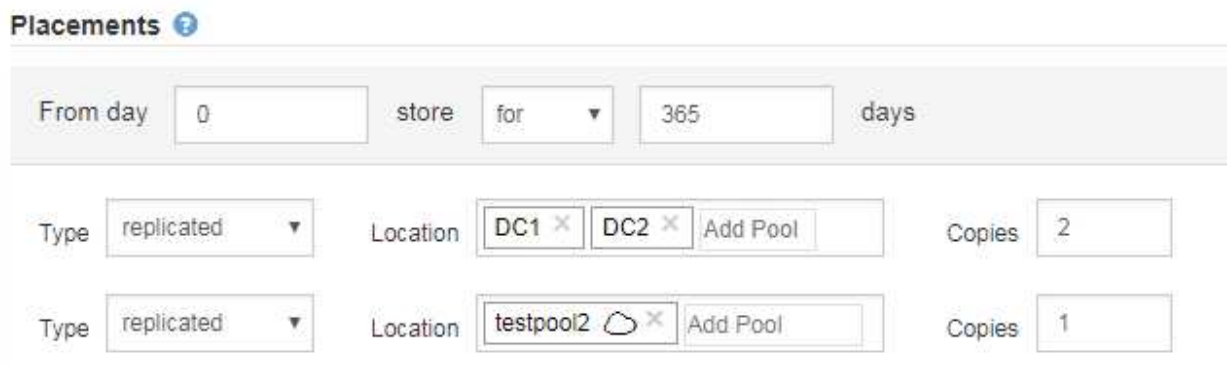
- È possibile memorizzare solo una copia di un oggetto in un determinato pool di storage cloud. Se si imposta **copie** su 2 o più, viene visualizzato un messaggio di errore.



- Non è possibile memorizzare più copie di un oggetto contemporaneamente in un pool di storage cloud. Viene visualizzato un messaggio di errore se più posizioni che utilizzano un pool di storage cloud presentano date sovrapposte o se più righe nello stesso posizionamento utilizzano un pool di storage cloud.



- È possibile memorizzare un oggetto in un pool di storage cloud nello stesso momento in cui l'oggetto viene memorizzato come copie replicate o erasure coded in StorageGRID. Tuttavia, come mostra questo esempio, è necessario includere più di una riga nelle istruzioni di posizionamento per il periodo di tempo, in modo da poter specificare il numero e i tipi di copie per ciascuna posizione.



5. Se si desidera creare una copia con codice di cancellazione:

   a. Dall'elenco a discesa **tipo**, selezionare **erasure coded**.

      Il numero di copie viene modificato in 1. Viene visualizzato un avviso se la regola non dispone di un filtro avanzato per ignorare oggetti di dimensioni pari o inferiori a 200 KB.

      Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

   b. Se viene visualizzato l'avviso relativo alle dimensioni dell'oggetto, attenersi alla seguente procedura per cancellarlo:

      i. Selezionare **Indietro** per tornare alla fase 1.

      ii. Selezionare **Advanced Filtering** (filtraggio avanzato).

      iii. Impostare il filtro dimensione oggetto (MB) su "maggiore di 0.2".

   c. Selezionare la posizione di storage.

      La posizione di storage per una copia con codice di cancellazione include il nome del pool di storage, seguito dal nome del profilo di codifica Erasure.

6. Facoltativamente, aggiungere periodi di tempo diversi o creare copie aggiuntive in posizioni diverse:
   - Fare clic sull'icona più per creare copie aggiuntive in una posizione diversa durante lo stesso periodo di tempo.
   - Fare clic su **Add** (Aggiungi) per aggiungere un periodo di tempo diverso alle istruzioni di posizionamento.

   Gli oggetti vengono eliminati automaticamente alla fine del periodo di tempo finale, a meno che il periodo di tempo finale non termini con **forever**.

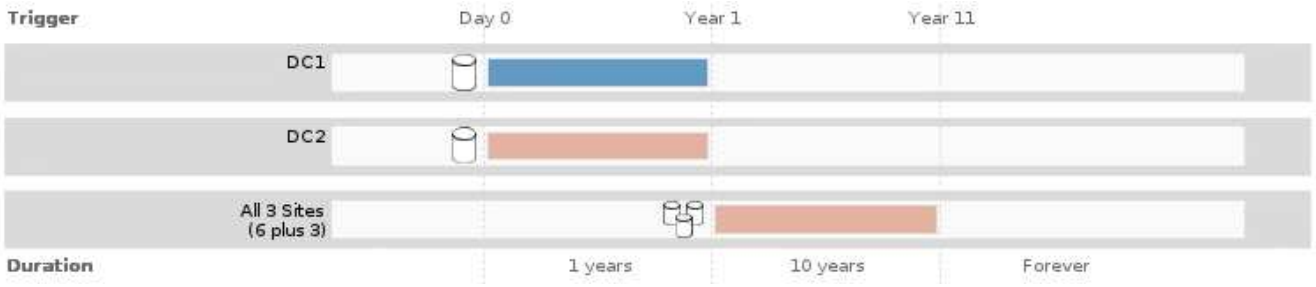
7. Fare clic su **Refresh** (Aggiorna) per aggiornare il diagramma di conservazione e confermare le istruzioni di posizionamento.

   Ogni riga del diagramma indica dove e quando verranno collocate le copie degli oggetti. Il tipo di copia è rappresentato da una delle seguenti icone:

	Copia replicata
	Copia con codifica erasure

	Copia del pool di cloud storage

In questo esempio, due copie replicate verranno salvate in due pool di storage (DC1 e DC2) per un anno. Quindi, una copia con codice di cancellazione verrà salvata per altri 10 anni, utilizzando uno schema di erasure coding 6+3 presso tre siti. Dopo 11 anni, gli oggetti verranno cancellati da StorageGRID.



8. Fare clic su **Avanti**.

   Viene visualizzato il punto 3 (definire il comportamento di Ingest).

Informazioni correlate

"Quali sono le istruzioni per il posizionamento delle regole ILM"

"Esempio 4: Regole ILM e policy per gli oggetti con versione S3"

"Perché non utilizzare la replica a copia singola"

"Gestione degli oggetti con S3 Object Lock"

"Utilizzo di un pool di storage come posizione temporanea (obsoleto)"

"Fase 3 di 3: Definizione del comportamento di acquisizione"

Utilizzo dell'ultimo tempo di accesso nelle regole ILM

In una regola ILM, è possibile utilizzare l'ora dell'ultimo accesso come ora di riferimento. Ad esempio, è possibile lasciare oggetti che sono stati visualizzati negli ultimi tre mesi sui nodi di storage locali, mentre si spostano oggetti che non sono stati visualizzati di recente in una posizione off-site. È inoltre possibile utilizzare l'ora dell'ultimo accesso come filtro avanzato se si desidera che una regola ILM si applichi solo agli oggetti a cui è stato effettuato l'ultimo accesso in una data specifica.

A proposito di questa attività

Prima di utilizzare l'ultimo tempo di accesso in una regola ILM, esaminare le seguenti considerazioni:

- Quando si utilizza l'ultimo tempo di accesso come tempo di riferimento, tenere presente che la modifica dell'ultimo tempo di accesso per un oggetto non attiva una valutazione ILM immediata. Al contrario, le posizioni dell'oggetto vengono valutate e l'oggetto viene spostato come richiesto quando ILM in background valuta l'oggetto. Questa operazione potrebbe richiedere due settimane o più dopo l'accesso all'oggetto.

  Tenere conto di questa latenza durante la creazione di regole ILM basate sull'ultimo tempo di accesso ed

evitare posizionamenti che utilizzano brevi periodi di tempo (meno di un mese).

- Quando si utilizza l'ultimo tempo di accesso come filtro avanzato o come tempo di riferimento, è necessario attivare gli ultimi aggiornamenti dell'ora di accesso per i bucket S3. È possibile utilizzare il tenant Manager o l'API di gestione tenant.

> Gli ultimi aggiornamenti dell'orario di accesso sono sempre attivati per i container Swift, ma sono disattivati per impostazione predefinita per i bucket S3.

> Tenere presente che l'attivazione degli ultimi aggiornamenti del tempo di accesso può ridurre le performance, soprattutto nei sistemi con oggetti di piccole dimensioni. L'impatto delle performance si verifica perché StorageGRID deve aggiornare gli oggetti con nuovi timestamp ogni volta che gli oggetti vengono recuperati.

La tabella seguente riassume se l'ora dell'ultimo accesso viene aggiornata per tutti gli oggetti nel bucket per diversi tipi di richieste.

Tipo di richiesta	Se l'ora dell'ultimo accesso viene aggiornata quando gli ultimi aggiornamenti dell'ora di accesso sono disattivati	Se l'ora dell'ultimo accesso viene aggiornata quando sono attivati gli ultimi aggiornamenti dell'ora di accesso
Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Informazioni correlate

"Utilizzare S3"

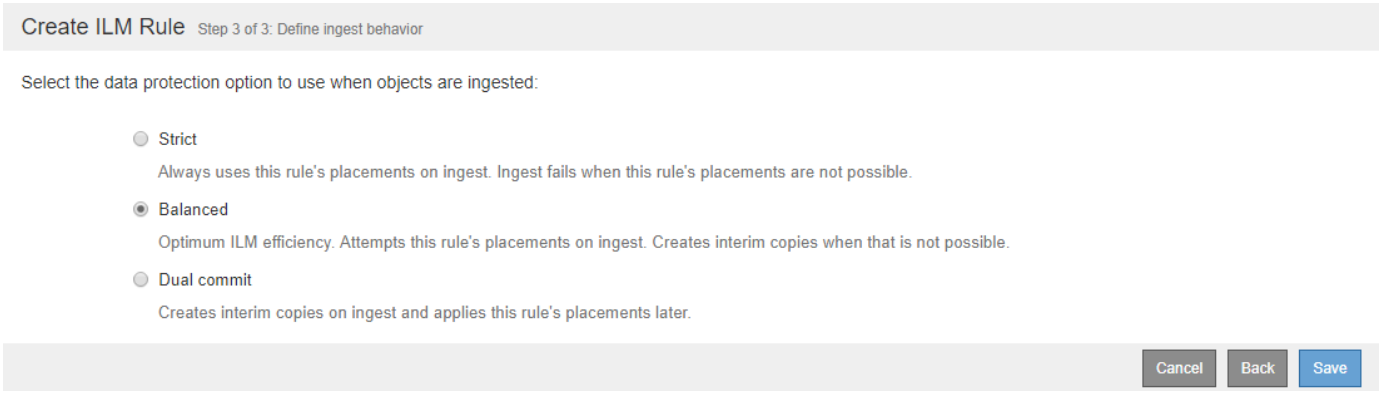
"Utilizzare un account tenant"

Fase 3 di 3: Definizione del comportamento di acquisizione

Il passaggio 3 (Definisci comportamento di acquisizione) della procedura guidata Crea regola ILM consente di scegliere come proteggere gli oggetti filtrati da questa regola durante l'acquisizione.

A proposito di questa attività

StorageGRID può eseguire copie temporanee e mettere in coda gli oggetti per la valutazione ILM in un secondo momento, oppure può eseguire copie per soddisfare immediatamente le istruzioni di posizionamento della regola.



Fasi

1. Selezionare l'opzione di protezione dei dati da utilizzare quando vengono acquisiti oggetti:

Opzione	Descrizione
Rigoroso	Utilizza sempre le posizioni di questa regola per l'acquisizione. L'acquisizione non riesce quando non è possibile eseguire il posizionamento di questa regola.
Bilanciato	Efficienza ILM ottimale. Tenta di inserire i posizionamenti di questa regola. Crea copie temporanee quando ciò non è possibile.
Commit doppio	Crea copie temporanee al momento dell'acquisizione e applica le posizioni di questa regola in un secondo momento.

   Balanced offre una combinazione di sicurezza ed efficienza dei dati adatta nella maggior parte dei casi. Per soddisfare requisiti specifici, vengono generalmente utilizzati i requisiti Strict o Dual Commit.

   Per ulteriori informazioni, consulta "quali sono le opzioni di protezione dei dati per l'acquisizione" e "vantaggi e svantaggi di ciascuna opzione di protezione dei dati".

   > Viene visualizzato un messaggio di errore se si seleziona l'opzione Strict (rigoroso) o Balanced (bilanciato) e la regola utilizza una delle seguenti posizioni:
   >
   > - Un pool di storage cloud al giorno 0
   > - Un nodo di archivio al giorno 0
   > - Un Cloud Storage Pool o un nodo di archivio quando la regola utilizza un tempo di creazione definito dall'utente come tempo di riferimento

2. Fare clic su **Save** (Salva).

   La regola ILM viene salvata. La regola non diventa attiva fino a quando non viene aggiunta a un criterio ILM e tale criterio non viene attivato.

Informazioni correlate

"Opzioni di protezione dei dati per l'acquisizione"

"Vantaggi, svantaggi e limitazioni delle opzioni di protezione dei dati"

"Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"

"Creazione di un criterio ILM"

Creazione di una regola ILM predefinita

Ogni policy ILM deve disporre di una regola predefinita che non filtra gli oggetti. Prima di creare un criterio ILM, è necessario creare almeno una regola ILM che possa essere utilizzata come regola predefinita per il criterio.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

La regola predefinita è l'ultima regola da valutare in un criterio ILM, pertanto non può utilizzare alcun filtro. Le istruzioni di posizionamento per la regola predefinita vengono applicate a tutti gli oggetti che non corrispondono a un'altra regola del criterio.

In questo esempio di policy, la prima regola si applica solo agli oggetti appartenenti al tenant A. La regola predefinita, ultima, si applica agli oggetti appartenenti a tutti gli altri account tenant.

Quando si crea la regola predefinita, tenere presenti i seguenti requisiti:

- La regola predefinita viene automaticamente inserita come ultima regola nel criterio.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita dovrebbe creare copie replicate.

> Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per un criterio. Le regole di erasure coding devono utilizzare un filtro avanzato per evitare che oggetti più piccoli vengano sottoposti a erasure coding.

- In generale, la regola predefinita deve conservare gli oggetti per sempre.
- Se si utilizza (o si intende attivare) l'impostazione globale S3 Object Lock (blocco oggetto S3), la regola predefinita per il criterio attivo o proposto deve essere conforme.

Fasi

1. Selezionare **ILM** > **regole**.

   Viene visualizzata la pagina ILM Rules (regole ILM).

2. Selezionare **Crea**.

   Viene visualizzata la fase 1 (Definisci le basi) della procedura guidata Crea regola ILM.

3. Immettere un nome univoco per la regola nel campo **Nome**.
4. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.
5. Lasciare vuoto il campo **account tenant**.

   La regola predefinita deve essere applicata a tutti gli account tenant.

6. Lasciare vuoto il campo **Nome bucket**.

   La regola predefinita deve essere applicata a tutti i bucket S3 e ai container Swift.

7. Non selezionare **Advanced Filtering**

   La regola predefinita non può specificare alcun filtro.

8. Selezionare **Avanti**.

   Viene visualizzato il punto 2 (definizione delle posizioni).

9. Specificare le istruzioni di posizionamento per la regola predefinita.
   - La regola predefinita deve conservare gli oggetti per sempre. Quando si attiva un nuovo criterio, viene visualizzato un avviso se la regola predefinita non conserva gli oggetti per sempre. Devi confermare che questo è il comportamento che ti aspetti.
   - La regola predefinita dovrebbe creare copie replicate.

     > Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per un criterio. Le regole di erasure coding devono includere il filtro avanzato **Object Size (MB) maggiore di 0.2** per evitare che oggetti più piccoli vengano sottoposti a erasure coding.

   - Se si utilizza (o si intende attivare) l'impostazione globale S3 Object Lock (blocco oggetto S3), la regola predefinita deve essere conforme:
     - 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 l'ora di inizio come ora di riferimento.
     - Almeno una riga delle istruzioni di posizionamento deve essere "forever".
10. Fare clic su **Refresh** (Aggiorna) per aggiornare il diagramma di conservazione e confermare le istruzioni di posizionamento.
11. Fare clic su **Avanti**.

    Viene visualizzato il punto 3 (definire il comportamento di Ingest).

12. Selezionare l'opzione di protezione dei dati da utilizzare quando vengono acquisiti oggetti e selezionare **Salva**.

Creazione di un criterio ILM

Quando si crea un criterio ILM, si inizia selezionando e ordinando le regole ILM. Quindi, verificare il comportamento della policy proposta simulandola rispetto agli oggetti precedentemente acquisiti. Quando si è soddisfatti del corretto funzionamento del criterio proposto, è possibile attivarlo per creare il criterio attivo.

> Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Considerazioni per la creazione di un criterio ILM

- Utilizzare la policy integrata del sistema, Baseline 2 Copies Policy, solo nei sistemi di test. La regola Make 2 copies di questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.
- Durante la progettazione di un nuovo criterio, considerare tutti i diversi tipi di oggetti che potrebbero essere inseriti nella griglia. Assicurarsi che il criterio includa regole per la corrispondenza e posizionare questi oggetti secondo necessità.
- Mantenere la policy ILM il più semplice possibile. In questo modo si evitano situazioni potenzialmente pericolose in cui i dati degli oggetti non sono protetti come previsto quando nel tempo vengono apportate modifiche al sistema StorageGRID.
- Assicurarsi che le regole della policy siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio. Ad esempio, se la prima regola di un criterio corrisponde a un oggetto, tale regola non verrà valutata da altre regole.
- L'ultima regola in ogni policy ILM è la regola ILM predefinita, che non può utilizzare alcun filtro. Se un oggetto non è stato associato da un'altra regola, la regola predefinita controlla la posizione e il tempo di conservazione dell'oggetto.
- Prima di attivare un nuovo criterio, esaminare le modifiche apportate dal criterio al posizionamento degli oggetti esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Informazioni correlate

"Che cos'è una policy ILM"

"Esempio 6: Modifica di un criterio ILM"

Creazione di una policy ILM proposta

È possibile creare un criterio ILM proposto da zero oppure clonare il criterio attivo corrente se si desidera iniziare con lo stesso insieme di regole.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver creato le regole ILM che si desidera aggiungere al criterio proposto. Se necessario, è possibile salvare una policy proposta, creare regole aggiuntive e quindi modificare la policy proposta per aggiungere le nuove regole.

- È necessario aver creato una regola ILM predefinita per il criterio che non contiene filtri.

  "Creazione di una regola ILM predefinita"

A proposito di questa attività

I motivi tipici per la creazione di una policy ILM proposta includono:

- È stato aggiunto un nuovo sito ed è necessario utilizzare nuove regole ILM per posizionare gli oggetti in tale sito.
- Si sta smantellando un sito ed è necessario rimuovere tutte le regole che fanno riferimento al sito.
- È stato aggiunto un nuovo tenant con requisiti speciali per la protezione dei dati.
- Hai iniziato a utilizzare un Cloud Storage Pool.

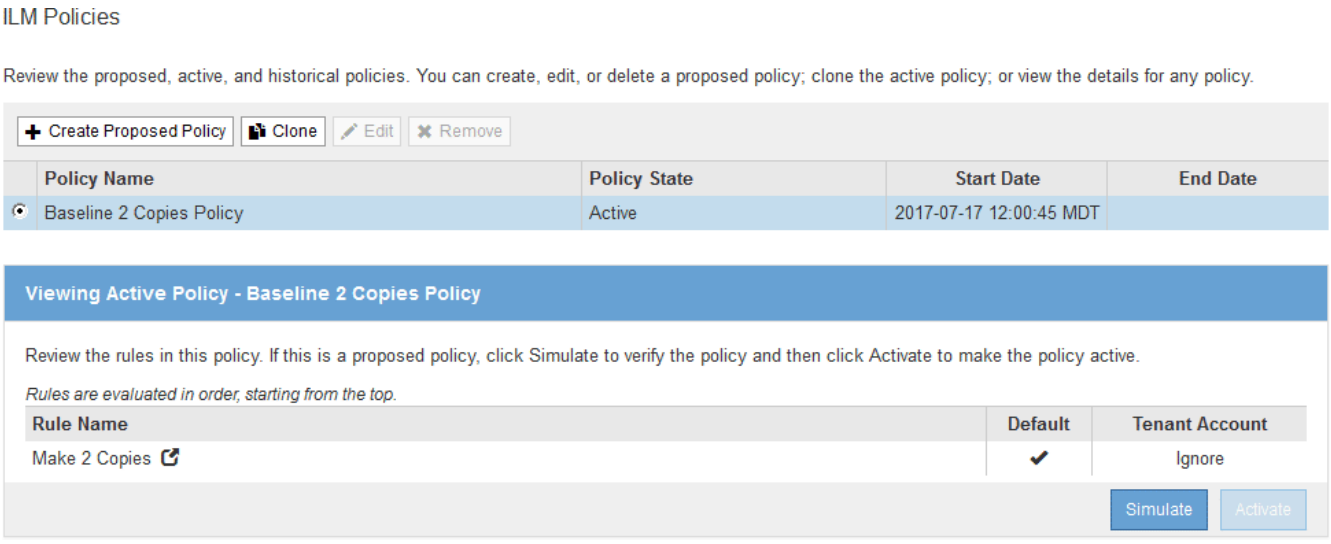
> Utilizzare la policy integrata del sistema, Baseline 2 Copies Policy, solo nei sistemi di test. La regola Make 2 copies di questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.

> Se è stata attivata l'impostazione blocco oggetti S3 globale, i passaggi per la creazione di un criterio sono leggermente diversi. È necessario assicurarsi che il criterio ILM sia conforme ai requisiti dei bucket che hanno attivato il blocco oggetti S3.
>
> "Creazione di un criterio ILM dopo l'attivazione del blocco oggetti S3"

Fasi

1. Selezionare **ILM** > **Policy**.

   Viene visualizzata la pagina ILM Policies (Criteri ILM). Da questa pagina, è possibile esaminare l'elenco dei criteri proposti, attivi e storici; creare, modificare, oppure rimuovere una policy proposta, clonare la policy attiva o visualizzare i dettagli di qualsiasi policy.

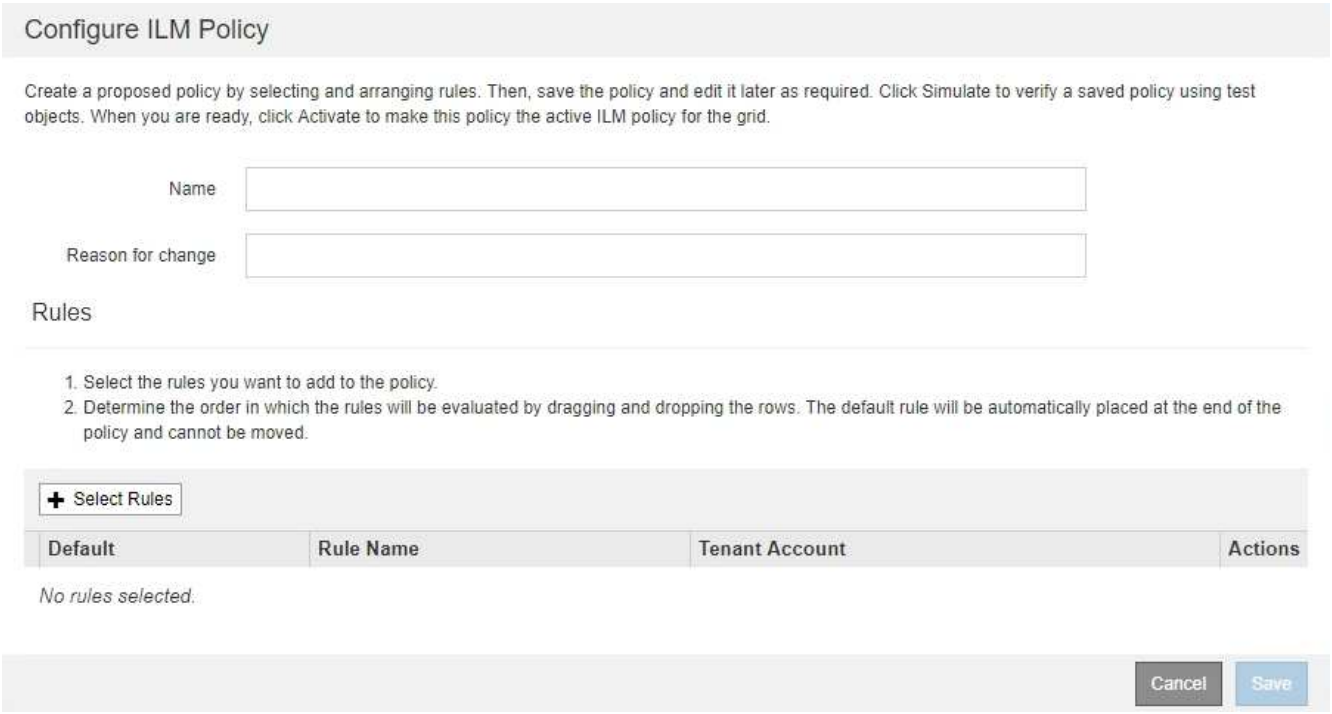
   

2. Determinare come si desidera creare il criterio ILM proposto.

Opzione	Fasi
Creare una nuova policy proposta senza regole già selezionate	a. Se esiste attualmente un criterio ILM proposto, selezionarlo e fare clic su **Rimuovi**. Non è possibile creare una nuova policy proposta se esiste già una policy proposta. b. Fare clic su **Crea policy proposta**.
Creare una policy proposta in base alla policy attiva	a. Se esiste attualmente un criterio ILM proposto, selezionarlo e fare clic su **Rimuovi**. Non è possibile clonare il criterio attivo se esiste già un criterio proposto. b. Selezionare il criterio attivo dalla tabella. c. Fare clic su **Clone**.
Modificare la policy proposta esistente	a. Selezionare la policy proposta dalla tabella. b. Fare clic su **Edit** (Modifica).

Viene visualizzata la finestra di dialogo Configure ILM Policy (Configura policy ILM).

Se si sta creando una nuova policy proposta, tutti i campi sono vuoti e non viene selezionata alcuna regola.



Se si esegue la clonazione del criterio attivo, il campo **Nome** mostra il nome del criterio attivo, aggiunto da un numero di versione ("v2" nell'esempio). Le regole utilizzate nel criterio attivo vengono selezionate e visualizzate nell'ordine corrente.

3. Immettere un nome univoco per la policy proposta nel campo **Nome**.

   Immettere almeno 1 e non più di 64 caratteri. Se si clonano i criteri attivi, è possibile utilizzare il nome corrente con il numero di versione aggiunto oppure immettere un nuovo nome.

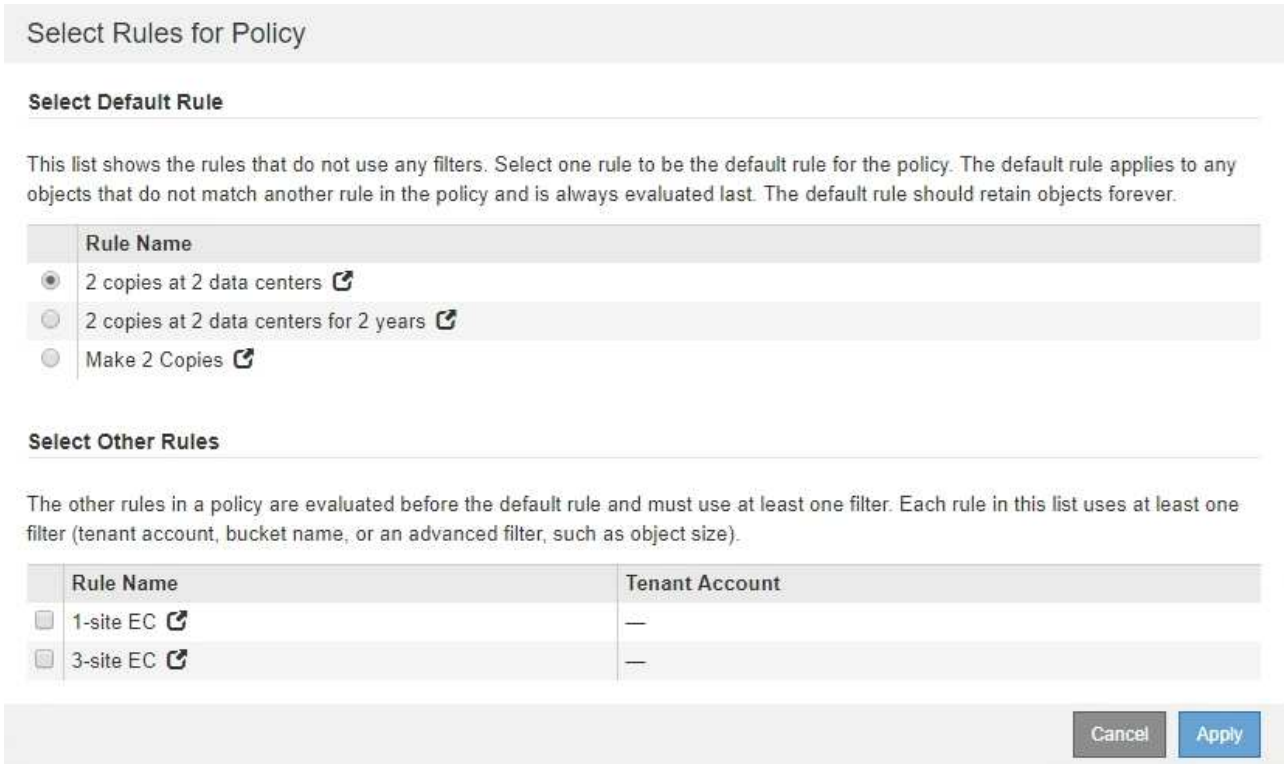
4. Inserire il motivo della creazione di una nuova policy proposta nel campo **motivo della modifica**.

   Immettere almeno 1 e non più di 128 caratteri.

