Gestire gli oggetti con ILM

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

Gestire gli oggetti con ILM . . . 1
- Gestire gli oggetti con ILM . . . 1
- ILM e ciclo di vita degli oggetti . . . 2
- Creare e assegnare i gradi di storage . . . 23
- Utilizzare i pool di storage . . . 25
- Utilizza i Cloud Storage Pools . . . 34
- Gestire i profili di erasure coding . . . 53
- Configurazione delle regioni (opzionale e solo S3) . . . 57
- Creare una regola ILM . . . 58
- Gestire le policy ILM . . . 75
- Utilizzare le policy ILM e le regole ILM . . . 92
- USA blocco oggetti S3 . . . 96
- Esempio di regole e policy ILM . . . 105

Gestire gli oggetti con ILM

Gestire gli oggetti con ILM

Le regole di gestione del ciclo di vita delle informazioni (ILM, Information Lifecycle Management) contenute in un criterio ILM indicano a StorageGRID come creare e distribuire copie dei dati degli oggetti e come gestirle nel tempo.

A proposito di queste istruzioni

La progettazione e l'implementazione di regole e politiche ILM richiedono 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.

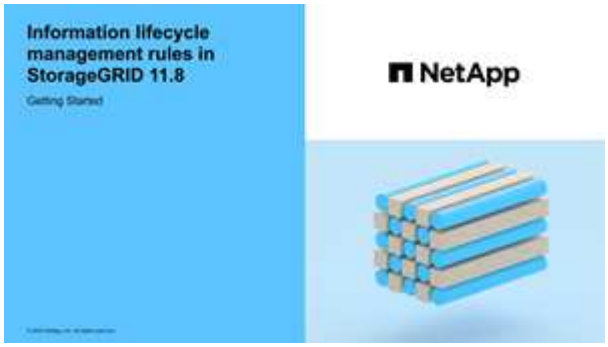
Seguire queste istruzioni per:

- Ulteriori informazioni su StorageGRID ILM, incluso "Come ILM opera per tutta la vita di un oggetto".
- Informazioni sulla configurazione di "pool di storage", , "Pool di cloud storage"e "Regole ILM".
- Scopri come "Creare, simulare e attivare un criterio ILM"proteggere i dati degli oggetti in uno o più siti.
- Imparare come fare "Gestire gli oggetti con S3 Object Lock", che aiuta a garantire che gli oggetti in specifici bucket S3 non vengano eliminati o sovrascritti per un determinato periodo di tempo.

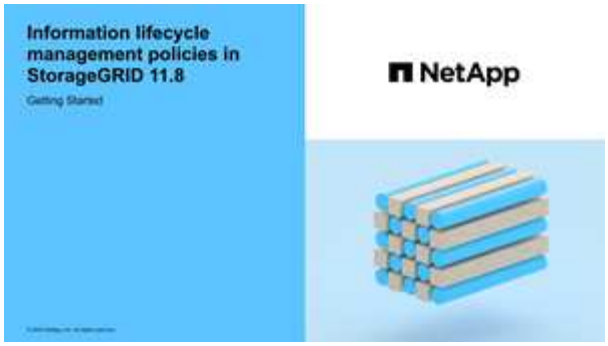
Scopri di più

Per ulteriori informazioni, consulta questi video:

- "Video: Panoramica delle regole ILM".



- "Video: Panoramica dei criteri ILM"



ILM e ciclo di vita degli oggetti

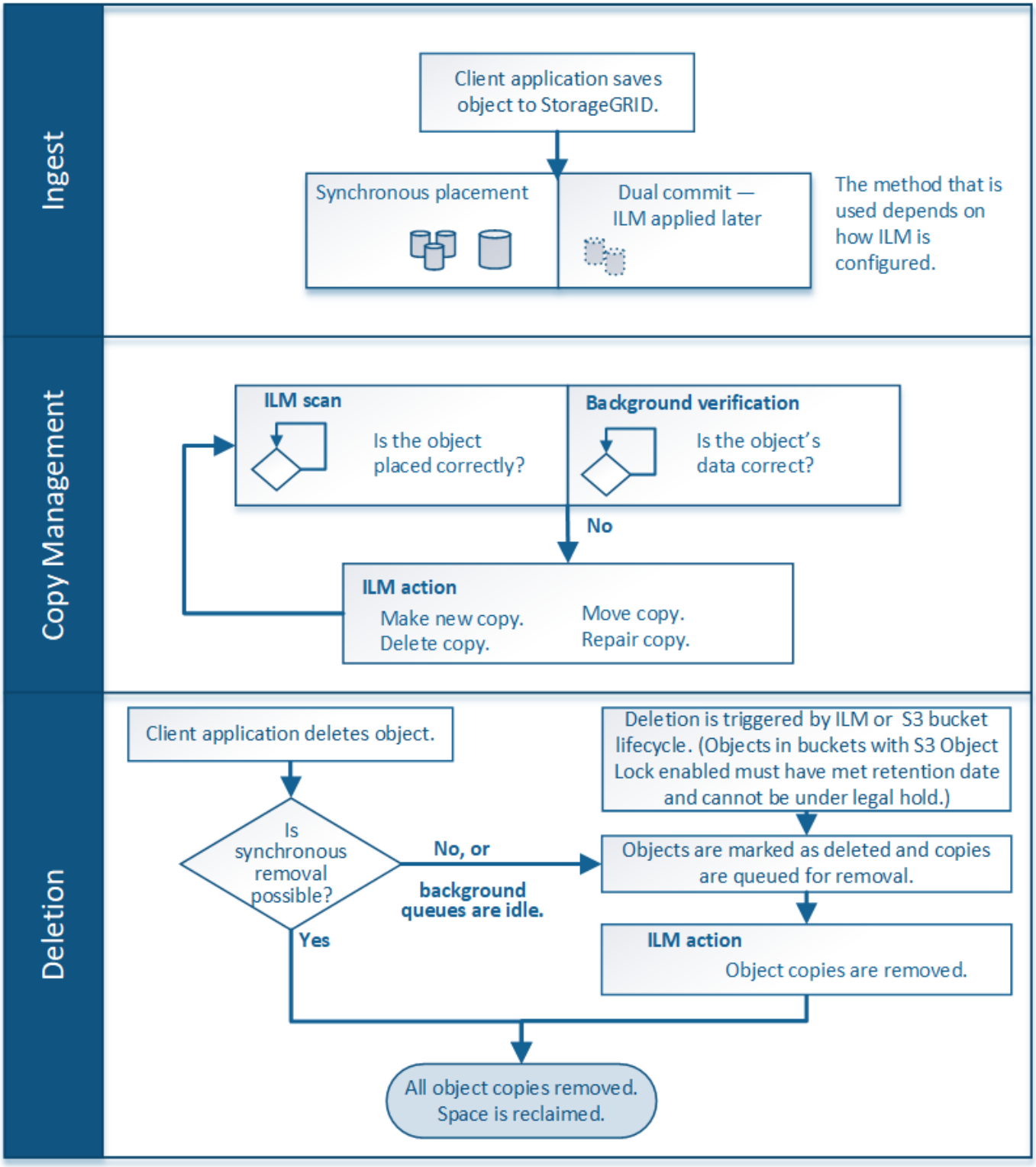
Come ILM opera per tutta la vita di un oggetto

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

- **Acquisizione**: L'acquisizione inizia quando un'applicazione client S3 stabilisce una connessione per salvare un oggetto nel sistema StorageGRID e viene completata quando StorageGRID restituisce un messaggio di acquisizione riuscita 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 la scansione continua dell'elenco degli 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 dello sfondo**: StorageGRID esegue continuamente la verifica dello sfondo 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. Vedere "Verificare l'integrità dell'oggetto".
- **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 stato specificato un periodo di conservazione fino alla data, ma non ancora soddisfatto.

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



Modalità di acquisizione degli oggetti

Opzioni di acquisizione

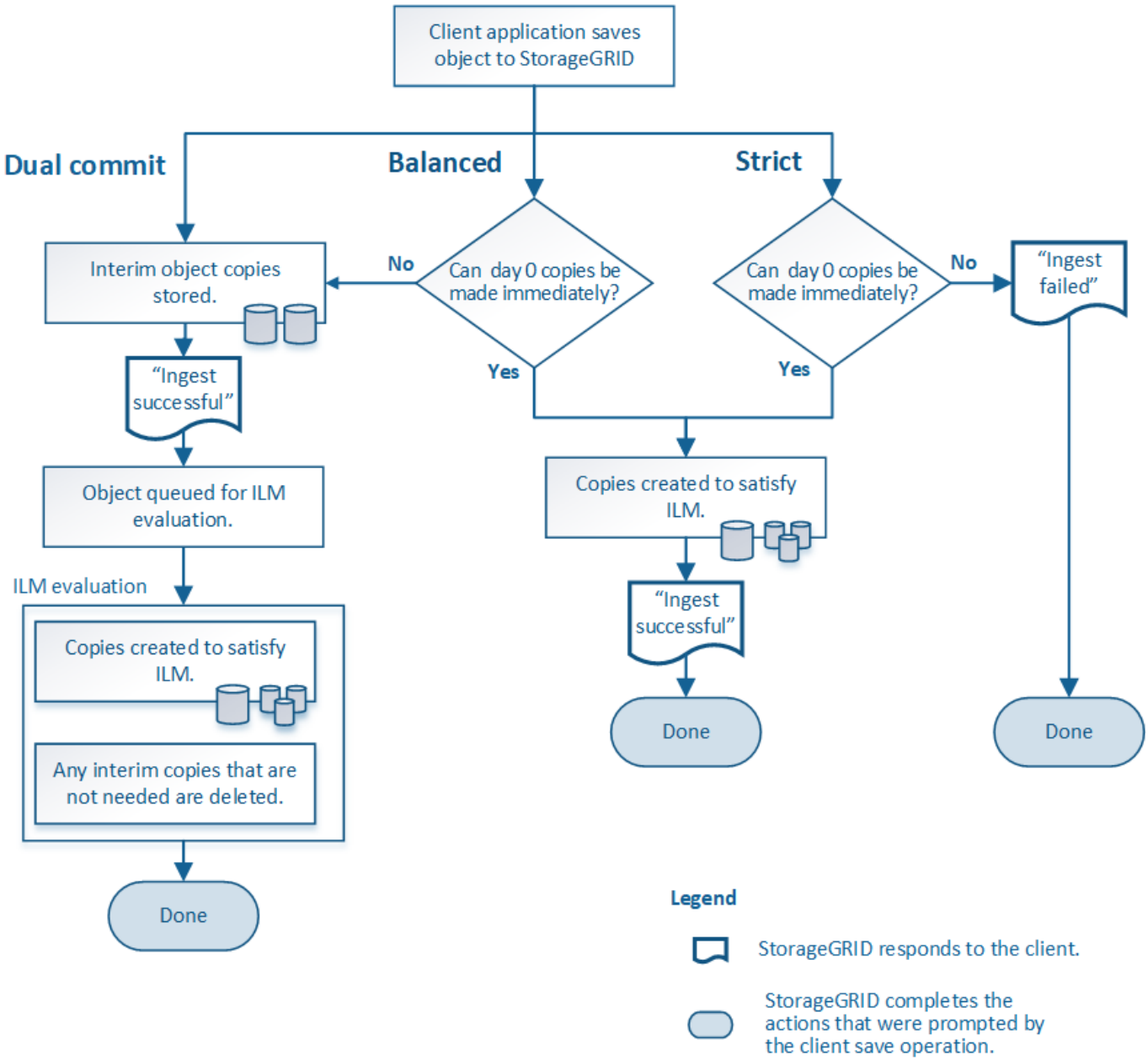
Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Dual commit, strict o Balanced.

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.

Diagramma di flusso delle opzioni di acquisizione

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



Commit doppio

Quando si seleziona l'opzione Dual Commit, StorageGRID crea immediatamente copie temporanee degli oggetti su due diversi nodi storage e restituisce un messaggio "acquisizione riuscita" 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. Se il criterio ILM non può essere elaborato immediatamente dopo il dual commit, la protezione in caso di perdita del sito potrebbe richiedere del tempo.

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.

Bilanciato (impostazione predefinita)

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 immediatamente a fare tutte le copie, utilizza invece il doppio commit. Se la policy ILM utilizza posizionamenti su più siti e non è possibile ottenere una protezione immediata in caso di perdita del sito, viene attivato l'avviso **posizionamento ILM non raggiungibile**.

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 regola ILM.

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 è temporaneamente non disponibile. Il client deve riprovare l'operazione.

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 determinati data center.

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

Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione

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.

Per una panoramica delle opzioni di acquisizione, vedere "Opzioni di acquisizione".

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 o rigorose, non viene restituito al client un messaggio di "acquisizione riuscita" finché non vengono creati e memorizzati tutti i frammenti con erasure coding 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 viene 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 e 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.
- Posizionamenti in un Cloud Storage Pool quando la regola ha un tempo di creazione definito dall'utente come tempo di riferimento.

Queste restrizioni esistono perché StorageGRID non è in grado di eseguire copie in modo sincrono in un pool di archiviazione cloud e un tempo di creazione definito dall'utente potrebbe essere risolto al momento.

L'interazione tra regole ILM e coerenza per influire sulla protezione dei dati

Sia la regola ILM che la scelta della coerenza influiscono sulla 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 la coerenza utilizzata durante la memorizzazione di un oggetto influisce sul posizionamento iniziale dei metadati degli oggetti. Poiché StorageGRID richiede l'accesso sia ai dati dell'oggetto che ai metadati per soddisfare le richieste del client, la selezione di livelli di protezione corrispondenti per il comportamento di coerenza e acquisizione può offrire una migliore protezione iniziale dei dati e risposte del sistema più prevedibili.

Di seguito viene riportato un breve riepilogo dei valori di coerenza disponibili in StorageGRID:

- **All**: Tutti i nodi ricevono immediatamente i metadati degli oggetti o la richiesta non riesce.
- **Strong-Global**: I metadati degli oggetti vengono immediatamente distribuiti 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 immediatamente distribuiti 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 lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

> Prima di selezionare un valore di coerenza, "leggi la descrizione completa della coerenza". Prima di modificare il valore predefinito, è necessario comprendere i vantaggi e le limitazioni.

Esempio di interazione tra le regole di coerenza e ILM

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

- **ILM rule**: Creare due copie di oggetti, una nel sito locale e una in un sito remoto. USA un comportamento di acquisizione rigoroso.
- **Coerenza**: Strong-Global (i metadati degli oggetti vengono immediatamente distribuiti 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 si è utilizzata la stessa regola ILM e la coerenza del sito sicuro, 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'interrelazione tra coerenza e regole ILM può essere complessa. Contattare NetApp per assistenza.

Informazioni correlate

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

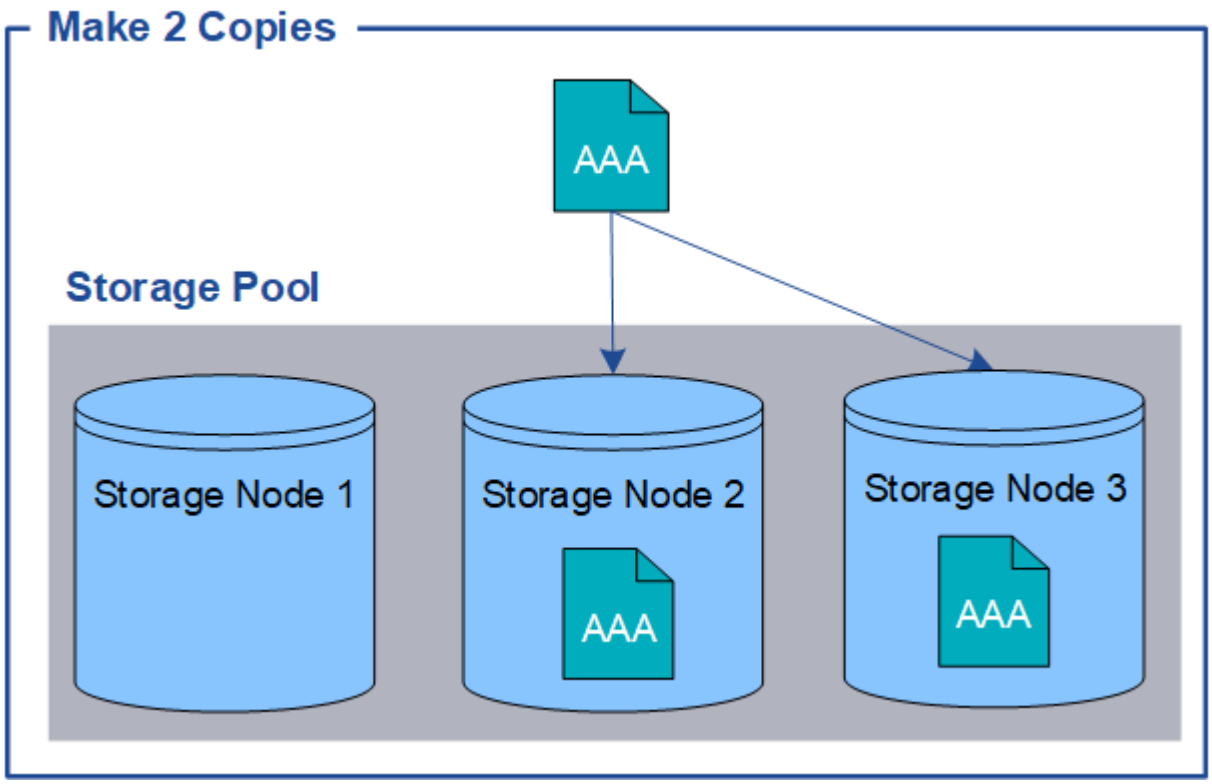
Modalità di archiviazione degli oggetti (replica o erasure coding)

Che cos'è la replica?

La replica è uno dei due metodi utilizzati da StorageGRID per archiviare i dati degli oggetti (l'erasure coding è l'altro metodo). Quando gli oggetti corrispondono a una regola ILM che utilizza la replica, il sistema crea copie esatte dei dati dell'oggetto e memorizza le copie sui nodi storage.

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

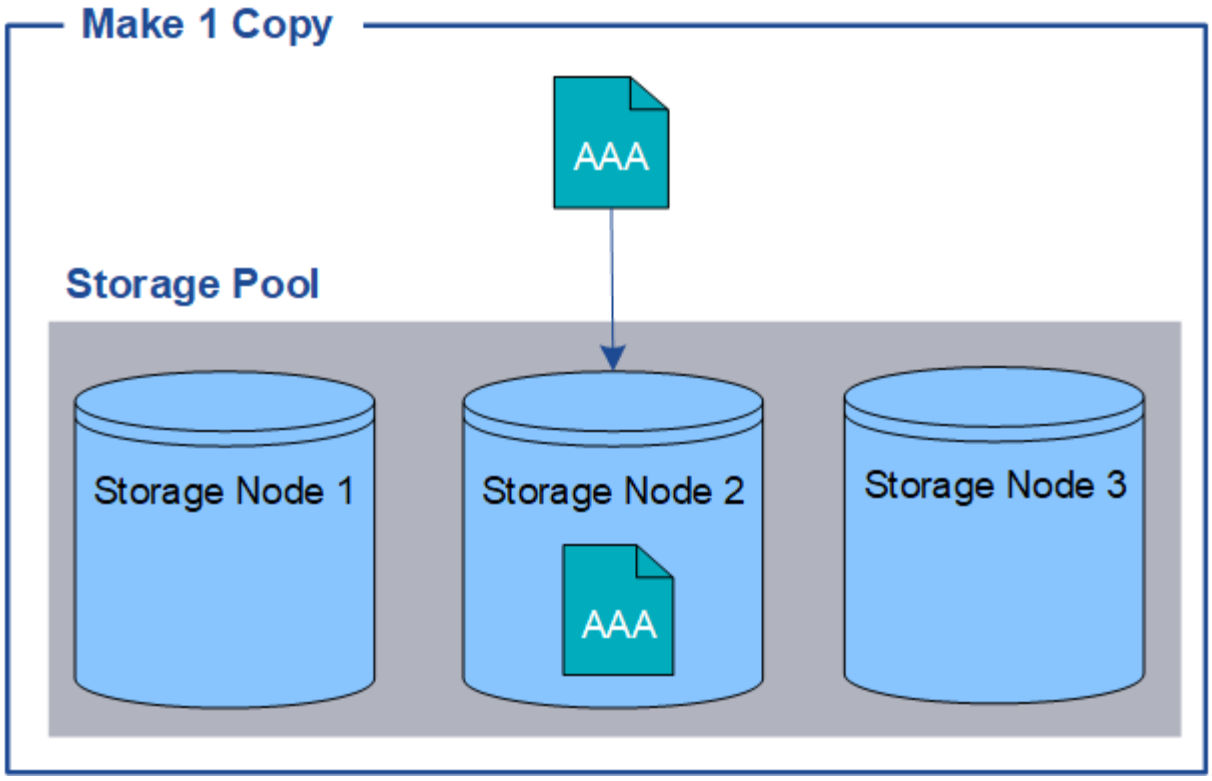
- "Che cos'è l'erasure coding"
- "Che cos'è un pool di storage"
- "Abilita la protezione contro la perdita di sito utilizzando la replica e l'erasure coding"

Perché non utilizzare la replica a copia singola

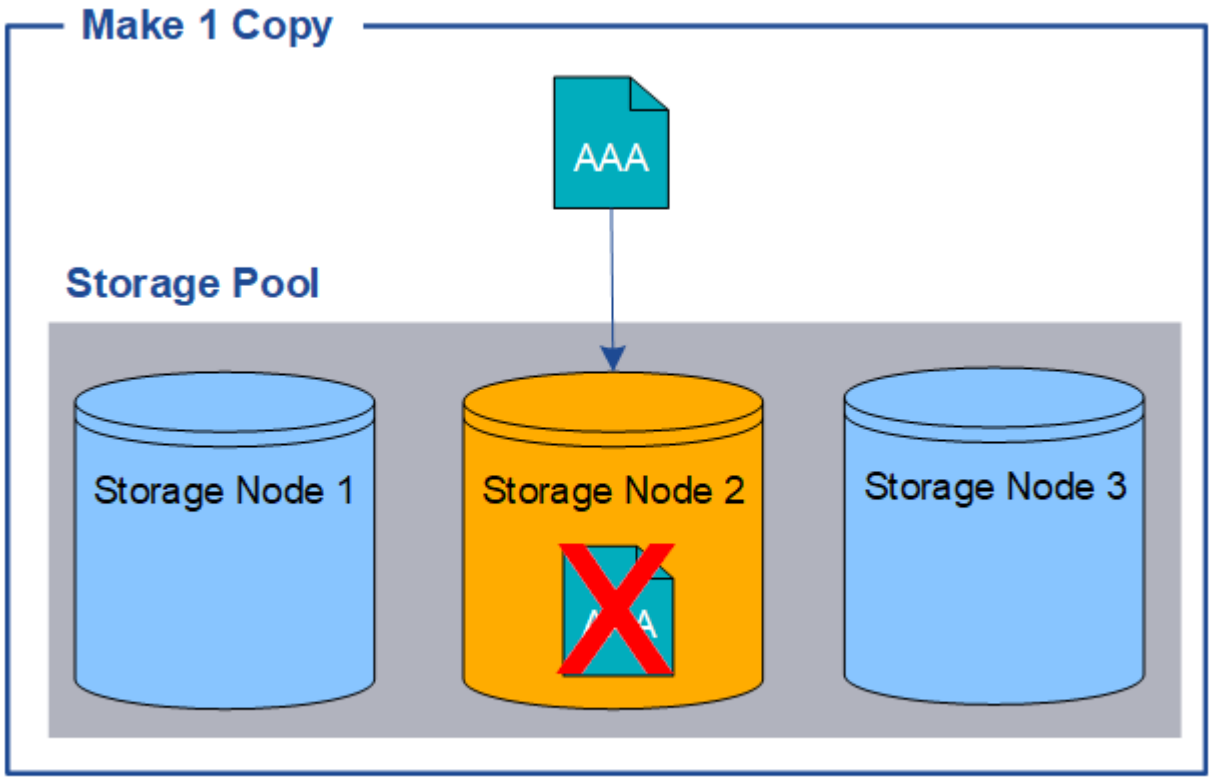
Quando si crea una regola ILM per creare copie replicate, è necessario specificare almeno due copie per un periodo di tempo qualsiasi nelle istruzioni di posizionamento.