5. Per aggiungere regole al criterio, selezionare **Seleziona regole**.

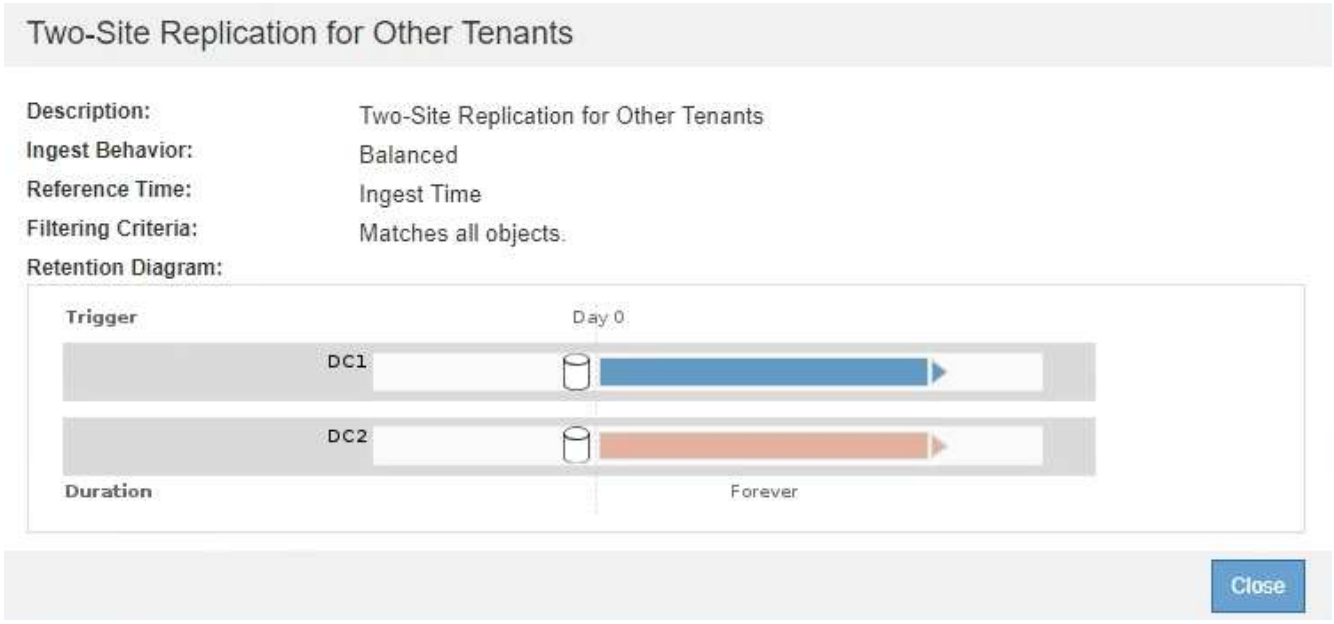
   Viene visualizzata la finestra di dialogo Select Rules for Policy (Seleziona regole per policy), con tutte le regole definite elencate. Se si sta clonando un criterio:

   - Vengono selezionate le regole utilizzate dal criterio che si sta clonando.
   - Se il criterio da clonare utilizza regole senza filtri che non erano la regola predefinita, viene richiesto di rimuovere tutte le regole tranne una di queste.
   - Se la regola predefinita utilizza un filtro, viene richiesto di selezionare una nuova regola predefinita.
   - Se la regola predefinita non è l'ultima, un pulsante consente di spostarla alla fine del nuovo criterio.



6. Selezionare il nome di una regola o l'icona ulteriori dettagli per visualizzare le impostazioni relative a tale regola.

   Questo esempio mostra i dettagli di una regola ILM che esegue due copie replicate in due siti.



7. Nella sezione **Select Default Rule** (Seleziona regola predefinita), selezionare una regola predefinita per il criterio proposto.

   La regola predefinita si applica a tutti gli oggetti che non corrispondono a un'altra regola del criterio. La regola predefinita non può utilizzare alcun filtro e viene sempre valutata per ultima.

   Se nella sezione Select Default Rule (Seleziona regola predefinita) non è elencata alcuna regola, uscire dalla pagina dei criteri ILM e creare una regola predefinita.

   "Creazione di una regola ILM predefinita"

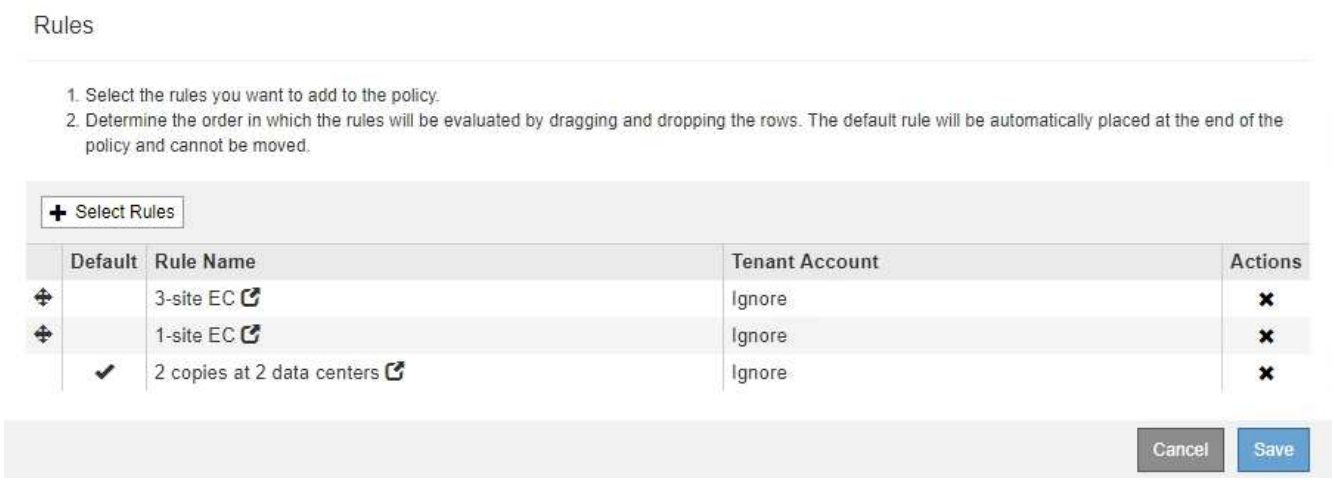
   Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.

8. Nella sezione **Seleziona altre regole**, selezionare le altre regole che si desidera includere nel criterio.

   Le altre regole vengono valutate prima della regola predefinita e devono utilizzare almeno un filtro (account tenant, nome bucket o filtro avanzato, ad esempio la dimensione dell'oggetto).

9. Una volta selezionate le regole, selezionare **Apply** (Applica).

   Vengono elencate le regole selezionate. La regola predefinita è alla fine, con le altre regole sopra di essa.



Viene visualizzato un avviso se la regola predefinita non conserva gli oggetti per sempre. Quando si attiva questo criterio, è necessario confermare che si desidera che StorageGRID elimini gli oggetti quando sono trascorse le istruzioni di posizionamento per la regola predefinita (a meno che un ciclo di vita del bucket non mantenga gli oggetti più a lungo).

10. Trascinare e rilasciare le righe per le regole non predefinite per determinare l'ordine in cui verranno valutate queste regole.

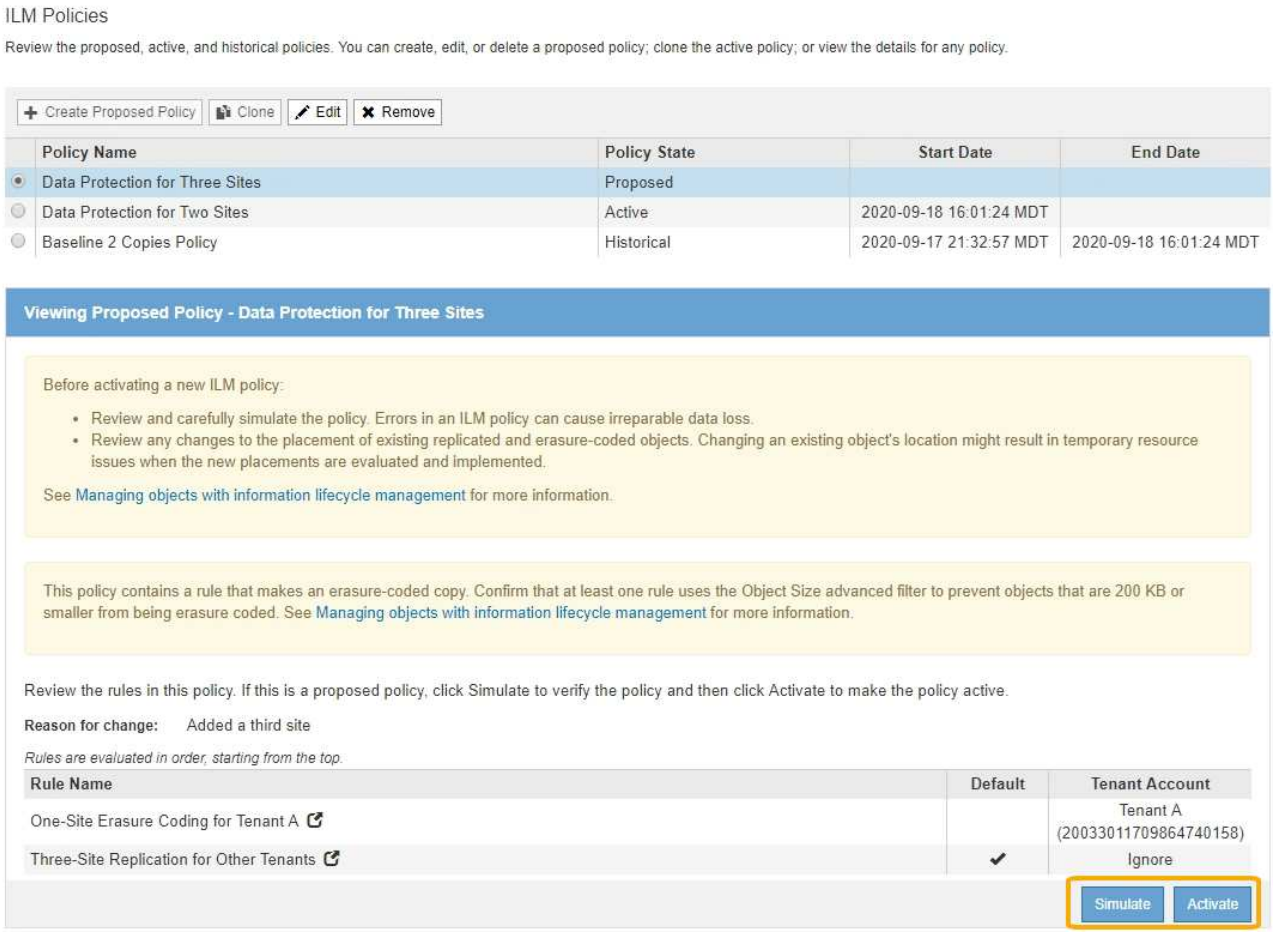
    Non è possibile spostare la regola predefinita.

    Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

11. Se necessario, fare clic sull'icona di eliminazione ✖ Per eliminare le regole che non si desidera inserire nel criterio, oppure selezionare **Select Rules** (Seleziona regole) per aggiungere altre regole.
12. Al termine, selezionare **Salva**.

    La pagina delle policy ILM viene aggiornata:

    - Il criterio salvato viene visualizzato come proposto. Le policy proposte non hanno date di inizio e fine.
    - I pulsanti **simulate** e **activate** sono abilitati.



13. Passare a. "Simulazione di un criterio ILM".

Informazioni correlate

"Che cos'è una policy ILM"

"Gestione degli oggetti con S3 Object Lock"

Creazione di un criterio ILM dopo l'attivazione del blocco oggetti S3

Se l'impostazione blocco oggetti S3 globale è attivata, i passaggi per la creazione di un criterio sono leggermente diversi. È necessario assicurarsi che il criterio ILM sia conforme ai requisiti dei bucket che hanno attivato il blocco oggetti S3.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- L'impostazione globale S3 Object Lock (blocco oggetti S3) deve essere già attivata per il sistema StorageGRID.

> Se l'impostazione globale S3 Object Lock non è stata attivata, utilizzare le istruzioni generali per creare un criterio proposto.
>
> "Creazione di una policy ILM proposta"

- È necessario aver creato le regole ILM conformi e non conformi che si desidera aggiungere al criterio proposto. Se necessario, è possibile salvare una policy proposta, creare regole aggiuntive e quindi modificare la policy proposta per aggiungere le nuove regole.

  "Esempio 7: Policy ILM conforme per il blocco oggetti S3"

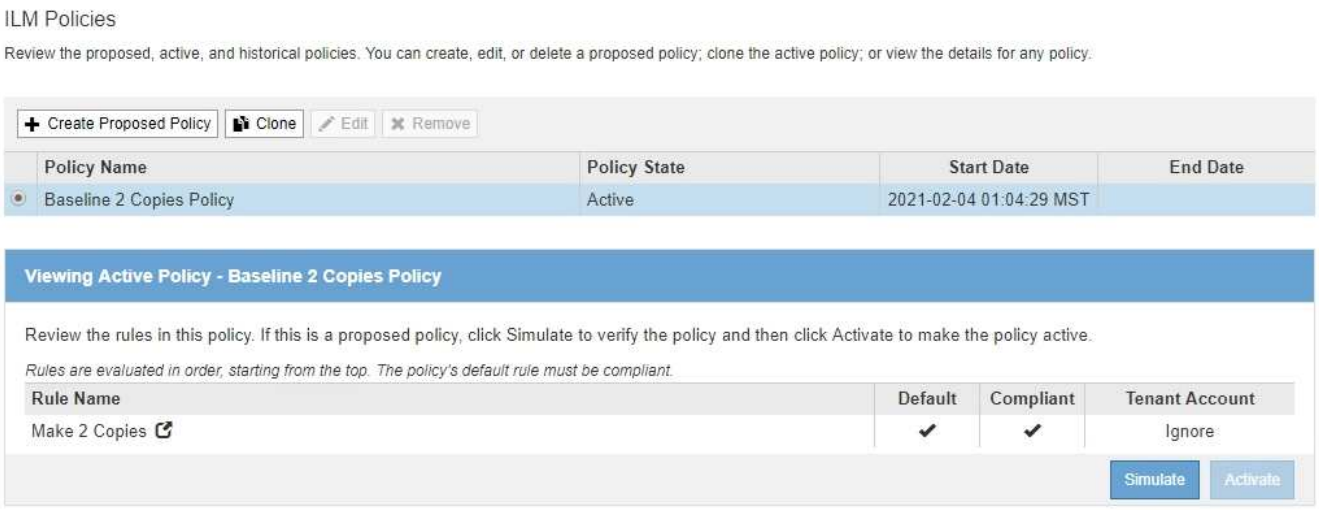
- È necessario aver creato una regola ILM predefinita conforme per il criterio.

  "Creazione di una regola ILM predefinita"

Fasi

1. Selezionare **ILM** > **Policy**.

   Viene visualizzata la pagina ILM Policies (Criteri ILM). Se l'impostazione globale S3 Object Lock è attivata, la pagina ILM Policies (Criteri ILM) indica quali regole ILM sono conformi.



2. Immettere un nome univoco per la policy proposta nel campo **Nome**.

   Immettere almeno 1 e non più di 64 caratteri.

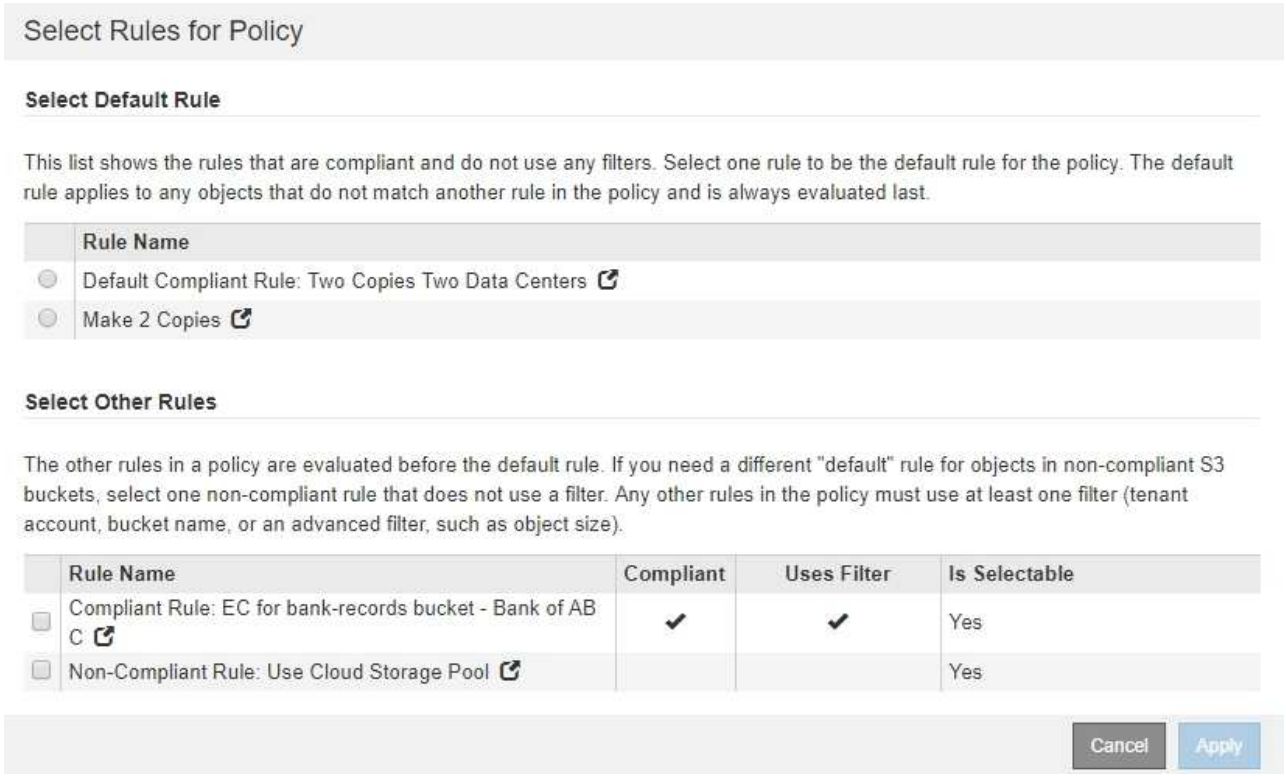
3. Inserire il motivo della creazione di una nuova policy proposta nel campo **motivo della modifica**.

   Immettere almeno 1 e non più di 128 caratteri.

4. Per aggiungere regole al criterio, selezionare **Seleziona regole**.

   Viene visualizzata la finestra di dialogo Select Rules for Policy (Seleziona regole per policy), con tutte le regole definite elencate.

   - La sezione Select Default Rule (Seleziona regola predefinita) elenca le regole che possono essere quelle predefinite per un criterio conforme. Include regole conformi che non utilizzano filtri.
   - La sezione Seleziona altre regole elenca le altre regole conformi e non compatibili che possono essere selezionate per questo
     criterio.



5. Selezionare il nome di una regola o l'icona ulteriori dettagli per visualizzare le impostazioni relative a tale regola.
6. Nella sezione **Select Default Rule** (Seleziona regola predefinita), selezionare una regola predefinita per il criterio proposto.

   La tabella di questa sezione elenca solo le regole conformi e non utilizzano filtri.

   > Se nella sezione Select Default Rule (Seleziona regola predefinita) non è elencata alcuna regola, uscire dalla pagina dei criteri ILM e creare una regola predefinita conforme.
   >
   > "Creazione di una regola ILM predefinita"

   > Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se si utilizza questa regola, sullo stesso sito potrebbero essere collocate più copie di un oggetto.

7. Nella sezione **Seleziona altre regole**, selezionare le altre regole che si desidera includere nel criterio.

   a. Se è necessaria una regola "default" diversa per gli oggetti nei bucket S3 non conformi, selezionare facoltativamente una regola non conforme che non utilizza un filtro.

      Ad esempio, è possibile utilizzare un Cloud Storage Pool o un nodo di archiviazione per memorizzare gli oggetti nei bucket che non hanno attivato il blocco oggetti S3.

      > È possibile selezionare solo una regola non conforme che non utilizza un filtro. Non appena si seleziona una regola, la colonna **è selezionabile** mostra **No** per qualsiasi altra regola non conforme senza filtri.

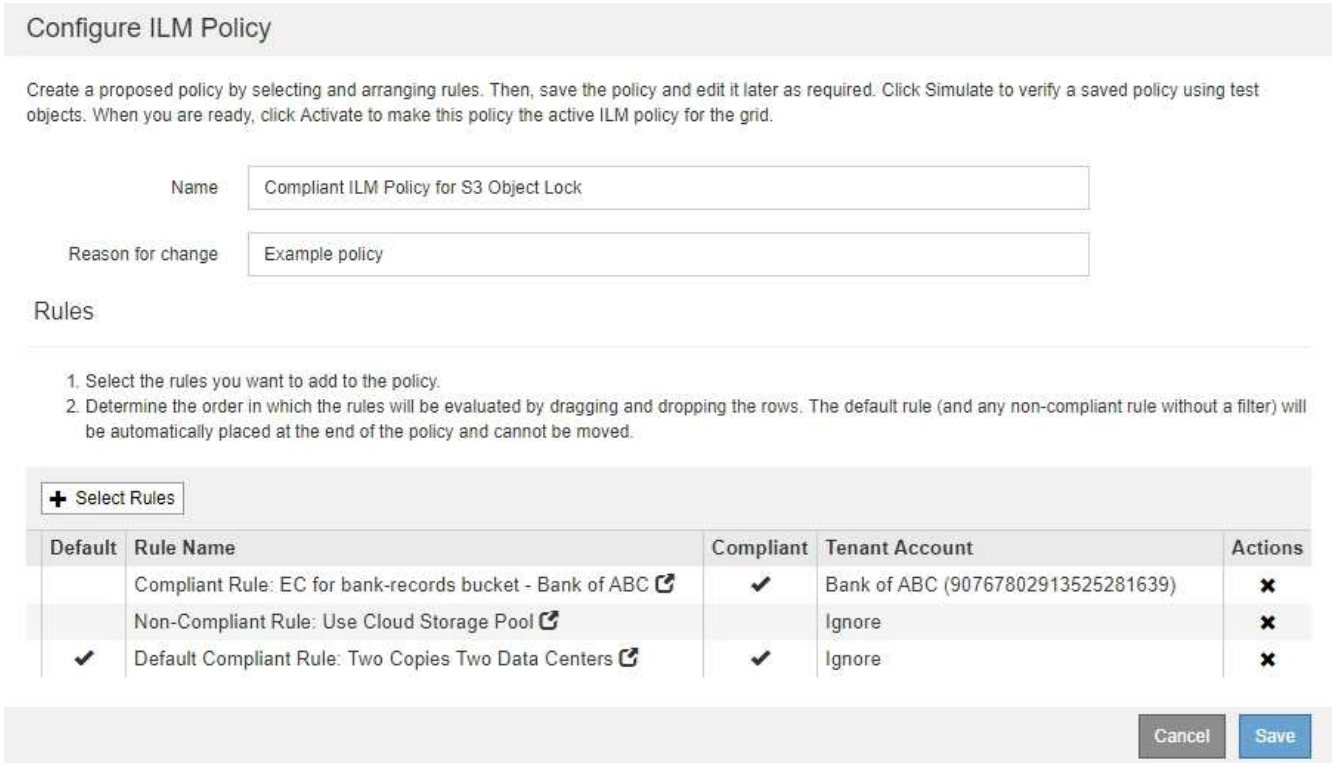
   a. Selezionare qualsiasi altra regola conforme o non conforme che si desidera utilizzare nel criterio.

Le altre regole devono utilizzare almeno un filtro (account tenant, nome bucket o filtro avanzato, ad esempio la dimensione dell'oggetto).

8. Una volta selezionate le regole, selezionare **Apply** (Applica).

   Vengono elencate le regole selezionate. La regola predefinita è alla fine, con le altre regole sopra di essa. Se è stata selezionata anche una regola "default" non conforme, tale regola viene aggiunta come seconda o ultima regola nel criterio.

   In questo esempio, l'ultima regola, 2 copie 2 data center, è la regola predefinita: È conforme e non dispone di filtri. La seconda all'ultima regola, Cloud Storage Pool, non ha filtri ma non è conforme.



   .

9. Trascinare e rilasciare le righe per le regole non predefinite per determinare l'ordine in cui verranno valutate queste regole.

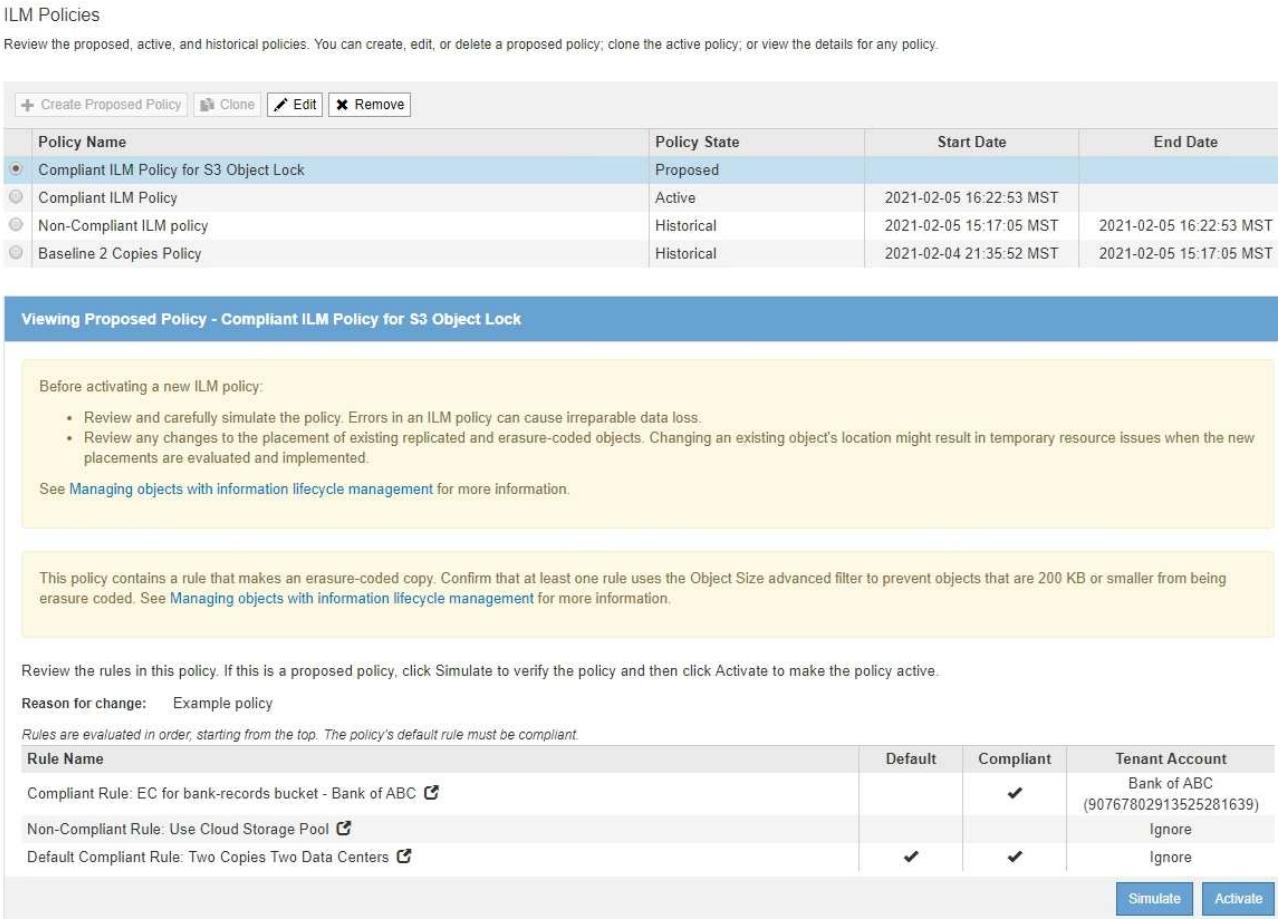
   Non è possibile spostare la regola predefinita o la regola "default" non conforme.

   > Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

10. Se necessario, fare clic sull'icona di eliminazione ✖ Per eliminare le regole che non si desidera inserire nel criterio, oppure selezionare **Select Rules** (Seleziona regole) per aggiungere altre regole.
11. Al termine, selezionare **Salva**.

    La pagina delle policy ILM viene aggiornata:

    - Il criterio salvato viene visualizzato come proposto. Le policy proposte non hanno date di inizio e fine.
    - I pulsanti **simulate** e **activate** sono abilitati.



12. Passare a. "Simulazione di un criterio ILM".

Simulazione di un criterio ILM

È necessario simulare una policy proposta sugli oggetti di test prima di attivare la policy e applicarla ai dati di produzione. La finestra di simulazione offre un ambiente standalone sicuro per le policy di test prima che vengano attivate e applicate ai dati nell'ambiente di produzione.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario conoscere il bucket S3/object-key o il container Swift/object-name per ciascun oggetto che si desidera sottoporre a test e che tali oggetti siano già stati acquisiti.

A proposito di questa attività

È necessario selezionare attentamente gli oggetti per i quali si desidera sottoporre a test il criterio proposto. Per simulare un criterio in maniera approfondita, è necessario testare almeno un oggetto per ciascun filtro in ogni regola.

Ad esempio, se un criterio include una regola per la corrispondenza degli oggetti nel bucket A e un'altra regola per la corrispondenza degli oggetti nel bucket B, è necessario selezionare almeno un oggetto dal bucket A e un oggetto dal bucket B per eseguire un test completo del criterio. Se il criterio include una regola predefinita per posizionare tutti gli altri oggetti, è necessario testare almeno un oggetto da un altro bucket.

Quando si simula un criterio, si applicano le seguenti considerazioni:

- Dopo aver apportato modifiche a un criterio, salvare il criterio proposto. Quindi, simulare il comportamento della policy proposta salvata.
- Quando si simula un criterio, le regole ILM del criterio filtrano gli oggetti di test, in modo da poter vedere quale regola è stata applicata a ciascun oggetto. Tuttavia, non vengono create copie di oggetti e non vengono posizionati oggetti. L'esecuzione di una simulazione non modifica in alcun modo i dati, le regole o i criteri.
- La pagina Simulation conserva gli oggetti testati fino alla chiusura, all'allontanamento o all'aggiornamento della pagina ILM Policies.
- Simulation restituisce il nome della regola corrispondente. Per determinare quale pool di storage o profilo di codifica Erasure è in vigore, è possibile visualizzare il diagramma di conservazione facendo clic sul nome della regola o sull'icona ulteriori dettagli .
- Se è attivata la versione S3, il criterio viene simulato solo rispetto alla versione corrente dell'oggetto.

Fasi

1. Selezionare e organizzare le regole e salvare la policy proposta.

   La policy in questo esempio ha tre regole:

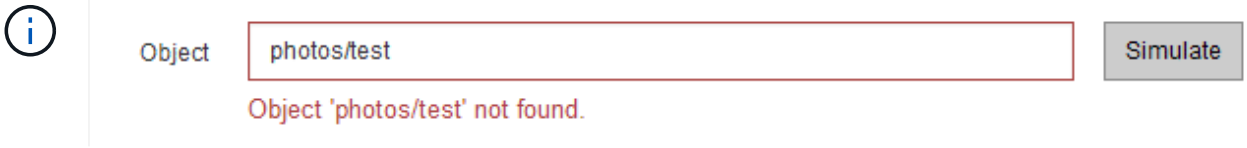
Nome regola	Filtro	Tipo di copie	Conservazione
X-men	• Tenant A. • Metadati dell'utente (serie=x-men)	2 copie in due data center	2 anni
PNG	La chiave termina con .png	2 copie in due data center	5 anni
Due copie di due data center	*Nessuno*	2 copie in due data center	Per sempre

2. Fare clic su **simulate**.

Viene visualizzata la finestra di dialogo Simulation ILM Policy (Criteri ILM di Simulation).