> 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.

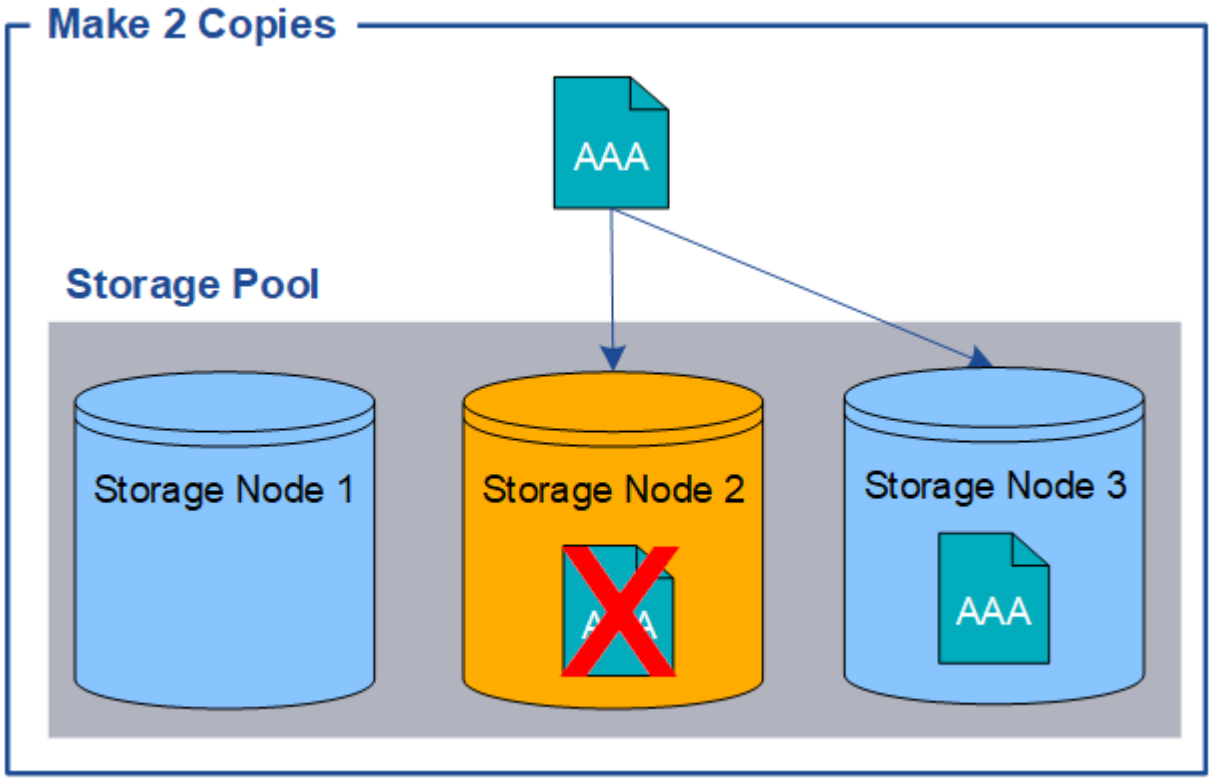
Nell'esempio seguente, la regola Make 1 Copy ILM specifica che una copia replicata di un oggetto deve essere inserita in un pool di storage che contiene tre nodi di storage. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID inserisce una singola copia su un solo nodo di storage.



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.



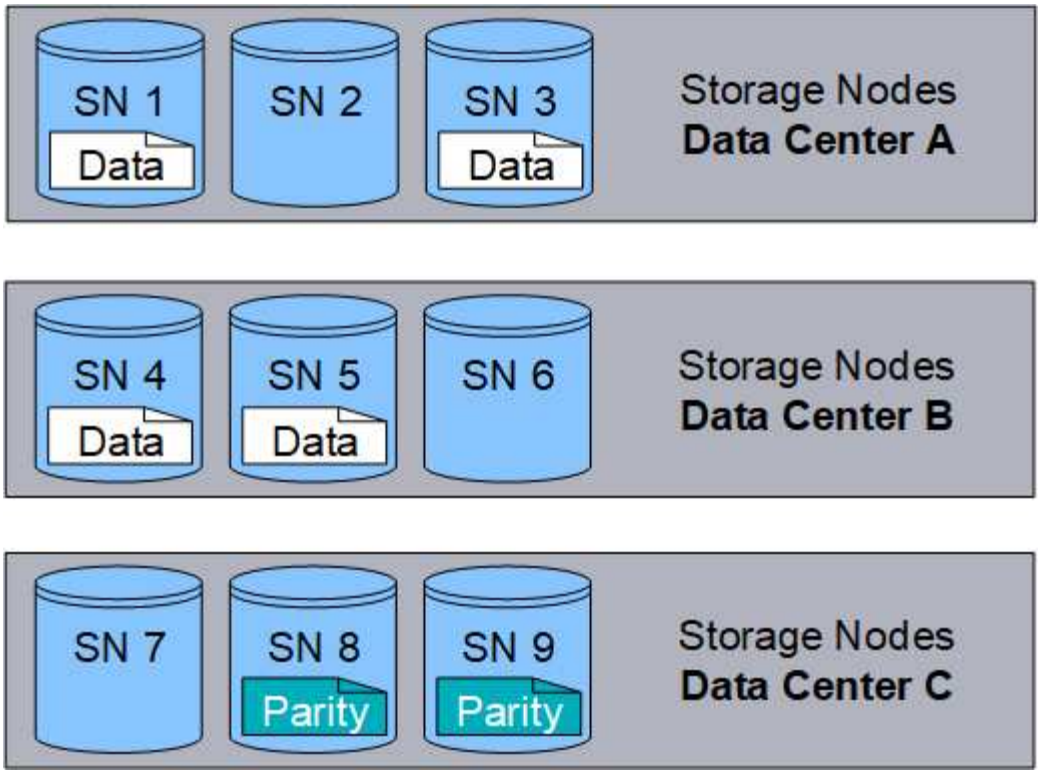
Cos'è la codifica erasure?

L'erasure coding è uno dei due metodi utilizzati da StorageGRID per memorizzare i dati degli oggetti (l'altro metodo è la replica). Quando gli oggetti corrispondono a una regola ILM che utilizza la codifica erasure, vengono suddivisi in frammenti di dati, vengono calcolati ulteriori frammenti di parità e ciascun frammento viene memorizzato in un nodo di storage diverso.

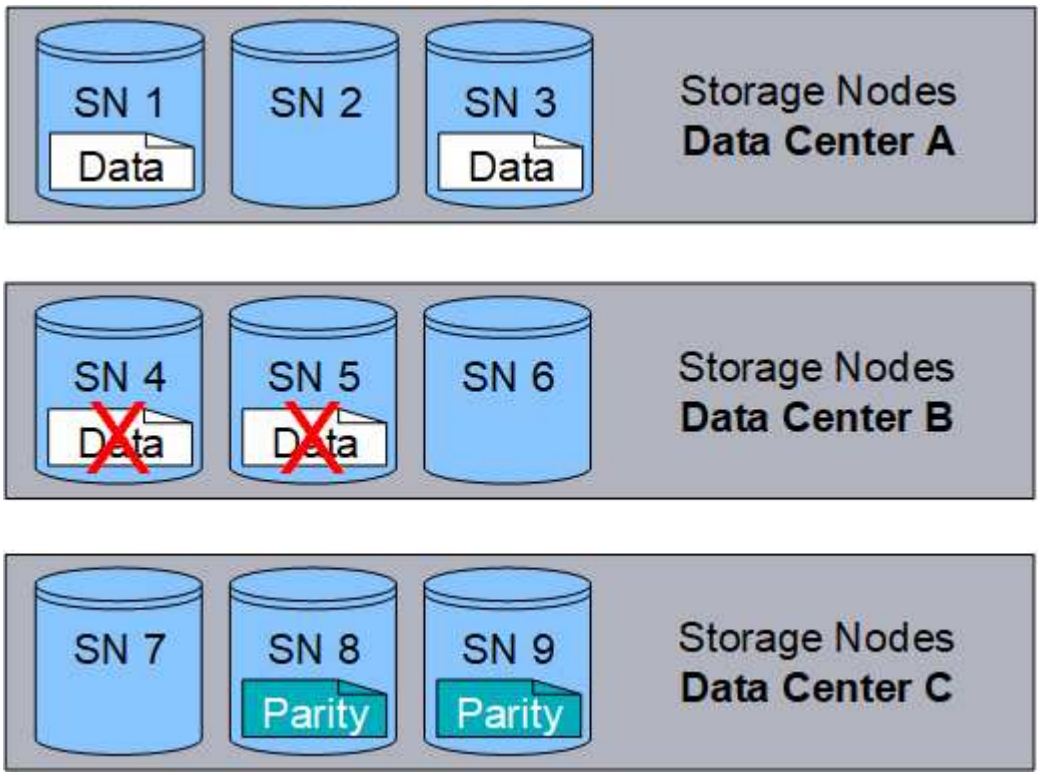
Quando si accede a un oggetto, questo viene riassemblato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità viene corrotto o perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei dati rimanenti e dei frammenti di parità.

Quando crei regole ILM, StorageGRID crea profili di erasure coding in grado di supportarle. È possibile visualizzare un elenco di profili di erasure coding, "rinominare un profilo con erasure coding", o "Disattivare un profilo di erasure coding se non è attualmente utilizzato in nessuna regola ILM".

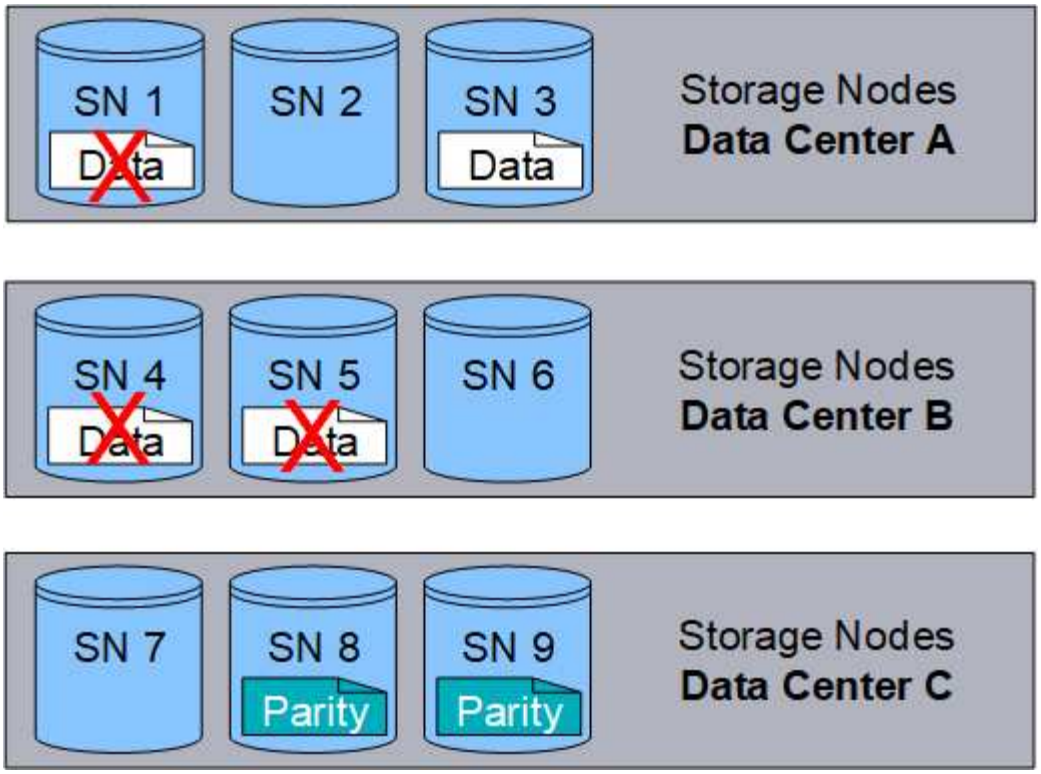
Nell'esempio seguente viene illustrato l'utilizzo di un algoritmo di erasure coding sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di erasure coding 4+2. Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati 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 può essere configurato in vari modi. Ad esempio, è possibile configurare un pool di storage a sito singolo che contiene sei nodi di storage. Per "protezione contro la perdita di sito", è possibile utilizzare un pool di archiviazione contenente tre siti con tre nodi di archiviazione in ciascun sito. 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, 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

- "Cos'è la replica"
- "Che cos'è un pool di storage"
- "Cosa sono gli schemi di erasure coding"
- "Rinominare un profilo con erasure coding"
- "Disattivare un profilo di erasure coding"

Cosa sono gli schemi di erasure coding?

Gli schemi di erasure coding controllano il numero di frammenti di dati e il numero di frammenti di parità creati per ciascun oggetto.

Quando si crea o modifica una regola ILM, si seleziona uno schema di erasure coding disponibile. StorageGRID crea automaticamente schemi di erasure coding in base al numero di nodi e siti storage che compongono il pool di storage che intendi utilizzare.

Protezione dei dati

Il sistema StorageGRID utilizza l'algoritmo di erasure coding Reed-Solomon. L'algoritmo suddivide un oggetto in `k` frammenti di dati e calcola i `m` frammenti di parità.

I `k + m = n` fragment sono distribuiti nei `n` nodi storage per garantire la protezione dei dati nel modo seguente:

- Per recuperare o riparare un oggetto, `k` sono necessari dei frammenti.
- Un oggetto può sopportare `m` frammenti persi o corrotti. Maggiore è il valore di `m`, maggiore è la tolleranza di errore.

La migliore data Protection è fornita dallo schema di erasure coding con la tolleranza ai guasti del nodo o del volume più elevata all'interno di un pool di storage.

Overhead dello storage

L'overhead di memorizzazione 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` quello che soddisfa le tue esigenze. Gli schemi di erasure coding con un numero inferiore di frammenti sono più efficienti dal punto di vista computazionale perché:

- Viene creato e distribuito (o recuperato) un numero inferiore di frammenti per oggetto
- Mostrano prestazioni migliori perché le dimensioni del frammento sono maggiori
- Possono richiedere un numero inferiore di nodi da aggiungere in un "espansione quando è richiesto più storage"

Linee guida per i pool di storage

Quando si seleziona il pool di storage da utilizzare per una regola che crea una copia con codice di cancellazione, utilizzare le 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 utilizzare la codifica di cancellazione 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 un pool di archiviazione che includa il sito All Sites.
- Il pool di storage deve includere almeno nodi storage `k+m +1` in grado di memorizzare i dati degli oggetti.

  > I nodi di storage possono essere configurati durante l'installazione in modo da contenere solo metadati di oggetti e non dati di oggetti. Per ulteriori informazioni, vedere "Tipi di nodi storage".

  Il numero minimo di nodi di archiviazione 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.

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 una protezione contro la perdita di sito. È possibile perdere un sito e l'oggetto sarà ancora accessibile.

Per gli schemi di erasure coding che forniscono la protezione in caso di perdita di sito, il numero consigliato di nodi storage nel pool di storage supera `k+m +1` poiché ciascun sito richiede un minimo di tre nodi 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%
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 Fault tolerance è aumentata avendo più segmenti di parità (cioè, quando `m` ha un valore più alto).
- **Traffico di rete**: Quando si effettua il recupero da errori, utilizzando uno schema con più frammenti (cioè un totale più elevato per `k+m`) si 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 archiviazione richiesto è `k+m`, ma si consiglia un pool di archiviazione con `k+m +1` nodi di archiviazione. 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%
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%

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 che è sottoposto a erasure coding in tre siti con uno schema di erasure coding 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 consigliato un maggior numero di siti e nodi di storage, a seconda dello schema di erasure coding. Al contrario, se si replicano i dati degli oggetti, è necessario un solo nodo di storage per ogni copia. Vedere "Schemi di erasure coding per pool di storage contenenti tre o più siti" e "Schemi di erasure coding per pool di storage a sito singolo".
- Aumento dei costi e della complessità delle espansioni dello storage. Per espandere un'implementazione che utilizza la replica, è necessario 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 storage, ma se si espandono quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e massimizzare la capacità dello storage utilizzabile. Per ulteriori informazioni, vedere "Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione".
- L'utilizzo di erasure coding in siti distribuiti geograficamente aumenta le latenze di recupero. I frammenti di oggetto per un oggetto sottoposto a erasure coding e distribuito tra i siti remoti richiedono più tempo per il recupero su connessioni WAN rispetto a un oggetto replicato e disponibile in locale (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.

L'erasure coding è più adatto per oggetti superiori a 1 MB. 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.

- 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.

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 tenant possono utilizzare questi metodi per controllare la durata della memorizzazione degli oggetti in StorageGRID:

- Se l'impostazione blocco oggetto S3 globale è attivata per la griglia, gli utenti tenant S3 possono creare bucket con blocco oggetto S3 abilitato e quindi selezionare un **periodo di conservazione predefinito** per ciascun bucket.
- 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 soggetta a blocco legale non può essere eliminata da 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 blocco oggetti S3 abilitato vengono conservati da ILM "per sempre". 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. Vedere "Gestire gli 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. Vedere "Creare la configurazione del ciclo di vita S3".
- Un client S3 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 di grid possono utilizzare questi metodi per controllare la conservazione degli oggetti:

- Impostare un periodo di conservazione massimo per il blocco degli oggetti S3 per ogni tenant. Quindi, gli utenti tenant possono impostare un periodo di conservazione predefinito per ciascun bucket. Il periodo di conservazione massimo viene applicato anche a tutti gli oggetti appena acquisiti per quel bucket (Retain-until-date dell'oggetto).
- Creare le istruzioni di posizionamento ILM per controllare la durata di 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 per le istruzioni di posizionamento viene specificato "per sempre".
- Indipendentemente da chi controlla la durata della conservazione degli oggetti, le impostazioni ILM determinano i tipi di copie degli oggetti (replicate o sottoposte a erasure coding) archiviati e la posizione delle copie (nodi storage o pool di cloud storage).

Come interagiscono il ciclo di vita del bucket S3 e ILM

Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita. 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 storage "per sempre"

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 storage "per sempre"

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.

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 richiede l'eliminazione e una o più di queste condizioni sono vere: ◦ Impossibile eliminare le copie entro 30 secondi perché, ad esempio, 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 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 S3 client effettuano richieste di eliminazione, StorageGRID inizia aggiungendo 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.

Tempo necessario per eliminare 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 sta monitorando attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, è possibile notare che la velocità di eliminazione sembra essere lenta 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.