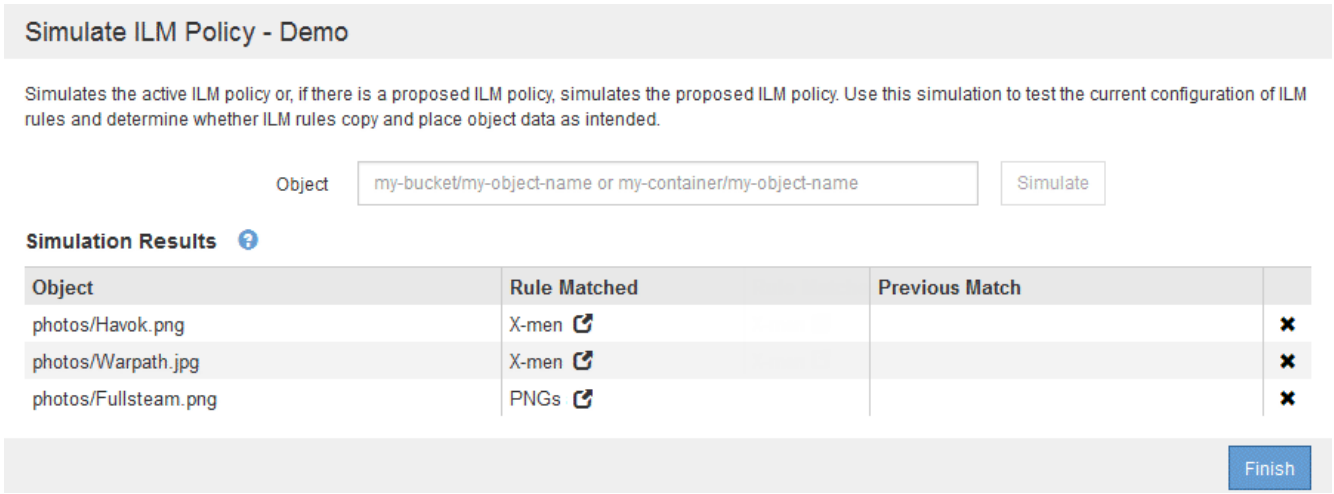
3. Nel campo **oggetto**, immettere il bucket S3/object-key o il container Swift/object-name per un oggetto di test e fare clic su **simulate**.

Se si specifica un oggetto non acquisito, viene visualizzato un messaggio.



4. In **risultati di simulazione**, confermare che ogni oggetto è stato associato dalla regola corretta.

Nell'esempio, il `Havok.png` e. `Warpath.jpg` Gli oggetti sono stati associati correttamente dalla regola X-MEN. Il `Fullsteam.png` oggetto, che non include `series=x-men` Metadati dell'utente, non corrispondenti alla regola X-MEN ma corrispondenti correttamente alla regola PNG. La regola predefinita non è stata utilizzata perché tutti e tre gli oggetti erano associati da altre regole.



Esempi di simulazione delle policy ILM

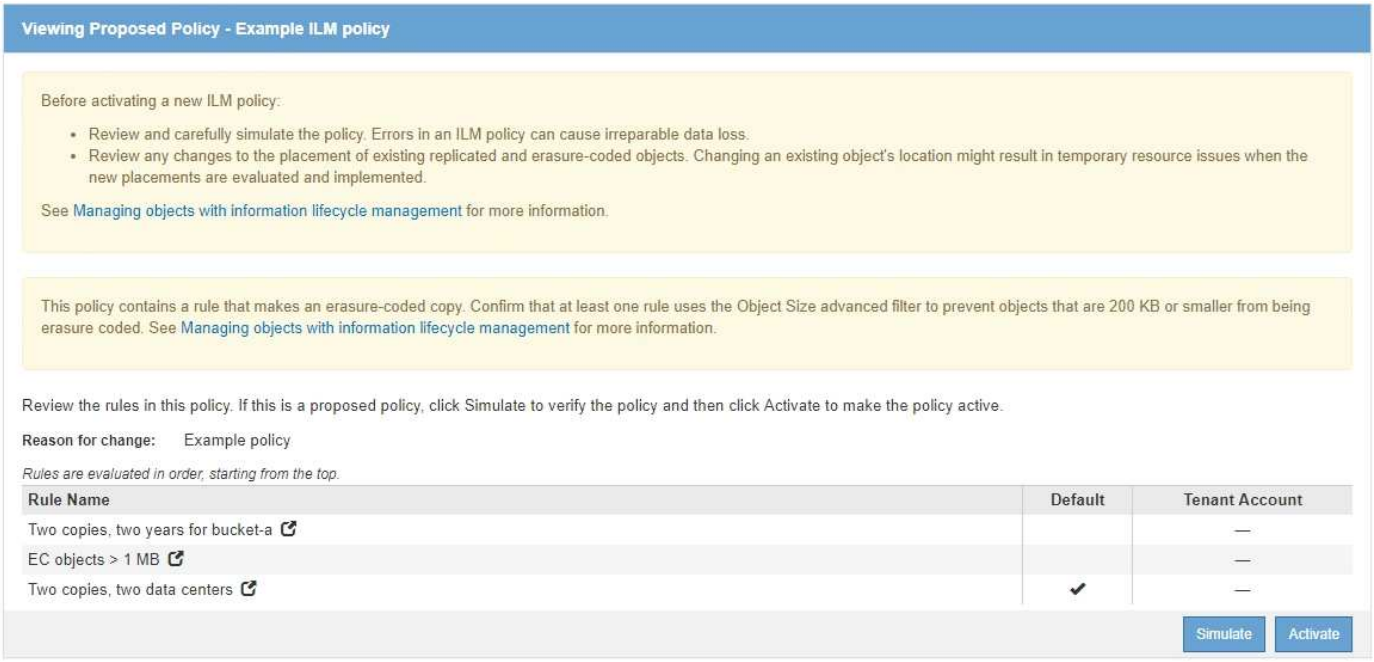
Questi esempi mostrano come è possibile verificare le regole ILM simulando il criterio ILM prima di attivarlo.

Esempio 1: Verifica delle regole durante la simulazione di una policy ILM proposta

Questo esempio mostra come verificare le regole quando si simula un criterio proposto.

In questo esempio, la **policy ILM di esempio** viene simulata rispetto agli oggetti acquisiti in due bucket. La policy include tre regole, come segue:

- La prima regola, **due copie, due anni per bucket-a**, si applica solo agli oggetti nel bucket-a.
- La seconda regola, **EC objects › 1 MB**, si applica a tutti i bucket, ma ai filtri sugli oggetti superiori a 1 MB.
- La terza regola è quella predefinita e non include alcun filtro.



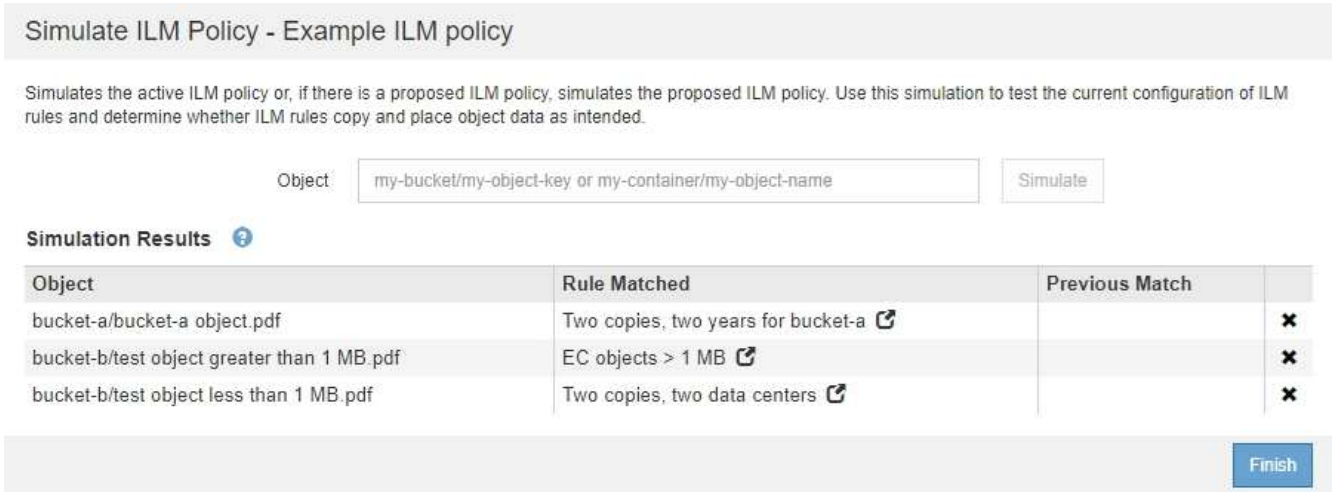
Fasi

1. Dopo aver aggiunto le regole e salvato il criterio, fare clic su **simulate**.

   Viene visualizzata la finestra di dialogo Simula policy ILM.

2. Nel campo **oggetto**, immettere il bucket S3/object-key o il container Swift/object-name per un oggetto di test e fare clic su **simulate**.

   Vengono visualizzati i risultati di Simulation, che mostrano quale regola del criterio corrisponde a ciascun oggetto testato.



3. Verificare che ogni oggetto sia stato associato alla regola corretta.

   In questo esempio:

   a. `bucket-a/bucket-a object.pdf` corrisponde correttamente alla prima regola, che filtra sugli oggetti in `bucket-a`.

   b. `bucket-b/test object greater than 1 MB.pdf` è in `bucket-b`, quindi non corrisponde alla prima regola. Al contrario, è stata associata correttamente dalla seconda regola, che filtra su oggetti

superiori a 1 MB.

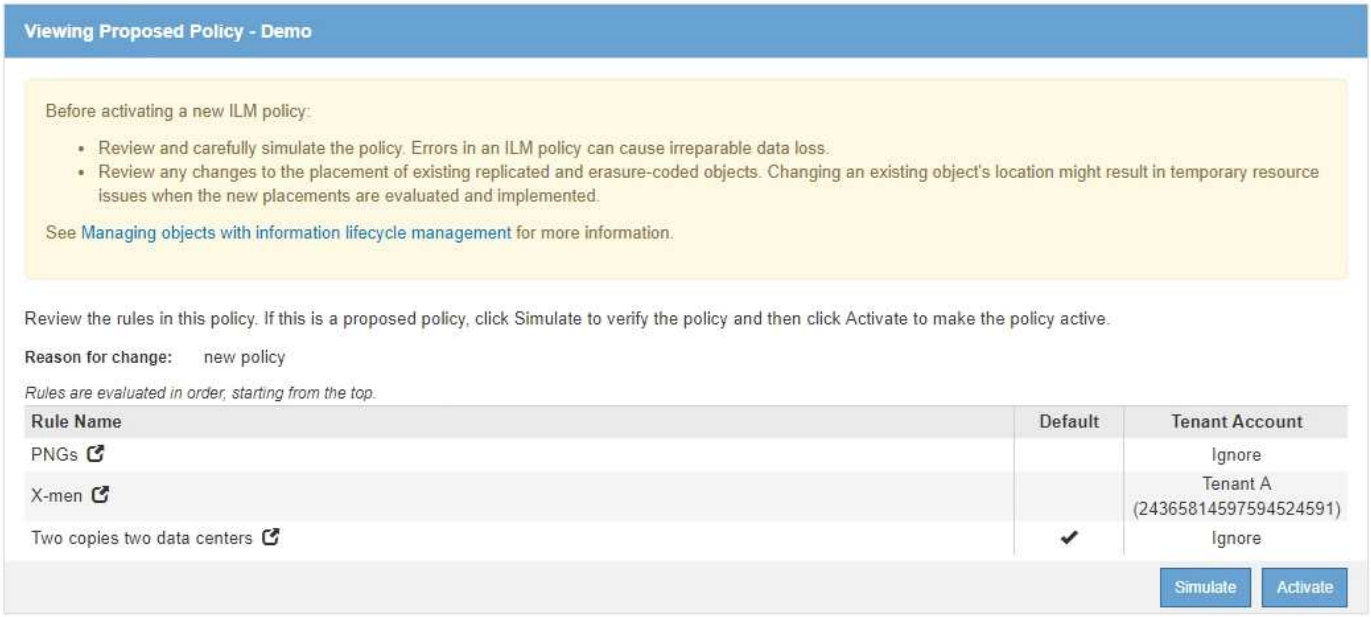
c. `bucket-b/test object less than 1 MB.pdf` i filtri non corrispondono alle prime due regole, quindi verranno posizionati in base alla regola predefinita, che non include filtri.

Esempio 2: Riordinamento delle regole durante la simulazione di una policy ILM proposta

Questo esempio mostra come è possibile riordinare le regole per modificare i risultati durante la simulazione di un criterio.

In questo esempio, viene simulata la policy **Demo**. Questo criterio, che ha lo scopo di trovare oggetti con metadati utente series=x-men, include tre regole, come segue:

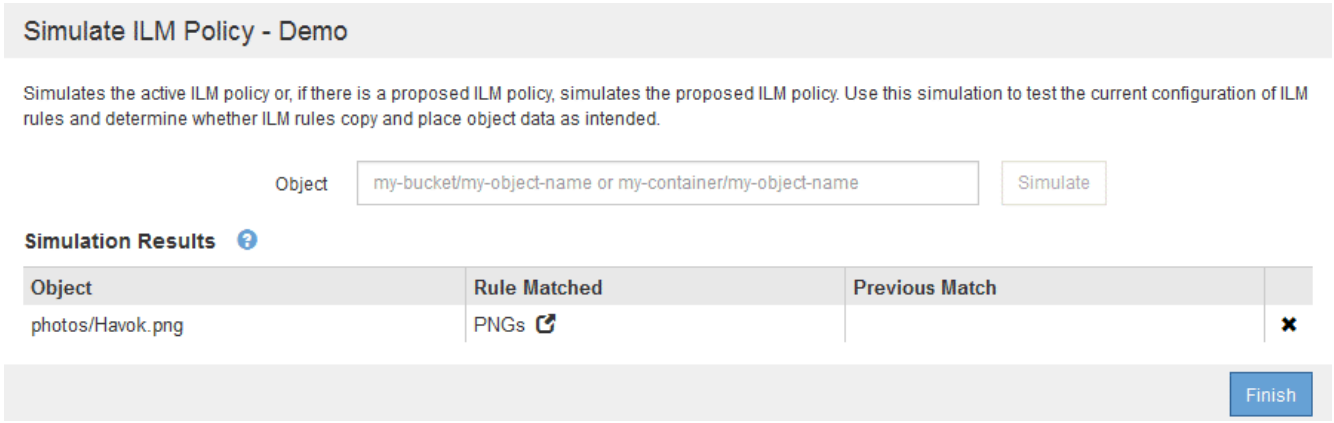
- La prima regola, **PNG**, filtra i nomi delle chiavi che terminano `.png`.
- La seconda regola, **X-MEN**, si applica solo agli oggetti per il tenant A e ai filtri per `series=x-men` metadati dell'utente.
- L'ultima regola, **due copie due data center**, è la regola predefinita, che corrisponde a tutti gli oggetti che non corrispondono alle prime due regole.



Fasi

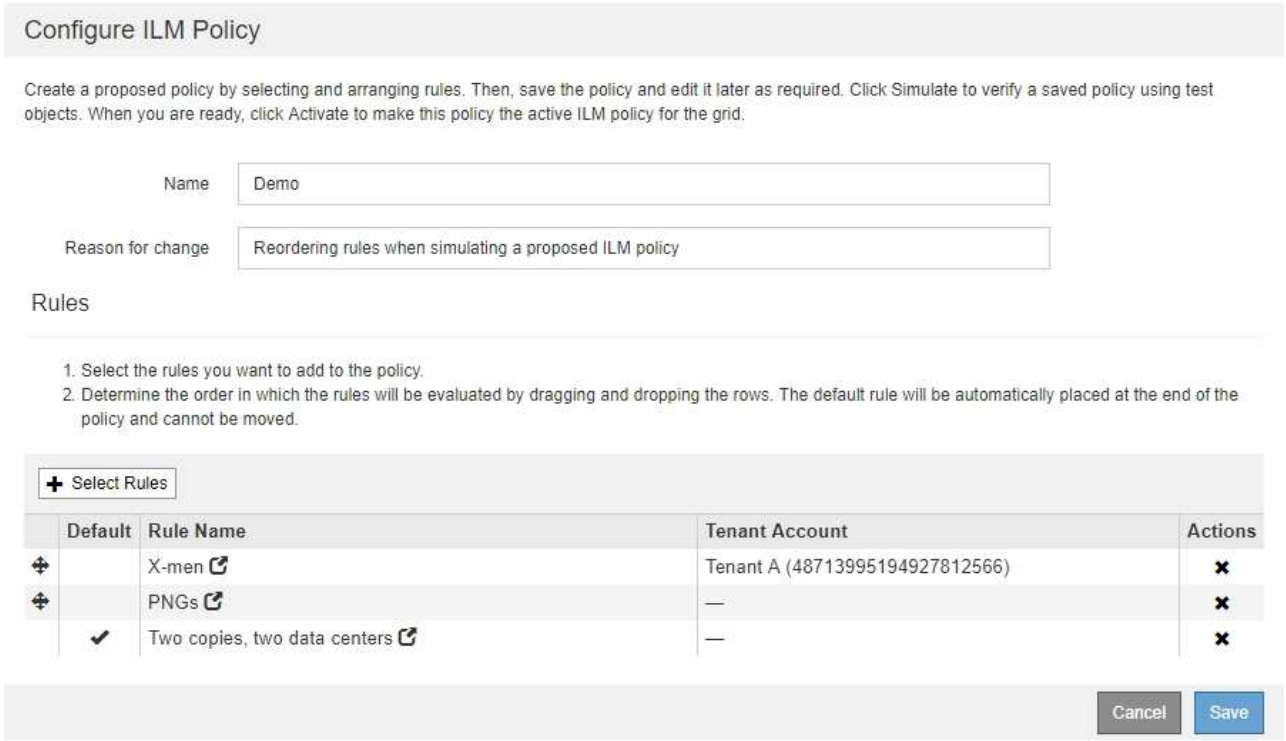
1. Dopo aver aggiunto le regole e salvato il criterio, fare clic su **simulate**.
2. Nel campo **oggetto**, immettere il bucket S3/object-key o il container Swift/object-name per un oggetto di test e fare clic su **simulate**.

   Vengono visualizzati i risultati di Simulation, che indicano che il `Havok.png` L'oggetto è stato associato dalla regola **PNG**.



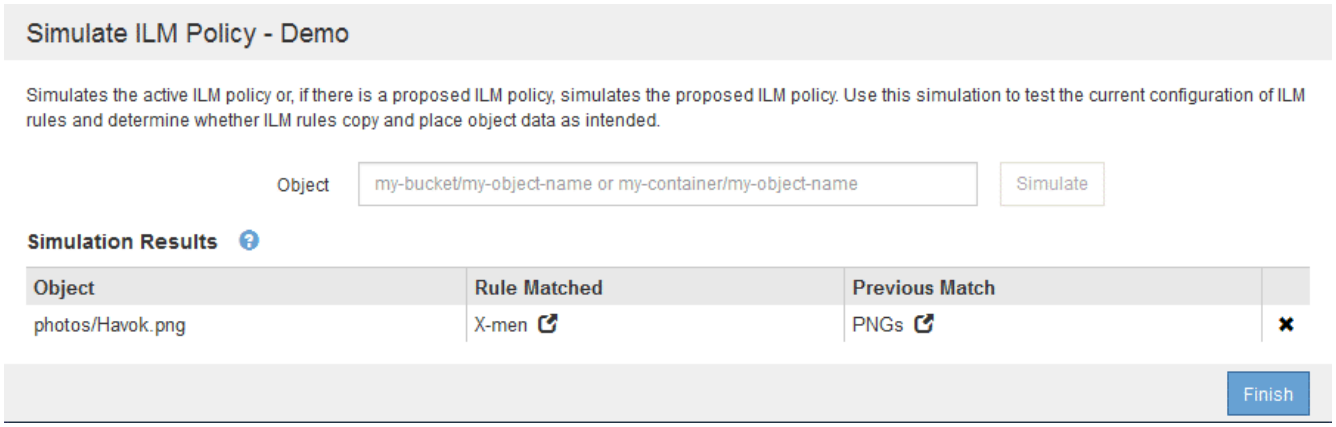
Tuttavia, la regola che il `Havok.png` L'oggetto doveva essere testato come la regola **X-MEN**.

3. Per risolvere il problema, riordinare le regole.
   a. Fare clic su **fine** per chiudere la pagina Simula policy ILM.
   b. Fare clic su **Edit** (Modifica) per modificare il criterio.
   c. Trascinare la regola **X-MEN** all'inizio dell'elenco.



   d. Fare clic su **Save** (Salva).
4. Fare clic su **simulate**.

   Gli oggetti precedentemente testati vengono rivalutati in base alla policy aggiornata e vengono visualizzati i risultati della nuova simulazione. Nell'esempio, la colonna Rule Matched mostra che il `Havok.png` L'oggetto ora corrisponde alla regola dei metadati X-MEN, come previsto. La colonna Previous Match (confronto precedente) mostra che la regola PNG ha trovato corrispondenza con l'oggetto nella simulazione precedente.

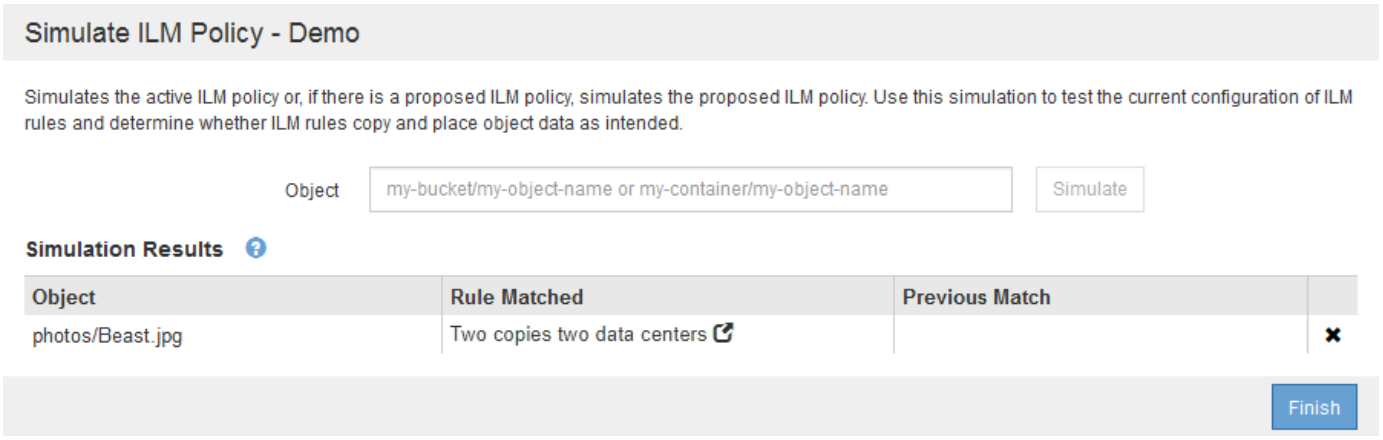


Se si rimane nella pagina Configura criteri, è possibile simulare nuovamente un criterio dopo aver apportato modifiche senza dover immettere nuovamente i nomi degli oggetti di test.

Esempio 3: Correzione di una regola durante la simulazione di una policy ILM proposta

Questo esempio mostra come simulare una policy, correggere una regola nella policy e continuare la simulazione.

In questo esempio, viene simulata la policy **Demo**. Questo criterio è destinato a trovare gli oggetti che hanno `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati imprevisti durante la simulazione di questa policy rispetto a. `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati X-MEN, l'oggetto corrisponde alla regola predefinita, due copie di due data center.

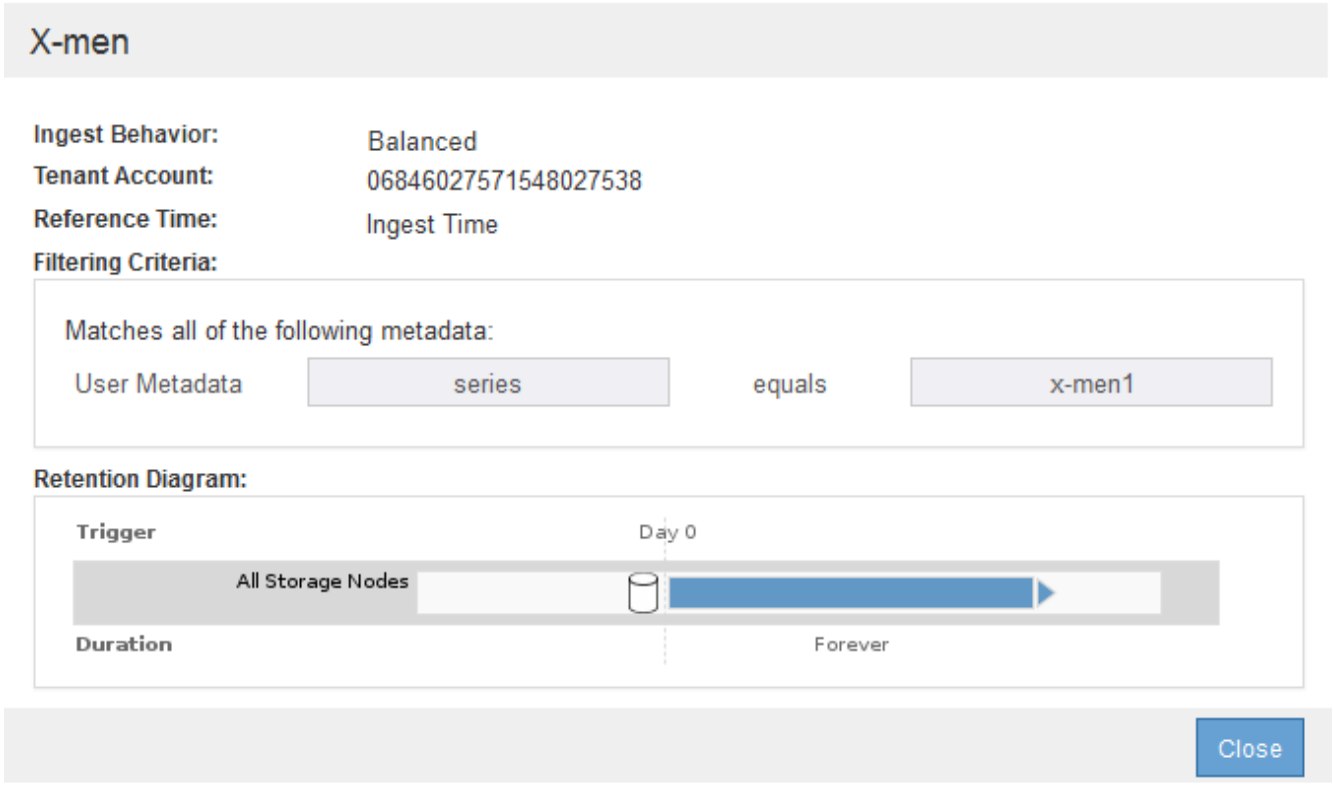


Quando un oggetto di test non corrisponde alla regola prevista nel criterio, è necessario esaminare ciascuna regola del criterio e correggere eventuali errori.

Fasi

1. Per ogni regola del criterio, visualizzare le impostazioni facendo clic sul nome della regola o sull'icona ulteriori dettagli in qualsiasi finestra di dialogo in cui viene visualizzata la regola.
2. Esaminare l'account tenant della regola, il tempo di riferimento e i criteri di filtraggio.

   In questo esempio, i metadati per la regola X-MEN includono un errore. Il valore dei metadati è stato immesso come "x-men1" invece di "x-men".



3. Per risolvere l'errore, correggere la regola come segue:
   - Se la regola fa parte del criterio proposto, è possibile clonarla o rimuoverla dal criterio e modificarla.
   - Se la regola fa parte del criterio attivo, è necessario clonarla. Non è possibile modificare o rimuovere una regola dal criterio attivo.

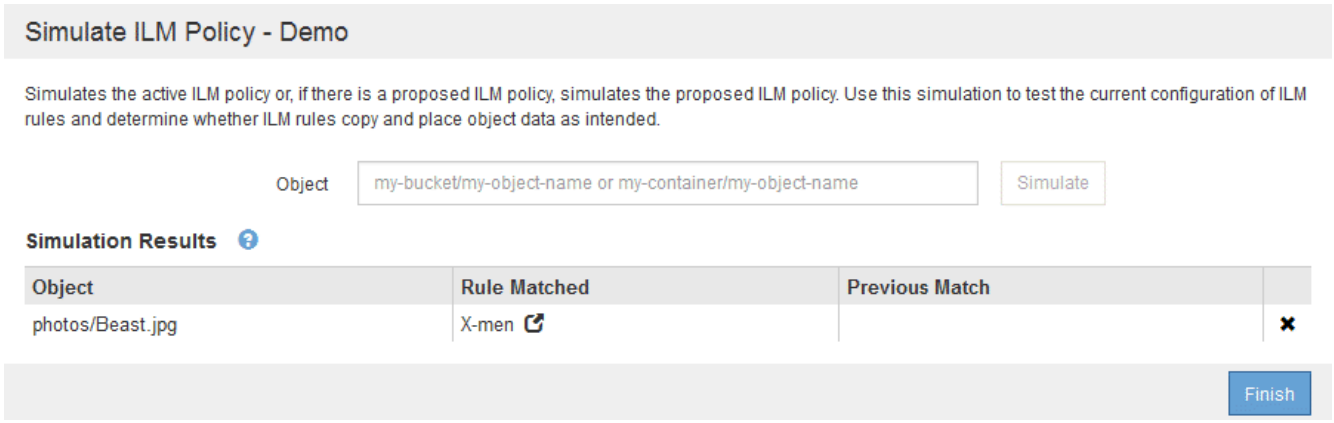
Opzione	Descrizione
Clonare la regola	i. Selezionare **ILM** > **regole**. ii. Selezionare la regola errata e fare clic su **Clone**. iii. Modificare le informazioni non corrette e fare clic su **Salva**. iv. Selezionare **ILM** > **Policy**. v. Selezionare la policy proposta e fare clic su **Modifica**. vi. Fare clic su **Seleziona regole**. vii. Selezionare la casella di controllo per la nuova regola, deselezionare la casella di controllo per la regola originale e fare clic su **Applica**. viii. Fare clic su **Save** (Salva).

Opzione	Descrizione
Modifica della regola	i. Selezionare la policy proposta e fare clic su **Modifica**. ii. Fare clic sull'icona di eliminazione ✖ Per rimuovere la regola errata, quindi fare clic su **Salva**. iii. Selezionare **ILM** > **regole**. iv. Selezionare la regola errata e fare clic su **Modifica**. v. Modificare le informazioni non corrette e fare clic su **Salva**. vi. Selezionare **ILM** > **Policy**. vii. Selezionare la policy proposta e fare clic su **Modifica**. viii. Selezionare la regola corretta, fare clic su **Applica** e fare clic su **Salva**.

4. Eseguire nuovamente la simulazione.

> Poiché si è allontanati dalla pagina ILM Policies per modificare la regola, gli oggetti precedentemente immessi per la simulazione non vengono più visualizzati. È necessario immettere nuovamente i nomi degli oggetti.

In questo esempio, la regola corretta X-men corrisponde ora a. `Beast.jpg` oggetto basato su `series=x-men` metadati dell'utente, come previsto.



Attivazione del criterio ILM

Dopo aver aggiunto le regole ILM a un criterio ILM proposto, aver simulato il criterio e aver confermato che si comporta come previsto, è possibile attivare il criterio proposto.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver salvato e simulato la policy ILM proposta.

> Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.

Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

A proposito di questa attività

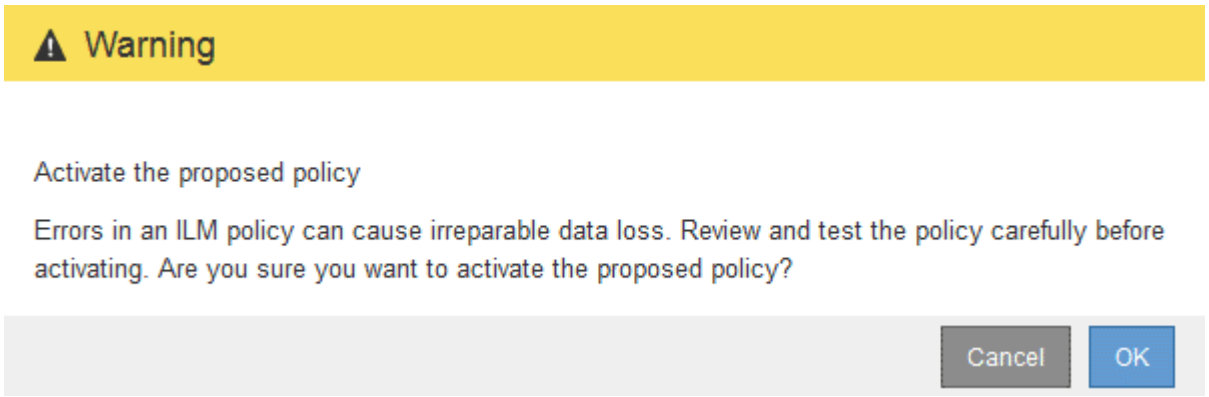
Quando si attiva un criterio ILM, il sistema distribuisce il nuovo criterio a tutti i nodi. Tuttavia, il nuovo criterio attivo potrebbe non essere effettivo fino a quando tutti i nodi della griglia non saranno disponibili per ricevere il nuovo criterio. In alcuni casi, il sistema attende l'implementazione di una nuova policy attiva per garantire che gli oggetti Grid non vengano rimossi accidentalmente.

- Se si apportano modifiche alle policy che aumentano la ridondanza o la durata dei dati, tali modifiche vengono implementate immediatamente. Ad esempio, se si attiva un nuovo criterio che include una regola di tre copie invece di una regola di due copie, tale criterio verrà implementato immediatamente perché aumenta la ridondanza dei dati.
- Se si apportano modifiche alle policy che potrebbero ridurre la ridondanza o la durata dei dati, tali modifiche non verranno implementate fino a quando non saranno disponibili tutti i nodi della griglia. Ad esempio, se si attiva una nuova policy che utilizza una regola di due copie invece di una regola di tre copie, la nuova policy verrà contrassegnata come "Active", ma non avrà effetto fino a quando tutti i nodi non saranno online e disponibili.

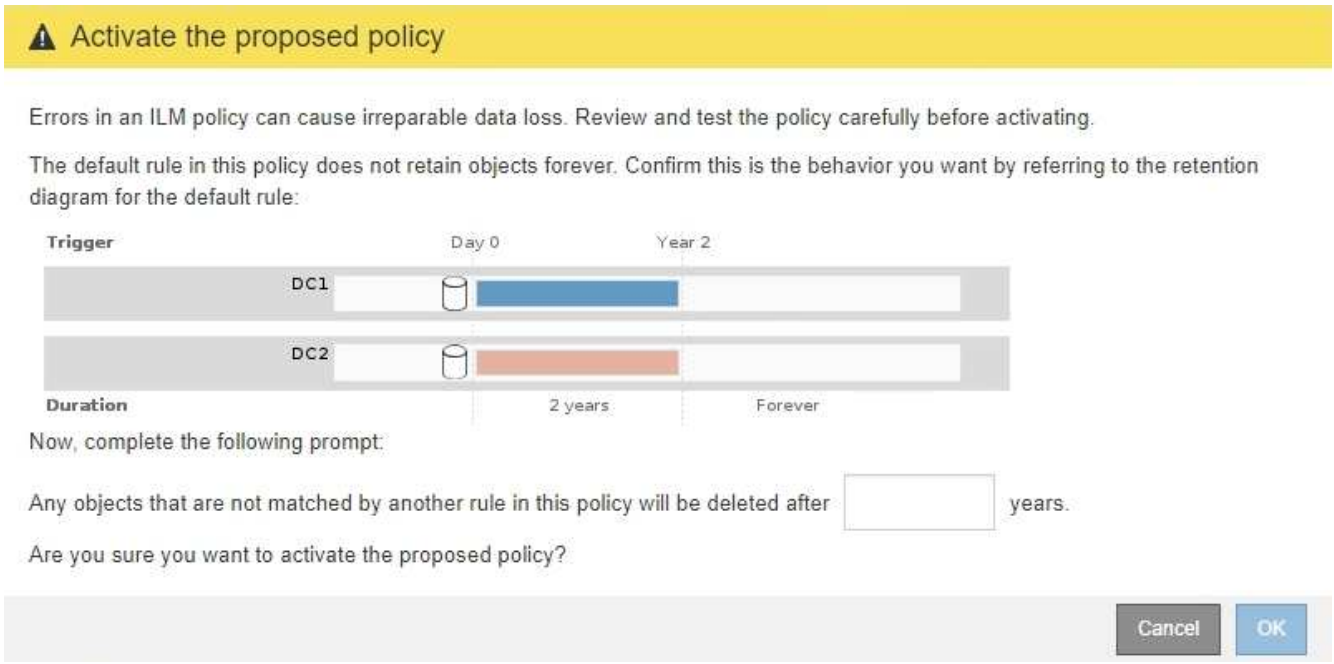
Fasi

1. Quando si è pronti ad attivare una policy proposta, selezionarla nella pagina ILM Policies (Criteri ILM) e fare clic su **Activate** (attiva).

   Viene visualizzato un messaggio di avviso che richiede di confermare l'attivazione della policy proposta.



   Se la regola predefinita per il criterio non mantiene gli oggetti per sempre, nel messaggio di avviso viene visualizzato un messaggio. In questo esempio, il diagramma di conservazione mostra che la regola predefinita elimina gli oggetti dopo 2 anni. È necessario digitare **2** nella casella di testo per riconoscere che gli oggetti non corrispondenti a un'altra regola del criterio verranno rimossi da StorageGRID dopo 2 anni.

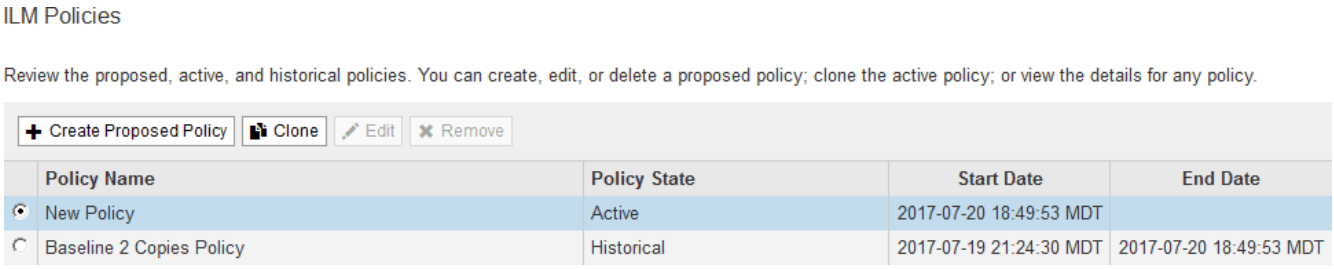


2. Fare clic su **OK**.

Risultato

Quando viene attivata una nuova policy ILM:

- Il criterio viene visualizzato con lo stato policy attivo nella tabella della pagina Criteri ILM. La voce Data di inizio indica la data e l'ora di attivazione della policy.



- Il criterio precedentemente attivo viene visualizzato con lo stato del criterio storico. Le voci Data di inizio e Data di fine indicano quando il criterio è diventato attivo e quando non è più in vigore.

Informazioni correlate

"Esempio 6: Modifica di un criterio ILM"

Verifica di un criterio ILM con la ricerca dei metadati degli oggetti

Dopo aver attivato un criterio ILM, è necessario acquisire oggetti di test rappresentativi nel sistema StorageGRID. Quindi, eseguire una ricerca dei metadati degli oggetti per confermare che le copie vengono eseguite come previsto e collocate nelle posizioni corrette.

Di cosa hai bisogno

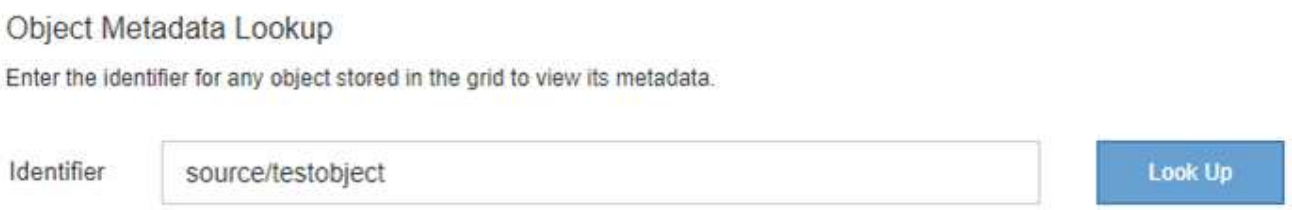
- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
  - **UUID**: Identificativo universalamente univoco dell'oggetto. Inserire l'UUID in tutte le lettere maiuscole.

- **CBID**: Identificatore univoco dell'oggetto all'interno di StorageGRID. È possibile ottenere il CBID di un oggetto dal log di audit. Inserire il CBID in tutte le lettere maiuscole.
- **S3 bucket e chiave oggetto**: Quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto.
- **Swift container and object name**: Quando un oggetto viene acquisito tramite l'interfaccia Swift, l'applicazione client utilizza una combinazione di container e object name per memorizzare e identificare l'oggetto.

Fasi

1. Acquisire l'oggetto.
2. Selezionare **ILM** > **Object Metadata Lookup**.
3. Digitare l'identificativo dell'oggetto nel campo **Identifier**.

   È possibile immettere UUID, CBID, S3 bucket/object-key o Swift container/object-name.



4. Fare clic su **Cerca**.

   Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

   - Metadati di sistema, tra cui l'ID oggetto (UUID), il nome dell'oggetto, il nome del contenitore, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta e la data e l'ora dell'ultima modifica dell'oggetto.
   - Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
   - Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
   - Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
   - Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
   - Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
   - Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
   - Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

     Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


5. Verificare che l'oggetto sia memorizzato nella posizione o nelle posizioni corrette e che si tratti del tipo di copia corretto.

> Se l'opzione Audit è attivata, è anche possibile monitorare il registro di audit per il messaggio ORLM Object Rules Met. Il messaggio di audit ORLM può fornire ulteriori informazioni sullo stato del processo di valutazione ILM, ma non può fornire informazioni sulla correttezza del posizionamento dei dati dell'oggetto o sulla completezza della policy ILM. È necessario valutarlo da soli. Per ulteriori informazioni, vedere le informazioni relative ai messaggi di audit.

Informazioni correlate

"Esaminare i registri di audit"

"Utilizzare S3"

"USA Swift"

Utilizzo delle regole ILM e delle policy ILM

Una volta create le regole ILM e un criterio ILM, è possibile continuare a utilizzarli, modificandone la configurazione man mano che cambiano i requisiti di storage.

Eliminazione di una regola ILM

Per mantenere gestibile l'elenco delle regole ILM correnti, eliminare eventuali regole ILM che non si intende utilizzare.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

> Non è possibile eliminare una regola ILM se è attualmente utilizzata nel criterio attivo o nel criterio proposto. Se è necessario eliminare una regola ILM che utilizza un criterio, è necessario eseguire prima questa procedura:
>
> 1. Clonare il criterio attivo o modificare il criterio proposto.
> 2. Rimuovere la regola ILM dal criterio.
> 3. Salvare, simulare e attivare il nuovo criterio per assicurarsi che gli oggetti siano protetti come previsto.

Fasi

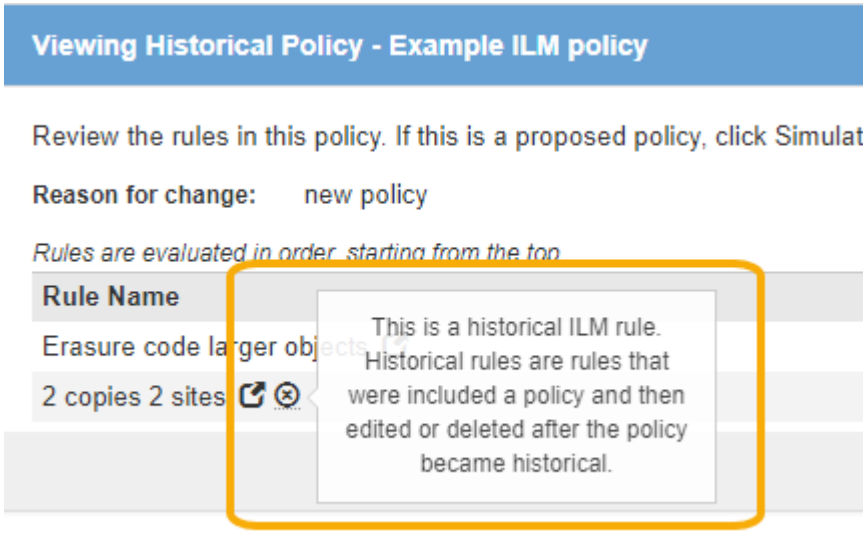
1. Selezionare **ILM** > **regole**.
2. Esaminare la voce della tabella relativa alla regola che si desidera rimuovere.

   Verificare che la regola non sia utilizzata nel criterio ILM attivo o nel criterio ILM proposto.

3. Se la regola che si desidera rimuovere non è in uso, selezionare il pulsante di opzione e selezionare **Rimuovi**.
4. Selezionare **OK** per confermare che si desidera eliminare la regola ILM.

   La regola ILM viene eliminata.

Se si elimina una regola utilizzata in un criterio storico, viene visualizzato ⊗ quando si visualizza il criterio, viene visualizzata un'icona che indica che la regola è diventata una regola storica.



Informazioni correlate

"Creazione di un criterio ILM"

Modifica di una regola ILM

Potrebbe essere necessario modificare una regola ILM per modificare un filtro o un'istruzione di posizionamento.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

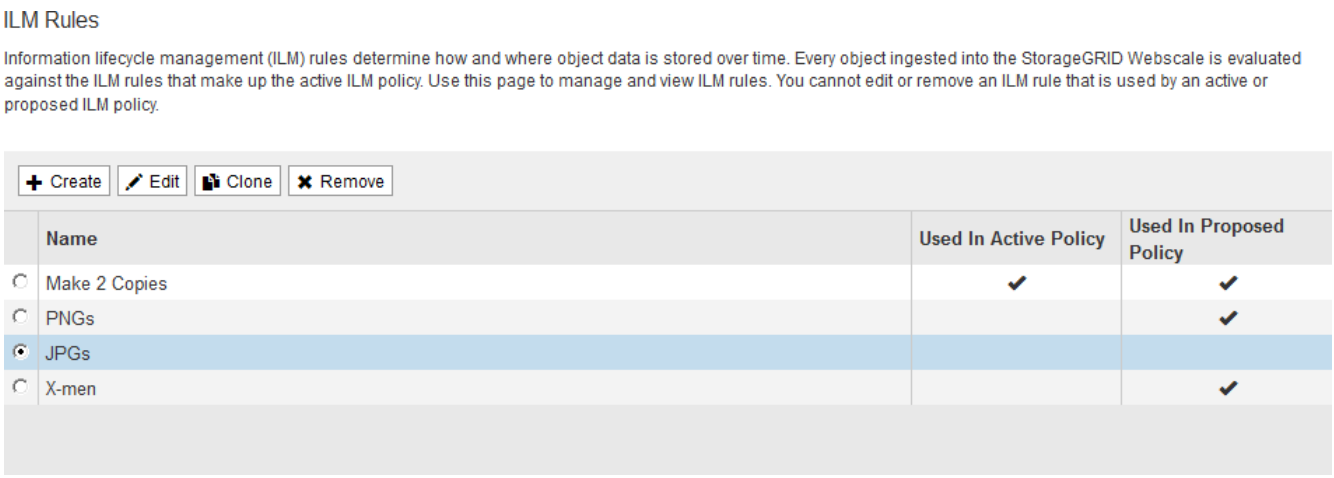
Non è possibile modificare una regola se utilizzata nel criterio ILM proposto o nel criterio ILM attivo. È invece possibile clonare queste regole e apportare le modifiche necessarie alla copia clonata. Inoltre, non è possibile modificare la regola ILM (creare 2 copie) o le regole ILM create prima della versione 10.3 di StorageGRID.

Prima di aggiungere una regola modificata al criterio ILM attivo, tenere presente che una modifica alle istruzioni di posizionamento di un oggetto potrebbe causare un aumento del carico sul sistema.

Fasi

1. Selezionare **ILM** > **regole**.

   Viene visualizzata la pagina ILM Rules (regole ILM). Questa pagina mostra tutte le regole disponibili e indica le regole utilizzate nel criterio attivo o nel criterio proposto.



2. Selezionare una regola non utilizzata e fare clic su **Modifica**.

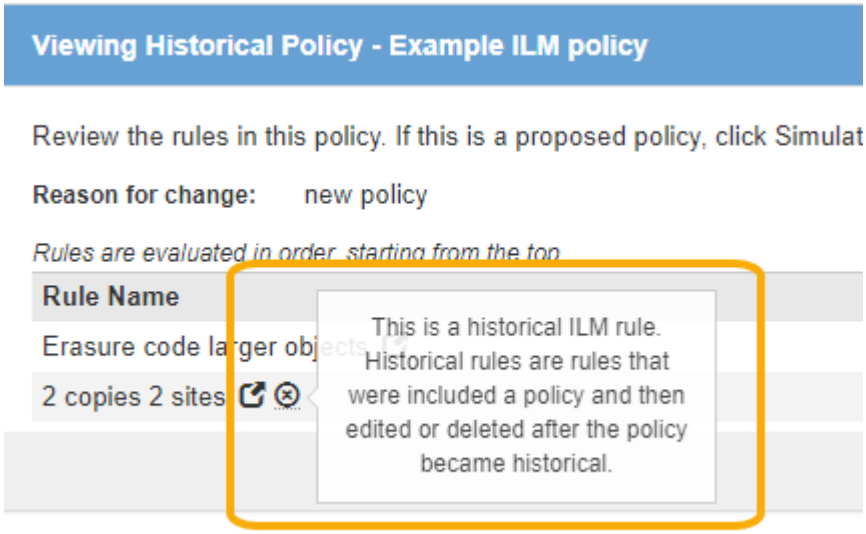
   Viene visualizzata la procedura guidata Edit ILM Rule (Modifica regola ILM).

3. Completare le pagine della procedura guidata Modifica regola ILM, seguendo la procedura per creare una regola ILM e utilizzare filtri avanzati, se necessario.

   Quando si modifica una regola ILM, non è possibile modificarne il nome.

4. Fare clic su **Save** (Salva).

Se si modifica una regola utilizzata in un criterio storico, viene visualizzato ⊗ quando si visualizza il criterio, viene visualizzata un'icona che indica che la regola è diventata una regola storica.



Informazioni correlate

"Creazione di una regola ILM"

"Utilizzo di filtri avanzati nelle regole ILM"

Clonazione di una regola ILM

Non è possibile modificare una regola se utilizzata nel criterio ILM proposto o nel criterio ILM attivo. È invece possibile clonare una regola e apportare le modifiche necessarie alla copia clonata. Quindi, se necessario, è possibile rimuovere la regola originale dal criterio proposto e sostituirla con la versione modificata. Non è possibile clonare una regola ILM se è stata creata utilizzando StorageGRID versione 10.2 o precedente.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

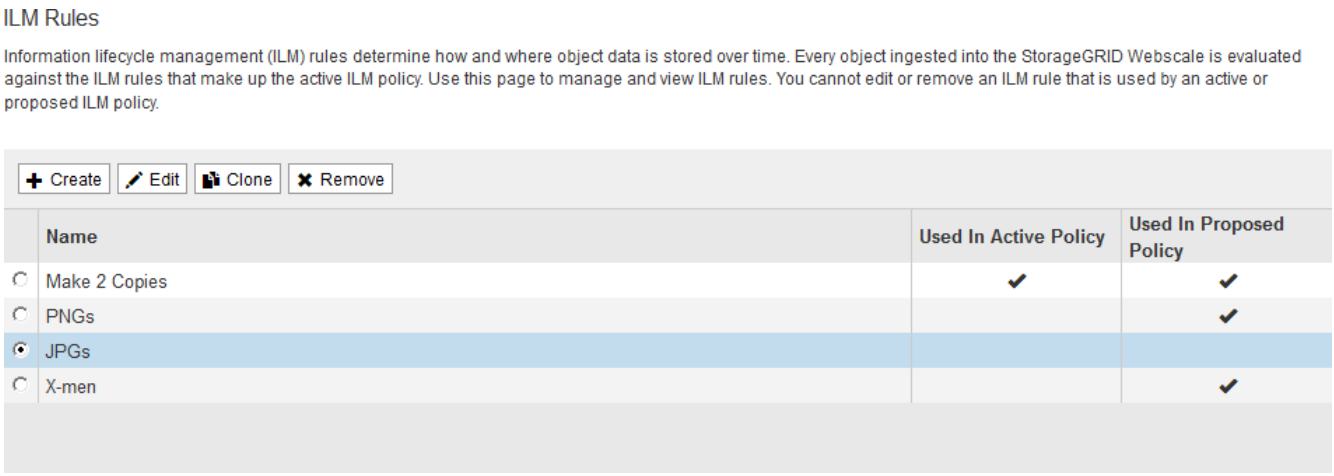
A proposito di questa attività

Prima di aggiungere una regola clonata al criterio ILM attivo, tenere presente che una modifica alle istruzioni di posizionamento di un oggetto potrebbe causare un aumento del carico sul sistema.

Fasi

1. Selezionare **ILM** > **regole**.

   Viene visualizzata la pagina ILM Rules (regole ILM).



2. Selezionare la regola ILM che si desidera clonare e fare clic su **Clone**.

   Viene visualizzata la procedura guidata Create ILM Rule (Crea regola ILM).

3. Aggiornare la regola clonata seguendo la procedura per modificare una regola ILM e utilizzando filtri avanzati.

   Quando si clonano una regola ILM, è necessario immettere un nuovo nome.

4. Fare clic su **Save** (Salva).

   Viene creata la nuova regola ILM.

Informazioni correlate

"Utilizzo delle regole ILM e delle policy ILM"

"Utilizzo di filtri avanzati nelle regole ILM"

Visualizzazione della coda di attività del criterio ILM

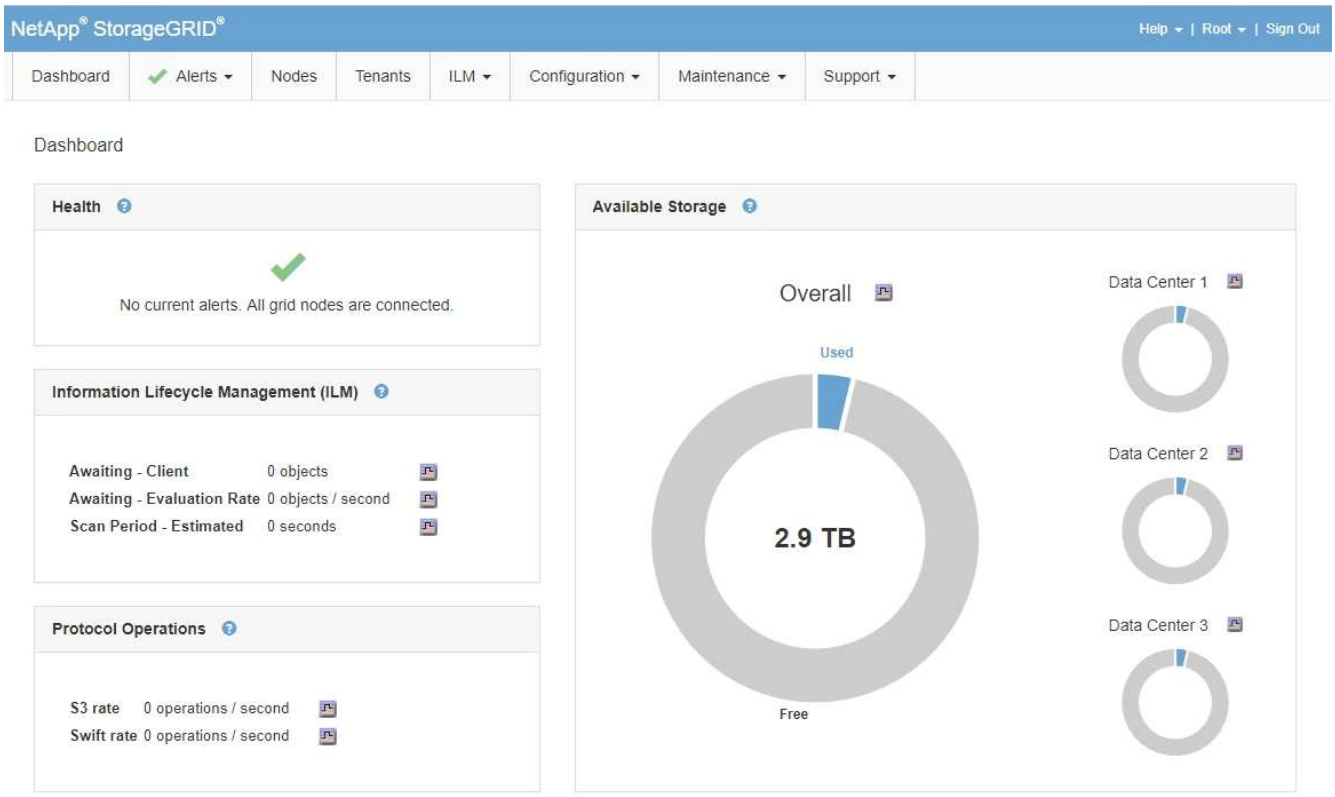
È possibile visualizzare il numero di oggetti presenti nella coda da valutare in base al criterio ILM in qualsiasi momento. È possibile monitorare la coda di elaborazione ILM per determinare le prestazioni del sistema. Una coda di grandi dimensioni potrebbe indicare che il sistema non è in grado di tenere il passo con la velocità di acquisizione, che il carico dalle applicazioni client è troppo elevato o che esiste una condizione anomala.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **Dashboard**.



2. Monitorare la sezione Information Lifecycle Management (ILM).

   È possibile fare clic sul punto interrogativo per visualizzare una descrizione degli elementi di questa sezione.

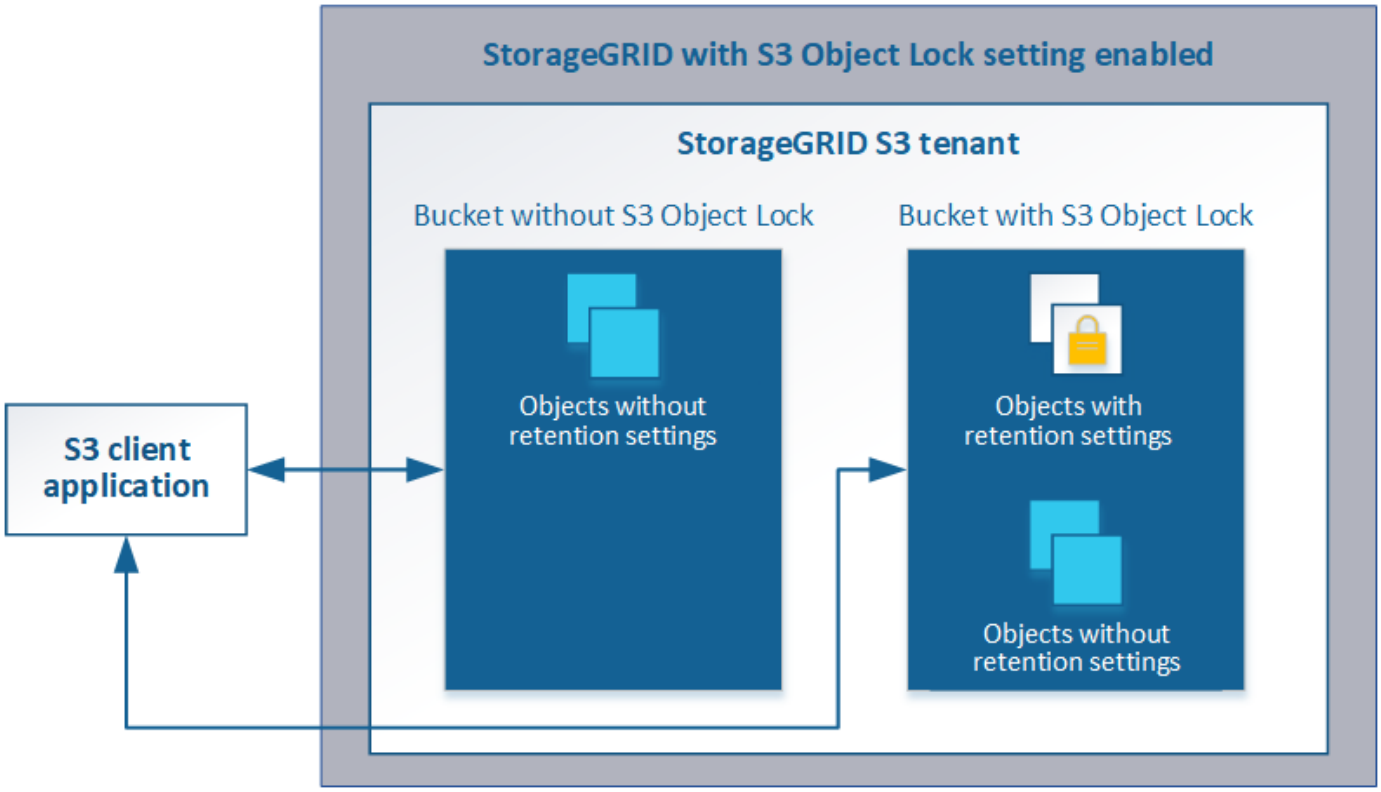
Gestione degli oggetti con S3 Object Lock

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.



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 su queste impostazioni, consultare "Using S3 Object lock" in "Operazioni e limitazioni supportate dall'API REST S3".

Confronto tra blocco oggetti S3 e conformità legacy

La funzionalità blocco oggetti S3 di StorageGRID 11.5 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Poiché la nuova funzione blocco oggetti S3 è conforme ai requisiti di Amazon S3, non è più compatibile con la funzionalità proprietaria di conformità StorageGRID, ora denominata "conformità legacy".

Se in precedenza è stata attivata l'impostazione di conformità globale, la nuova impostazione di blocco oggetti S3 globale viene attivata automaticamente quando si esegue l'aggiornamento a StorageGRID 11.5. Gli utenti del tenant non saranno più in grado di creare nuovi bucket con la conformità abilitata in StorageGRID 11.5; tuttavia, come richiesto, 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.