La quantità di tempo necessaria 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 in 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 un marcatore di eliminazione di zero byte come versione corrente dell'oggetto, rendendo la versione precedente dell'oggetto "non corrente". Un marcatore di eliminazione di un oggetto diventa un marcatore di eliminazione di un oggetto scaduto quando è la versione corrente e non ci sono versioni non correnti.

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 quando si eliminano gli oggetti con versione o per rimuovere i marcatori di eliminazione, utilizzare una delle seguenti opzioni:

- **S3 client request**: Specificare l'ID della versione dell'oggetto nella richiesta di ELIMINAZIONE DELL'oggetto S3 (`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 benna**: Utilizzare l' `NoncurrentVersionExpiration`azione nella configurazione del ciclo di vita benna. 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.

  L' `NewerNoncurrentVersions`azione nella configurazione del ciclo di vita del bucket specifica il numero di versioni non correnti mantenute in un bucket S3 versione. Se sono presenti più versioni non correnti di quelle `NewerNoncurrentVersions` specificate, StorageGRID rimuove le versioni precedenti una volta scaduto il valore NoncurrentDays. La `NewerNoncurrentVersions` soglia sovrascrive le regole del ciclo di vita fornite da ILM, il che significa che un oggetto non corrente con una versione compresa nella `NewerNoncurrentVersions` soglia viene mantenuto se ILM richiede la sua eliminazione.

  Per rimuovere i marcatori di eliminazione degli oggetti scaduti, utilizzare l' `Expiration`azione con uno dei seguenti tag: `ExpiredObjectDeleteMarker`, , `Days` O `Date`.

- **ILM**: "Clonazione di una policy attiva" E aggiungere due regole ILM alla nuova policy:

    - Prima regola: Utilizzare "ora non corrente" come ora di riferimento per far corrispondere le versioni non correnti dell'oggetto. In "Fase 1 (immettere i dettagli) della procedura guidata Crea una regola ILM", selezionare **Sì** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?"
    - Seconda regola: Utilizzare **Ingest Time** per corrispondere alla versione corrente. La regola "ora non corrente" deve essere visualizzata nel criterio sopra la regola **ora acquisizione**.

      Per rimuovere i marcatori di eliminazione degli oggetti scaduti, utilizzare una regola **tempo di acquisizione** che corrisponda ai marcatori di eliminazione correnti. I marcatori di eliminazione vengono rimossi solo quando è trascorso un **periodo di tempo** di **giorni** e il creatore di eliminazione corrente è scaduto (non ci sono versioni non correnti).

- **Elimina oggetti nel bucket**: Utilizza il gestore tenant per "elimina tutte le versioni degli oggetti", compresi i marcatori di eliminazione, da un bucket.

Quando un oggetto con versione viene eliminato, StorageGRID crea un marcatore di eliminazione a byte zero come versione corrente dell'oggetto. Tutti gli oggetti e i marcatori di eliminazione devono essere rimossi prima di poter eliminare un bucket in versione.

- I marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti possono essere rimossi solo tramite richieste client S3, ma non tramite ILM, regole del ciclo di vita bucket o Elimina oggetti nelle operazioni bucket.
- I marcatori di eliminazione da un bucket creato in StorageGRID 11,8 o versioni successive possono essere rimossi da ILM, regole del ciclo di vita bucket, Elimina oggetti nelle operazioni bucket o un'eliminazione client S3 esplicita.

Informazioni correlate

- "UTILIZZARE L'API REST S3"
- "Esempio 4: Regole ILM e policy per gli oggetti con versione S3"

Creare e assegnare i 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.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".

A proposito di questa attività

Quando si installa StorageGRID per la prima volta, il livello di storage **predefinito** viene assegnato automaticamente a ogni nodo di storage del sistema. In base alle esigenze, è possibile definire gradazioni di storage personalizzate e assegnarle a diversi nodi di storage.

L'utilizzo di storage grades personalizzati consente di creare pool di storage ILM che contengono solo un tipo specifico di Storage Node. Ad esempio, è possibile che alcuni oggetti vengano memorizzati nei nodi di storage più veloci, ad esempio le appliance di storage all-flash StorageGRID.

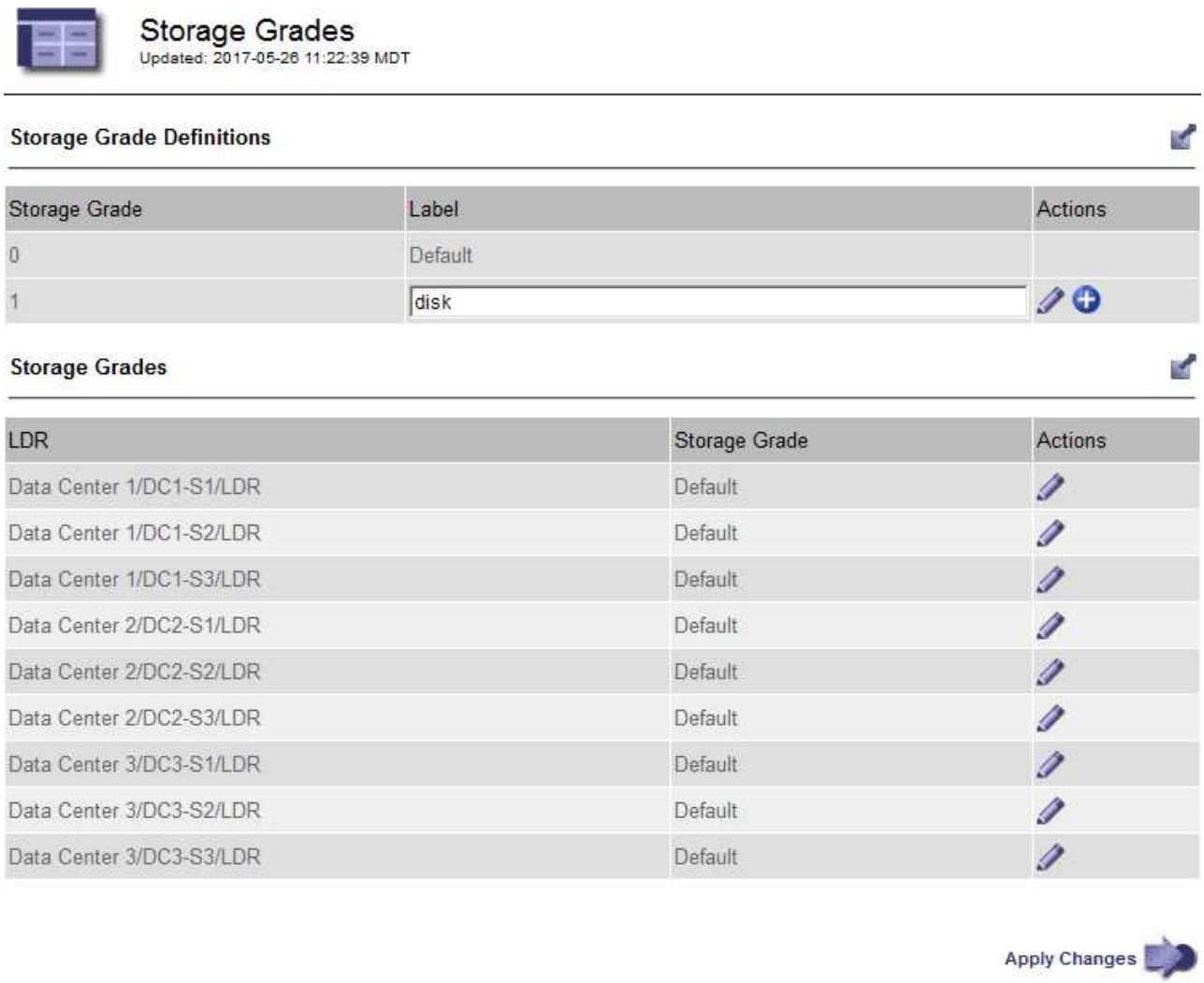
I nodi di storage possono essere configurati durante l'installazione in modo da contenere solo metadati di oggetti e non dati di oggetti. Ai nodi di storage con soli metadati non può essere assegnato un livello di storage. Per ulteriori informazioni, vedere "Tipi di nodi storage".

Se il grado di archiviazione non è un problema (ad esempio, tutti i nodi di archiviazione sono identici), è possibile ignorare questa procedura e utilizzare la selezione **include tutti i gradi di archiviazione** per il grado di archiviazione quando si "creare pool di storage". L'utilizzo di questa selezione garantisce che il pool di storage includa ogni nodo di storage del sito, indipendentemente dal suo livello di storage.

Non creare più storage di quanto 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. Definire i livelli di storage personalizzati:
   a. Per ogni grado di archiviazione personalizzato che si desidera aggiungere, selezionare **Inserisci** per aggiungere una riga.
   b. Inserire un'etichetta descrittiva.



c. Selezionare **Applica modifiche**.

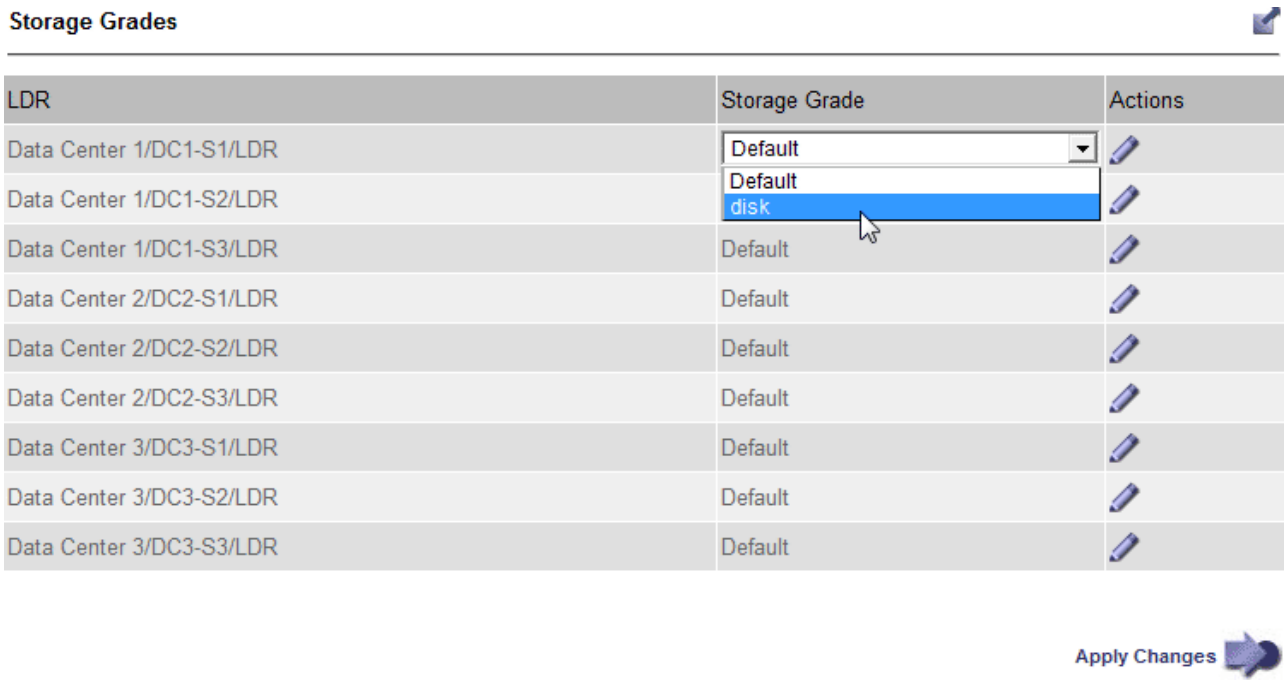
d. In alternativa, se è necessario modificare un'etichetta salvata, selezionare **Modifica** e selezionare **Applica modifiche**.

Non puoi eliminare i gradi di storage.

3. Assegnare nuovi gradi di storage ai nodi di storage:

a. Individuare il nodo di archiviazione nell'elenco LDR e selezionare la relativa icona **Modifica**.

b. Selezionare il livello di storage appropriato 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 della policy ILM. Se l'assegnazione viene modificata, i dati vengono memorizzati in base al nuovo livello di storage.

a. Selezionare **Applica modifiche**.

Utilizzare i pool di storage

Che cos'è un pool di storage?

Un pool di storage è un raggruppamento logico di nodi storage.

Quando si installa StorageGRID, viene creato automaticamente un pool di storage per sito. È possibile configurare ulteriori pool di storage in base alle esigenze di storage.

È possibile configurare i nodi di storage durante l'installazione in modo che contengano dati di oggetti e metadati di oggetti o solo metadati di oggetti. I nodi di storage solo metadati non possono essere utilizzati nei pool di storage. Per ulteriori informazioni, vedere "Tipi di nodi storage".

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 e il tipo di storage utilizzato. Quando si configurano le regole ILM per la replica, si selezionano uno o più pool di storage.

Linee guida per la creazione di pool di storage

Configurare e utilizzare i pool di storage per proteggersi dalla perdita di dati distribuendo i dati su più siti. Le copie replicate e le copie con codice di cancellazione richiedono diverse configurazioni del pool di storage.

Vedere "Esempi di attivazione della protezione dalle perdite di sito mediante la replica e la cancellazione del codice".

Linee guida per tutti i pool di storage

- 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.
- In generale, non utilizzare il pool di storage All Storage Node (StorageGRID 11.6 e versioni precedenti) o il sito All Sites. Questi elementi vengono aggiornati automaticamente per includere i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato.

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

- Per la protezione contro la perdita del sito mediante "replica", specificare uno o più pool di archiviazione specifici del sito in "Istruzioni di posizionamento per ogni regola ILM".

  Un pool di storage viene creato automaticamente per ogni sito durante l'installazione di StorageGRID.

  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 che contenga solo il nuovo sito. Quindi, "Aggiornare le regole ILM" per controllare quali oggetti vengono memorizzati nel nuovo sito.
- Se il numero di copie è inferiore al numero di pool di storage, il sistema distribuisce le copie per bilanciare

l'utilizzo del disco tra i pool.

- 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.

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

- Per la protezione delle perdite di sito mediante "erasure coding", creare pool di archiviazione composti da almeno tre siti. 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.
- Il numero di nodi e siti di archiviazione contenuti nel pool di archiviazione determina quali "schemi di erasure coding" sono disponibili.
- 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.
- Se si hanno requisiti di throughput elevati, si sconsiglia di utilizzare un pool di storage che include più siti 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 vengono selezionati come comportamento di acquisizione bilanciati o rigorosi) o può portare a backlog di coda ILM (quando viene selezionato il doppio commit come comportamento di acquisizione). Vedere "Comportamento di acquisizione delle regole ILM".

> ⓘ Se il grid include un solo sito, è impossibile utilizzare il pool di storage All Storage Nodes (StorageGRID 11,6 e versioni precedenti) o il sito All Sites in un profilo di erasure coding. Questo comportamento impedisce che il profilo diventi non valido se viene aggiunto un secondo sito.

Abilita la protezione contro la perdita di sito

Se l'implementazione di StorageGRID include più di un sito, è possibile utilizzare la replica e la cancellazione del codice con pool di storage configurati in modo appropriato per abilitare la protezione dalla perdita di sito.

La replica e l'erasure coding richiedono diverse configurazioni del pool di storage:

- Per utilizzare la replica per la protezione dalla perdita di sito, utilizzare i pool di storage specifici del sito creati automaticamente durante l'installazione di StorageGRID. Quindi, creare regole ILM "istruzioni per il posizionamento"che specificano più pool di storage in modo da collocare una copia di ciascun oggetto in ogni sito.
- Per utilizzare l'erasure coding per la protezione in caso di perdita del sito, "creare pool di storage composti da più siti". Quindi, creare regole ILM che utilizzano un pool di storage costituito da più siti e qualsiasi schema di erasure coding disponibile.

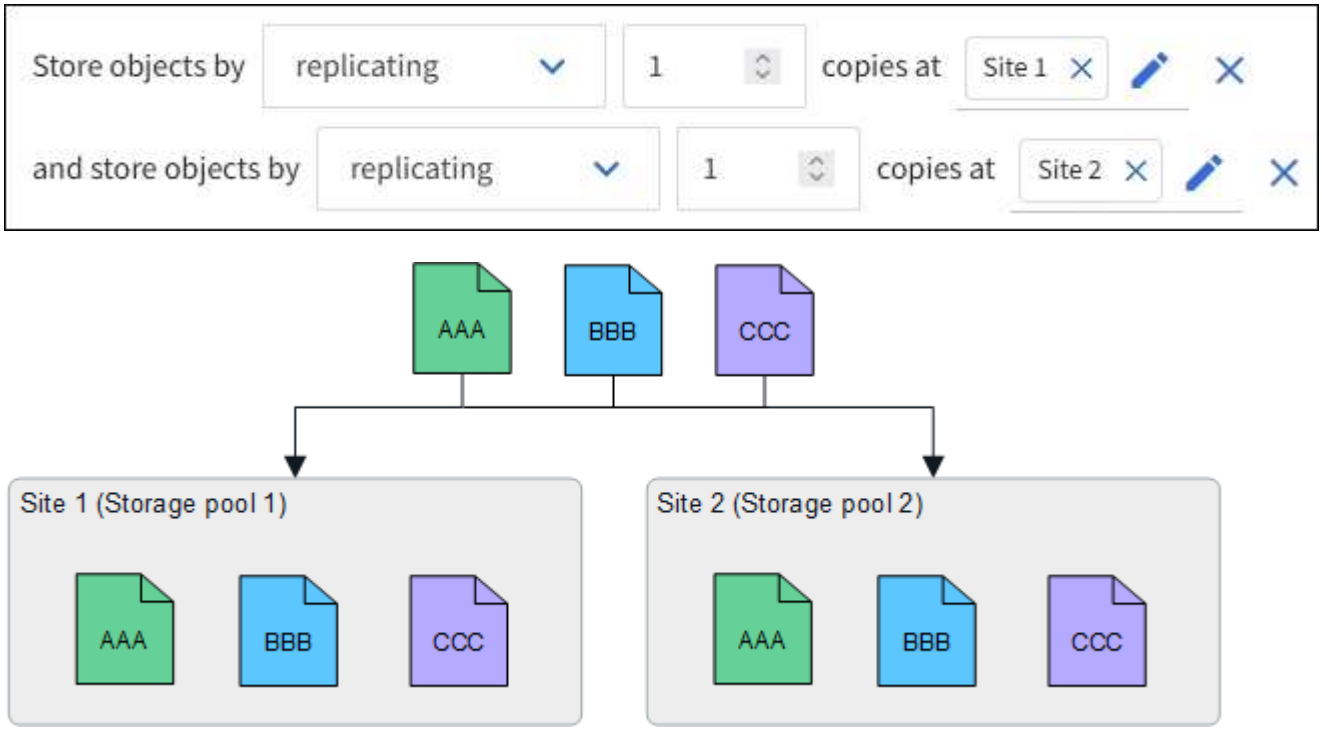
Quando si configura la distribuzione di StorageGRID per la protezione contro la perdita di siti, è necessario tenere conto anche degli effetti di "opzioni di acquisizione" e "coerenza".

Esempio di replica

Per impostazione predefinita, viene creato un pool di storage per ciascun sito durante l'installazione di StorageGRID. La disponibilità di pool di storage costituiti da un solo sito consente di configurare le regole ILM che utilizzano la replica per la protezione dalla perdita di sito. In questo esempio:

- Il pool di archiviazione 1 contiene il sito 1
- Il pool di archiviazione 2 contiene il sito 2
- La regola ILM contiene due posizioni:
  - Memorizzare gli oggetti replicando 1 copia nel sito 1
  - Memorizzare gli oggetti replicando 1 copia nel sito 2

Posizionamento delle regole ILM:



In caso di perdita di un sito, le copie degli oggetti sono disponibili nell'altro sito.

Esempio di erasure coding

La disponibilità di pool di storage costituiti da più di un sito per pool di storage consente di configurare le regole ILM che utilizzano la codifica di cancellazione per la protezione dalla perdita di sito. In questo esempio:

- Il pool di storage 1 contiene i siti da 1 a 3
- La regola ILM contiene un unico posizionamento: Memorizzare gli oggetti tramite erasure coding utilizzando uno schema EC 4+2 nello Storage Pool 1, che contiene tre siti

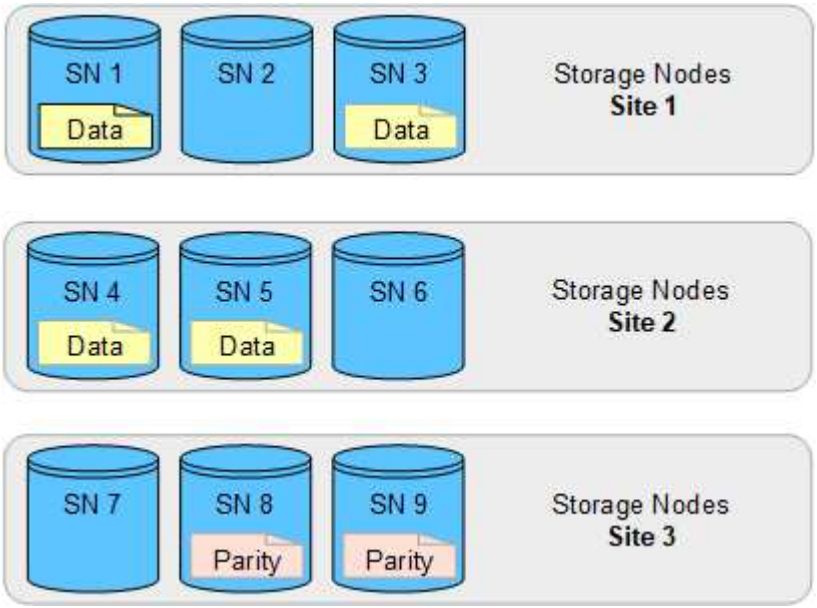
Posizionamento delle regole ILM:

In questo esempio:

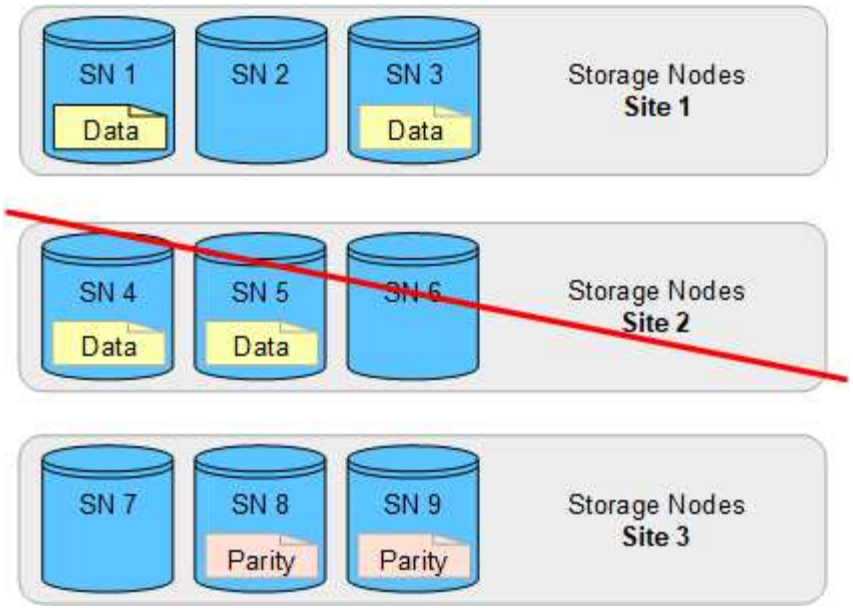
- La regola ILM utilizza uno schema di erasure coding 4+2.
- Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati dell'oggetto.
- Ciascuno dei sei frammenti viene memorizzato su un nodo diverso in tre siti del data center per fornire protezione dei dati in caso di guasti al nodo o perdita del sito.

La codifica di cancellazione è consentita nei pool di storage contenenti un numero qualsiasi di siti, ad eccezione di due siti.

Regola ILM con schema di erasure coding 4+2:



In caso di perdita di un sito, è possibile recuperare i dati:



Creare 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.

> Quando si installa StorageGRID 11,9 su un nuovo grid, vengono creati automaticamente dei pool di storage per ogni sito. Tuttavia, se inizialmente è stato installato StorageGRID 11,6 o versione precedente, i pool di storage non vengono creati automaticamente per ogni sito.

Se si desidera creare pool di cloud storage per archiviare i dati degli oggetti al di fuori del sistema StorageGRID, vedere la "Informazioni sull'utilizzo dei Cloud Storage Pools".

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".
- Hai 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.

> Non includere il sito All Sites in un pool di storage che verrà utilizzato in un profilo di erasure coding. Invece, Aggiungi una voce separata al pool di storage per ogni sito che memorizzerà i dati sottoposti a erasure coding. Vedere questo passo per un 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. Consultare la "Linee guida per la creazione di pool di storage".

Fasi

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

   La scheda Storage Pools elenca tutti i pool di storage definiti.

   > Per le nuove installazioni di StorageGRID 11.6 o versioni precedenti, il pool di storage di tutti i nodi di storage viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti del data center. Non utilizzare questo pool nelle regole ILM.

2. Per creare un nuovo pool di storage, selezionare **Crea**.
3. Immettere un nome univoco per il pool di storage. Utilizzare un nome che sia facile da identificare quando si configurano i profili di erasure coding 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 archiviazione nella tabella viene aggiornato automaticamente.

   In generale, non utilizzare il sito All Sites in alcun pool di storage. Le regole ILM che utilizzano un pool di storage All Sites posizionano gli oggetti in qualsiasi sito disponibile, offrendo un minore controllo sul posizionamento degli oggetti. Inoltre, un pool di storage All Sites utilizza immediatamente i nodi di storage in un nuovo sito, il che potrebbe non essere il comportamento previsto.

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

   Il grado dello storage, *include tutti i gradi dello storage*, include tutti i nodi storage 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 archiviazione in un profilo di erasure coding multisito, selezionare **Aggiungi più nodi** per aggiungere una voce per ciascun sito al pool di archiviazione.

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

   Per rimuovere una voce, selezionare l'icona Elimina ✕.

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

   Il nuovo pool di storage viene aggiunto all'elenco.

Visualizzare i 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.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

- Si dispone di "autorizzazioni di accesso specifiche".

Fasi

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

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

   - **Name**: Il nome univoco del pool di storage.
   - **Node count**: Numero di nodi nel pool di storage.
   - **Utilizzo dello storage**: Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto su questo nodo. Questo valore non include i metadati degli oggetti.
   - **Capacità totale**: Dimensione del pool di storage, che equivale alla quantità totale di spazio utilizzabile per i dati oggetto per tutti i nodi del pool di storage.
   - **Utilizzo ILM**: Modalità di utilizzo del pool di storage. Un pool di storage potrebbe essere inutilizzato o potrebbe essere utilizzato in una o più regole ILM, profili di erasure coding o entrambe.

2. Per visualizzare i dettagli di un pool di archiviazione specifico, selezionarne il nome.

   Viene visualizzata la pagina dei dettagli del pool di storage.

3. Visualizzare la scheda **nodi** per informazioni sui nodi di archiviazione inclusi nel pool di archiviazione.

   La tabella include le seguenti informazioni per ciascun nodo:

   - Nome del nodo
   - Nome del sito
   - Storage grade
   - Storage usage (utilizzo storage): La percentuale dello spazio utilizzabile totale per i dati degli oggetti utilizzati per il nodo di storage.

   > Lo stesso valore di utilizzo dello storage (%) viene visualizzato anche nel grafico Storage Used - Object Data per ciascun nodo di storage (selezionare **NODE** > ***Storage Node*** > **Storage**).

4. Visualizzare la scheda **utilizzo ILM** per determinare se il pool di storage è attualmente utilizzato in qualsiasi regola ILM o profilo di erasure coding.
5. Se si desidera, accedere alla pagina **ILM rules** per informazioni e gestione delle regole che utilizzano il pool di storage.

   Consultare la "Istruzioni per l'utilizzo delle regole ILM".

Modificare il pool di storage

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

- Si dispone di "autorizzazioni di accesso specifiche".
- È stata esaminata la "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, si è preso in considerazione il modo in cui le modifiche influiranno sul posizionamento dei dati degli oggetti.

A proposito di questa attività

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

Fasi

1. Selezionare **ILM** > **Storage Pools**.
2. Selezionare la casella di controllo del pool di storage che si desidera modificare.

   Non è possibile modificare il pool di storage di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti).

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

   Al cliente viene impedito di modificare il livello del sito o dello storage se il pool di storage viene utilizzato in un profilo di erasure coding e la modifica porterebbe all'invalidità dello schema di erasure coding. Ad esempio, se un pool di storage utilizzato in un profilo di erasure coding include al momento un livello dello storage con un solo sito, è impossibile utilizzare un livello dello storage con due siti, perché la modifica renderebbe lo schema di erasure coding non valido.

   > L'aggiunta o la rimozione di siti da un pool di storage non sposterà i dati esistenti sottoposti a erasure coding. Se si desidera spostare i dati esistenti dal sito, è necessario creare un nuovo pool di archiviazione e un profilo EC per ricodificare i dati.

6. Selezionare **Salva**.

Al termine

Se è stato aggiunto un nuovo livello di sito o 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 o di sito. Ad esempio, clonare il criterio ILM esistente e attivare il clone. Vedere "Utilizzare le regole ILM e i criteri ILM".

Rimuovere un pool di storage

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso richieste".

Fasi

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

2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il pool di storage.

   Non puoi rimuovere un pool di storage se è utilizzato in una regola ILM o in un profilo di erasure coding. Se necessario, selezionare ***nome pool di storage*** > **utilizzo ILM** per determinare dove viene utilizzato il pool di storage.

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

Utilizza i Cloud Storage Pools

Che 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, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud 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 all'interno del sistema StorageGRID, un Cloud Storage Pool è composto da un bucket esterno (S3) o da un container (storage BLOB di Azure).

La 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.	Utilizzando l'opzione **ILM** > **Storage Pools** > **Cloud 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 storage all'interno di StorageGRID.	In un bucket Amazon S3, un container di storage BLOB di Azure o Google Cloud 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 S3 RestoreObject. • 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 RestoreObject sugli oggetti nel Cloud Storage Pool possono essere interessate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nei criteri ILM attivi.	Una regola ILM nei criteri ILM attivi.
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. **Nota**: Non è possibile eseguire il tiering dei dati FabricPool nei pool di storage cloud.

Ciclo di vita di un oggetto Cloud Storage Pool

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

S3: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool S3.

> "Glacier" si riferisce sia alla classe di storage Glacier che a quella Glacier Deep Archive, con una sola eccezione: La classe di storage Glacier Deep Archive non supporta il Tier di ripristino Expedited. È supportato solo il recupero in blocco o standard.

> Google Cloud Platform (GCP) supporta il recupero di oggetti dallo storage a lungo termine senza richiedere un'operazione POST-ripristino.

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 Cloud Storage Pool S3, l'applicazione client può recuperarlo utilizzando una richiesta GetObject S3 da StorageGRID, a meno che l'oggetto non sia stato spostato nello 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.

     > Per trasferire oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

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

   Se un oggetto è stato spostato nello storage Glacier, l'applicazione client può emettere una richiesta S3 RestoreObject 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 sui nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. **Oggetto recuperato**

   Una volta ripristinato un oggetto, l'applicazione client può emettere una richiesta GetObject per recuperare l'oggetto ripristinato.

Azure: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool di Azure.

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 Azure Cloud Storage Pool come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di storage BLOB di Azure esterno specificato dal Cloud Storage Pool.

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 spostato nel Tier Archive, l'applicazione client può emettere una richiesta S3 RestoreObject per ripristinare una copia recuperabile nell'Azure Cloud Storage Pool.

   Quando StorageGRID riceve il RestoreObject, trasferisce temporaneamente l'oggetto al livello di raffreddamento dell'archiviazione BLOB di Azure. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID trasferisce nuovamente l'oggetto al livello Archive.

   > Se una o più copie dell'oggetto sono presenti anche nei nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso di archiviazione mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. **Oggetto recuperato**

   Una volta ripristinato un oggetto in Azure Cloud Storage Pool, l'applicazione client può emettere una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

"UTILIZZARE L'API REST S3"

Quando utilizzare i Cloud Storage Pools

Utilizzando i Cloud Storage Pools, è possibile eseguire il backup o il tiering dei dati in una posizione esterna. Inoltre, puoi eseguire il backup o il Tier dei dati in più cloud.

Eseguire il 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 la richiesta S3 RestoreObject 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.

Dati di Tier da StorageGRID a 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

È possibile configurare più endpoint del Cloud Storage Pool se si desidera eseguire il Tier o il backup dei dati degli oggetti in più 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 endpoint multipli del 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 gli oggetti dal bucket A nel pool di cloud storage A

e gli oggetti dal bucket B nel pool di cloud storage B. oppure gli oggetti nel pool di cloud storage A per un certo periodo di tempo, quindi spostarli nel pool di cloud storage 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.
- 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.
- Gli oggetti con blocco oggetti S3 abilitato non possono essere posizionati nei pool di storage cloud.
- Se nel bucket S3 di destinazione per un Cloud Storage Pool è attivato il blocco degli oggetti S3, il tentativo di configurare la replica del bucket (PutBucketReplication) non riesce e viene visualizzato un errore AccessDenied.
- Le seguenti combinazioni di piattaforma, autenticazione e protocollo con blocco oggetto S3 non sono supportate per i pool di archiviazione cloud:
  - **Piattaforme**: Google Cloud Platform e Azure
  - **Tipi di autenticazione**: I ruoli IAM ovunque e l'accesso anonimo
  - **Protocollo**: HTTP

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 anche "configurare un proxy di archiviazione"consentire l'invio di 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, le regole e i criteri ILM vengono riconfigurati. 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

Le policy per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono garantire a StorageGRID l'autorizzazione a spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando necessario e altro ancora. Idealmente, StorageGRID dovrebbe avere accesso con controllo 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 dalle policy ILM attive 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.

Per trasferire oggetti da Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata nel bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

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.

Per trasferire oggetti in Cloud Storage Pool in S3 Glacier Deep Archive (invece di su Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tieni presente che non puoi utilizzare il `Expedited` livello 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 Cloud Storage Pool. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

"Creare un pool di storage cloud"

Confronto tra Cloud Storage Pools e la replica di 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?	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 conservare due copie in loco, puoi conservarne una all'interno di StorageGRID e inviarne una copia al pool di storage cloud.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). Crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come viene configurato?	Definito allo stesso modo dei pool di storage, utilizzando Grid Manager o l'API Grid Management. Può essere selezionata 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 • Piattaforma Google Cloud (GCP)	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Piattaforma Google Cloud (GCP)
Qual è la causa dello spostamento degli oggetti nella destinazione?	Una o più regole ILM nei criteri ILM attivi. 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 cloud storage sono 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 anche eliminato dal 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.

Creare un pool di storage cloud

Un Cloud Storage Pool specifica un singolo bucket esterno Amazon S3 o un altro provider compatibile con S3 o un container di storage BLOB di Azure.

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 (storage Amazon S3/GCP o Azure Blob) e le informazioni StorageGRID necessarie per accedere al bucket o al container esterno.

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.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

- Si dispone di "autorizzazioni di accesso richieste".
- È stata esaminata la "Considerazioni per i Cloud Storage Pools".
- Il bucket o contenitore esterno a cui fa riferimento il Cloud Storage Pool esiste già e si dispone di informazioni sull'endpoint di servizio.
- Per accedere al secchio o al contenitore, è informazioni sull'account per il tipo di autenticazionepossibile scegliere.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Selezionare **Crea**, quindi immettere le seguenti informazioni:

Campo	Descrizione
Nome del pool di cloud storage	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/GCP**: Selezionare questa opzione per Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o altri provider compatibili con S3. • **Azure Blob Storage**
Bucket o container	Il nome del bucket S3 esterno o del container Azure. Non puoi modificare questo valore dopo il salvataggio del Cloud Storage Pool.

3. in base alla selezione del tipo di provider, immettere le informazioni sull'endpoint del servizio.

Amazon S3/GCP

a. Per il protocollo, selezionare HTTPS o HTTP.

> Non utilizzare connessioni HTTP per dati sensibili.

b. Inserire il nome host. Esempio:

`s3-aws-region.amazonaws.com`

c. Selezionare lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tentare di rilevare automaticamente lo stile URL da utilizzare, in base alle informazioni fornite. Ad esempio, se si specifica un indirizzo IP, StorageGRID utilizzerà un URL di tipo path. Selezionare questa opzione solo se non si conosce lo stile specifico da utilizzare.
Stile virtual-hosted	Utilizza un URL di tipo virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del nome di dominio. Esempio: `https://bucket-name.s3.company.com/key-name`
Stile di percorso	Utilizzare un URL stile percorso per accedere al bucket. Gli URL stile percorso includono il nome del bucket alla fine Esempio: `https://s3.company.com/bucket-name/key-name` **Nota:** l'opzione URL stile percorso non è consigliata e sarà obsoleta in una release futura di StorageGRID.

d. Se si desidera, inserire il numero della porta o utilizzare la porta predefinita: 443 per HTTPS o 80 per HTTP.

Azure Blob Storage

a. Utilizzando uno dei seguenti formati, immettere l'URI per l'endpoint del servizio.

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

Esempio: `https://myaccount.blob.core.windows.net:443`

Se non si specifica una porta, per impostazione predefinita viene utilizzata la porta 443 per HTTPS e la porta 80 per HTTP.

4. selezionare **Continue**. Quindi, selezionare il tipo di autenticazione e immettere le informazioni richieste per l'endpoint del Cloud Storage Pool:

Tasto di accesso

Per Amazon S3/GCP o altro provider compatibile con S3

a. **ID chiave di accesso**: Immettere l'ID della chiave di accesso per l'account proprietario del bucket esterno.
b. **Chiave di accesso segreta**: Immettere la chiave di accesso segreta.

Ruoli IAM ovunque

Per AWS IAM Roles Anywhere service

StorageGRID utilizza AWS Security Token Service (STS) per generare dinamicamente un token di breve durata per accedere alle risorse AWS.

a. **AWS IAM Roles Anywhere Region**: Selezionare la regione per il Cloud Storage Pool. Ad esempio, `us-east-1`.
b. **Trust anchor URN**: Immettere l'URN dell'ancoraggio trust che convalida le richieste per le credenziali STS di breve durata. Può essere una CA principale o intermedia.
c. **URN profilo**: Immettere l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia attendibile.
d. **Role URN**: Inserire l'URN del ruolo IAM che può essere assunto da chiunque sia attendibile.
e. **Durata sessione**: Immettere la durata delle credenziali di protezione temporanee e della sessione ruolo. Immettere almeno 15 minuti e non più di 12 ore.
f. **Certificato CA del server** (opzionale): Uno o più certificati CA attendibili, in formato PEM, per la verifica del server IAM Roles Anywhere. Se omesso, il server non verrà verificato.
g. **Certificato dell'entità finale**: La chiave pubblica, in formato PEM, del certificato X509 firmato dall'ancoraggio trust. AWS IAM Roles Anywhere utilizza questa chiave per emettere un token STS.
h. **Chiave privata dell'entità finale**: La chiave privata per il certificato dell'entità finale.

CAP (portale di accesso C2S)

Per il servizio Commercial Cloud Services (C2S) S3

a. **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. **Certificato CA del server**: Selezionare **Sfoglia** e caricare il certificato CA utilizzato da StorageGRID per verificare il CAP server. Il certificato deve essere codificato PEM ed emesso da un'autorità di certificazione pubblica competente (CA).
c. **Certificato client**: Selezionare **Sfoglia** e caricare il certificato che StorageGRID utilizzerà per identificarsi nel CAP server. Il certificato client deve essere codificato PEM, rilasciato da un'autorità di certificazione pubblica (CA) appropriata e deve essere concesso l'accesso al conto C2S.
d. **Chiave privata client**: Selezionare **Sfoglia** e caricare la chiave privata codificata PEM per il certificato client.
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 **Password chiave privata client**.

Se il certificato client viene crittografato, utilizzare il formato tradizionale per la crittografia. Il formato crittografato PKCS n. 8 non è supportato.

Azure Blob Storage

Per l'archiviazione BLOB di Azure, solo chiave condivisa

a. **Nome account**: Immettere il nome dell'account di archiviazione proprietario del contenitore esterno
b. **Codice account**: Immettere la chiave segreta per l'account di archiviazione

È possibile utilizzare il portale Azure per trovare questi valori.

Anonimo

Non sono richieste informazioni aggiuntive.

5. Selezionare **continua**. Quindi scegliere il tipo di verifica del server che si desidera utilizzare:

Opzione	Descrizione
Utilizzare i certificati della CA principale nel sistema operativo del nodo di storage	Utilizzare i certificati Grid CA installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Selezionare **Sfoglia** e caricare il certificato codificato PEM.
Non verificare il certificato	La selezione di questa opzione indica che le connessioni TLS al Cloud Storage Pool non sono sicure.

6. Selezionare **Salva**.

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

   - Convalida l'esistenza del bucket o del container e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
   - Scrive un file marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere mai questo file, che è 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 o il container specificato non esiste già, potrebbe essere visualizzato un errore.

7. Se si verifica un errore, consultare la sezione "Istruzioni per la risoluzione dei problemi dei Cloud Storage Pools", risolvere eventuali problemi, quindi provare a salvare nuovamente il Cloud Storage Pool.

Visualizzare i dettagli dei pool di storage cloud

Puoi visualizzare i dettagli di un Cloud Storage Pool per determinare dove viene utilizzato e per vedere quali nodi e gradi di storage sono inclusi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".

Fasi

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

   La tabella Cloud Storage Pools include le seguenti informazioni per ogni Cloud Storage Pool che include i nodi di storage:

   - **Nome**: Il nome univoco visualizzato del pool.
   - **URI**: L'Uniform Resource Identifier del Cloud Storage Pool.
   - **Tipo di provider**: Quale provider cloud viene utilizzato per questo pool di archiviazione cloud.
   - **Container**: Il nome del bucket utilizzato per il pool di archiviazione cloud.
   - **Utilizzo ILM**: Modalità di utilizzo del pool. Un Cloud Storage Pool potrebbe essere inutilizzato o potrebbe essere utilizzato in una o più regole ILM, profili di erasure coding o entrambe.
   - **Ultimo errore**: L'ultimo errore rilevato durante un controllo dello stato di salute di questo pool di archiviazione cloud.

2. Per visualizzare i dettagli di un pool di cloud storage specifico, selezionarne il nome.

   Viene visualizzata la pagina dei dettagli del pool.