"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.

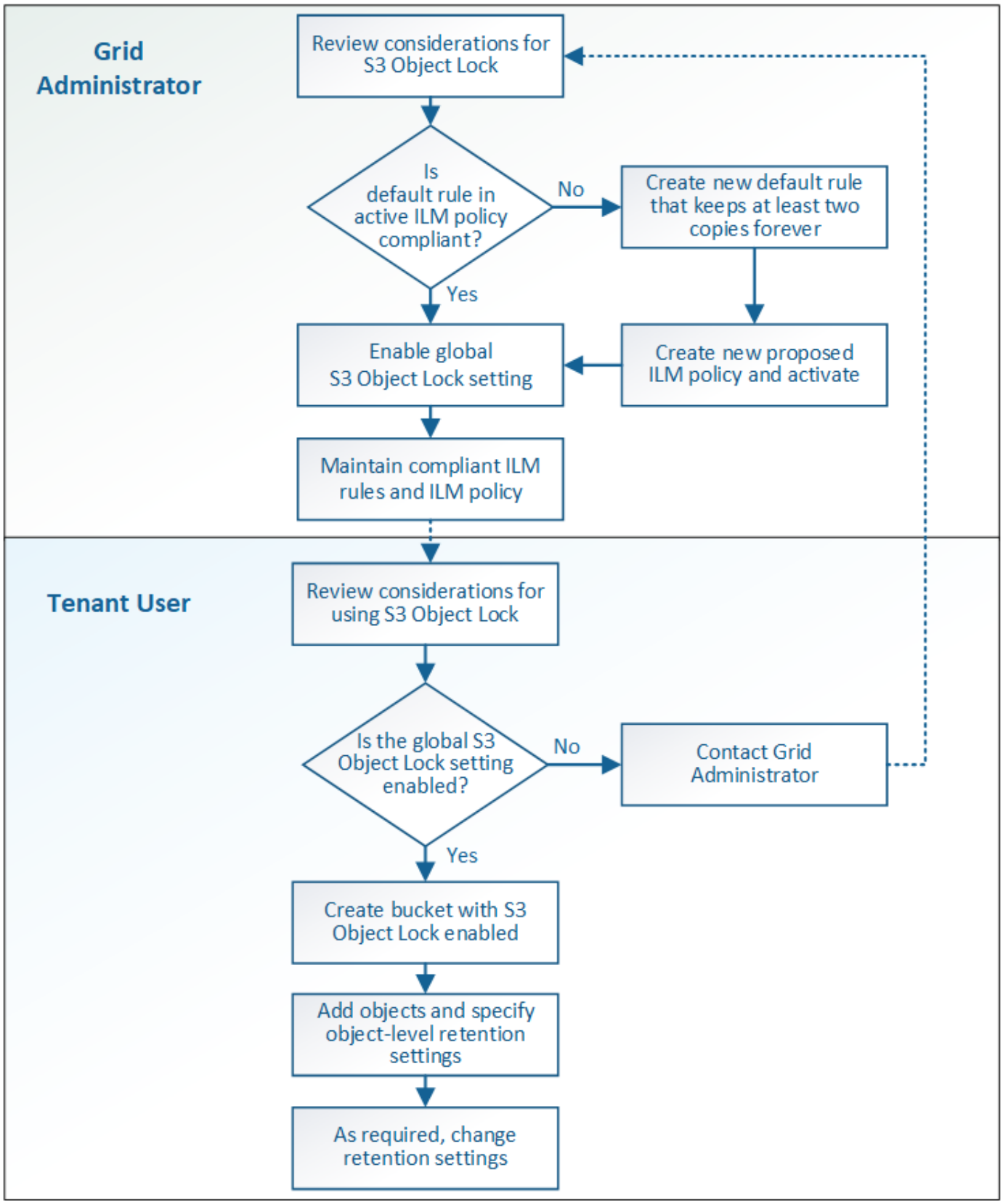
	Blocco oggetti S3 (nuovo)	**Compliance (legacy)**
In che modo la funzionalità è abilitata a livello globale?	Da Grid Manager, selezionare **Configuration** > **System Settings** > **S3 Object Lock**.	Non più supportato. **Nota:** se in precedenza è stata attivata l'impostazione di conformità globale, l'impostazione di blocco oggetti S3 globale viene attivata automaticamente quando si esegue l'aggiornamento a StorageGRID 11.5.
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.

	Blocco oggetti S3 (nuovo)	Compliance (legacy)
Un bucket può avere impostazioni predefinite per la conservazione e la conservazione legale?	No I bucket StorageGRID con blocco oggetti S3 attivato non hanno un periodo di conservazione predefinito. È invece possibile specificare una data di conservazione per ogni versione dell'oggetto.	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.
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. Aggiungere oggetti a tali bucket e specificare i periodi di conservazione a livello di oggetto e le impostazioni di conservazione a livello legale.
3. 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"

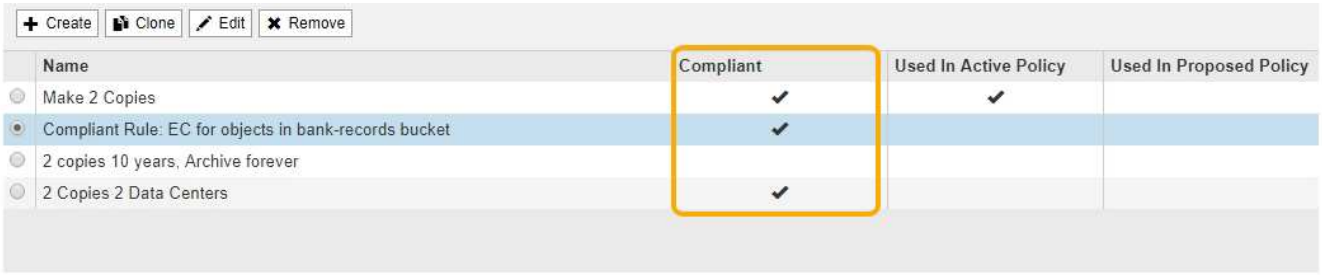
Requisiti per il blocco oggetti S3

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.

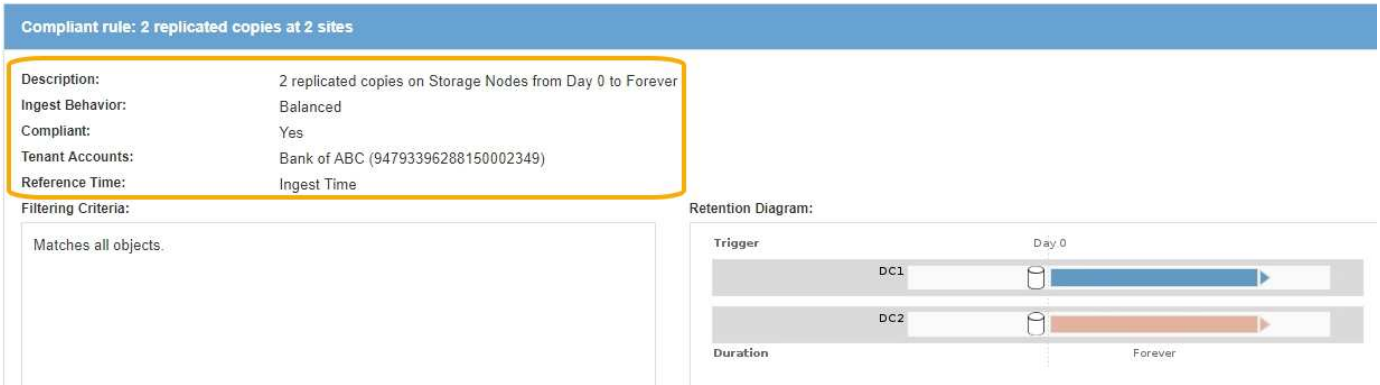


Requisiti per le regole ILM conformi

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.

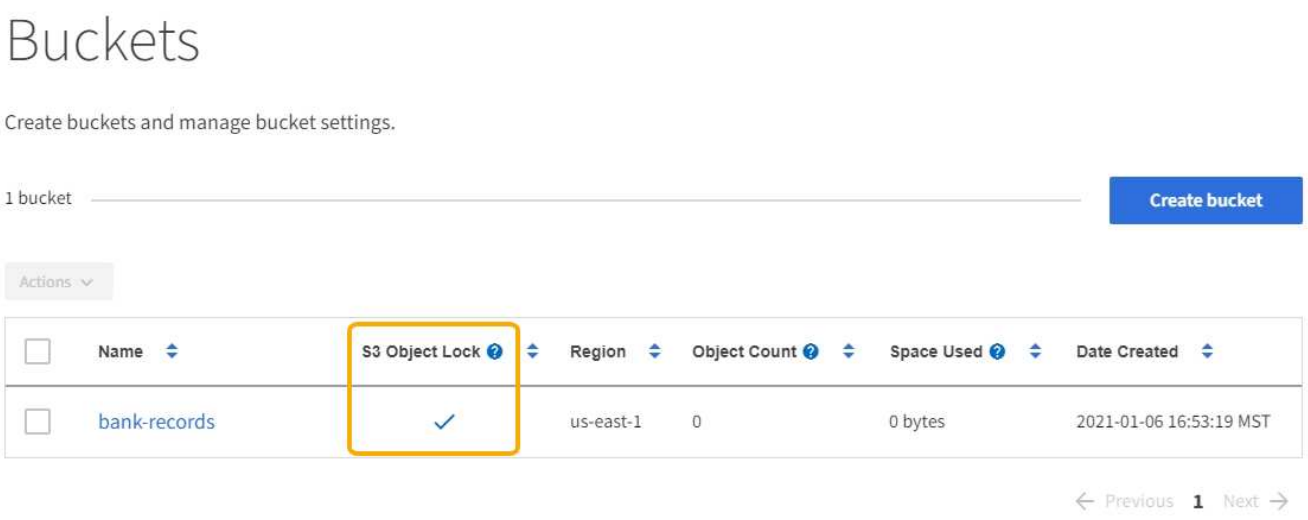
Un criterio ILM conforme potrebbe includere le seguenti tre regole:

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.
- Un bucket StorageGRID con blocco oggetti S3 attivato non ha un periodo di conservazione predefinito. L'applicazione client S3 può invece specificare una data di conservazione e un'impostazione di conservazione legale per ogni versione di oggetto aggiunta a quel bucket.
- 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

- L'applicazione client S3 deve specificare le impostazioni di conservazione per ciascun oggetto che deve essere protetto da S3 Object Lock.
- 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 specificare facoltativamente 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"

Abilitazione di S3 Object Lock 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

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario aver esaminato il flusso di lavoro S3 Object Lock e comprendere le considerazioni.
- La regola predefinita nel criterio ILM attivo deve essere conforme.

  "Creazione di una regola ILM predefinita"

  "Creazione di un criterio ILM"

A proposito di questa attività

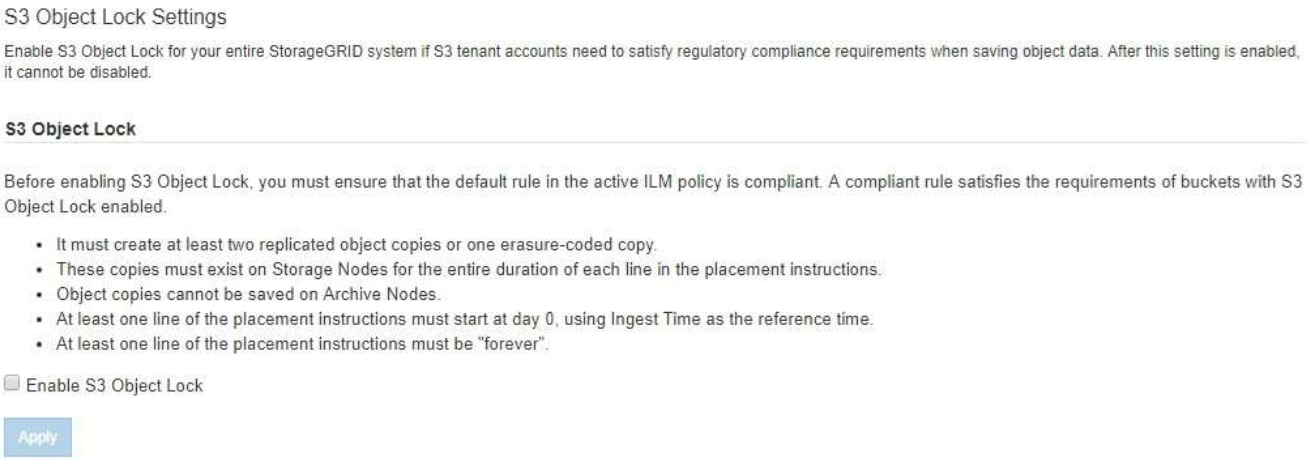
Un amministratore della griglia deve attivare l'impostazione globale S3 Object Lock per consentire agli utenti tenant di creare nuovi bucket con S3 Object Lock attivato. Una volta attivata, questa impostazione non può essere disattivata.

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

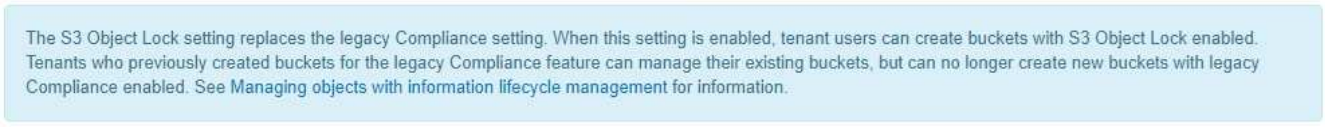
Fasi

1. Selezionare **Configuration** > **System Settings** > **S3 Object Lock**.

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

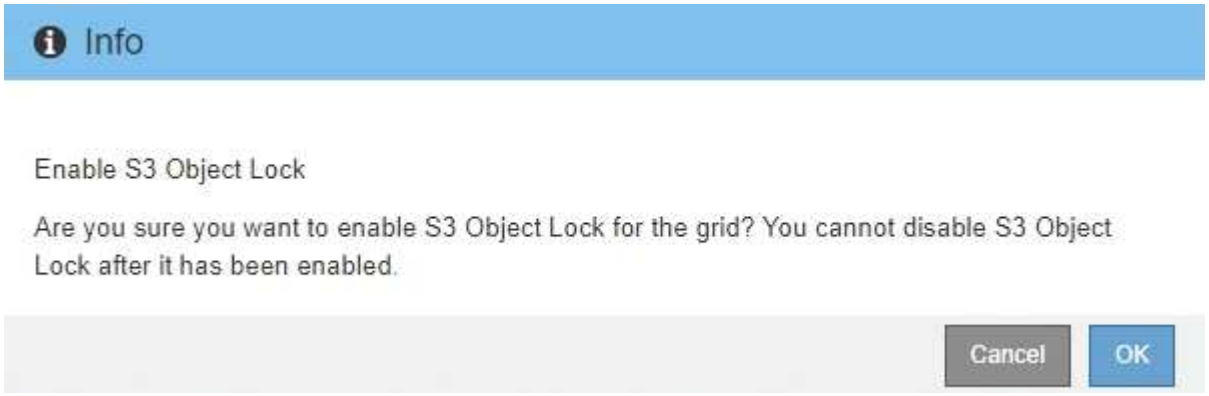


Se l'impostazione di conformità globale era stata attivata utilizzando una versione precedente di StorageGRID, la pagina contiene la seguente nota:



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

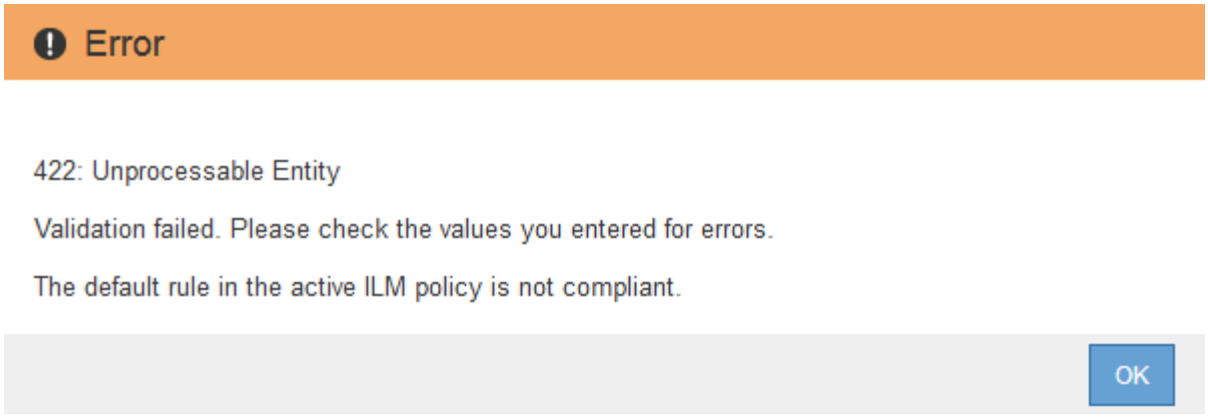
   Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare il blocco oggetti S3 dopo averlo attivato.



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 di blocco oggetti S3 globale, potrebbe essere necessario creare un nuovo criterio ILM. 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

"Creazione di un criterio ILM dopo l'attivazione del blocco oggetti S3"

"Creazione di una regola ILM"

"Creazione di un criterio ILM"

"Confronto tra blocco oggetti S3 e conformità legacy"

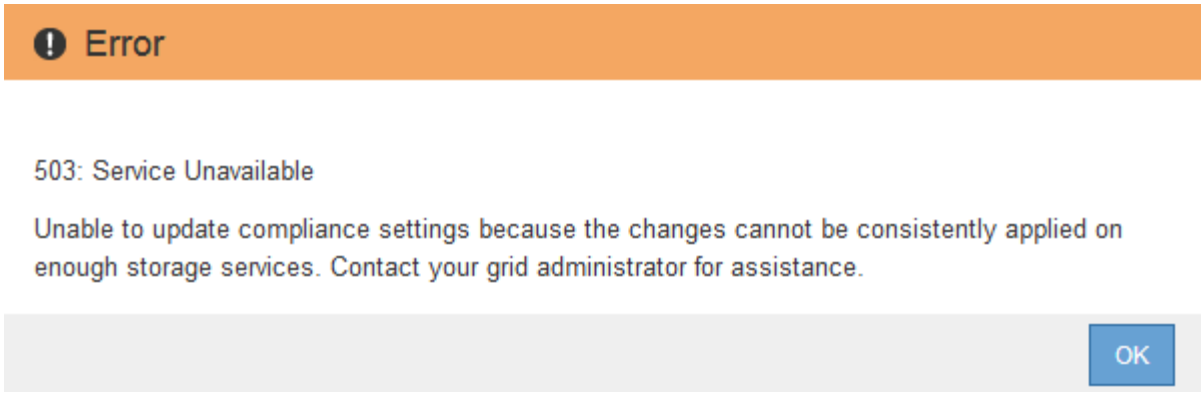
Risoluzione degli errori di coerenza durante l'aggiornamento della configurazione S3 Object Lock o Compliance legacy

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"

"Mantieni Ripristina"

Esempio di regole e policy ILM

Puoi utilizzare gli esempi di questa sezione come punto di partenza per le tue regole e policy ILM.

- "Esempio 1: Regole ILM e policy per lo storage a oggetti"
- "Esempio 2: Regole ILM e policy per il filtraggio delle dimensioni degli oggetti EC"
- "Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine"
- "Esempio 4: Regole ILM e policy per gli oggetti con versione S3"
- "Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"
- "Esempio 6: Modifica di un criterio ILM"
- "Esempio 7: Policy ILM conforme per il blocco oggetti S3"

Esempio 1: Regole ILM e policy per lo storage a oggetti

È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per la definizione di un criterio ILM in modo da soddisfare i requisiti di protezione e

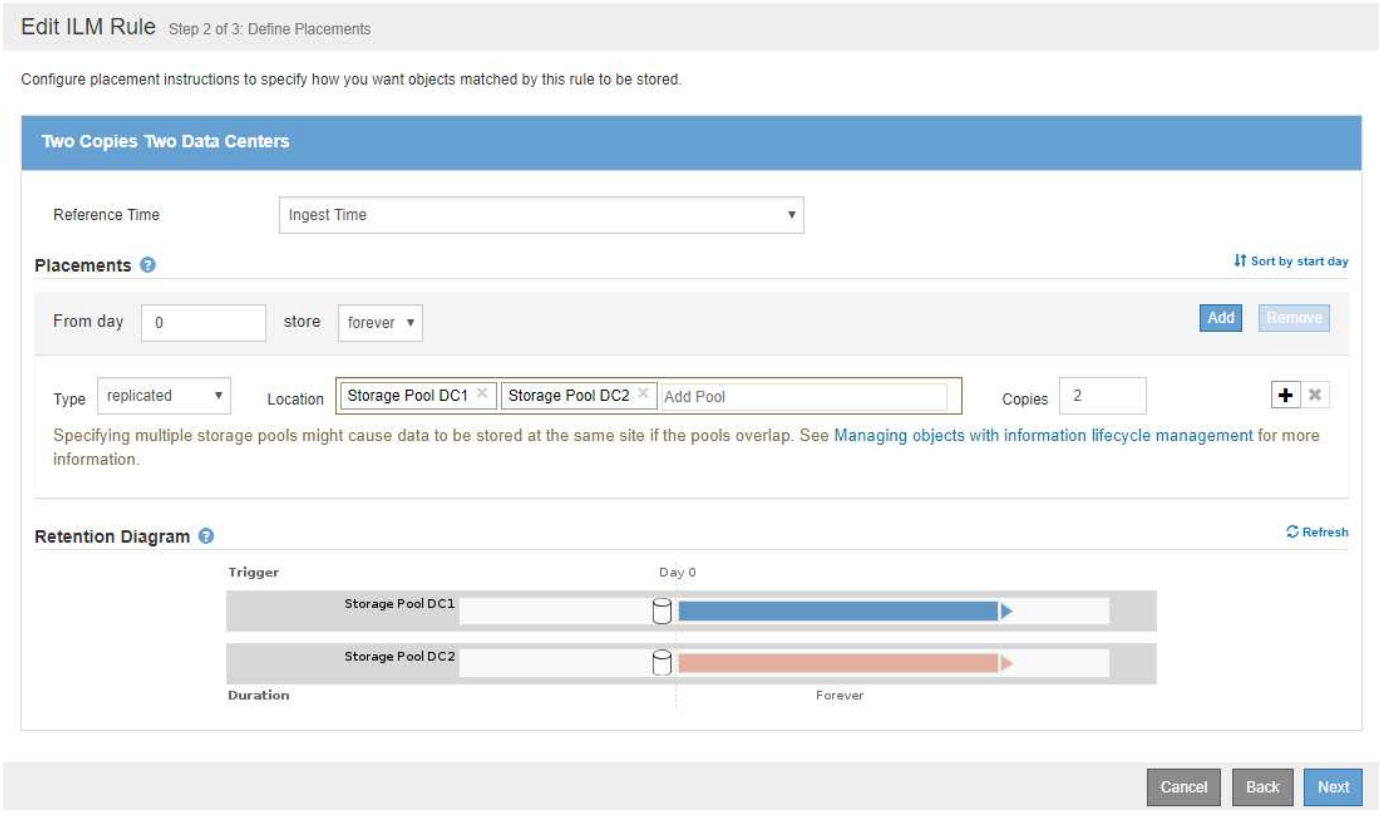
conservazione degli oggetti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 1: Copia dei dati degli oggetti in due data center

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due data center.

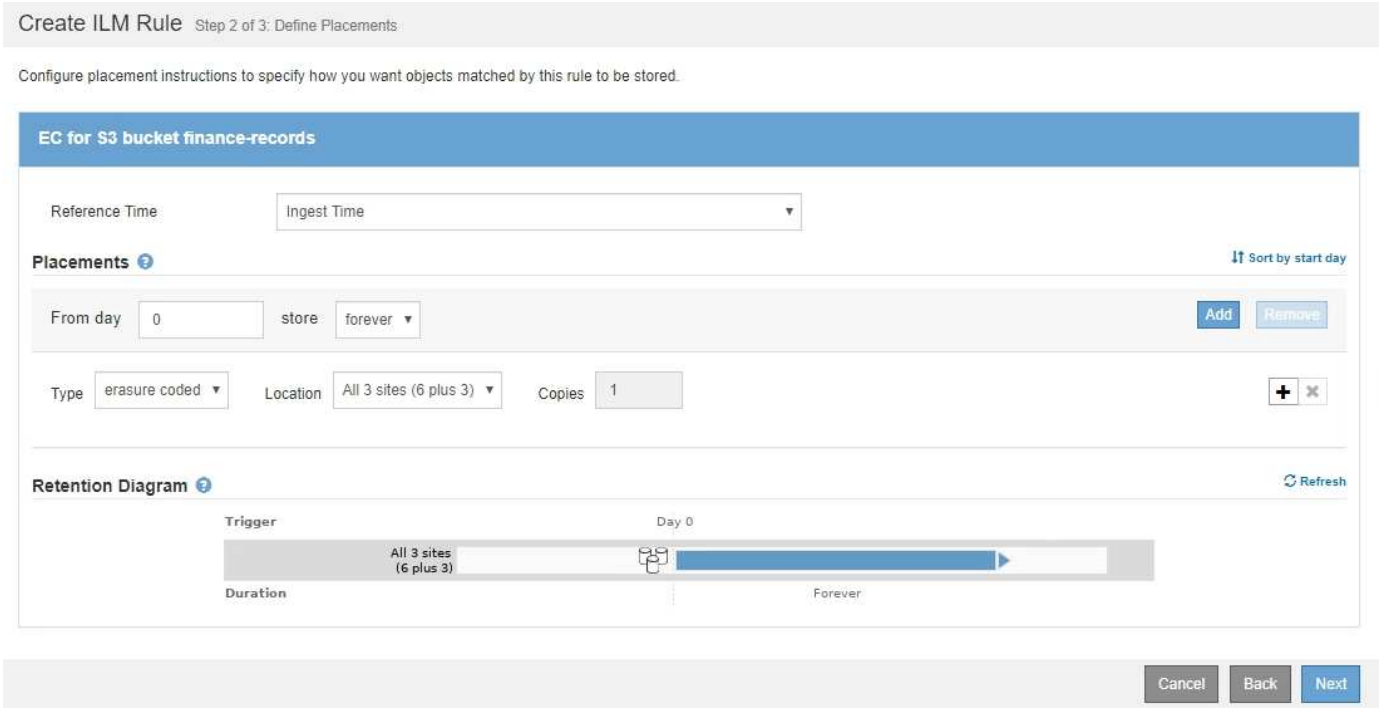
Definizione della regola	Valore di esempio
Pool di storage	Due pool di storage, ciascuno in diversi data center, denominati Storage Pool DC1 e Storage Pool DC2.
Nome regola	Due copie di due data center
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva due copie replicate per sempre, una nello Storage Pool DC1 e una nello Storage Pool DC2.



ILM regola 2 per esempio 1: Erasure coding profile with bucket matching

Questa regola ILM di esempio utilizza un profilo di codifica Erasure e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene memorizzato.

Definizione della regola	Valore di esempio
Erasure Coding Profile (erasure Coding Profile	• Un pool di storage in tre data center (tutti e 3 i siti) • Utilizzare uno schema di erasure coding 6+3
Nome regola	EC per i record finanziari del bucket S3
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Per gli oggetti nel bucket S3 denominati finance-records, creare una copia con codice di cancellazione nel pool specificato dal profilo di codifica Erasure. Conserva questa copia per sempre.

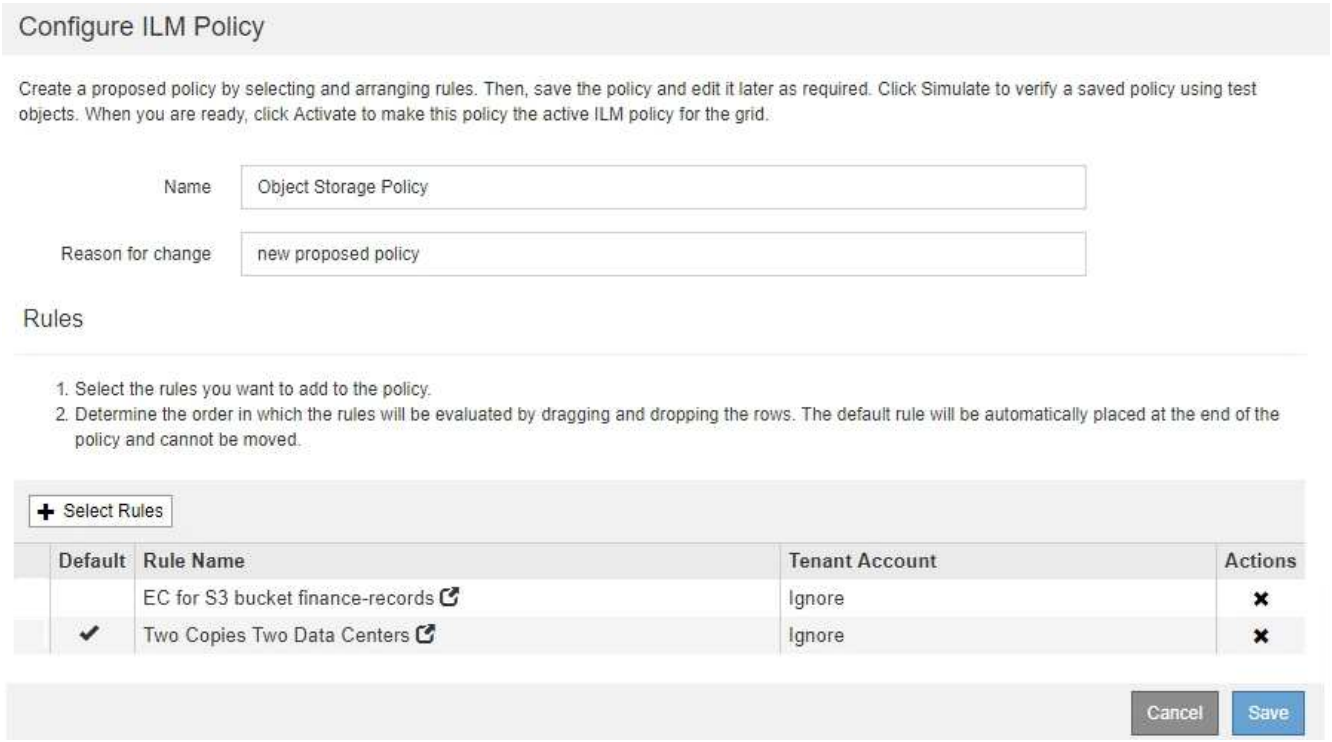


Policy ILM per esempio 1

Il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse; tuttavia, in pratica, la maggior parte delle policy ILM è semplice.

Un tipico criterio ILM per una topologia multi-sito potrebbe includere regole ILM come le seguenti:

- Al momento dell'acquisizione, utilizzare la codifica di cancellazione 6+3 per memorizzare tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in tre data center.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita del criterio, due copie due data center, per memorizzare una copia di tale oggetto in due data center, DC1 e DC2.