3. Visualizzare la scheda **autenticazione** per informazioni sul tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Visualizzare la scheda **verifica server** per informazioni sui dettagli della verifica, modificare la verifica, scaricare un nuovo certificato o copiare il PEM del certificato.
5. Visualizzare la scheda **utilizzo ILM** per determinare se il Cloud Storage Pool è attualmente utilizzato in qualsiasi regola ILM o profilo di erasure coding.
6. In alternativa, andare alla pagina **regole ILM** "informazioni e gestione di eventuali regole"che utilizzano il Cloud Storage Pool.

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.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".
- È stata esaminata la "Considerazioni per i Cloud Storage Pools".

Fasi

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

   La tabella Cloud Storage Pools elenca i Cloud Storage Pools esistenti.

2. Seleziona la casella di controllo per il Cloud Storage Pool che desideri modificare, quindi seleziona **azioni** > **Modifica**.

   In alternativa, selezionare il nome del pool di archiviazione cloud, quindi selezionare **Modifica**.

3. Come richiesto, modificare il nome del Cloud Storage Pool, l'endpoint del servizio, le credenziali di autenticazione o il metodo di verifica del certificato.

   > Non puoi 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 espandere la fisarmonica **Dettagli certificato** per rivedere il certificato attualmente in uso.

4. Selezionare **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 "Risoluzione dei problemi relativi ai pool di storage cloud", risolvere il problema, quindi riprovare a salvare il Cloud Storage Pool.

Rimuovere un pool di storage cloud

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso richieste".

Se necessario, utilizzare ILM per spostare i dati dell'oggetto

Se il Cloud Storage Pool che si desidera rimuovere contiene dati a oggetti, è necessario utilizzare ILM per spostare i dati in una posizione diversa. Ad esempio, è possibile spostare i dati su nodi di storage nel proprio grid o su un pool di storage cloud diverso.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il Cloud Storage Pool.

   Non puoi rimuovere un Cloud Storage Pool se viene utilizzato in una regola ILM o in un profilo di erasure coding.

3. Se si utilizza il Cloud Storage Pool, selezionare ***cloud storage pool name*** > **ILM usage**.
4. "Clonare ogni regola ILM" Che attualmente colloca gli oggetti nel pool di cloud storage da rimuovere.
5. Determinare dove si desidera spostare gli oggetti esistenti gestiti da ciascuna regola clonata.

È possibile utilizzare uno o più pool di storage o un pool di storage cloud diverso.

6. Modificare ciascuna regola clonata.

   Per la fase 2 della creazione guidata regola ILM, selezionare la nuova posizione dal campo **copie at**.

7. "Creare un nuovo criterio ILM" e sostituire ciascuna delle vecchie regole con una regola clonata.
8. Attivare la nuova policy.
9. Attendere che ILM rimuova gli oggetti dal Cloud Storage Pool e li inseri nella nuova posizione.

Eliminare il pool di storage cloud

Quando il Cloud Storage Pool è vuoto e non viene utilizzato in alcuna regola ILM, è possibile eliminarlo.

Prima di iniziare

- Sono state rimosse tutte le regole ILM che potrebbero aver utilizzato il pool.
- 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. Vedere "Risolvere i problemi dei 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, che è denominato `x-ntap-sgws-cloud-pool-uuid`.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Se la colonna ILM Usage (utilizzo ILM) indica che il Cloud Storage Pool non è in uso, selezionare la casella di controllo.
3. Selezionare **azioni** > **Rimuovi**.
4. Selezionare **OK**.

Risolvere i problemi dei pool di storage cloud

Utilizzare questi passaggi per la risoluzione dei problemi per risolvere gli errori che potrebbero verificarsi durante la creazione, la modifica o l'eliminazione di un pool di storage cloud.

Determinare se si è verificato un errore

StorageGRID esegue un semplice controllo dello stato di salute di ogni pool di cloud storage leggendo l'oggetto noto `x-ntap-sgws-cloud-pool-uuid` per assicurarsi che il pool di cloud storage sia accessibile e funzioni correttamente. Quando StorageGRID rileva un errore nell'endpoint, esegue un controllo di integrità ogni minuto da ogni nodo di storage. Quando l'errore viene risolto, i controlli dello stato si interrompono. Se un controllo di integrità rileva un problema, viene visualizzato un messaggio nella colonna ultimo errore della tabella Pool di archiviazione cloud nella pagina Pool di archiviazione.

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 Pools (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.

Controllare se un errore è stato risolto

Dopo aver risolto eventuali problemi sottostanti, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, selezionare l'endpoint e selezionare **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: Controllo dello stato di salute non riuscito. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si attiva S3 Object Lock con conservazione predefinita per il bucket Amazon S3 dopo aver iniziato a utilizzare questo bucket per un Cloud Storage Pool. Questo errore si verifica quando l'operazione PUT non ha un'intestazione HTTP con un valore checksum payload come `Content-MD5` . Questo valore della testata è richiesto da AWS per le operazioni di INSERIMENTO nei bucket con blocco oggetti S3 abilitato.

Per risolvere questo problema, seguire i passaggi descritti in "Modifica di un pool di storage cloud" senza apportare modifiche. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag blocco oggetto S3 in una configurazione endpoint di Cloud Storage Pool.

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 contenitore include il `x-ntap-sgws-cloud-pool-uuid` file marcatore, ma quel file non ha il campo metadati con 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 tutti gli oggetti esistenti nel bucket di destinazione, incluso il `x-ntap-sgws-cloud-pool-uuid` file, e provare a configurare di nuovo Cloud Storage Pool.

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

Questo errore potrebbe verificarsi nelle seguenti circostanze:

- Quando si tenta di creare o modificare un Cloud Storage Pool.
- Quando si seleziona una combinazione di piattaforma, autenticazione o protocollo non supportata con blocco oggetto S3 durante la configurazione di un nuovo Cloud Storage Pool. Vedere "Considerazioni per i Cloud Storage Pools".

Questo errore indica che un problema di connettività o di configurazione impedisce la scrittura di StorageGRID 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`, controllare che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi HTTP per un contenitore o un 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 archiviazione di accedere all'endpoint del servizio utilizzato per il pool di archiviazione cloud.
- Se l'errore è dovuto a una piattaforma, autenticazione o protocollo non supportati, passare a una configurazione supportata con blocco oggetti S3 e provare a salvare nuovamente il nuovo 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 pool di cloud storage non include il `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:

- Segui le istruzioni per riportare gli oggetti in StorageGRID in "ciclo di vita di un oggetto Cloud Storage Pool".
- 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

È possibile che si verifichi questo errore se è stato configurato un proxy di 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 di archiviazione.

Errore: Il certificato X,509 non è valido

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore si verifica quando l'autenticazione richiede un certificato X,509 per garantire la convalida del Cloud Storage Pool esterno corretto e il pool esterno è vuoto prima di eliminare la configurazione del Cloud Storage Pool.

Per risolvere il problema, attenersi alla seguente procedura:

- Aggiornare il certificato configurato per l'autenticazione al Cloud Storage Pool.
- Assicurarsi che qualsiasi avviso di scadenza del certificato su questo Cloud Storage Pool sia stato risolto.

Informazioni correlate

"Ciclo di vita di un oggetto Cloud Storage Pool"

Gestire i profili di erasure coding

È possibile visualizzare i dettagli di un profilo di erasure coding e rinominare un profilo, se necessario. È possibile disattivare un profilo di erasure coding se non è attualmente utilizzato in nessuna regola ILM.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso richieste".

Visualizza i dettagli del profilo di erasure coding

È possibile visualizzare i dettagli di un profilo di erasure coding per determinarne lo stato, lo schema di erasure coding utilizzato e altre informazioni.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Erasure Coding**.
2. Selezionare il profilo. Viene visualizzata la pagina dei dettagli del profilo.
3. In alternativa, è possibile visualizzare la scheda regole ILM per un elenco di regole ILM che utilizzano il profilo e i criteri ILM che utilizzano tali regole.
4. Facoltativamente, visualizzare la scheda nodi di archiviazione per i dettagli su ciascun nodo di archiviazione nel pool di archiviazione del profilo, ad esempio il sito in cui si trova e l'utilizzo dello storage.

Rinominare un profilo con erasure coding

Si consiglia di rinominare un profilo di erasure coding in modo da renderlo più ovvio.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Erasure Coding**.
2. Selezionare il profilo che si desidera rinominare.
3. Selezionare **Rinomina**.
4. Immettere un nome univoco per il profilo di erasure coding.

   Il nome del profilo di erasure coding viene aggiunto al nome del pool di storage nelle istruzioni di posizionamento di 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. Selezionare **Salva**.

Disattivare un profilo di erasure coding

È possibile disattivare un profilo di erasure coding se non si prevede più di utilizzarlo e se il profilo non è attualmente utilizzato in nessuna regola ILM.

> Verificare che non siano in corso operazioni di riparazione dei dati sottoposte a erasure coding o procedure di decommissionamento. Viene visualizzato un messaggio di errore se si tenta di disattivare un profilo di erasure coding mentre è in corso una di queste operazioni.

A proposito di questa attività

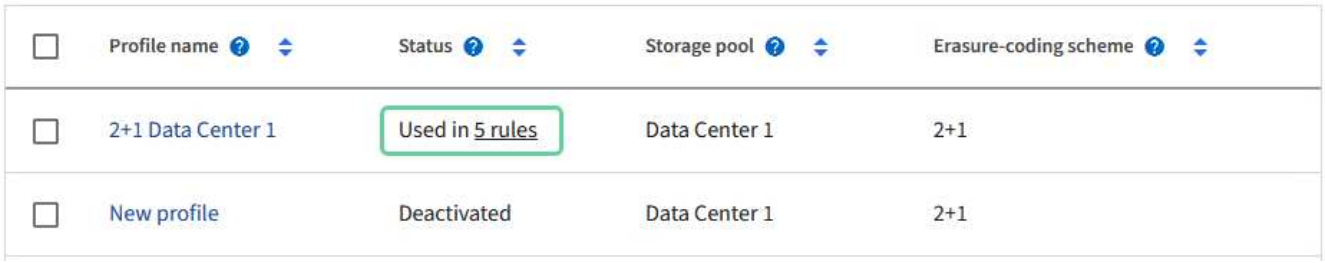
StorageGRID ti impedisce di disattivare un profilo di erasure coding se si verifica una delle seguenti condizioni:

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

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Erasure Coding**.
2. Nella scheda attivo, esaminare la colonna **Stato** per confermare che il profilo di erasure coding che si desidera disattivare non è utilizzato in nessuna regola ILM.

   Non è possibile disattivare un profilo di erasure coding se è utilizzato in qualsiasi regola ILM. Nell'esempio, il profilo 2+1 Data Center 1 viene utilizzato in almeno una regola ILM.



3. Se il profilo viene utilizzato in una regola ILM, attenersi alla seguente procedura:
   a. Selezionare **ILM** > **regole**.
   b. Selezionare ciascuna regola ed esaminare il diagramma di conservazione per determinare se la regola utilizza il profilo di erasure coding che si desidera disattivare.
   c. Se la regola ILM utilizza il profilo di erasure coding che si desidera disattivare, determinare se la regola è utilizzata in qualsiasi criterio ILM.
   d. Completare i passaggi aggiuntivi nella tabella, in base alla posizione in cui viene utilizzato il profilo di erasure coding.

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 tutti i posizionamenti che utilizzano il profilo di erasure coding. ii. Continuare con questa procedura.	"Utilizzare le regole ILM e i criteri 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 è attualmente in un criterio ILM attivo	i. Clonazione della policy. ii. Rimuovere la regola ILM che utilizza il profilo di erasure coding. 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. Mentre è possibile tentare di disattivare un profilo di erasure coding 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 tutti i posizionamenti che utilizzano il profilo di erasure coding. vii. Continuare con questa procedura.	"Creare un criterio ILM" "Utilizzare le regole ILM e i criteri ILM"
In una regola ILM che è attualmente in un criterio ILM	i. Modificare il criterio. ii. Rimuovere la regola ILM che utilizza il profilo di erasure coding. iii. Aggiungere una o più nuove regole ILM per garantire la protezione di tutti gli oggetti. iv. Salvare il criterio. v. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutti i posizionamenti che utilizzano il profilo di erasure coding. vi. Continuare con questa procedura.	"Creare un criterio ILM" "Utilizzare le regole ILM e i criteri ILM"

e. 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 di erasure coding.

> È possibile selezionare più profili da disattivare contemporaneamente, a condizione che ciascun profilo non venga utilizzato in alcuna regola.

5. Se sei sicuro di voler disattivare il profilo, seleziona **Disattiva**.

Risultati

- Se StorageGRID è in grado di disattivare il profilo di erasure coding, il suo stato è disattivato. Non è più possibile selezionare questo profilo per nessuna regola ILM. Non puoi riattivare un profilo disattivato.
- 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.

> Una volta creato il bucket, non è possibile modificare l'area di un bucket.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone 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 nell' `us-west-2`area. 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 appartenenti alla `us-east-1` regione.
- 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 rilevano la distinzione tra maiuscole e minuscole. 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 utilizzata in una regola assegnata a qualsiasi criterio (attivo o inattivo).
- Se si utilizza un'area non valida come filtro avanzato in una regola ILM, non è possibile aggiungere tale regola a un criterio.

  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.

- 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 modificata o rimossa.

2. Per aggiungere una regione:
   a. Selezionare **Aggiungi un'altra regione**.
   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 inutilizzata, selezionare l'icona di eliminazione ✕.

   Se si tenta di rimuovere una regione attualmente utilizzata in qualsiasi criterio (attivo o inattivo), viene visualizzato un messaggio di errore.

4. Una volta apportate le modifiche, selezionare **Salva**.

   È ora possibile selezionare queste regioni dalla sezione Advanced filters (filtri avanzati) nel passaggio 1 della creazione guidata regola ILM. Vedere "Utilizzare filtri avanzati nelle regole ILM".

Creare una regola ILM

Utilizzare le regole ILM per gestire gli oggetti

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.

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.

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.
- **Comportamento acquisizione**: Il comportamento di acquisizione di una regola consente di scegliere il modo in cui gli oggetti filtrati dalla regola sono protetti durante l'acquisizione (quando un client S3 salva un oggetto nella griglia).

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. Questi filtri consentono di applicare una regola a specifici account tenant, bucket S3 specifici o entrambi.

  I filtri di base offrono un metodo 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.

- I filtri avanzati offrono 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)
  - Vincolo di posizione (solo S3)
  - Dimensione dell'oggetto
  - Metadati dell'utente
  - Tag Object (solo 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 possibile combinare i filtri 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 i filtri in ciascuna regola per identificare il tipo specifico di oggetti a cui si applica la regola.

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.

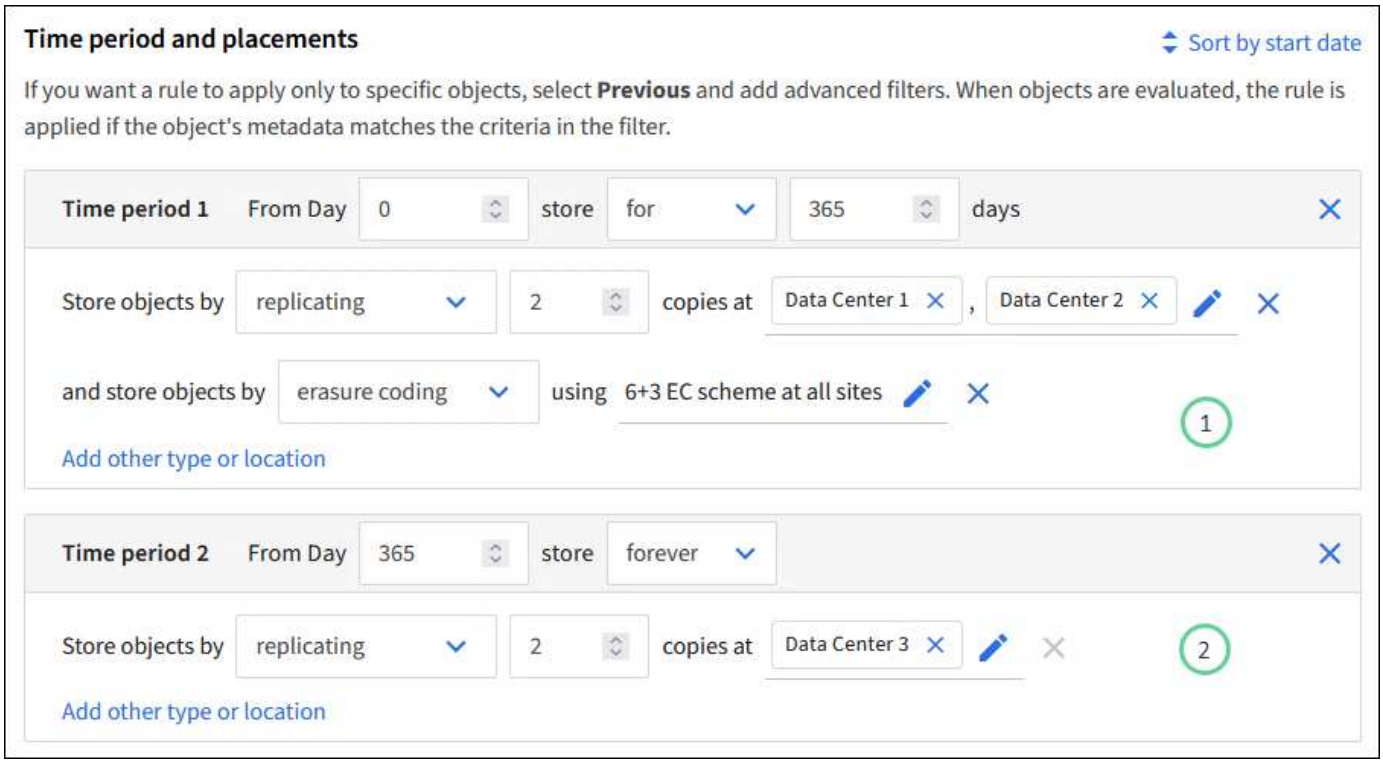
Quando si creano le istruzioni per il posizionamento:

- Si inizia specificando l'ora di riferimento, che determina quando iniziano le istruzioni di posizionamento. Il tempo di riferimento potrebbe essere quando un oggetto viene acquisito, quando si accede a un oggetto, quando un oggetto con versione diventa non corrente o un tempo definito dall'utente.
- Quindi, specificare quando applicare il posizionamento rispetto al tempo di riferimento. Ad esempio, un posizionamento potrebbe iniziare il giorno 0 e continuare per 365 giorni, rispetto a quando l'oggetto è stato acquisito.
- Infine, specificare il tipo di copie (replica o erasure coding) e la posizione in cui sono memorizzate le copie. Ad esempio, è possibile memorizzare due copie replicate in due siti diversi.

Ciascuna regola può definire più posizioni per un singolo periodo di tempo e posizioni diverse per periodi di tempo diversi.

- Per posizionare oggetti in più posizioni durante un singolo periodo di tempo, selezionare **Aggiungi altro tipo o posizione** per aggiungere più di una riga per quel periodo di tempo.
- Per posizionare oggetti in posizioni diverse in periodi di tempo diversi, selezionare **Aggiungi un altro periodo di tempo** per aggiungere il periodo di tempo successivo. Quindi, specificare una o più righe entro il periodo di tempo.

L'esempio mostra due istruzioni di posizionamento nella pagina Definisci posizioni della creazione guidata regola ILM.



La prima istruzione di inserimento (1) ha due righe per il primo anno:

- La prima riga crea due copie di oggetti replicate in due siti del data center.
- La seconda riga crea una copia con erasure coding pari a 6+3 usando tutti i siti del data center.

La seconda istruzione di posizionamento (2) crea due copie 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.

Comportamento di acquisizione delle regole ILM

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. Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Balanced**: StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono eseguite copie temporanee e viene restituito il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.
- **Strict**: Tutte le copie specificate nella regola ILM devono essere eseguite prima che il client sia riuscito.
- **Doppio commit**: StorageGRID esegue immediatamente copie temporanee dell'oggetto e restituisce il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Informazioni correlate

- "Opzioni di acquisizione"
- "Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione"
- "L'interazione tra coerenza e regole ILM per influire sulla protezione dei dati"

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applicano solo agli oggetti appartenenti al tenant A.
- Eseguire due copie replicate di tali oggetti e memorizzare ciascuna copia in un sito diverso.
- Conserva le due copie "per sempre", 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.
- Utilizzare l'opzione bilanciato 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

- "Che cos'è un pool di storage"
- "Che cos'è un Cloud Storage Pool"

Accedere alla procedura guidata Crea una regola ILM

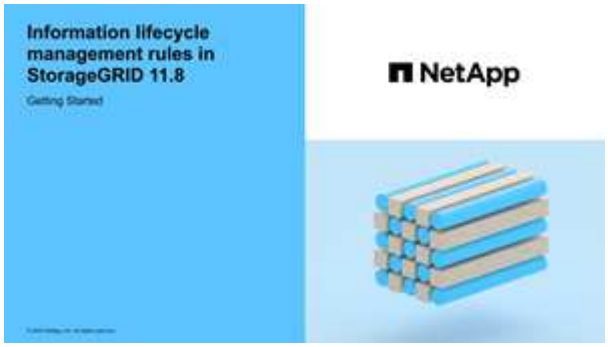
Le regole ILM consentono di gestire il posizionamento dei dati degli oggetti nel tempo. Per creare una regola ILM, utilizzare la procedura guidata Crea una regola ILM.

> Se si desidera creare la regola ILM predefinita per un criterio, seguire invece l'"Istruzioni per la creazione di una regola ILM predefinita".