Esempio 2: Regole ILM e policy per il filtraggio delle dimensioni degli oggetti EC

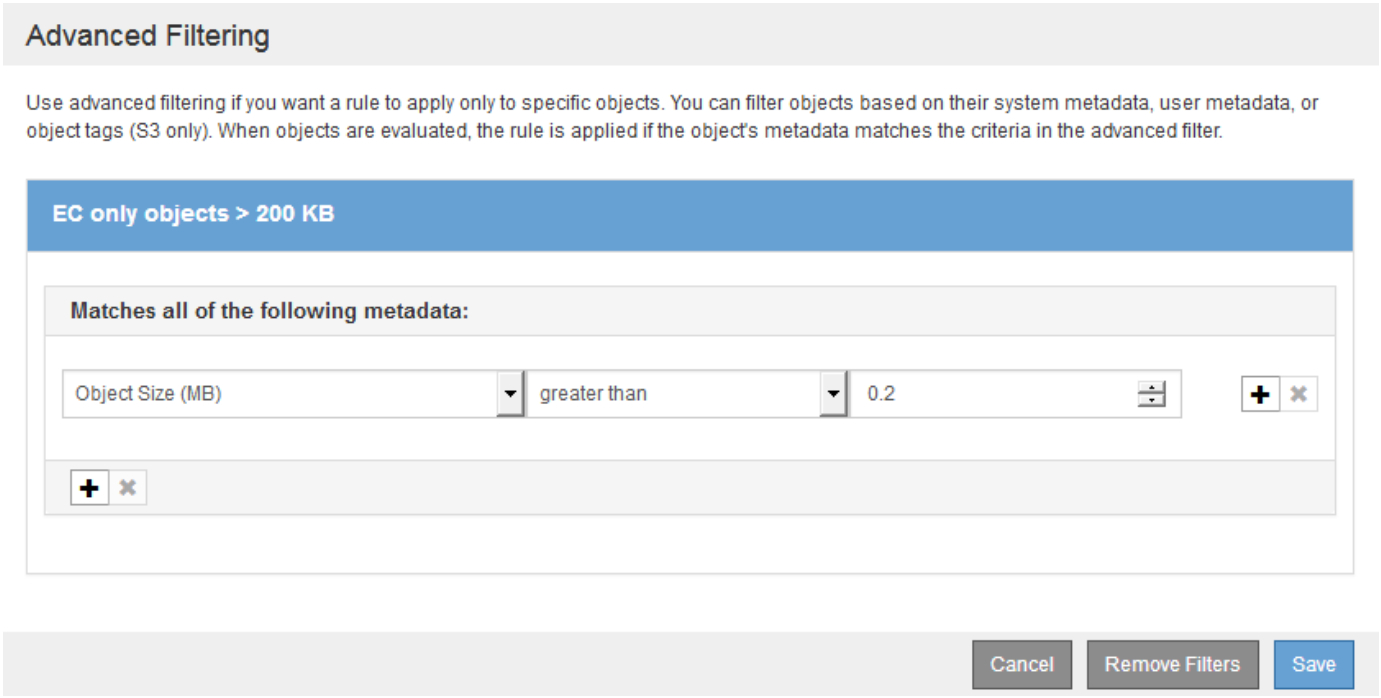
È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire un criterio ILM che filtra in base alle dimensioni dell'oggetto per soddisfare i requisiti EC consigliati.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

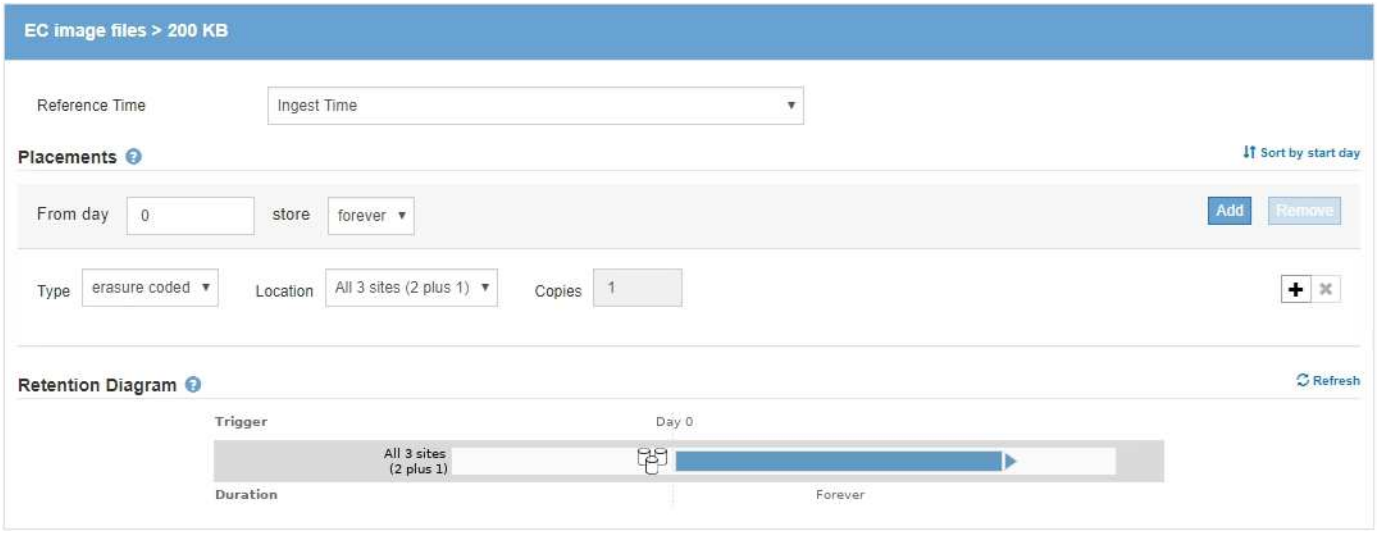
ILM regola 1 per esempio 2: Utilizzare EC per tutti gli oggetti di dimensioni superiori a 200 KB

Questo esempio di cancellazione della regola ILM codifica tutti gli oggetti di dimensioni superiori a 200 KB (0.20 MB).

Definizione della regola	Valore di esempio
Nome regola	Solo oggetti EC > 200 KB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per le dimensioni dell'oggetto	Dimensione oggetto (MB) maggiore di 0.20
Posizionamento dei contenuti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti



Le istruzioni di posizionamento specificano che una copia 2+1 con codice di cancellazione deve essere creata utilizzando tutti e tre i siti.

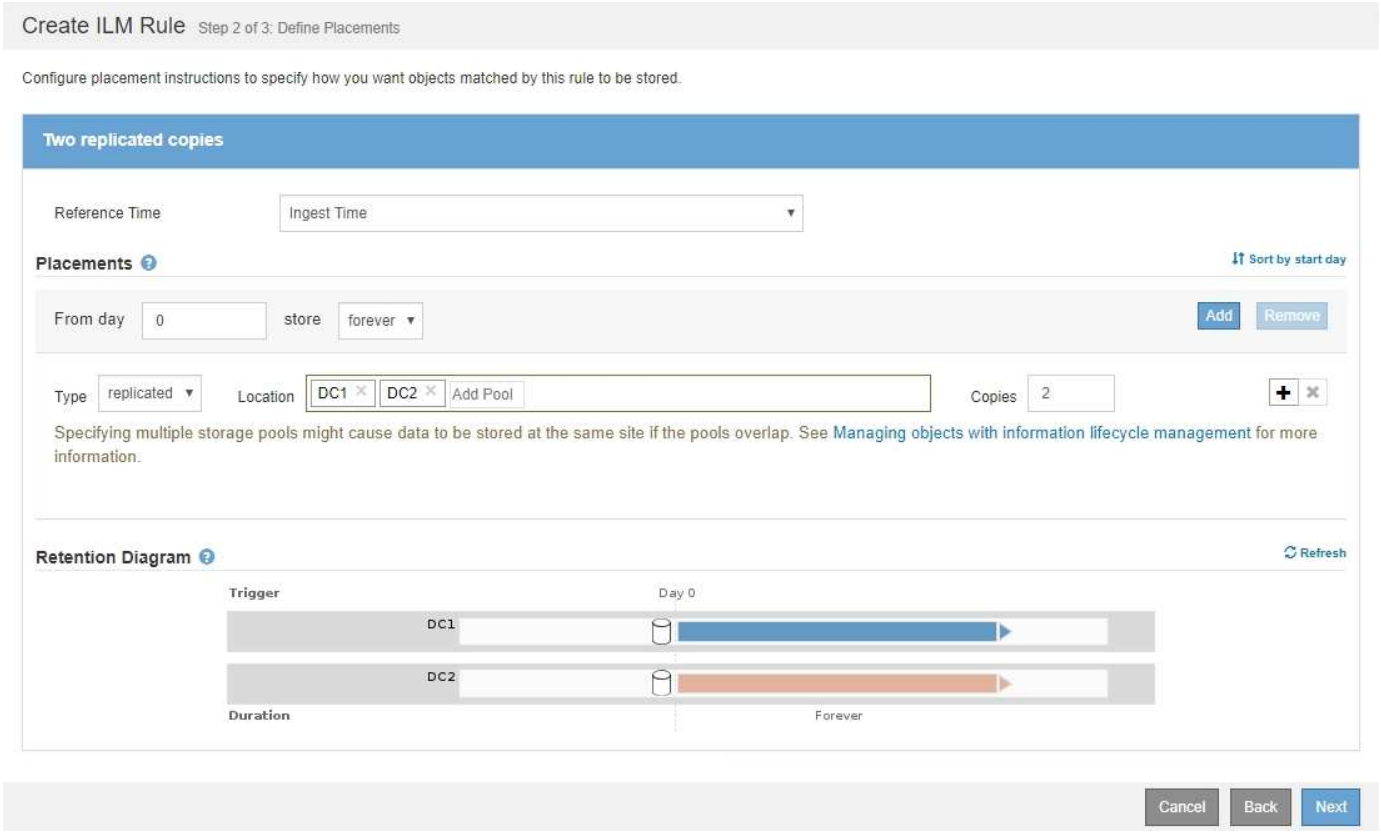


ILM regola 2 per esempio 2: Due copie replicate

Questa regola ILM di esempio crea due copie replicate e non filtra in base alle dimensioni dell'oggetto. Questa è la seconda regola del criterio. Poiché la regola ILM 1, ad esempio 2, filtra tutti gli oggetti di dimensioni superiori a 200 KB, la regola ILM 2, ad esempio 2, si applica solo agli oggetti di dimensioni inferiori o pari a 200 KB.

Definizione della regola	Valore di esempio
Nome regola	Due copie replicate
Tempo di riferimento	Tempo di acquisizione

Definizione della regola	Valore di esempio
Filtro avanzato per le dimensioni dell'oggetto	Nessuno
Posizionamento dei contenuti	Creare due copie replicate e salvarle in due data center, DC1 e DC2

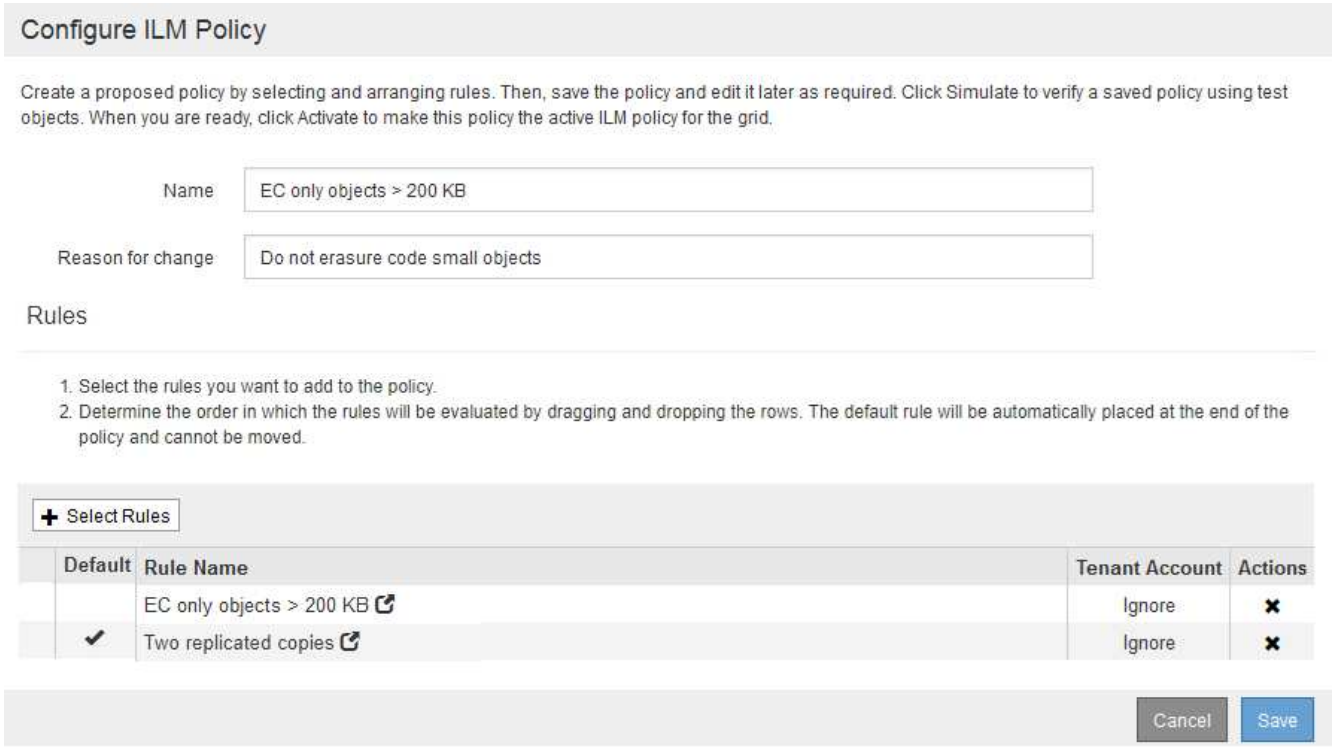


Criterio ILM per esempio 2: Utilizzare EC per oggetti di dimensioni superiori a 200 KB

In questo esempio di policy, gli oggetti di dimensioni superiori a 200 KB vengono sottoposti a erasure coding. Vengono create due copie replicate di tutti gli altri oggetti.

Questo esempio di policy ILM include le seguenti regole ILM:

- Erasure coding di tutti gli oggetti di dimensioni superiori a 200 KB.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita per creare due copie replicate di tale oggetto. Poiché gli oggetti di dimensioni superiori a 200 KB sono stati filtrati dalla regola 1, la regola 2 si applica solo agli oggetti di dimensioni inferiori o pari a 200 KB.



Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine

È possibile utilizzare le seguenti regole e policy di esempio per garantire che le immagini di dimensioni superiori a 200 KB vengano erasure coded e che vengano eseguite tre copie di immagini più piccole.

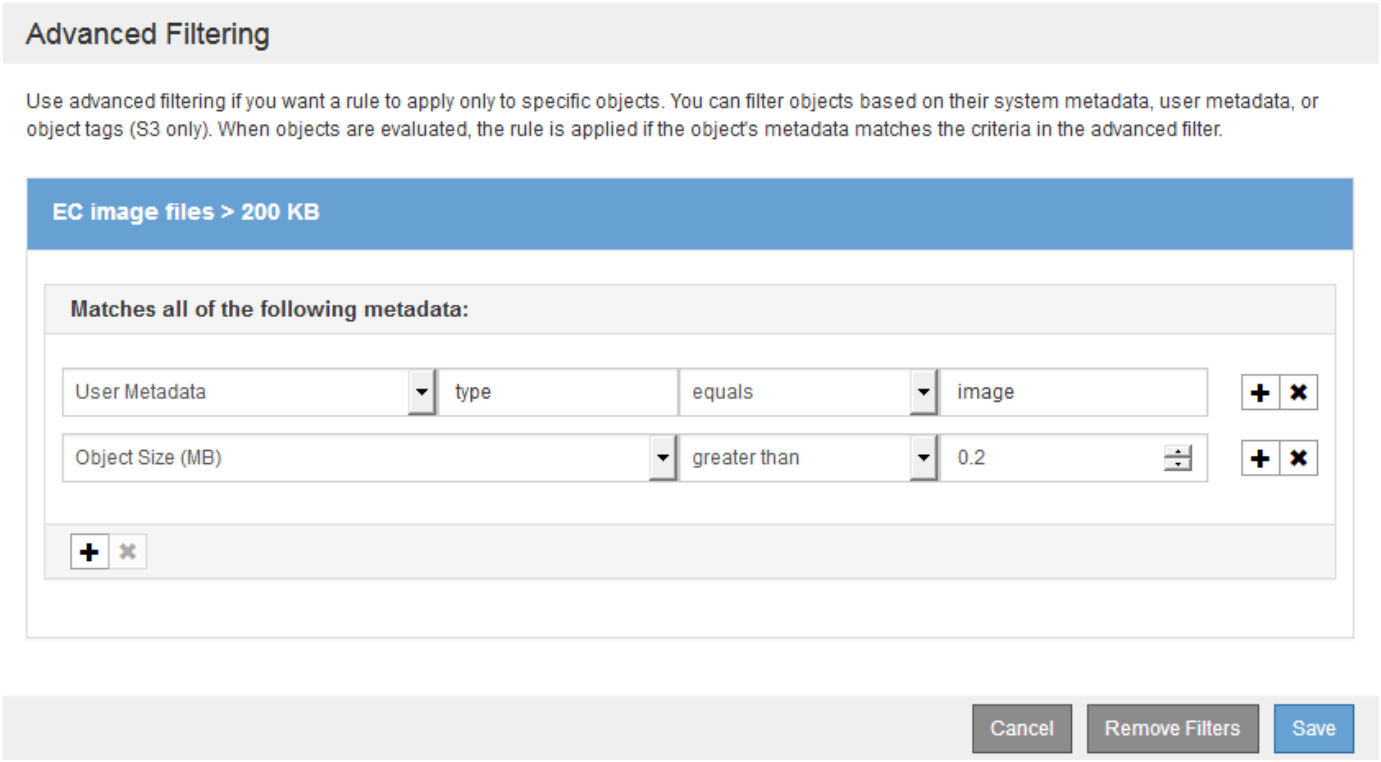
> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 3: Utilizzare EC per file di immagine di dimensioni superiori a 200 KB

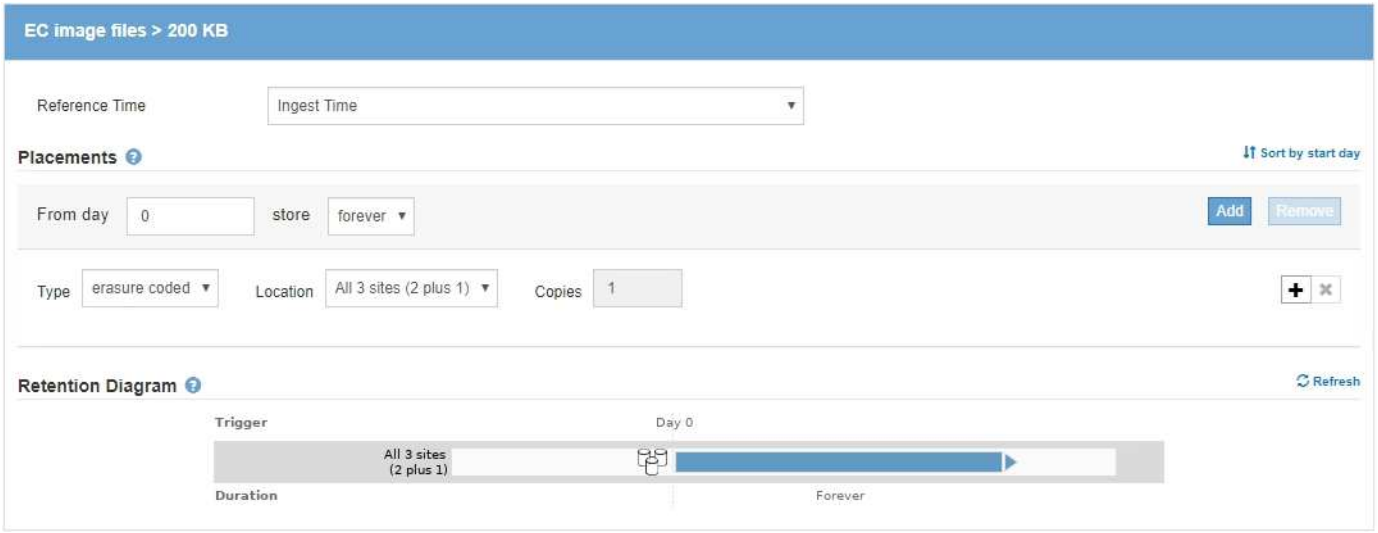
Questa regola ILM di esempio utilizza un filtro avanzato per eseguire la cancellazione di tutti i file di immagine di dimensioni superiori a 200 KB.

Definizione della regola	Valore di esempio
Nome regola	File immagine EC > 200 KB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per i metadati utente	Il tipo di metadati utente equivale ai file di immagine
Filtro avanzato per le dimensioni dell'oggetto	Dimensione oggetto (MB) maggiore di 0.2

Definizione della regola	Valore di esempio
Posizionamento dei contenuti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti



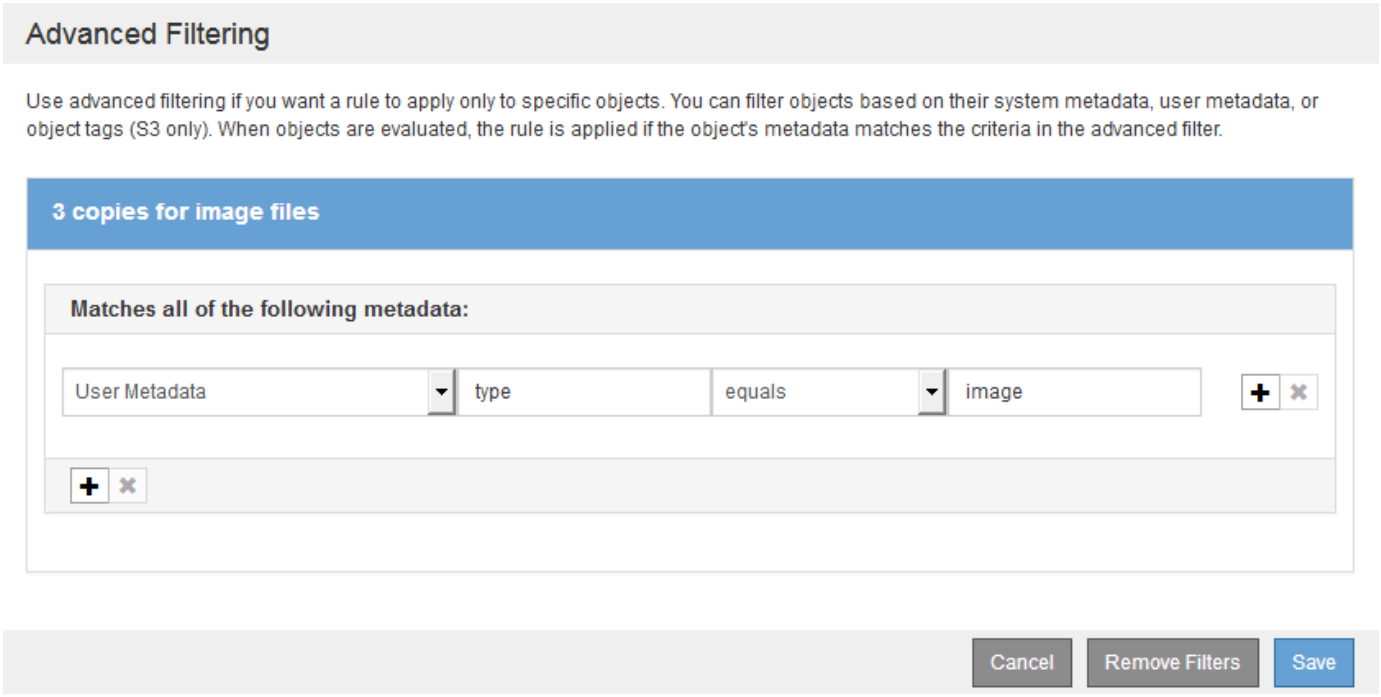
Poiché questa regola è configurata come prima regola del criterio, l'istruzione di posizionamento della codifica di cancellazione si applica solo alle immagini di dimensioni superiori a 200 KB.



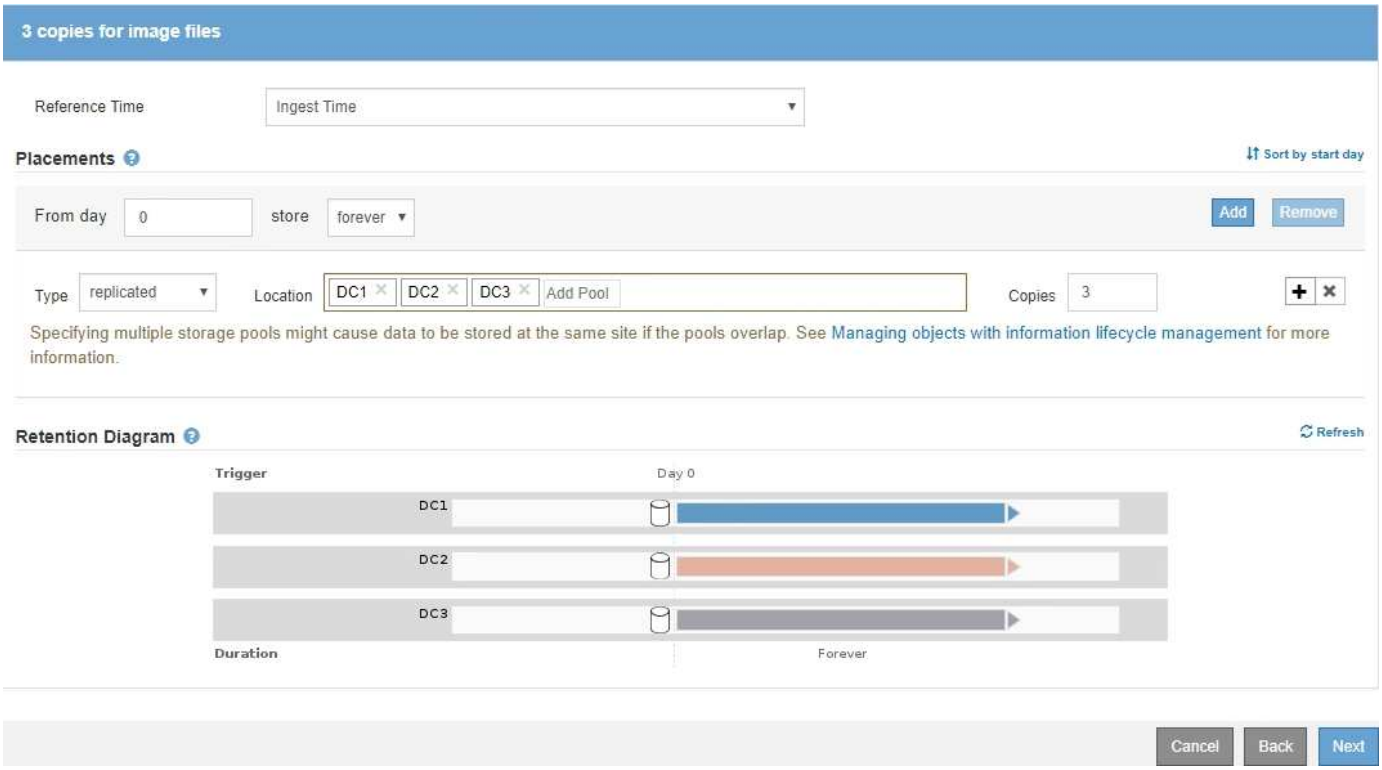
ILM regola 2 per esempio 3: Replica 3 copie per tutti i file immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file di immagine devono essere replicati.

Definizione della regola	Valore di esempio
Nome regola	3 copie per i file di immagine
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per i metadati utente	Il tipo di metadati utente equivale ai file di immagine
Posizionamento dei contenuti	Creare 3 copie replicate in tutti i nodi di storage



Poiché la prima regola del criterio ha già trovato corrispondenza con file di immagine di dimensioni superiori a 200 KB, queste istruzioni di posizionamento si applicano solo ai file di immagine di dimensioni pari o inferiori a 200 KB.

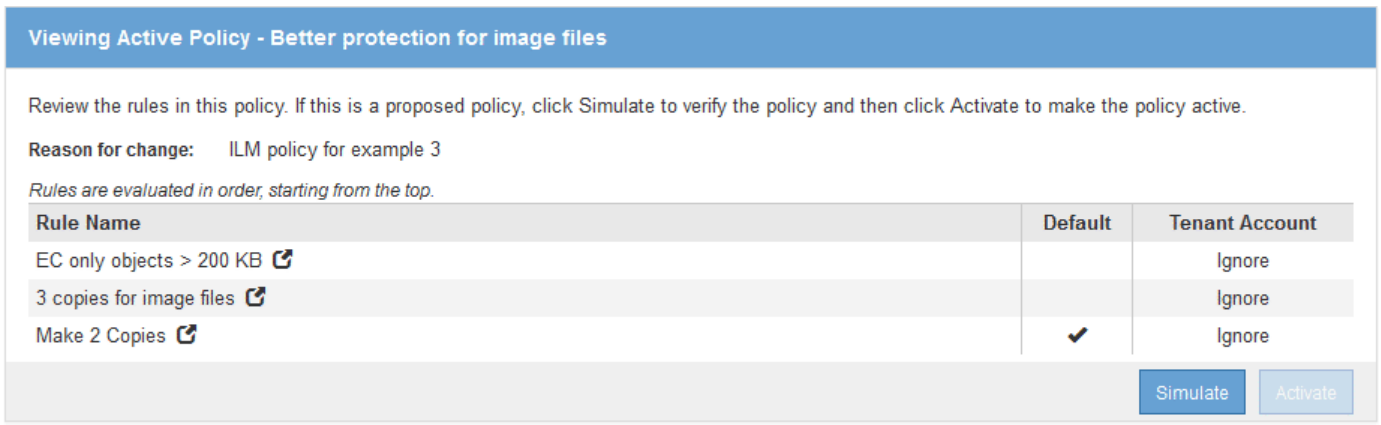


Policy ILM per esempio 3: Migliore protezione per i file di immagine

In questo esempio, il criterio ILM utilizza tre regole ILM per creare un criterio che erasure i file immagine di dimensioni superiori a 200 KB (0.2 MB), crea copie replicate per i file immagine di dimensioni pari o inferiori a 200 KB e crea due copie replicate per i file non immagine.

Questo esempio di policy ILM include regole che eseguono le seguenti operazioni:

- Erasure coding tutti i file di immagine di dimensioni superiori a 200 KB.
- Creare tre copie dei file immagine rimanenti (ovvero, immagini di dimensioni pari o inferiori a 200 KB).
- Applicare la regola predefinita a tutti gli oggetti rimanenti (ovvero tutti i file non immagine).



Esempio 4: Regole ILM e policy per gli oggetti con versione S3

Se si dispone di un bucket S3 con la versione attivata, è possibile gestire le versioni degli oggetti non correnti includendo regole nella policy ILM che utilizzano **tempo non**

corrente come tempo di riferimento.