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".
- Se si desidera specificare a quali account tenant si applica questa regola, si dispone dell'"Autorizzazione account tenant"ID account per ciascun account.
- Se si desidera che la regola filtri gli oggetti sui metadati dell'ora dell'ultimo accesso, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati dal bucket S3.
- Hai configurato qualsiasi pool di storage cloud che intendi utilizzare. Vedere "Creare un pool di storage cloud".
- Si ha familiarità con "opzioni di acquisizione".
- Se è necessario creare una regola conforme da utilizzare con blocco oggetti S3, si ha familiarità con "Requisiti per il blocco oggetti S3".

- Se si desidera, è stato guardato il video: "Video: Panoramica delle regole ILM".



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 degli oggetti da creare (replicate o sottoposte a erasure coding) e il numero di copie di ciascun oggetto necessario.
- 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 di acquisizione utilizzare (Balanced, Strict o Dual Commit).

Fasi

1. Selezionare **ILM** > **regole**.
2. Selezionare **Crea**. "Fase 1 (inserire i dettagli)" Viene visualizzata la procedura guidata Crea una regola ILM.

Fase 1 di 3: Inserire i dettagli

La fase **Enter details** della creazione guidata di una regola ILM consente di immettere un nome e una descrizione per la regola e di definire i filtri per la regola.

L'immissione di una descrizione e la definizione dei filtri per la regola sono facoltativi.

A proposito di questa attività

Quando si valuta un oggetto rispetto a "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**.
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 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 di accesso root o dell'autorizzazione per gli account tenant, 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 a cui si applica questa regola.

   Se si seleziona **Applica a tutti i bucket** (impostazione predefinita), la regola si applica a tutti i bucket S3.

5. Per i tenant S3, selezionare **Yes** (Sì) per applicare la regola solo alle versioni di oggetti precedenti nei bucket S3 che hanno attivato il controllo delle versioni.

   Se si seleziona **Sì**, l'opzione "ora non corrente" verrà selezionata automaticamente per ora di riferimento in "Passaggio 2 della creazione guidata di una regola ILM".

   > ⓘ L'ora non corrente si applica solo agli oggetti S3 nei bucket abilitati per il controllo delle versioni. Vedere "Operazioni su benne, PutBucketVersioning" e "Gestire gli oggetti con S3 Object Lock".

   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".

6. In alternativa, selezionare **Aggiungi un filtro 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. Per ulteriori informazioni sul filtraggio avanzato, vedere Utilizzare filtri avanzati nelle regole ILM e Specificare più tipi di metadati e valori.

7. Selezionare **continua**. "Fase 2 (definizione delle posizioni)" Viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare 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	• è • non lo è • è prima • è acceso o prima • è dopo • sia acceso o dopo	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 la nuova policy verrà applicata 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 oggetto S3 univoca. Ad esempio, è possibile associare oggetti che terminano con `.txt` o iniziano con `test-object/`.
Ora dell'ultimo accesso	• è • non lo è • è prima • è acceso o prima • è dopo • sia acceso o dopo	Ora e data dell'ultimo recupero dell'oggetto (letto o visualizzato). **Nota:** se si prevede di utilizzare "usa l'ultimo tempo di accesso"un filtro avanzato, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati per il bucket S3.
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. Vedere "Configurazione delle regioni (opzionale e solo S3)".

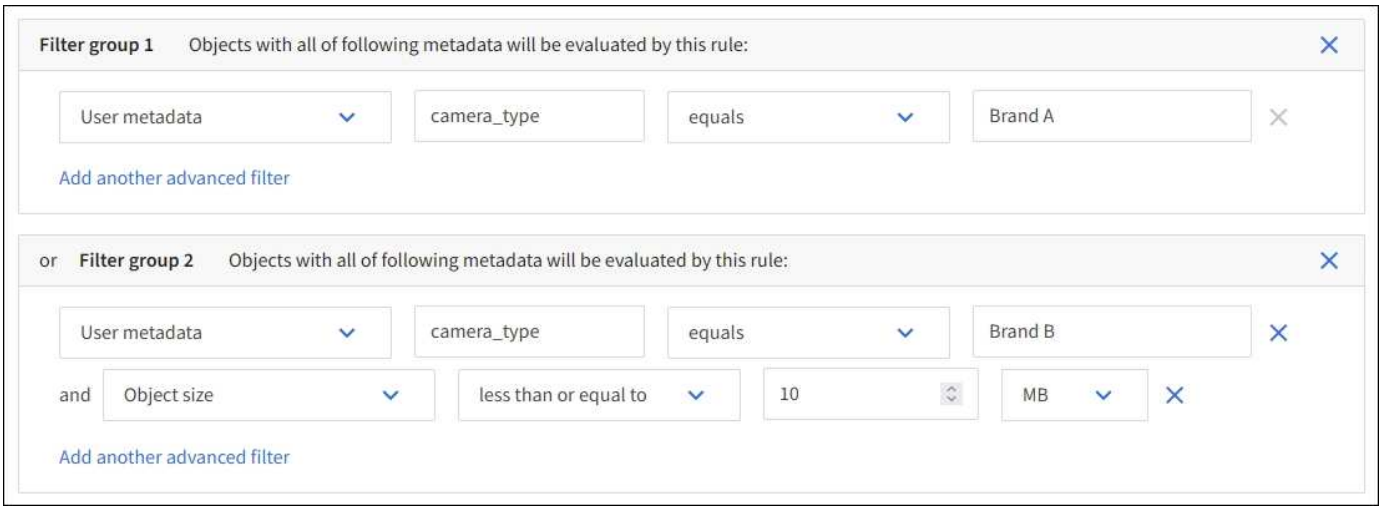
Tipo di metadati	Operatori supportati	Valore dei metadati
Dimensione dell'oggetto	• uguale a • non uguale • inferiore a. • minore o uguale a. • maggiore di • maggiore o uguale a.	La dimensione dell'oggetto. L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.
Metadati dell'utente	• contiene • termina con • uguale a • esiste • inizia con • non contiene • non finisce con • non uguale • non esiste • non inizia con	Coppia valore-chiave, dove **Nome metadati utente** è la chiave e **valore metadati** è il valore. Ad esempio, per filtrare gli oggetti che hanno metadati utente di `color=blue`, specificare `color` per **Nome metadati utente**, per l'operatore e `blue` per **valore metadati** `equals`. **Nota:** i nomi dei metadati utente non distinguono tra maiuscole e minuscole; i valori dei metadati utente distinguono tra maiuscole e minuscole.
Tag Object (solo S3)	• contiene • termina con • uguale a • esiste • inizia con • non contiene • non finisce con • non uguale • non esiste • non inizia con	Coppia key-value, dove **nome tag oggetto** è la chiave e **valore tag oggetto** è il valore. Ad esempio, per filtrare gli oggetti che hanno un tag di oggetto di `Image=True`, specificare `Image` per **nome tag di oggetto**, `equals` per l'operatore e `True` per **valore tag di 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.

Specificare 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 il marchio A o il marchio B come valore dei metadati utente camera_TYPE. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.



Fase 2 di 3: Definizione delle posizioni

La fase **Definisci posizionamenti** della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano la durata dell'archiviazione degli oggetti, il tipo di copie (replicate o sottoposte a erasure coding), la posizione di archiviazione e il numero di copie.

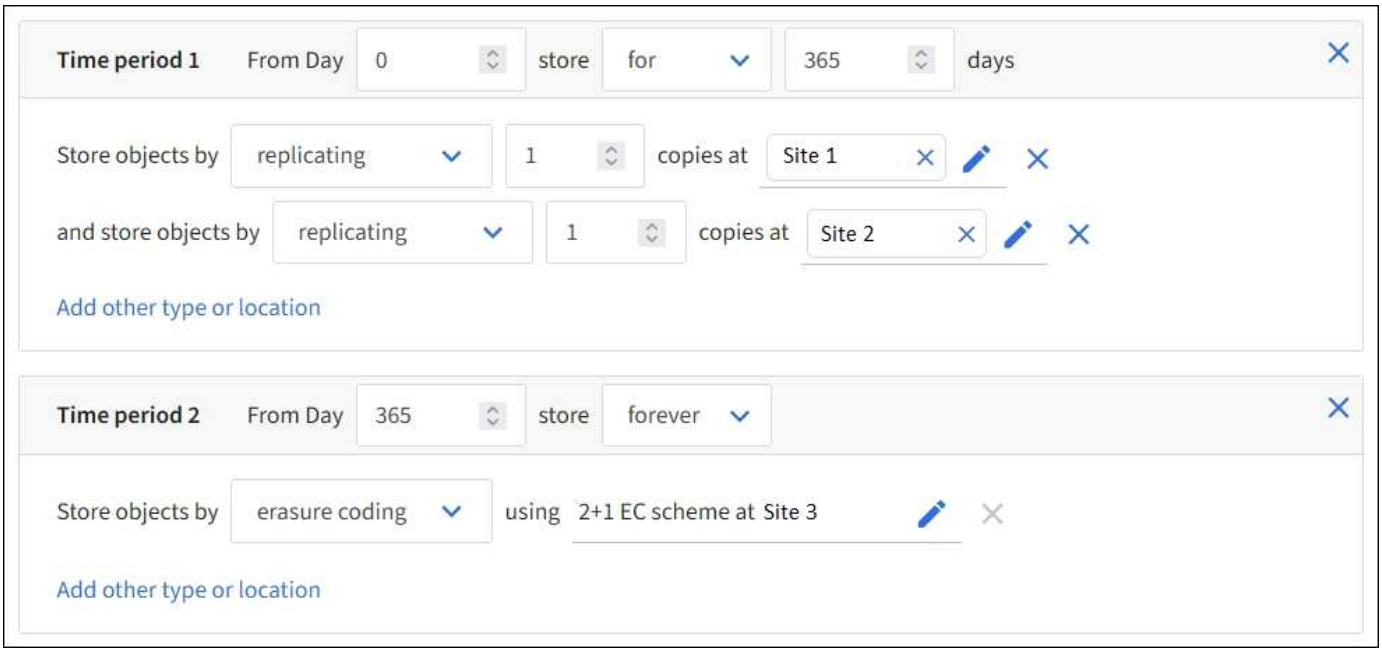
Le schermate mostrate sono esempi. I risultati possono variare a seconda della versione di StorageGRID in uso.

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.

In questo esempio, la regola ILM memorizza una copia replicata nel sito 1 e una copia replicata nel sito 2 per il primo anno. 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 dell'ultimo accesso	L'ora in cui l'oggetto è stato recuperato per l'ultima volta (letto o visualizzato). Per utilizzare questa opzione, è necessario attivare gli aggiornamenti dell'ora dell'ultimo accesso per il bucket S3. Fare riferimento alla "USA l'ultimo tempo di accesso nelle regole ILM".
Tempo di creazione definito dall'utente	Tempo specificato nei metadati definiti dall'utente.
Ora non corrente	L'opzione "ora non corrente" viene selezionata automaticamente se si seleziona **Sì** per la domanda "Applica questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con versione abilitata)?" in "Passaggio 1 della creazione guidata di una regola ILM".

   Se si desidera creare una regola *conforme*, è necessario selezionare **ora di acquisizione**. Fare riferimento alla "Gestire gli oggetti con S3 Object Lock".

2. Nella sezione **periodo di tempo e posizionamenti**, inserire 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 (*dal giorno 0 memorizzare per 365 giorni*). Almeno un'istruzione deve iniziare al giorno 0.

3. Se si desidera creare copie replicate:

a. Dall'elenco a discesa **Memorizza oggetti per**, selezionare **replica**.

b. 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. Fare riferimento alla "Perché non utilizzare la replica a copia singola".

   Per evitare il rischio, effettuare una o più delle seguenti operazioni:

   - Aumentare il numero di copie per il periodo di tempo.
   - Aggiungere copie ad altri pool di storage o a un pool di storage cloud.
   - Selezionare **erasure coding** invece di **Replicing**.

     È possibile ignorare questo avviso se questa regola crea già più copie per tutti i periodi di tempo.

c. Nel campo **Copies at**, selezionare i 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 e 8212 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, una copia viene memorizzata nel sito di acquisizione e il sistema distribuisce le copie rimanenti per mantenere bilanciato l'utilizzo del disco tra i pool, garantendo 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 di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti) e un altro pool di storage.

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

   a. Dall'elenco a discesa **Memorizza oggetti per**, selezionare **erasure coding**.

      > L'erasure coding è più adatto per oggetti superiori a 1 MB. 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 non è stato aggiunto un filtro delle dimensioni dell'oggetto per un valore superiore a 200 KB, selezionare **precedente** per tornare al passaggio 1. Quindi, selezionare **Aggiungi un filtro avanzato** e impostare un filtro **dimensione oggetto** su qualsiasi valore maggiore di 200 KB.

   c. Selezionare il pool di storage che si desidera aggiungere e lo schema di erasure coding che si desidera utilizzare.

      La posizione dello storage per una copia sottoposta a erasure coding include il nome dello schema di

erasure coding, seguito dal nome del pool di storage.

Gli schemi di erasure coding disponibili sono limitati dal numero di nodi storage nel pool di storage selezionato. Accanto agli schemi che forniscono la "migliore protezione o l'overhead dello storage più basso", viene visualizzato un `Recommended` badge.

5. Facoltativamente:
   a. Selezionare **Aggiungi altro tipo o ubicazione** per creare copie aggiuntive in posizioni diverse.
   b. Selezionare **Add another time period** (Aggiungi un altro periodo di tempo) per aggiungere diversi periodi di tempo.

> L'eliminazione degli oggetti avviene in base alle seguenti impostazioni:
>
> - Gli oggetti vengono eliminati automaticamente alla fine del periodo di tempo finale, a meno che un altro periodo di tempo non termini con **per sempre**.
> - A seconda di "impostazioni del periodo di conservazione del bucket e del tenant", gli oggetti potrebbero non essere eliminati anche al termine del periodo di conservazione di ILM.

6. Se si desidera memorizzare oggetti in un pool di storage cloud:
   a. Nell'elenco a discesa **Memorizza oggetti per**, selezionare **replica**.
   b. Selezionare il campo **Copies at**, quindi selezionare un Cloud Storage Pool.

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

      - Non puoi 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 nessun Cloud Storage Pool. 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 Cloud Storage Pool contemporaneamente all'archiviazione dell'oggetto come copie replicate o con erasure coding in StorageGRID. Tuttavia, è necessario includere più di una riga nelle istruzioni di posizionamento per il periodo di tempo, in modo da poter specificare il numero e il tipo di copie per ciascuna posizione.

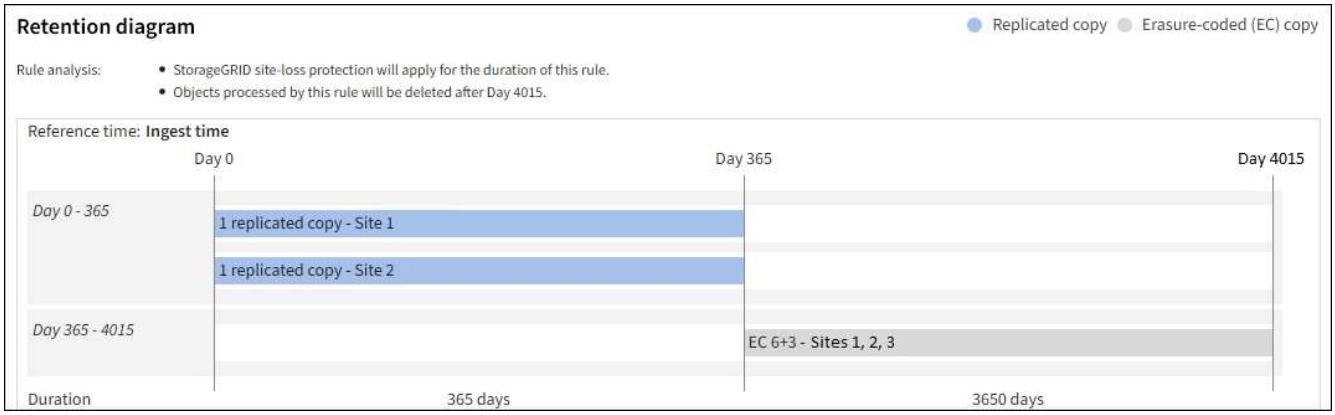
7. Nel diagramma di conservazione, confermare le istruzioni per il posizionamento.

   In questo esempio, la regola ILM memorizza una copia replicata nel sito 1 e una copia replicata nel sito 2 per il primo anno. Dopo un anno e per altri 10 anni, una copia con codice di cancellazione 6+3 verrà salvata in tre sedi. Dopo 11 anni totali, gli oggetti verranno cancellati da StorageGRID.

   La sezione analisi delle regole del diagramma di conservazione riporta:

   - La protezione contro la perdita di sito di StorageGRID verrà applicata per tutta la durata di questa regola.
   - Gli oggetti elaborati da questa regola verranno cancellati dopo il giorno 4015.

Fare riferimento alla "Abilita la protezione contro la perdita di sito."



8. Selezionare **continua**. "Fase 3 (selezionare il comportamento di acquisizione)" Viene visualizzata la procedura guidata Crea una regola ILM.

USA l'ultimo tempo di accesso nelle regole ILM

In una regola ILM, è possibile utilizzare l'ultimo tempo di 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'ultimo tempo di 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'ultima ora di accesso come filtro avanzato o come ora di riferimento, è necessario attivare gli ultimi aggiornamenti dell'ora di accesso per i bucket S3. È possibile utilizzare "Manager tenant"o "API di gestione del tenant".

> Gli aggiornamenti dell'ora dell'ultimo accesso sono disabilitati 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

Fase 3 di 3: Selezionare il comportamento di acquisizione

La fase **Select ingest behavior** della procedura guidata Create ILM Rule 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 il "comportamento di acquisizione" da utilizzare.

   Per ulteriori informazioni, vedere "Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione".

   > Non è possibile utilizzare l'opzione bilanciato o rigoroso se la regola utilizza uno dei seguenti posizionamenti:
   >
   > - Un pool di storage cloud al giorno 0
   > - Un Cloud Storage Pool quando la regola utilizza un tempo di creazione definito dall'utente come tempo di riferimento
   >
   > Vedere "Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione".

2. Selezionare **Crea**.

   Viene creata la regola ILM. La regola non diventa attiva fino a quando non viene aggiunta a e il criterio non "Policy ILM"viene attivato.

   Per visualizzare i dettagli della regola, selezionare il nome della regola nella pagina delle regole ILM.

Creare una regola ILM predefinita

Prima di creare un criterio ILM, è necessario creare una regola predefinita per inserire nel criterio gli oggetti non corrispondenti a un'altra regola. La regola predefinita non può utilizzare alcun filtro. Deve essere applicato a tutti i tenant, a tutti i bucket e a tutte le versioni degli oggetti.

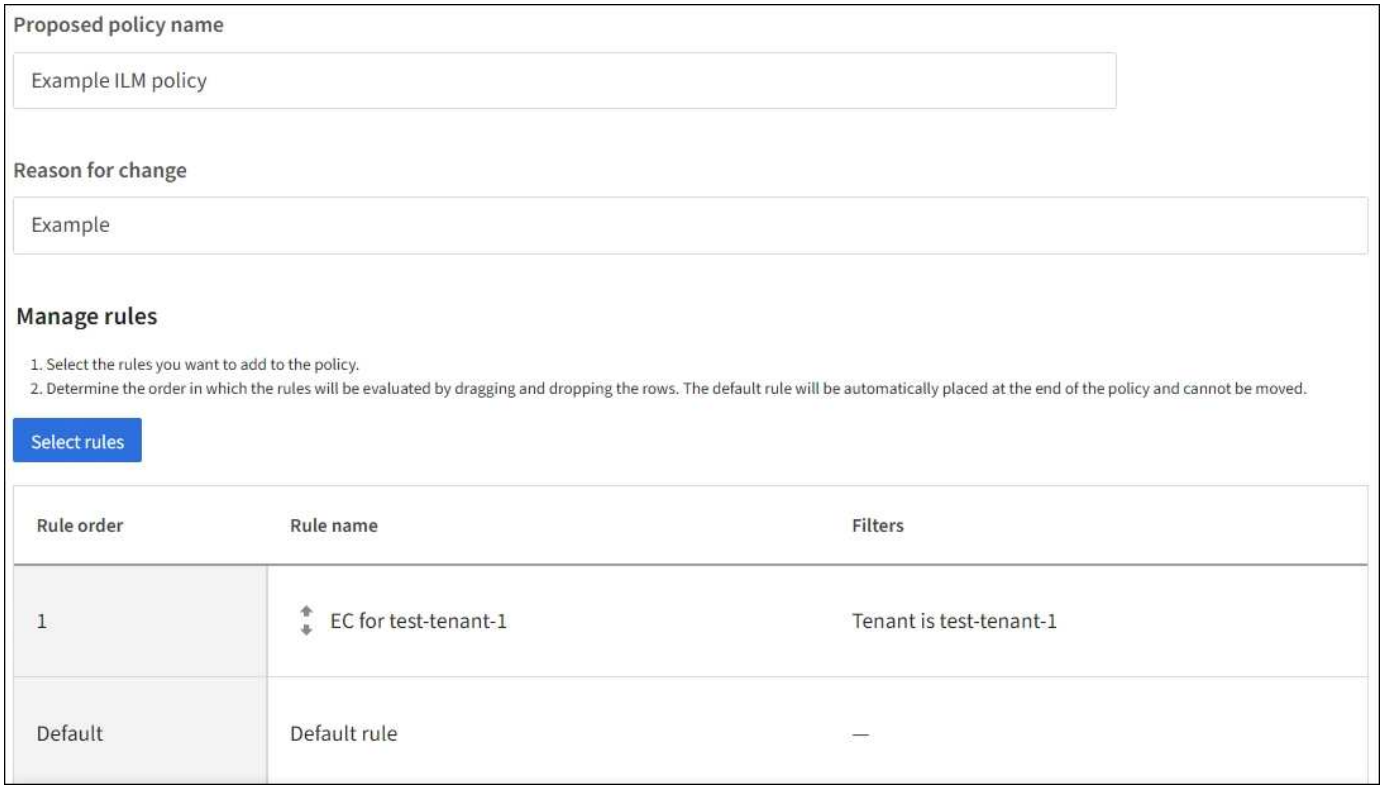
Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".