Come illustrato in questo esempio, è possibile controllare la quantità di storage utilizzata dagli oggetti con versione utilizzando istruzioni di posizionamento diverse per le versioni degli oggetti non correnti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

> Se si creano criteri ILM per gestire le versioni degli oggetti non correnti, tenere presente che è necessario conoscere l'UUID o il CBID della versione dell'oggetto per simulare il criterio. Per trovare UUUID e CBID di un oggetto, utilizzare Object Metadata Lookup (Ricerca metadati oggetto) mentre l'oggetto è ancora aggiornato.

Informazioni correlate

"Modalità di eliminazione degli oggetti con versione S3"

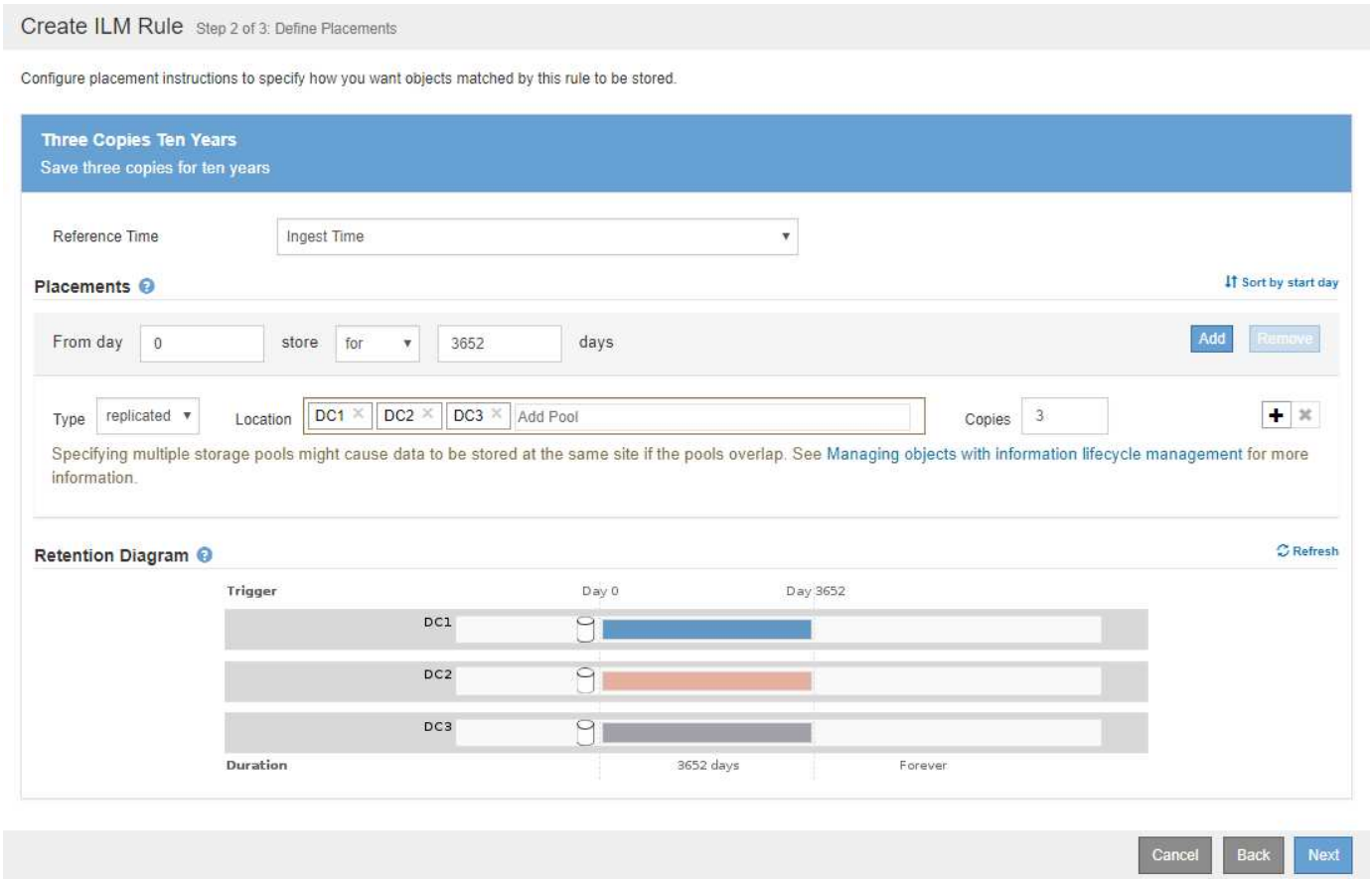
"Verifica di un criterio ILM con la ricerca dei metadati degli oggetti"

ILM regola 1 per esempio 4: Salva tre copie per 10 anni

Questa regola ILM di esempio memorizza una copia di ciascun oggetto in tre data center per 10 anni.

Questa regola si applica a tutti gli oggetti, indipendentemente dal fatto che siano con versione.

Definizione della regola	Valore di esempio
Pool di storage	Tre pool di storage, ciascuno in diversi data center, denominati DC1, DC2 e DC3.
Nome regola	Tre copie dieci anni
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva tre copie replicate per 10 anni (3,652 giorni), una in DC1, una in DC2 e una in DC3. Alla fine dei 10 anni, eliminare tutte le copie dell'oggetto.



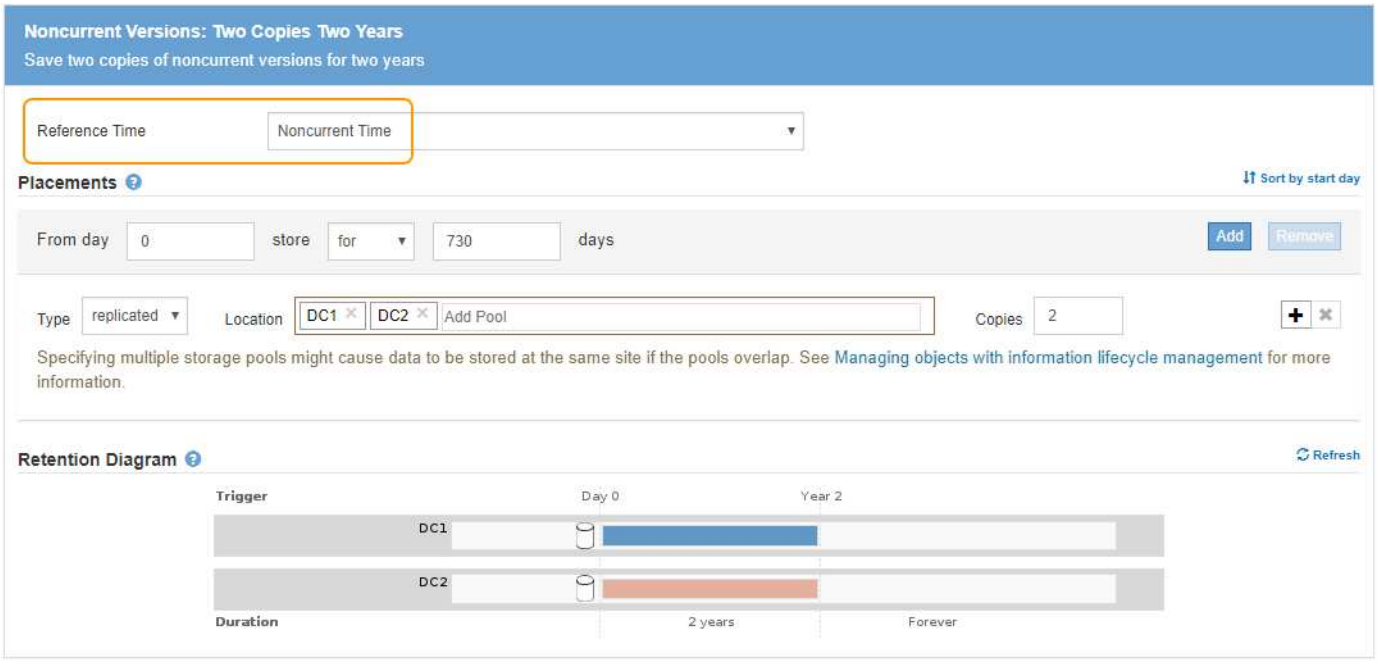
ILM regola 2 per esempio 4: Salva due copie di versioni non correnti per 2 anni

Questa regola ILM di esempio memorizza due copie delle versioni non correnti di un oggetto con versione S3 per 2 anni.

Poiché la regola ILM 1 si applica a tutte le versioni dell'oggetto, è necessario creare un'altra regola per filtrare le versioni non correnti. Questa regola utilizza l'opzione **ora non corrente** per il tempo di riferimento.

In questo esempio, vengono memorizzate solo due copie delle versioni non correnti, che verranno memorizzate per due anni.

Definizione della regola	Valore di esempio
Pool di storage	Due pool di storage, ciascuno in diversi data center, denominati DC1 e DC2.
Nome regola	Versioni non correnti: Due copie per due anni
Tempo di riferimento	Ora non corrente
Posizionamento dei contenuti	Il giorno 0 relativo all'ora non corrente (ovvero, a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), mantenere due copie replicate delle versioni dell'oggetto non correnti per 2 anni (730 giorni), una in DC1 e una in DC2. Alla fine di 2 anni, eliminare le versioni non aggiornate.



Policy ILM per esempio 4: Oggetti con versione S3

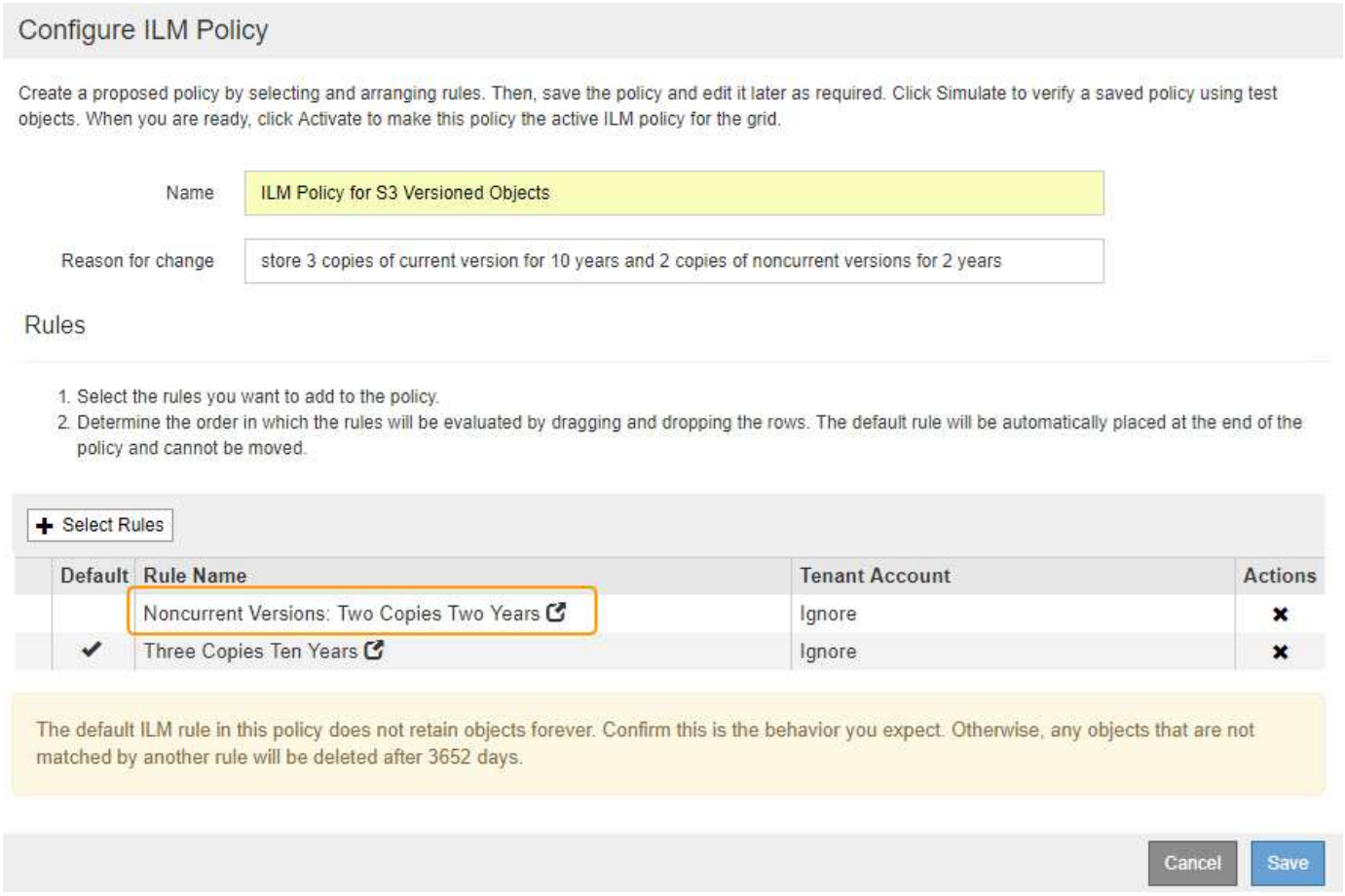
Se si desidera gestire le versioni precedenti di un oggetto in modo diverso dalla versione corrente, le regole che utilizzano **ora non corrente** come ora di riferimento devono essere visualizzate nel criterio ILM prima delle regole che si applicano alla versione corrente dell'oggetto.

Un criterio ILM per gli oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

- Mantenere le versioni precedenti (non aggiornate) di ciascun oggetto per 2 anni, a partire dal giorno in cui la versione è diventata non aggiornata.

> Le regole dell'ora non corrente devono essere visualizzate nel criterio prima delle regole applicabili alla versione corrente dell'oggetto. In caso contrario, le versioni degli oggetti non correnti non verranno mai associate alla regola dell'ora non corrente.

- Al momento dell'acquisizione, creare tre copie replicate e memorizzare una copia in ciascuno dei tre data center. Conserva le copie della versione corrente dell'oggetto per 10 anni.



Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Qualsiasi versione dell'oggetto non corrente verrebbe associata dalla prima regola. Se una versione dell'oggetto non corrente ha più di 2 anni, viene eliminata in modo permanente da ILM (tutte le copie della versione non corrente vengono rimosse dalla griglia).

> Per simulare versioni di oggetti non correnti, è necessario utilizzare UUID o CBID di tale versione. Mentre l'oggetto è ancora aggiornato, è possibile utilizzare Object Metadata Lookup (Ricerca metadati oggetto) per trovare UUID e CBID.

- La seconda regola corrisponde alla versione corrente dell'oggetto. Quando la versione corrente dell'oggetto è stata memorizzata per 10 anni, il processo ILM aggiunge un indicatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente dell'oggetto "non aggiornata". La prossima volta che si verifica la valutazione ILM, questa versione non corrente corrisponde alla prima regola. Di conseguenza, la copia di DC3 viene eliminata e le due copie di DC1 e DC2 vengono conservate per altri 2 anni.

Informazioni correlate

"Verifica di un criterio ILM con la ricerca dei metadati degli oggetti"

Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione

È possibile utilizzare un filtro di posizione e il rigoroso comportamento di acquisizione in una regola per impedire che gli oggetti vengano salvati in una determinata posizione del data center.

In questo esempio, un tenant con sede a Parigi non desidera memorizzare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, inclusi tutti gli oggetti di altri account tenant, possono essere memorizzati nel data center di Parigi o nel data center statunitense.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

"Modalità di acquisizione degli oggetti"

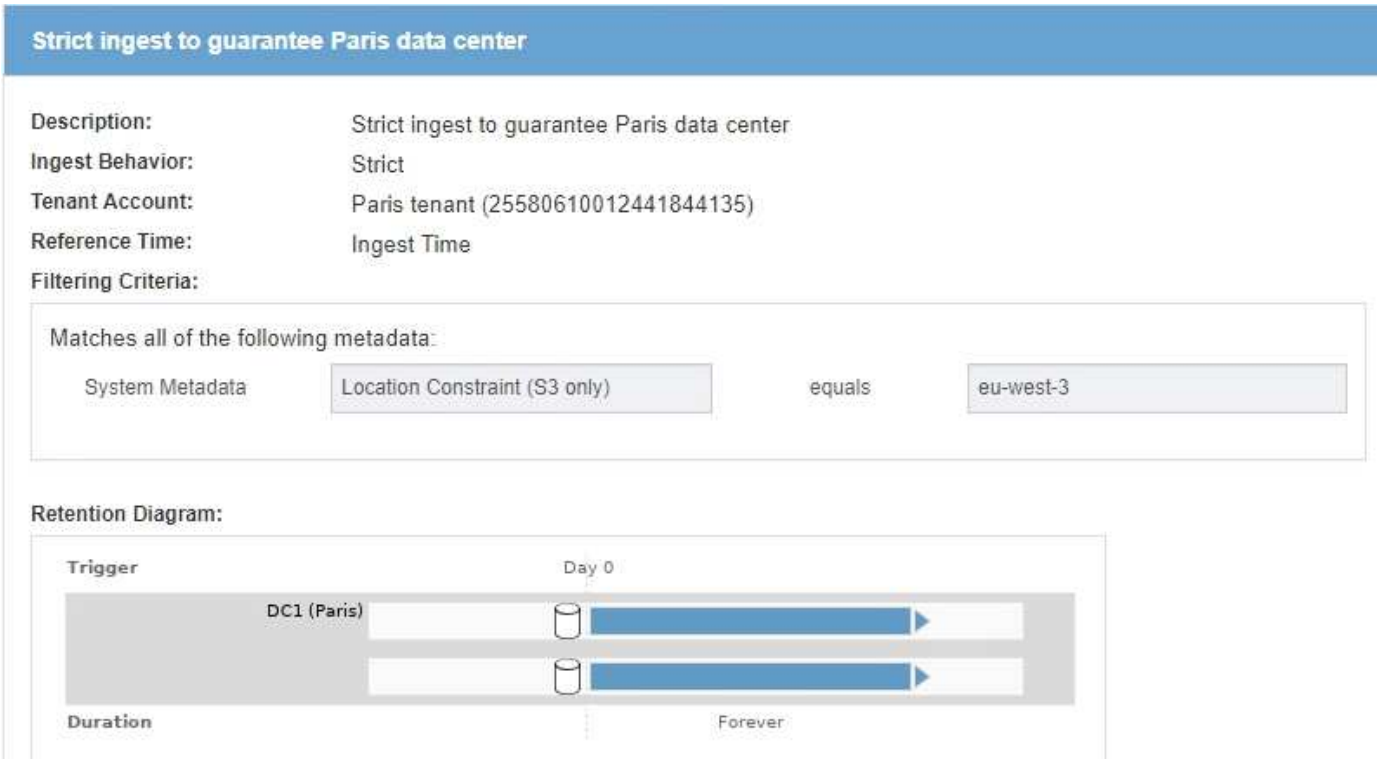
"Fase 3 di 3: Definizione del comportamento di acquisizione"

ILM regola 1 per esempio 5: Ingest rigoroso per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento rigoroso dell'acquisizione per garantire che gli oggetti salvati da un tenant basato su Parigi nei bucket S3 con la regione impostata su ue-West-3 (Parigi) non vengano mai memorizzati nel data center statunitense.

Questa regola si applica agli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 (Parigi).

Definizione della regola	Valore di esempio
Account tenant	Tenant di Parigi
Filtraggio avanzato	Il vincolo di posizione equivale a eu-West-3
Pool di storage	DC1 (Parigi)
Nome regola	Un ingest rigoroso per garantire il data center di Parigi
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva due copie replicate per sempre in DC1 (Parigi)
Comportamento di acquisizione	Rigoroso. Utilizza sempre le posizioni di questa regola per l'acquisizione. L'acquisizione non riesce se non è possibile memorizzare due copie dell'oggetto nel data center di Parigi.



ILM regola 2 per esempio 5: Acquisizione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciata per fornire un'efficienza ILM ottimale per qualsiasi oggetto non associato alla prima regola. Verranno memorizzate due copie di tutti gli oggetti corrispondenti a questa regola: Una nel data center degli Stati Uniti e una nel data center di Parigi. Se la regola non può essere soddisfatta immediatamente, le copie temporanee vengono memorizzate in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi area.

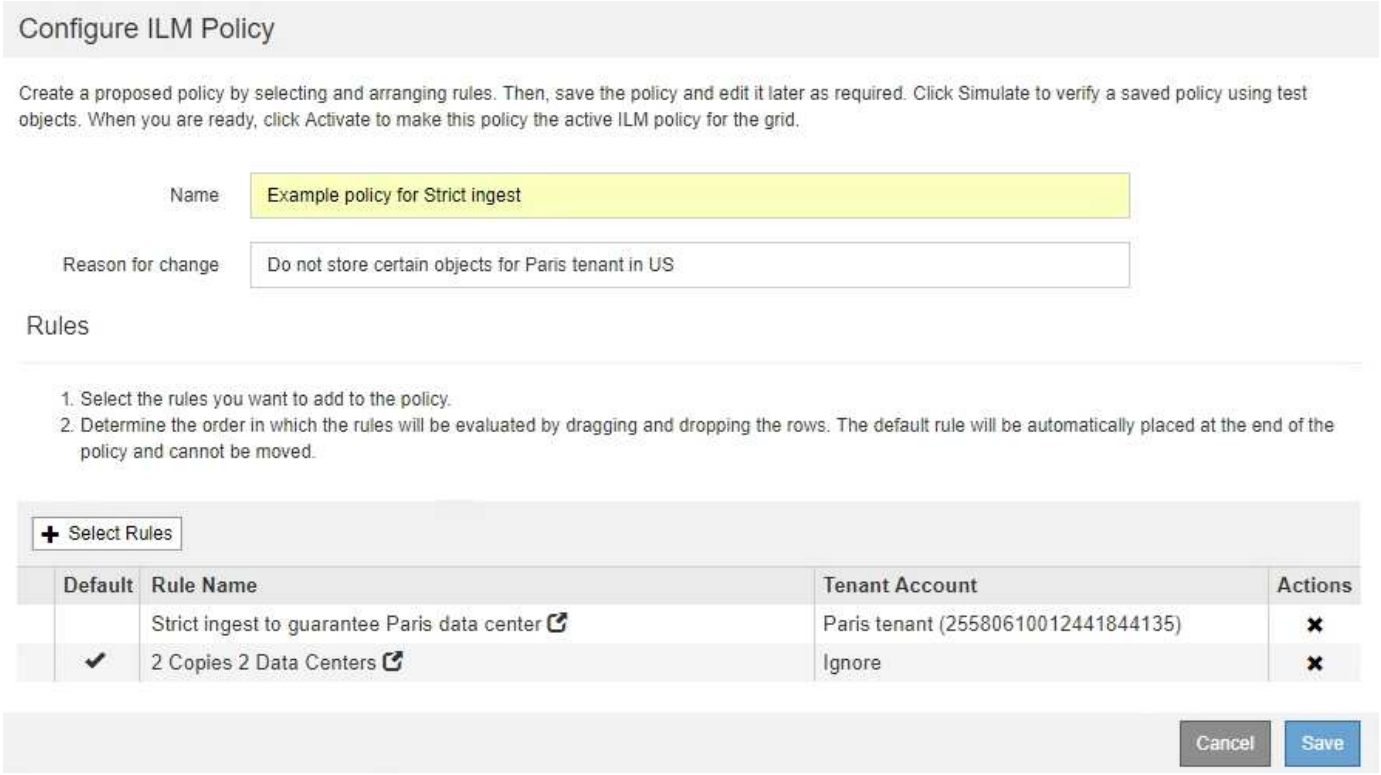
Definizione della regola	Valore di esempio
Account tenant	Ignorare
Filtraggio avanzato	*Non specificato*
Pool di storage	DC1 (Parigi) e DC2 (Stati Uniti)
Nome regola	2 copie di 2 data center
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva due copie replicate per sempre in due data center
Comportamento di acquisizione	Bilanciato. Gli oggetti che corrispondono a questa regola vengono posizionati in base alle istruzioni di posizionamento della regola, se possibile. In caso contrario, le copie temporanee vengono eseguite in qualsiasi ubicazione disponibile.

Policy ILM per esempio 5: Combinazione di comportamenti di acquisizione

Il criterio ILM di esempio include due regole che hanno comportamenti di acquisizione diversi.

Un criterio ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Memorizzare gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 (Parigi) solo nel data center di Parigi. Non eseguire l'acquisizione se il data center di Parigi non è disponibile.
- Memorizzare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) nel data center statunitense e nel data center di Parigi. Se le istruzioni di posizionamento non possono essere soddisfatte, eseguire copie temporanee in qualsiasi ubicazione disponibile.



Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Tutti gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 vengono abbinati alla prima regola e memorizzati nel data center di Parigi. Poiché la prima regola utilizza un ingest rigoroso, questi oggetti non vengono mai memorizzati nel data center statunitense. Se i nodi di storage nel data center di Parigi non sono disponibili, l'acquisizione non riesce.
- Tutti gli altri oggetti sono abbinati dalla seconda regola, inclusi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-West-3. Una copia di ciascun oggetto viene salvata in ciascun data center. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie temporanee in qualsiasi posizione disponibile.

Esempio 6: Modifica di un criterio ILM

Potrebbe essere necessario creare e attivare una nuova policy ILM se la protezione dei dati deve cambiare o se si aggiungono nuovi siti.

Prima di modificare una policy, è necessario comprendere in che modo le modifiche apportate ai posizionamenti ILM possono influire temporaneamente sulle prestazioni generali di un sistema StorageGRID.

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione e il criterio ILM attivo deve essere rivisto per memorizzare i dati nel nuovo sito.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

In che modo la modifica di un criterio ILM influisce sulle performance

Quando si attiva un nuovo criterio ILM, le prestazioni del sistema StorageGRID potrebbero risentirne temporaneamente, soprattutto se le istruzioni di posizionamento nel nuovo criterio richiedono lo spostamento

di molti oggetti esistenti in nuove posizioni.

> Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

I tipi di modifiche ai criteri ILM che possono influire temporaneamente sulle prestazioni di StorageGRID includono:

- Applicazione di un profilo di codifica Erasure diverso agli oggetti con codifica erasure esistenti.

  > StorageGRID considera ogni profilo di codifica Erasure unico e non riutilizza i frammenti di codifica Erasure quando viene utilizzato un nuovo profilo.

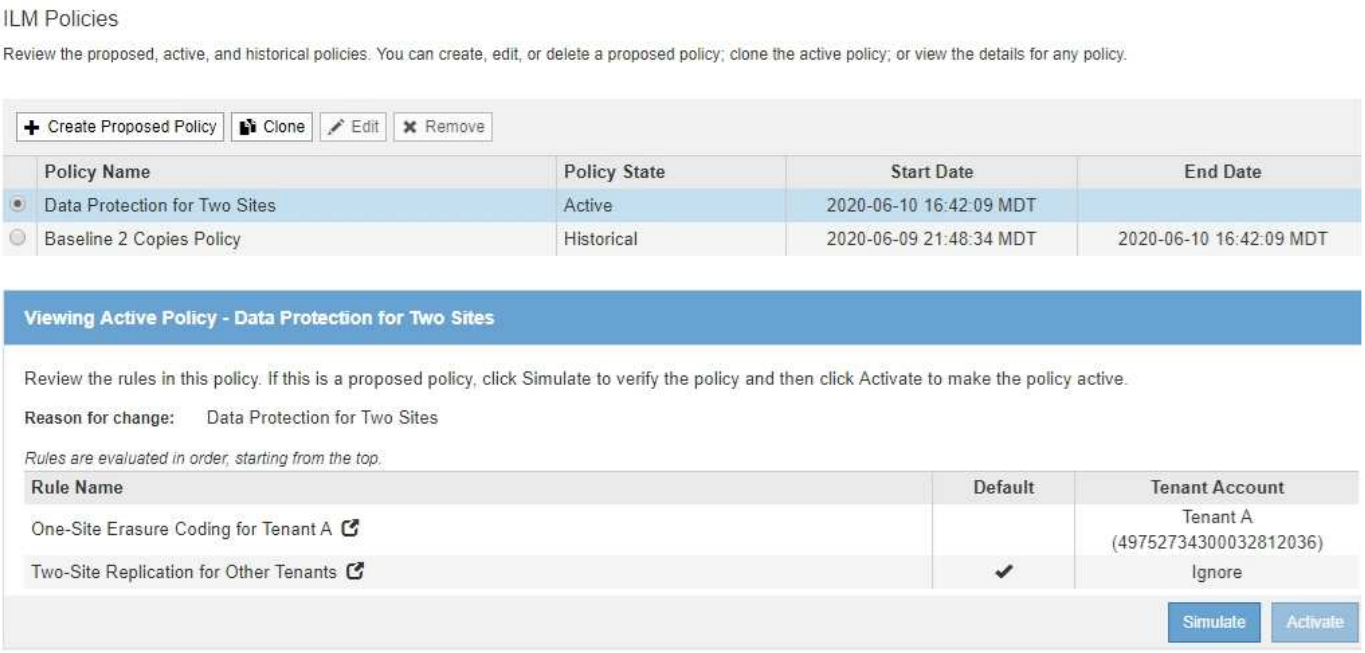
- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, conversione di una grande percentuale di oggetti replicati in oggetti con codifica per la cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un numero elevato di oggetti da o verso un Cloud Storage Pool o da o verso un sito remoto.

Informazioni correlate

"Creazione di un criterio ILM"

Policy ILM attiva ad esempio 6: Protezione dei dati in due siti

In questo esempio, la policy ILM attiva è stata inizialmente progettata per un sistema StorageGRID a due siti e utilizza due regole ILM.



In questa policy ILM, gli oggetti appartenenti al tenant A sono protetti da una codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti in due siti utilizzando la replica a 2 copie.

La prima regola di questo esempio utilizza un filtro avanzato per garantire che la codifica erasure non venga utilizzata per oggetti di piccole dimensioni. Qualsiasi oggetto del tenant A di dimensioni inferiori a 200 KB sarà protetto dalla seconda regola, che utilizza la replica.

Regola 1: Erasure coding per un sito per il tenant A.