A proposito di questa attività

La regola predefinita è l'ultima regola da valutare in un criterio ILM, quindi 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 criterio di esempio, la prima regola si applica solo agli oggetti appartenenti a test-tenant-1. 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 posizionata automaticamente come ultima regola quando viene aggiunta a un criterio.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita deve essere applicata a tutte le versioni degli oggetti.
- 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 gli oggetti più piccoli vengano sottoposti a erasure coding.

- In generale, la regola predefinita deve conservare gli oggetti per sempre.
- Se si utilizza (o si prevede di abilitare) l'impostazione blocco oggetti S3 globale, la regola predefinita deve essere conforme.

Fasi

1. Selezionare **ILM** > **regole**.
2. Selezionare **Crea**.

   Viene visualizzata la fase 1 (immettere i dettagli) della creazione guidata regola ILM.

3. Immettere un nome univoco per la regola nel campo **Nome regola**.
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 la selezione a discesa Nome bucket come **si applica a tutti i bucket**.

   La regola predefinita deve essere applicata a tutti i bucket S3.

7. Mantenere la risposta predefinita, **No**, per la domanda, "applicare questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?"
8. Non aggiungere filtri avanzati.

   La regola predefinita non può specificare alcun filtro.

9. Selezionare **Avanti**.

   Viene visualizzato il punto 2 (definizione delle posizioni).

10. Per Reference Time (ora di riferimento), selezionare un'opzione qualsiasi.

    Se è stata mantenuta la risposta predefinita, **No**, per la domanda "applicare questa regola solo alle versioni precedenti degli oggetti?" L'ora non corrente non verrà inclusa nell'elenco a discesa. La regola predefinita deve applicare tutte le versioni degli oggetti.

11. 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 **dimensione oggetto (MB) maggiore di 200 KB** per evitare che gli 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 Cloud Storage Pool.
  - 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 "per sempre".

12. Consultare il diagramma di conservazione per confermare le istruzioni di posizionamento.
13. Selezionare **continua**.

    Viene visualizzato il passaggio 3 (selezionare il comportamento di acquisizione).

14. Selezionare l'opzione di acquisizione da utilizzare e selezionare **Crea**.

Gestire le policy ILM

Utilizzare i criteri 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.

> 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.

Policy ILM predefinita

Quando si installa StorageGRID e si aggiungono siti, viene creato automaticamente un criterio ILM predefinito, come segue:

- Se la griglia contiene un sito, il criterio predefinito contiene una regola predefinita che replica due copie di ciascun oggetto in quel sito.
- Se la griglia contiene più siti, la regola predefinita replica una copia di ciascun oggetto in ciascun sito.

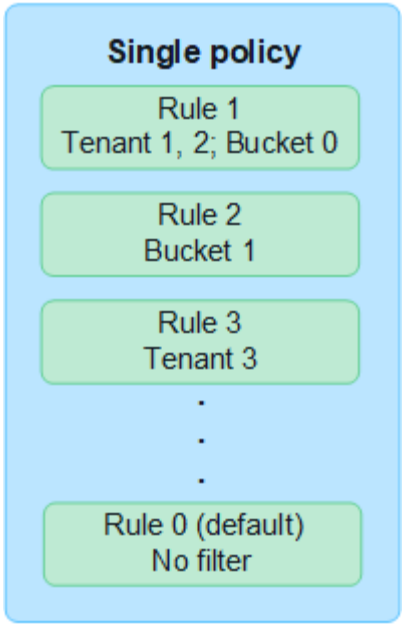
Se il criterio predefinito non soddisfa i requisiti di storage, è possibile creare regole e policy personalizzate. Vedere "Creare una regola ILM" e "Creare un criterio ILM".

Una o più policy ILM attive?

È possibile disporre di uno o più criteri ILM attivi alla volta.

Un'unica policy

Se il grid usa un semplice schema di data Protection con poche regole specifiche del tenant e del bucket, utilizza una singola policy ILM attiva. Le regole ILM possono contenere filtri per gestire bucket o tenant diversi.



Quando si dispone di un solo criterio e i requisiti di un tenant cambiano, è necessario creare un nuovo criterio ILM o clonare il criterio esistente per applicare le modifiche, simulare e attivare quindi il nuovo criterio ILM. Le modifiche alla policy ILM possono comportare spostamenti degli oggetti che possono richiedere molti giorni e causare la latenza del sistema.

Policy multiple

Per offrire opzioni di qualità del servizio diverse ai tenant, è possibile disporre di più policy attive alla volta. Ogni policy può gestire tenant specifici, bucket S3 e oggetti. Quando si applicano o si modifica una policy per un insieme specifico di tenant o oggetti, le policy applicate agli altri tenant e oggetti non verranno influenzate.

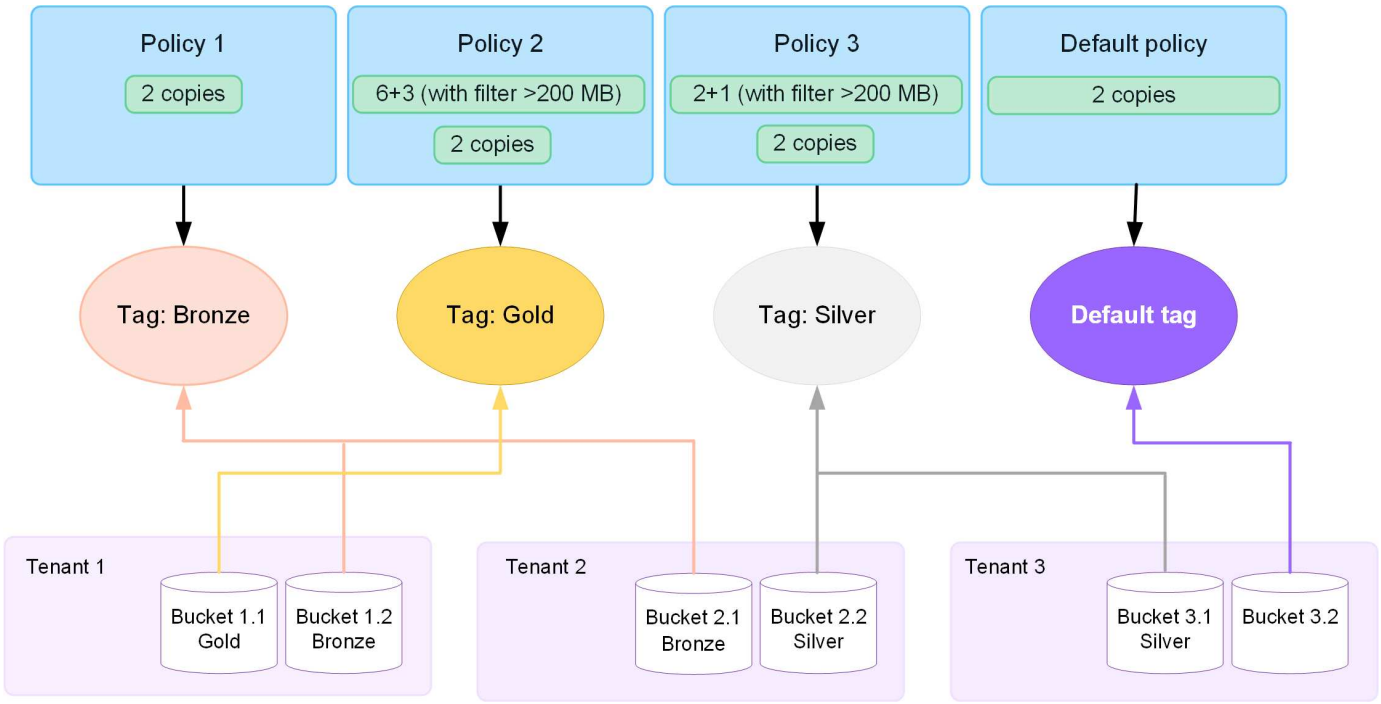
Tag dei criteri ILM

Se desideri consentire ai tenant di alternare facilmente tra più policy di data Protection in base al bucket, utilizza policy ILM multiple con *tag policy ILM*. Ogni policy ILM viene assegnata a un tag, quindi i tenant etichettano un bucket per applicare la policy a quel bucket. È possibile impostare tag di policy ILM solo su bucket S3.

Ad esempio, potresti avere tre tag denominati Gold, Silver e Bronze. È possibile assegnare un criterio ILM a ciascun tag in base alla durata e alla posizione in cui tale criterio memorizza gli oggetti. I tenant possono scegliere la policy da utilizzare contrassegnando i propri bucket. Un bucket con tag Gold viene gestito dalla policy Gold e riceve il livello Gold di data Protection e performance.

Tag criterio ILM predefinito

Quando si installa StorageGRID, viene creato automaticamente un tag di criterio ILM predefinito. Ogni griglia deve avere un criterio attivo assegnato al tag predefinito. Il criterio predefinito si applica a tutti i bucket S3 non contrassegnati.



In che modo un criterio ILM valuta gli oggetti?

Una policy ILM attiva controlla il posizionamento, la durata e la protezione dei dati degli oggetti.

Quando i client salvano gli oggetti in StorageGRID, gli oggetti vengono valutati in base all'insieme ordinato di regole ILM nel criterio, 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. La regola predefinita deve essere applicata a tutti i tenant, a tutti i bucket S3 e a tutte le versioni degli oggetti e non può utilizzare alcun filtro avanzato.

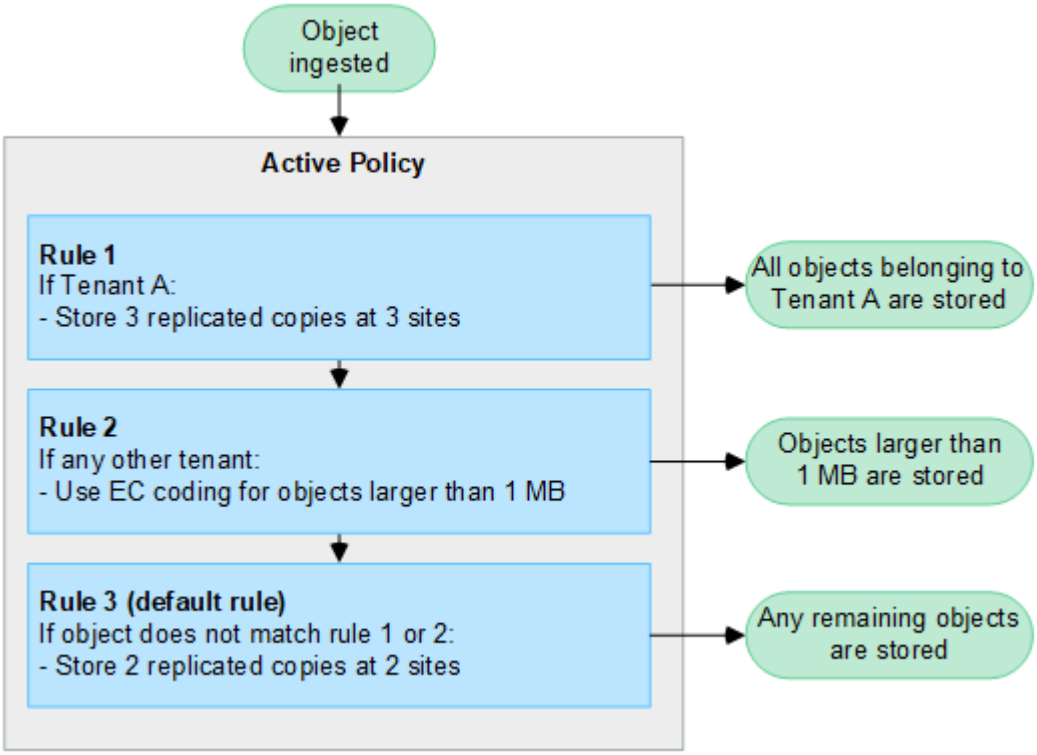
Esempio di policy ILM

Ad esempio, un criterio ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per il tenant A**
  - Abbina tutti gli oggetti appartenenti al tenant A.
  - Memorizzare questi oggetti 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.
- **Regola 2: Erasure coding per oggetti superiori a 1 MB**
  - Associare tutti gli oggetti degli altri tenant, ma solo se sono superiori a 1 MB. Questi oggetti più grandi vengono memorizzati utilizzando la codifica di cancellazione 6+3 in tre siti.

- Non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati in base alla regola 3.

- **Regola 3: 2 copie 2 data center** (impostazione predefinita)
  - È l'ultima regola predefinita del criterio. Non utilizza filtri.
  - Creare 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).



Cosa sono i criteri attivi e inattivi?

Ogni sistema StorageGRID deve avere almeno una policy ILM attiva. Se si desidera disporre di più criteri ILM attivi, è necessario creare tag dei criteri ILM e assegnare un criterio a ciascun tag. I tenant applicano quindi i tag ai bucket S3. Il criterio predefinito viene applicato a tutti gli oggetti nei bucket che non hanno un tag di criterio assegnato.

Quando si crea per la prima volta un criterio ILM, selezionare una o più regole ILM e disporle in un ordine specifico. Dopo aver simulato il criterio per confermarne il comportamento, lo si attiva.

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

Se si attivano più policy ILM alla volta e i tenant applicano tag ai bucket S3, gli oggetti in ogni bucket vengono gestiti in base alla policy assegnata al tag.

Un sistema StorageGRID tiene traccia della cronologia delle policy attivate o disattivate.

Considerazioni per la creazione di un criterio ILM

- Utilizzare solo il criterio fornito dal sistema, il criterio di base 2 copie, nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola Make 2 Copies in 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.

> Il pool di storage All Storage Node viene creato automaticamente durante l'installazione di StorageGRID 11.6 e versioni precedenti. Se si esegue l'aggiornamento a una versione successiva di StorageGRID, il pool di tutti i nodi di storage continuerà a esistere. Se si installa StorageGRID 11.7 o versione successiva come nuova installazione, il pool di tutti i nodi di storage non viene creato.

- 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 oggetto non verrà valutato 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.

Creare policy ILM

Create una o più policy ILM per soddisfare i vostri requisiti di qualità del servizio.

La presenza di una policy ILM attiva ti consente di applicare le stesse regole ILM a tutti i tenant e bucket.

La disponibilità di più policy ILM attive ti consente di applicare le regole ILM appropriate a tenant e bucket specifici per soddisfare più requisiti di qualità del servizio.

Creare un criterio ILM

A proposito di questa attività

Prima di creare un criterio personalizzato, verificare che "Policy ILM predefinita"non soddisfi i requisiti di archiviazione.

> Utilizzare solo i criteri forniti dal sistema, 2 Copies Policy (per le griglie a un sito) o 1 Copy per Site (per le griglie a più siti), nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola predefinita in 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 la "L'impostazione Global S3 Object Lock (blocco oggetti S3 globale) è stata attivata", è necessario assicurarsi che il criterio ILM sia conforme ai requisiti dei bucket che hanno attivato blocco oggetti S3. In questa sezione, seguire le istruzioni relative all'attivazione del blocco oggetti S3.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso richieste".
- L'utente si "Regole ILM create"basa sull'attivazione di blocco oggetti S3.

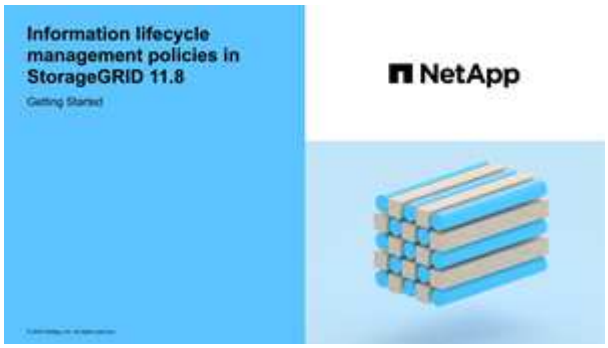
Blocco oggetti S3 non abilitato

- Da "Creazione delle regole ILM"aggiungere al criterio. Se necessario, è possibile salvare un criterio, creare regole aggiuntive e quindi modificarlo per aggiungerne di nuove.
- Non sono presenti "Creazione di una regola ILM predefinita"filtri.

Blocco oggetti S3 attivato

- "L'impostazione Global S3 Object Lock (blocco oggetti S3 globale) è già attivata"Per il sistema StorageGRID.
- Da "Creazione delle regole ILM conformi e non conformi"aggiungere al criterio. Se necessario, è possibile salvare un criterio, creare regole aggiuntive e quindi modificarlo per aggiungerne di nuove.
- Si dispone di "Creazione di una regola ILM predefinita" per il criterio che è conforme.

- Se si desidera, è stato guardato il video: "Video: Panoramica dei criteri ILM"



Vedere anche "Utilizzare i criteri ILM".

Fasi

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

   Se l'impostazione blocco oggetti S3 globale è attivata, la pagina dei criteri ILM indica quali regole ILM sono conformi.

2. Stabilire come si desidera creare il criterio ILM.

Creare una nuova policy

a. Selezionare **Crea policy**.

Clonazione della policy esistente

a. Selezionare la casella di controllo relativa al criterio che si desidera iniziare, quindi selezionare **Clona**.

Modifica criterio esistente

a. Se un criterio è inattivo, è possibile modificarlo. Selezionare la casella di controllo per il criterio inattivo che si desidera iniziare, quindi selezionare **Modifica**.

3. Nel campo **Nome criterio**, immettere un nome univoco per la policy.
4. Facoltativamente, nel campo **motivo della modifica**, immettere il motivo per cui si sta creando un nuovo criterio.
5. Per aggiungere regole al criterio, selezionare **Seleziona regole**. Selezionare il nome di una regola per visualizzare le relative impostazioni.

   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, è possibile spostarla alla fine del nuovo criterio.

Blocco oggetti S3 non abilitato

a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, selezionare **pagina regole ILM**.

   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.

   > 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.

Blocco oggetti S3 attivato

a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, selezionare **pagina regole ILM**.

   L'elenco delle regole contiene solo le regole che sono conformi e non utilizzano filtri.

   > 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.

b. Se è necessaria una regola "predefinita" diversa per gli oggetti nei bucket S3 non conformi, selezionare **Includi una regola senza filtri per i bucket S3 non conformi** e selezionare una regola non conforme che non utilizza un filtro.

   Ad esempio, è possibile utilizzare un Cloud Storage Pool per memorizzare oggetti in bucket che non hanno attivato il blocco oggetti S3.

   > È possibile selezionare solo una regola non conforme che non utilizza un filtro.

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

6. Una volta selezionata la regola predefinita, selezionare **continua**.
7. Per il passo altre regole, selezionare le altre regole che si desidera aggiungere al criterio. Queste regole utilizzano almeno un filtro (account tenant, nome bucket, filtro avanzato o tempo di riferimento non corrente). Quindi selezionare **Seleziona**.

   La finestra Crea un criterio elenca ora le regole selezionate. La regola predefinita è alla fine, con le altre regole sopra di essa.

   Se S3 Object Lock è attivato e è stata selezionata anche una regola "predefinita" non conforme, tale regola viene aggiunta come regola dalla seconda all'ultima nel criterio.

Viene visualizzato un avviso se una regola non mantiene 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 per un periodo di tempo più lungo).

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

   Impossibile spostare la regola predefinita. Se S3 Object Lock è attivato, non è possibile spostare la regola "predefinita" non conforme se ne è stata selezionata una.

   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.

9. Se necessario, selezionare **Select rules** (Seleziona regole) per aggiungere o rimuovere le regole.
10. Al termine, selezionare **Salva**.
11. Ripetere questa procedura per creare ulteriori criteri ILM.
12. Simulare un criterio ILM. È necessario simulare sempre un criterio prima di attivarlo per assicurarsi che funzioni come previsto.

Simulare una policy

Simula una policy sugli oggetti di test prima di attivarla e applicarla ai dati di produzione.

Prima di iniziare

- Si conosce il bucket S3/oggetto-chiave per ogni oggetto che si desidera testare.

Fasi

1. Utilizzando un client S3 o "S3 Console", acquisire gli oggetti necessari per testare ciascuna regola.
2. Nella pagina criteri ILM, selezionare la casella di controllo relativa al criterio, quindi selezionare **simula**.
3. Nel campo **oggetto**, immettere S3 `bucket/object-key` per un oggetto di test. Ad esempio, `bucket-01/filename.png`.
4. Se la versione S3 è attivata, è possibile immettere un ID versione per l'oggetto nel campo **ID versione**.
5. Selezionare **simulate**.
6. Nella sezione risultati di Simulation, verificare che ogni oggetto sia stato associato alla regola corretta.
7. Per determinare quale profilo di pool storage o erasure coding è in vigore, seleziona il nome della regola abbinata e vai alla pagina dei dettagli della regola.