Definizione della regola	Valore di esempio
Nome regola	Codifica di cancellazione one-site per il tenant A.
Account tenant	Tenant A.
Pool di storage	Data center 1
Posizionamento dei contenuti	2+1 erasure coding in Data Center 1 dal giorno 0 a per sempre

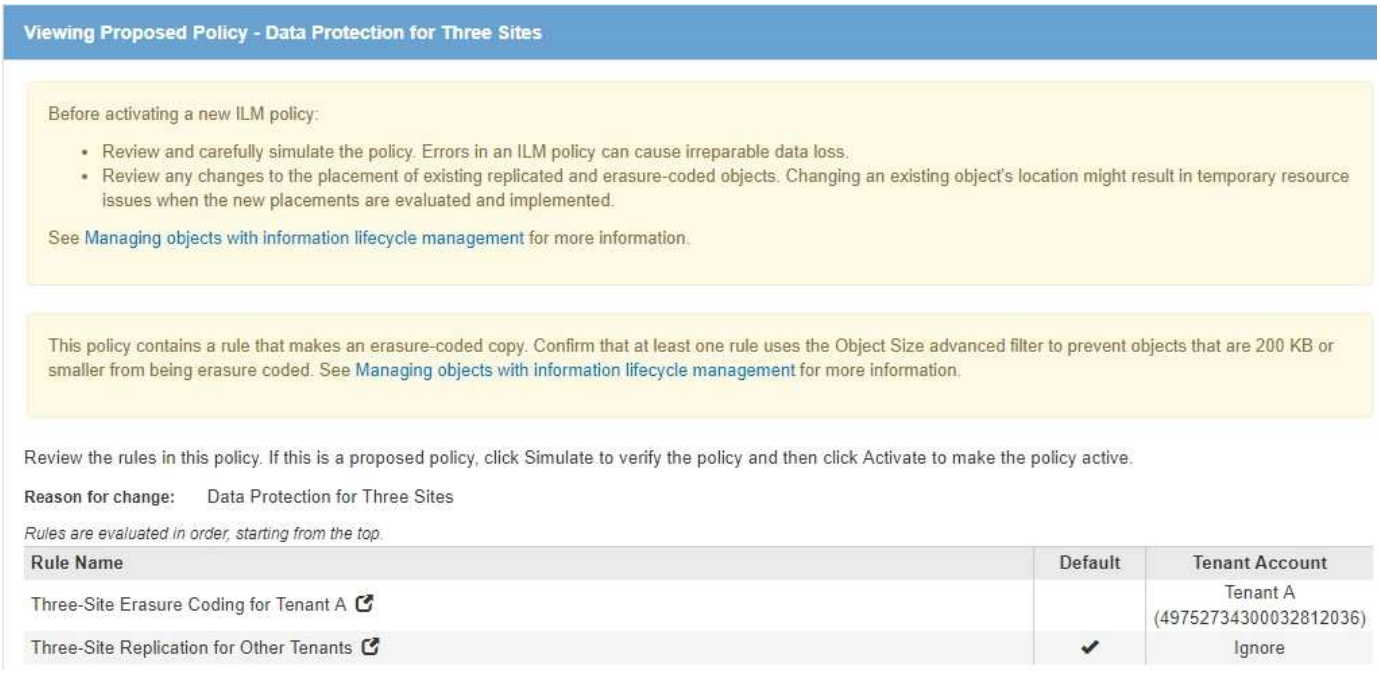
Regola 2: Replica a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome regola	Replica a due siti per altri tenant
Account tenant	Ignorare
Pool di storage	Data Center 1 e Data Center 2
Posizionamento dei contenuti	Due copie replicate dal giorno 0 all'infinito: Una copia nel data center 1 e una copia nel data center 2.

Policy ILM proposta per esempio 6: Protezione dei dati in tre siti

In questo esempio, il criterio ILM viene aggiornato per un sistema StorageGRID a tre siti.

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore del grid ha creato due nuovi pool di storage: Un pool di storage per Data Center 3 e un pool di storage contenente tutti e tre i siti (non lo stesso del pool di storage predefinito di tutti i nodi di storage). Quindi, l'amministratore ha creato due nuove regole ILM e una nuova policy ILM proposta, progettata per proteggere i dati in tutti e tre i siti.



Quando viene attivata questa nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti da una cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e gli oggetti più piccoli appartenenti al tenant A) saranno protetti in tre siti utilizzando la replica a 3 copie.

Regola 1: Erasure coding a tre siti per il tenant A.

Definizione della regola	Valore di esempio
Nome regola	Codifica di cancellazione a tre siti per il tenant A.
Account tenant	Tenant A.
Pool di storage	Tutti e 3 i data center (inclusi data center 1, data center 2 e data center 3)
Posizionamento dei contenuti	2+1 erasure coding in tutti e 3 i data center, dal giorno 0 fino all'eterno

Regola 2: Replica a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome regola	Replica a tre siti per altri tenant
Account tenant	Ignorare
Pool di storage	Data Center 1, Data Center 2 e Data Center 3
Posizionamento dei contenuti	Tre copie replicate dal giorno 0 a sempre: Una copia presso il data center 1, una copia presso il data center 2 e una copia presso il data center 3.

Attivazione della policy ILM proposta, ad esempio 6

Quando si attiva un nuovo criterio ILM proposto, gli oggetti esistenti potrebbero essere spostati in nuove posizioni oppure potrebbero essere create nuove copie degli oggetti per gli oggetti esistenti, in base alle istruzioni di posizionamento in qualsiasi regola nuova o aggiornata.

> Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.

> Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Cosa succede quando cambiano le istruzioni di erasure coding

Nella policy ILM attualmente attiva, per questo esempio, gli oggetti appartenenti al tenant A sono protetti utilizzando la codifica di cancellazione 2+1 nel data center 1. Nella nuova policy ILM proposta, gli oggetti appartenenti al tenant A verranno protetti utilizzando la codifica di cancellazione 2+1 nei data center 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- I nuovi oggetti acquisiti dal tenant A vengono suddivisi in due frammenti di dati e viene aggiunto un frammento di parità. Quindi, ciascuno dei tre frammenti viene memorizzato in un data center diverso.
- Gli oggetti esistenti appartenenti al tenant A vengono rivalutati durante il processo di scansione ILM in corso. Poiché le istruzioni di posizionamento di ILM utilizzano un nuovo profilo di codifica Erasure, vengono creati e distribuiti frammenti completamente nuovi con codifica erasure nei tre data center.

> I frammenti 2+1 esistenti nel data center 1 non vengono riutilizzati. StorageGRID considera ogni profilo di codifica Erasure unico e non riutilizza i frammenti di codifica Erasure quando viene utilizzato un nuovo profilo.

Cosa succede quando cambiano le istruzioni di replica

Nel criterio ILM attualmente attivo per questo esempio, gli oggetti appartenenti ad altri tenant vengono protetti utilizzando due copie replicate nei pool di storage dei data center 1 e 2. Nella nuova policy ILM proposta, gli oggetti appartenenti ad altri tenant verranno protetti utilizzando tre copie replicate nei pool di storage dei data center 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID crea tre copie e salva una copia in ogni data center.
- Gli oggetti esistenti appartenenti a questi altri tenant vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie di oggetti esistenti nel data center 1 e nel data center 2 continuano a soddisfare i requisiti di replica della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il data center 3.

Impatto delle performance dell'attivazione di questa policy

Quando viene attivata la policy ILM proposta in questo esempio, le prestazioni generali di questo sistema StorageGRID saranno temporaneamente compromesse. Per creare nuovi frammenti erasure-coded per gli oggetti esistenti del tenant A e nuove copie replicate nel data center 3 per gli oggetti esistenti degli altri tenant saranno necessari livelli di risorse grid superiori al normale.

Come conseguenza della modifica del criterio ILM, le richieste di lettura e scrittura del client potrebbero temporaneamente riscontrare latenze superiori al normale. Le latenze torneranno ai livelli normali dopo che le istruzioni di posizionamento sono state completamente implementate nella griglia.

Per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui il nuovo criterio verrà applicato per garantire che gli oggetti esistenti non vengano spostati inutilmente.

Contattare il supporto tecnico se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

Esempio 7: Policy ILM conforme per il blocco oggetti S3

È possibile utilizzare il bucket S3, le regole ILM e il criterio ILM in questo esempio come punto di partenza quando si definisce un criterio ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con blocco oggetti S3 attivato.

Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti di StorageGRID, puoi anche utilizzare questo esempio per gestire qualsiasi bucket esistente con la funzionalità di conformità legacy attivata.

Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

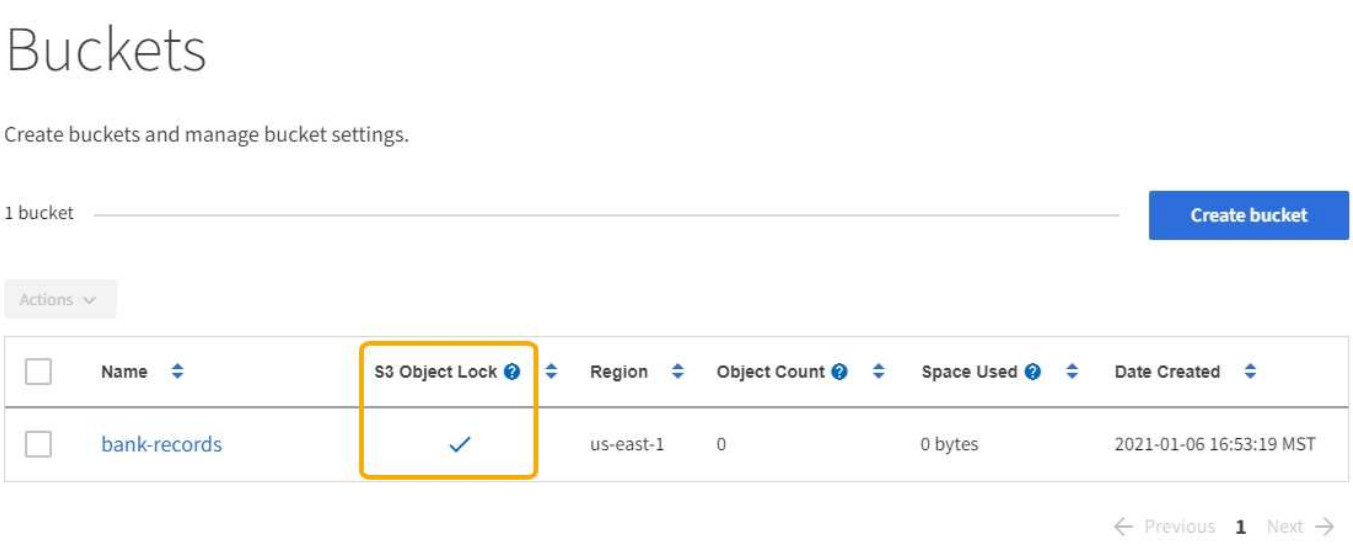
"Gestione degli oggetti con S3 Object Lock"

"Creazione di un criterio ILM"

Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato il tenant Manager per creare un bucket con blocco oggetti S3 abilitato per memorizzare i record bancari critici.

Definizione del bucket	Valore di esempio
Nome account tenant	Banca di ABC
Nome bucket	banca-record
Area bucket	us-east-1 (impostazione predefinita)



Ogni versione di oggetto e oggetto aggiunta al bucket dei record bancari utilizzerà i seguenti valori per `retain-until-date` e. `legal hold` impostazioni.

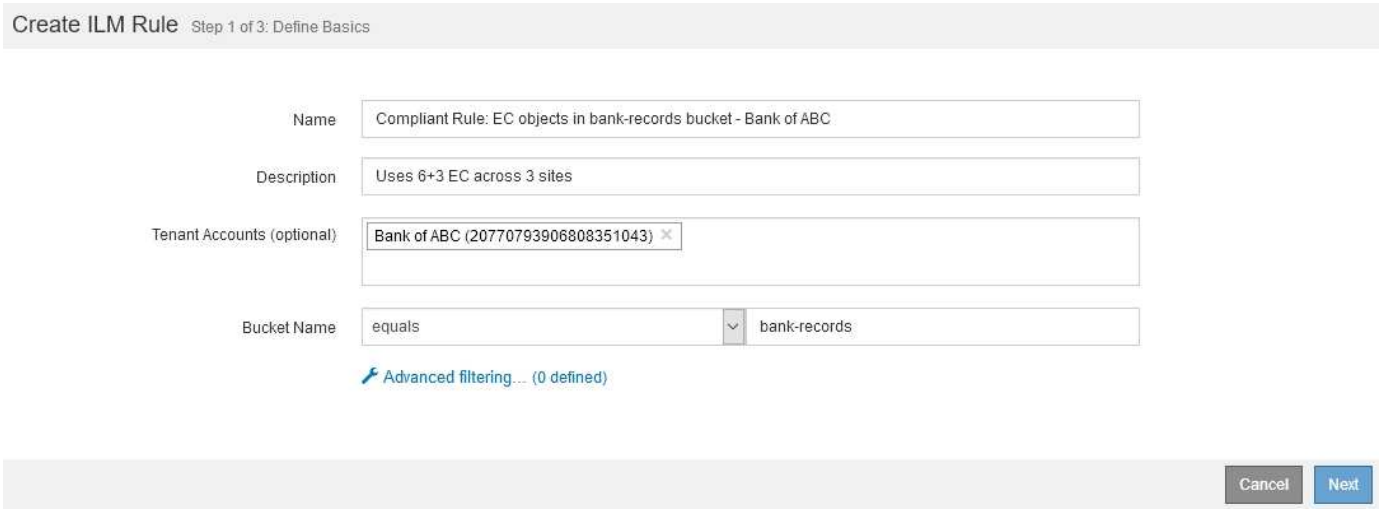
Impostazione per ciascun oggetto	Valore di esempio
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30 dicembre 2030) Ogni versione dell'oggetto ha il proprio `retain-until-date` impostazione. Questa impostazione può essere aumentata, ma non ridotta.
`legal hold`	`"OFF"` (Non in vigore) È possibile mettere o revocare un blocco legale su qualsiasi versione oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è sottoposto a un blocco legale, non è possibile eliminarlo anche se `retain-until-date` è stato raggiunto.

ILM regola 1 per S3 Object Lock esempio: Erasure coding profile with bucket matching

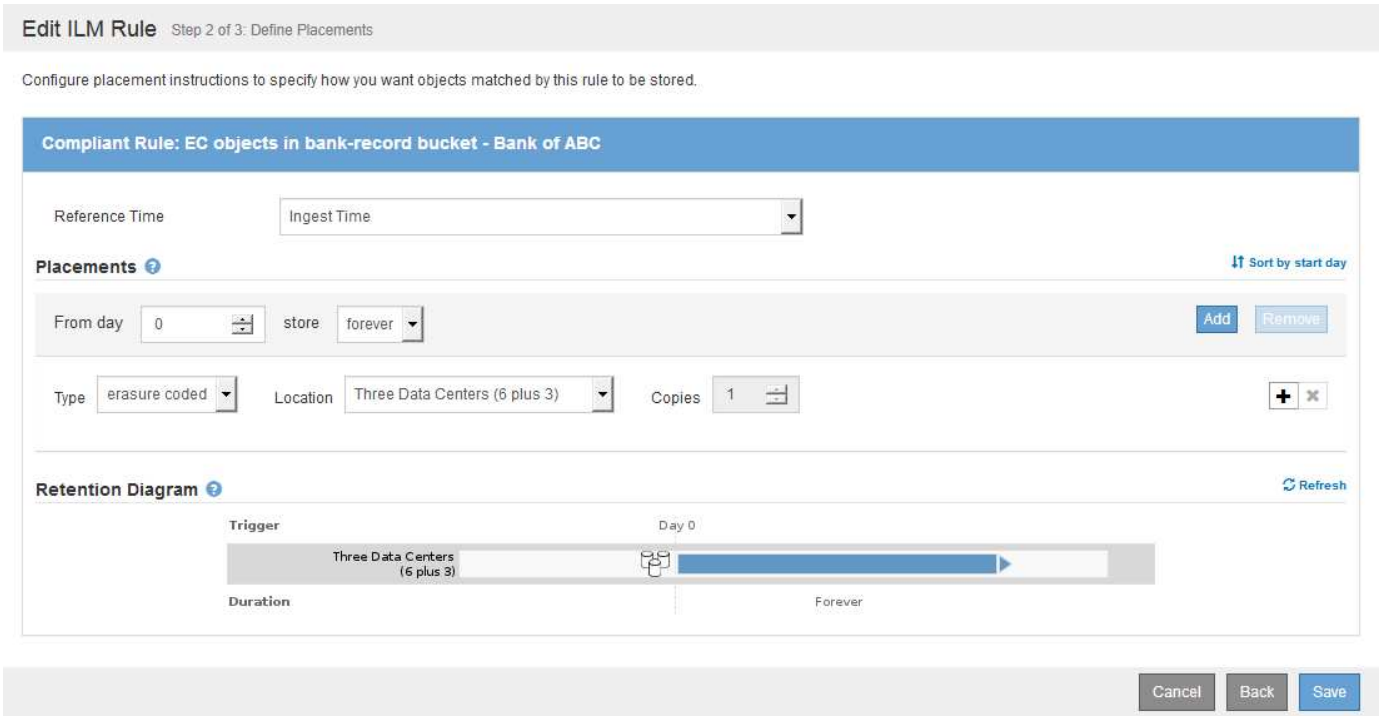
Questa regola ILM di esempio si applica solo all'account tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto in `bank-records` Quindi utilizza la codifica di cancellazione per memorizzare l'oggetto su nodi di storage in tre siti del data center utilizzando un profilo di codifica Erasure 6+3. Questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato: Una copia codificata in cancellazione viene conservata nei nodi di storage dal giorno 0 all'eterno, utilizzando l'ora di Ingest come ora di riferimento.

Definizione della regola	Valore di esempio
Nome regola	Compliant Rule (regola conforme): Oggetti EC nel bucket dei record bancari - Bank of ABC
Account tenant	Banca di ABC

Definizione della regola	Valore di esempio
Nome bucket	`bank-records`
Filtraggio avanzato	Dimensione oggetto (MB) maggiore di 0.20 **Nota:** questo filtro garantisce che la codifica erasure non venga utilizzata per oggetti di dimensioni pari o inferiori a 200 KB.



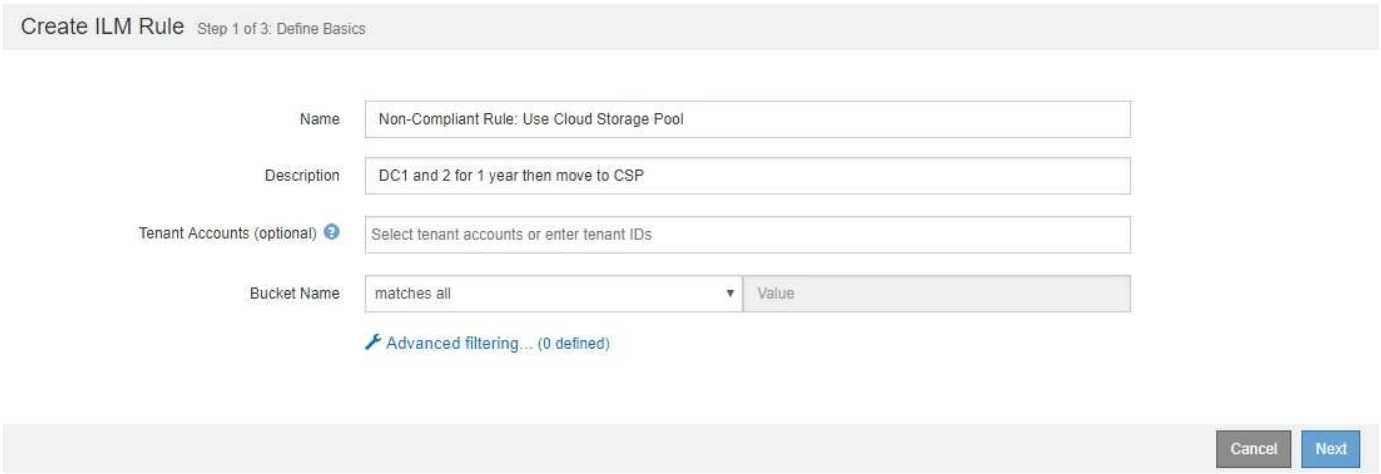
Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 memorizzare per sempre
Erasure Coding Profile (erasure Coding Profile	• Creare una copia con codifica di cancellazione sui nodi di storage in tre siti del data center • Utilizza uno schema di erasure coding 6+3



ILM regola 2 per S3 Object Lock esempio: Regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie di oggetti replicate sui nodi di storage. Dopo un anno, memorizza una copia su un Cloud Storage Pool per sempre. Poiché questa regola utilizza un Cloud Storage Pool, non è conforme e non si applica agli oggetti nei bucket con S3 Object Lock attivato.

Definizione della regola	Valore di esempio
Nome regola	Regola non conforme: Utilizza il pool di storage cloud
Account tenant	Non specificato
Nome bucket	Non specificato, ma si applica solo ai bucket che non hanno S3 Object Lock (o la funzione Compliance legacy) abilitato.
Filtraggio avanzato	Non specificato

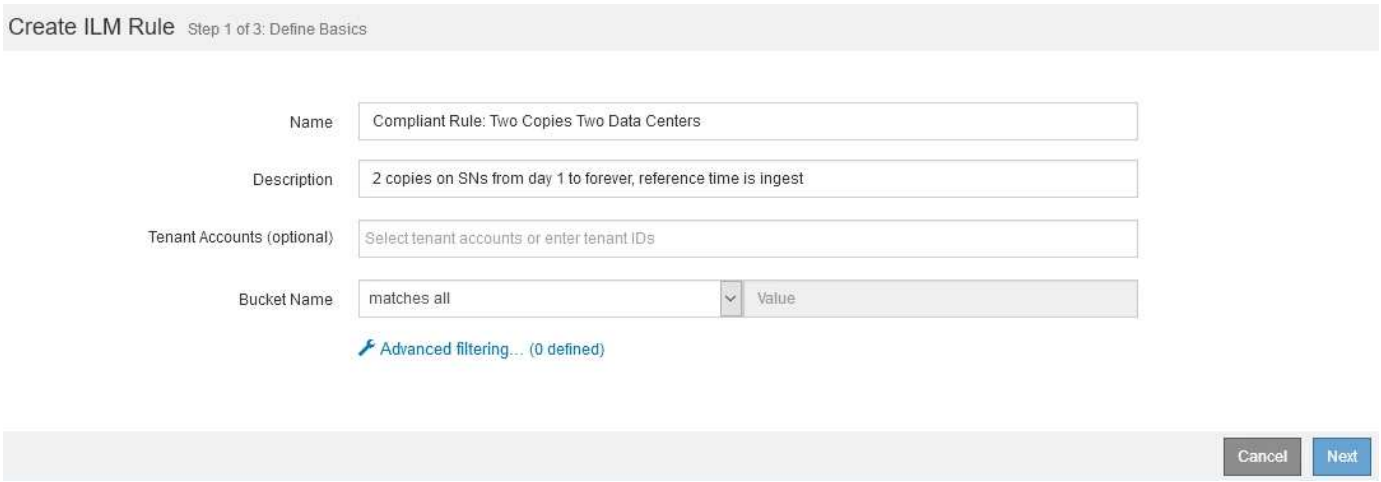


Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	• Il giorno 0, conserva due copie replicate sui nodi di storage nel data center 1 e nel data center 2 per 365 giorni • Dopo 1 anno, conserva per sempre una copia replicata in un Cloud Storage Pool

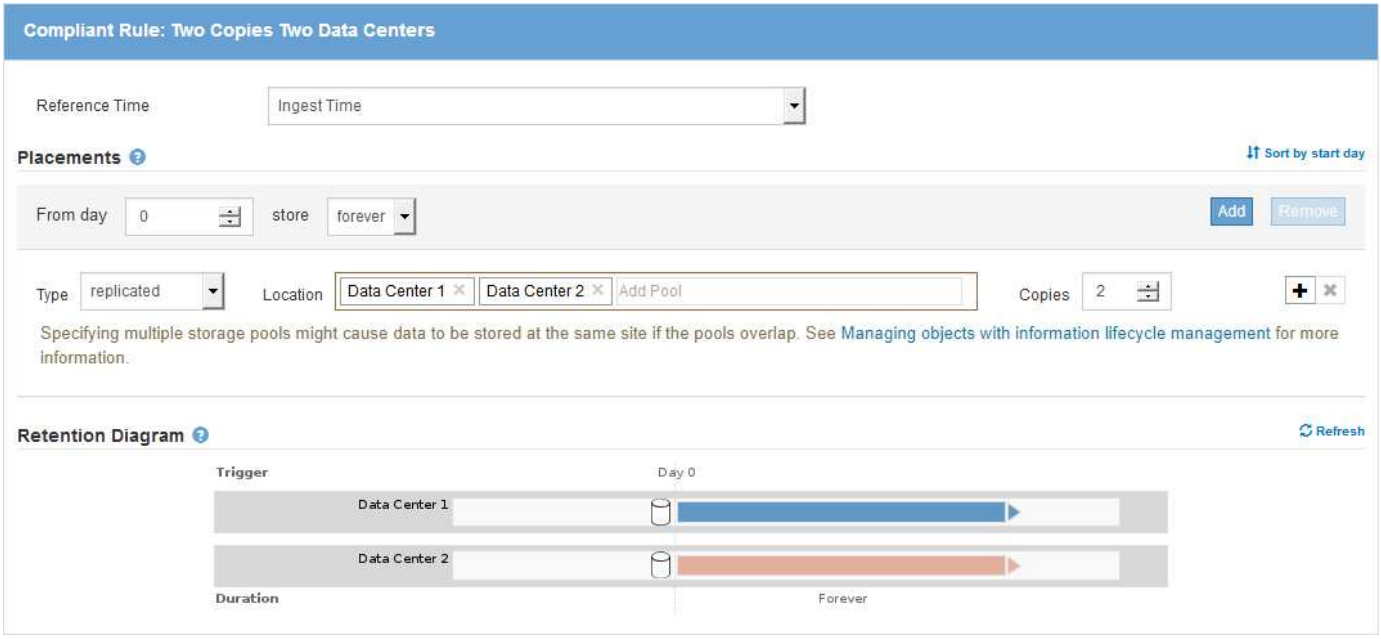
ILM regola 3 per S3 Object Lock esempio: Regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due data center. Questa regola di conformità è stata progettata per essere la regola predefinita nel criterio ILM. Non include alcun filtro e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: Due copie di oggetti vengono conservate sui nodi di storage dal giorno 0 all'eterno, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome regola	Default CompacCompacant Rule: Due copie di due data center
Account tenant	Non specificato
Nome bucket	Non specificato
Filtraggio avanzato	Non specificato



Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 all'anno, conserva due copie replicate, una sui nodi di storage nel data center 1 e una sui nodi di storage nel data center 2.



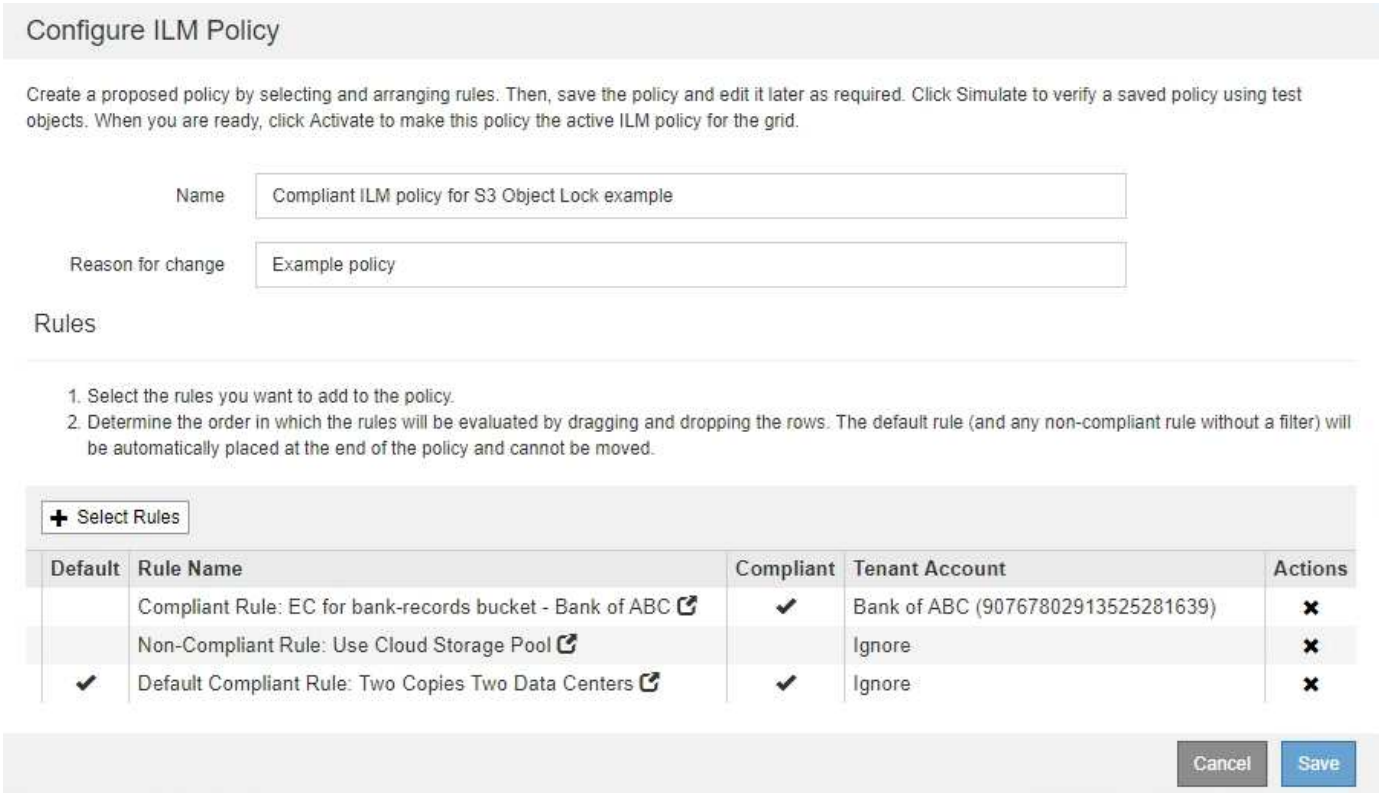
Esempio di policy ILM conforme per S3 Object Lock

Per creare un criterio ILM che protegga efficacemente tutti gli oggetti del sistema, inclusi quelli nei bucket con S3 Object Lock attivato, è necessario selezionare le regole ILM che soddisfano i requisiti di storage per tutti gli oggetti. Quindi, è necessario simulare e attivare la policy proposta.

Aggiunta di regole al criterio

In questo esempio, il criterio ILM include tre regole ILM, nel seguente ordine:

1. Regola conforme che utilizza la codifica erasure per proteggere oggetti di dimensioni superiori a 200 KB in un bucket specifico con blocco oggetti S3 attivato. Gli oggetti vengono memorizzati 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 e sposta una copia di oggetto in un pool di storage cloud per sempre. Questa regola non si applica ai bucket con blocco oggetti S3 attivato perché utilizza un pool di storage cloud.
3. La regola di conformità predefinita che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a per sempre.



Simulazione della policy proposta

Dopo aver aggiunto le regole nella policy proposta, aver scelto una regola di conformità predefinita e aver disposto le altre regole, è necessario simulare la policy testando gli oggetti dal bucket con S3 Object Lock abilitato e da altri bucket. Ad esempio, quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- La prima regola corrisponde solo agli oggetti di test di dimensioni superiori a 200 KB nei record bancari bucket per il tenant Bank of ABC.
- La seconda regola corrisponde a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri account tenant.
- La regola predefinita corrisponde ai seguenti oggetti:
  - Oggetti di 200 KB o inferiori nei bucket bank-record per il tenant Bank of ABC.
  - Oggetti in qualsiasi altro bucket con S3 Object Lock attivato per tutti gli altri account tenant.

Attivazione del criterio

Quando si è completamente soddisfatti del fatto che il nuovo criterio protegga i dati degli oggetti come previsto, è possibile attivarlo.

Informazioni sul copyright

Informazioni sul marchio commerciale