Esaminare eventuali modifiche al posizionamento degli oggetti replicati e con erasure coding esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Risultati

Eventuali modifiche alle regole del criterio verranno riflesse nei risultati di Simulation e mostreranno la nuova corrispondenza e la corrispondenza precedente. La finestra dei criteri di simulazione mantiene gli oggetti testati fino a quando non si seleziona **Cancella tutto** o l'icona di rimozione per ogni oggetto nell'elenco dei risultati di Simulation.

Informazioni correlate

"Esempi di simulazioni dei criteri ILM"

Attivare un criterio

Quando si attiva un singolo nuovo criterio ILM, gli oggetti esistenti e gli oggetti appena acquisiti vengono gestiti da tale criterio. Quando si attivano più policy, i tag dei criteri ILM assegnati ai bucket determinano gli oggetti da gestire.

Prima di attivare un nuovo criterio:

1. Simulare il criterio per confermare che si comporta come previsto.
2. Esaminare eventuali modifiche al posizionamento degli oggetti replicati e con erasure coding esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

> Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile.

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. In particolare:

- Se si apportano modifiche ai criteri 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 ai criteri che **potrebbero ridurre la ridondanza o la durata dei dati**, tali modifiche non verranno implementate finché non saranno disponibili tutti i nodi della griglia. Ad esempio, se si attiva un nuovo criterio che utilizza una regola di due copie invece di una regola di tre copie, il nuovo criterio viene visualizzato nella scheda criterio attivo, ma non avrà effetto fino a quando tutti i nodi non saranno online e disponibili.

Fasi

Seguire la procedura per attivare uno o più criteri:

Attivare un criterio

Se si dispone di un solo criterio attivo, procedere come segue. Se si dispone già di uno o più criteri attivi e si stanno attivando criteri aggiuntivi, seguire la procedura per l'attivazione di più criteri.

1. Quando si è pronti ad attivare un criterio, selezionare **ILM** > **Criteri**.

   In alternativa, è possibile attivare un singolo criterio dalla pagina **ILM** > **Policy tags**.

2. Nella scheda Criteri, selezionare la casella di controllo relativa al criterio che si desidera attivare, quindi selezionare **attiva**.
3. Seguire la procedura appropriata:
   - Se viene visualizzato un messaggio di avviso che richiede di confermare l'attivazione del criterio, selezionare **OK**.
   - Se viene visualizzato un messaggio di avviso contenente i dettagli relativi al criterio:
     i. Esaminare i dettagli per assicurarsi che i criteri gestiscano i dati come previsto.
     ii. Se la regola predefinita memorizza gli oggetti per un numero limitato di giorni, esaminare il diagramma di conservazione e digitare il numero di giorni nella casella di testo.
     iii. Se la regola predefinita memorizza gli oggetti per sempre, ma una o più altre regole hanno una conservazione limitata, digitare **yes** nella casella di testo.
     iv. Selezionare **attiva criterio**.

Attivare più policy

Per attivare più criteri, è necessario creare tag e assegnare un criterio a ciascun tag.

> Quando vengono utilizzati più tag, se i tenant riassegnano frequentemente i tag delle policy ai bucket, le performance del grid potrebbero risentirne. Se si dispone di tenant non attendibili, utilizzare solo il tag predefinito.

1. Selezionare **ILM** > **Policy tag**.
2. Selezionare **Crea**.
3. Nella finestra di dialogo Crea tag criterio, digitare un nome di tag e, facoltativamente, una descrizione per il tag.

   > I nomi e le descrizioni dei tag sono visibili ai locatari. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se il criterio assegnato eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni riservate in questi campi.

4. Selezionare **Crea tag**.
5. Nella tabella tag criteri ILM, utilizzare il menu a discesa per selezionare un criterio da assegnare al tag.
6. Se gli avvisi vengono visualizzati nella colonna limitazioni criteri, selezionare **Visualizza dettagli criteri** per rivedere il criterio.
7. Assicurarsi che ogni policy gestisca i dati come previsto.
8. Selezionare **attiva criteri assegnati**. In alternativa, selezionare **Cancella modifiche** per rimuovere

l'assegnazione dei criteri.

9. Nella finestra di dialogo attiva criteri con nuovi tag, rivedere le descrizioni di come ciascun tag, criterio e regola gestirà gli oggetti. Apportare le modifiche necessarie per garantire che le policy gestiscano gli oggetti nel modo previsto.
10. Quando si è certi di voler attivare i criteri, digitare **yes** nella casella di testo, quindi selezionare **Activate policies** (attiva criteri).

Informazioni correlate

"Esempio 6: Modifica di un criterio ILM"

Esempi di simulazioni dei criteri ILM

Gli esempi di simulazioni dei criteri ILM forniscono linee guida per strutturare e modificare le simulazioni per l'ambiente in uso.

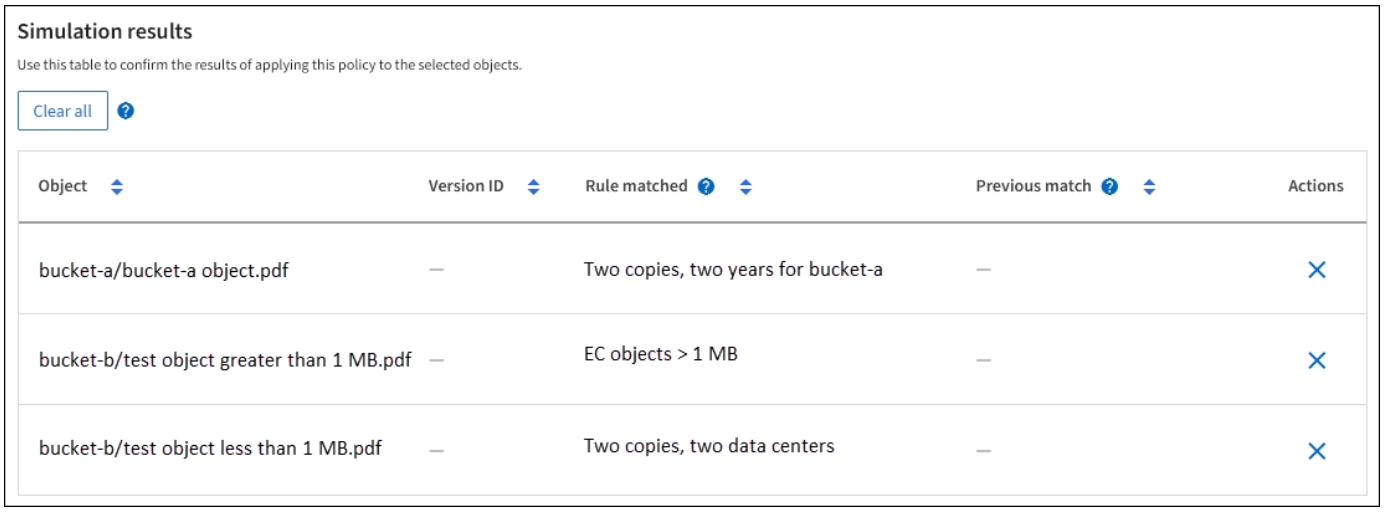
Esempio 1: Verifica delle regole durante la simulazione di un criterio ILM

In questo esempio viene descritto come verificare le regole durante la simulazione di un criterio.

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, **due copie, due data center**, è la regola predefinita. Non include filtri e non utilizza il tempo di riferimento non corrente.

Dopo aver simulato il criterio, verificare che ogni oggetto sia stato associato alla regola corretta.



In questo esempio:

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

- `bucket-b/test object less than 1 MB.pdf` non corrisponde ai filtri nelle prime due regole, quindi viene posizionata in base alla regola predefinita, che non include filtri.

Esempio 2: Riordinare le regole durante la simulazione di un criterio ILM

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

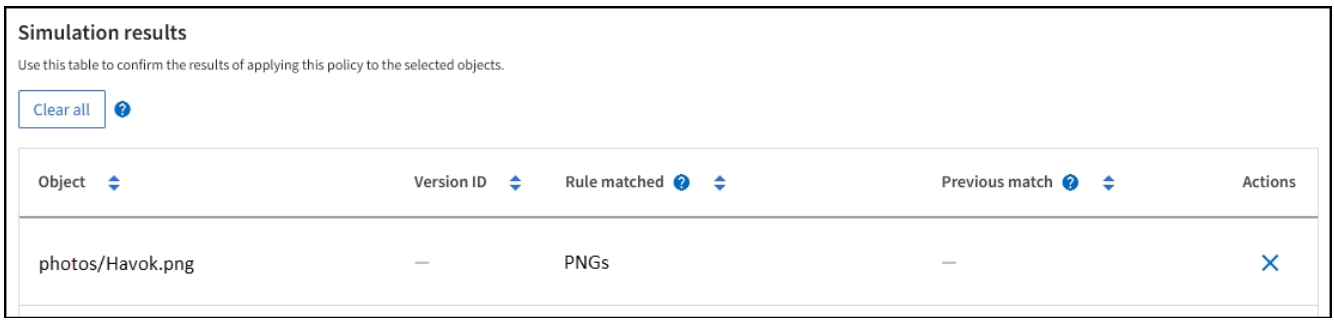
In questo esempio, viene simulata la policy **Demo**. Questo criterio, che ha lo scopo di trovare oggetti con metadati utente series=x-men, include tre regole, come segue:

- La prima regola, **PNGS**, filtra i nomi delle chiavi che terminano in `.png`.
- La seconda regola, **X-men**, si applica solo agli oggetti per il tenant A e ai filtri per i `series=x-men` metadati 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, selezionare **simulate**.
2. Nel campo **Object**, immettere il bucket S3/object-key per un oggetto test e selezionare **simulate**.

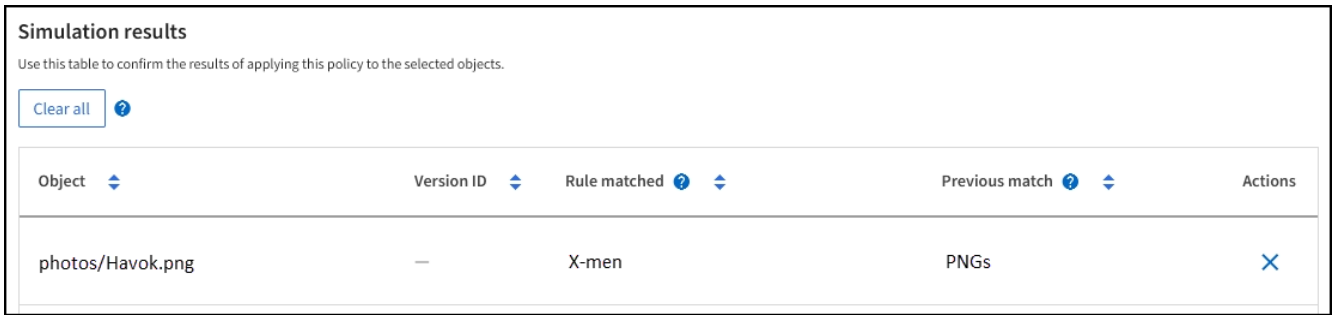
   Vengono visualizzati i risultati di Simulation, che mostrano che l' `Havok.png`oggetto è stato associato alla regola **PNGS**.



   Tuttavia, `Havok.png` era destinato a testare la regola **X-men**.

3. Per risolvere il problema, riordinare le regole.
   a. Selezionare **fine** per chiudere la finestra Simula policy ILM.
   b. Selezionare **Edit** (Modifica) per modificare la policy.
   c. Trascinare la regola **X-MEN** all'inizio dell'elenco.
   d. Selezionare **Salva**.
4. Selezionare **simulate**.

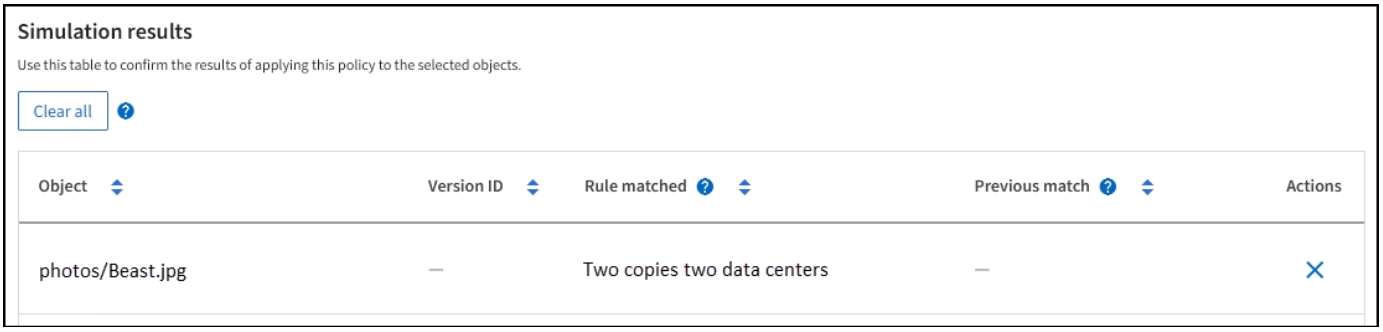
   Gli oggetti precedentemente testati vengono rivalutati in base alla policy aggiornata e vengono visualizzati i risultati della nuova simulazione. Nell'esempio, la colonna regola corrispondente mostra che l' `Havok.png`oggetto ora corrisponde alla regola dei metadati X-MEN, come previsto. La colonna di confronto precedente mostra che la regola PNG corrisponde all'oggetto nella simulazione precedente.



Esempio 3: Correggere una regola durante la simulazione di un criterio ILM

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 consente di trovare oggetti che contengono `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati imprevisti durante la simulazione di questo criterio rispetto all' `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.

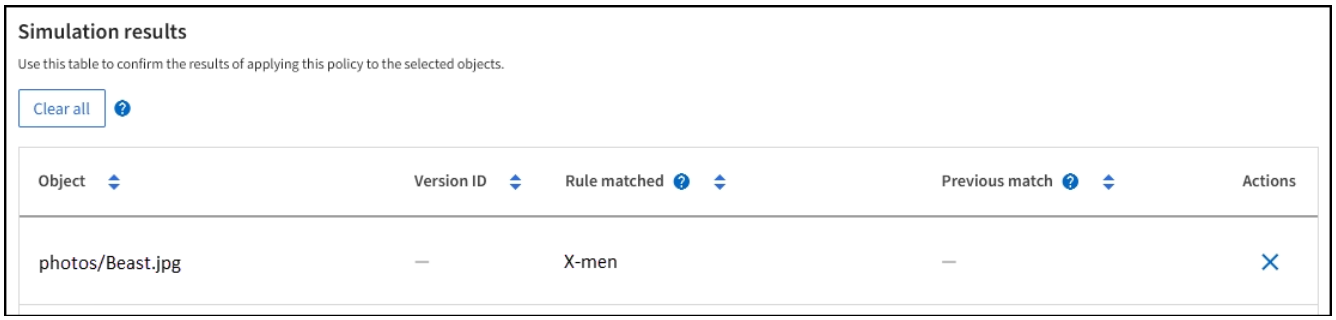
Fasi

1. Selezionare **fine** per chiudere la finestra di dialogo Simula policy. Nella pagina dei dettagli del criterio, selezionare **diagramma di conservazione**. Quindi, selezionare **Espandi tutto** o **Visualizza dettagli** per ogni regola in base alle necessità.
2. Esaminare l'account tenant della regola, il tempo di riferimento e i criteri di filtraggio.

   Ad esempio, supponiamo che i metadati per la regola X-men siano stati immessi come "x-men01" invece di "x-men".

3. Per risolvere l'errore, correggere la regola come segue:
   - Se la regola fa parte del criterio, 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.
4. Eseguire nuovamente la simulazione.

   In questo esempio, la regola X-MEN corretta corrisponde ora all' `Beast.jpg`oggetto in base ai `series=x-men` metadati dell'utente, come previsto.



Gestire i tag dei criteri ILM

È possibile visualizzare i dettagli dei tag dei criteri ILM, modificare un tag o rimuovere un tag.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso richieste".

Visualizzare i dettagli dei tag dei criteri ILM

Per visualizzare i dettagli di un tag:

1. Selezionare **ILM** > **Policy tag**.
2. Selezionare il nome del criterio dalla tabella. Viene visualizzata la pagina dei dettagli del tag.
3. Nella pagina dei dettagli, visualizzare la cronologia precedente dei criteri assegnati.
4. Consente di visualizzare un criterio selezionandolo.

Modifica tag criterio ILM

> I nomi e le descrizioni dei tag sono visibili ai locatari. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se il criterio assegnato eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni riservate in questi campi.

Per modificare la descrizione di un tag esistente:

1. Selezionare **ILM** > **Policy tag**.
2. Seleziona la casella di controllo per il tag, quindi seleziona **Modifica**.

   In alternativa, selezionare il nome del tag. Viene visualizzata la pagina dei dettagli del tag ed è possibile selezionare **Modifica** in quella pagina.

3. Modificare la descrizione del tag secondo necessità
4. Selezionare **Salva**.

Rimuovere il tag criterio ILM

Quando si rimuove un tag di criterio, a tutti i bucket a cui è assegnato tale tag verrà applicato il criterio predefinito.

Per rimuovere un'etichetta:

1. Selezionare **ILM** > **Policy tag**.
2. Selezionare la casella di controllo per il tag, quindi selezionare **Rimuovi**. Viene visualizzata una finestra di dialogo di conferma.

   In alternativa, selezionare il nome del tag. Viene visualizzata la pagina dei dettagli del tag ed è possibile selezionare **Rimuovi** in quella pagina.

3. Selezionare **Sì** per eliminare il tag.

Verificare un criterio ILM con la ricerca dei metadati degli oggetti

Dopo aver attivato una policy ILM, acquisire gli oggetti di test rappresentativi nel sistema StorageGRID, quindi eseguire una ricerca nei metadati degli oggetti per confermare la creazione delle copie nella maniera prevista e il posizionamento nelle posizioni corrette.

Prima di iniziare

Si dispone di un identificatore di oggetto, che può essere uno di: * **UUID**: L'identificatore univoco universale dell'oggetto. * **CBID**: L'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. * **Bucket S3 e oggetto chiave**: Quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di bucket e oggetto chiave per memorizzare e identificare l'oggetto. Se il bucket S3 è dotato di versione e si desidera cercare una versione specifica di un oggetto S3 utilizzando il bucket e la chiave Object, si dispone dell' **version ID**.

Fasi

1. Acquisire l'oggetto.
2. Selezionare **ILM** > **Object metadata lookup**.
3. Digitare l'identificativo dell'oggetto nel campo **Identifier**. È possibile immettere un UUID, CBID o un bucket/oggetto S3.
4. Facoltativamente, inserire un ID versione per l'oggetto (solo S3).
5. Selezionare **Cerca**.

   Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

   - Metadati di sistema, come ID oggetto (UUID), tipo di risultato (oggetto, marker di eliminazione, bucket S3) e dimensioni logiche dell'oggetto. Per ulteriori dettagli, fare riferimento alla schermata di esempio riportata di seguito.
   - 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.

6. Verificare che l'oggetto sia memorizzato nella posizione o nelle posizioni corrette e che sia il 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 "Esaminare i registri di audit".

Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.

> La seguente schermata è un esempio. I risultati variano a seconda della versione di StorageGRID in uso.

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",
```


Informazioni correlate

"UTILIZZARE L'API REST S3"

Utilizzare le policy ILM e le regole ILM

In caso di cambiamento dei requisiti di storage, potrebbe essere necessario implementare criteri aggiuntivi o modificare le regole ILM associate a un criterio. È possibile visualizzare le metriche ILM per determinare le performance del sistema.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".

Visualizza i criteri ILM

Per visualizzare i criteri ILM attivi e inattivi e la cronologia di attivazione dei criteri:

1. Selezionare **ILM** > **Policy**.
2. Selezionare **Criteri** per visualizzare un elenco di criteri attivi e inattivi. La tabella elenca il nome di ciascun criterio, i tag a cui è assegnato il criterio e se il criterio è attivo o inattivo.
3. Selezionare **Cronologia attivazioni** per visualizzare un elenco delle date di inizio e di fine delle attivazioni per i criteri.
4. Selezionare il nome di un criterio per visualizzarne i dettagli.

> Se si visualizzano i dettagli di un criterio il cui stato è modificato o eliminato, viene visualizzato un messaggio che spiega che si sta visualizzando la versione del criterio che era attiva per l'intervallo di tempo specificato e che è stata successivamente modificata o eliminata.

Modificare un criterio ILM

È possibile modificare solo un criterio inattivo. Se si desidera modificare un criterio attivo, disattivarlo o creare un clone e modificarlo.

Per modificare un criterio:

1. Selezionare **ILM** > **Policy**.
2. Selezionare la casella di controllo relativa al criterio che si desidera modificare, quindi selezionare **Modifica**.
3. Modificare il criterio seguendo le istruzioni riportate in "Creare policy ILM".
4. Simulare il criterio prima di riattivarlo.

> 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.

Clonazione di una policy ILM

Per clonare un criterio ILM:

1. Selezionare **ILM** > **Policy**.
2. Selezionare la casella di controllo relativa al criterio da clonare, quindi selezionare **Clona**.
3. Creare un nuovo criterio a partire dal criterio clonato seguendo le istruzioni riportate in "Creare policy ILM".

> 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.

Rimuovere un criterio ILM

È possibile rimuovere un criterio ILM solo se è inattivo. Per rimuovere un criterio:

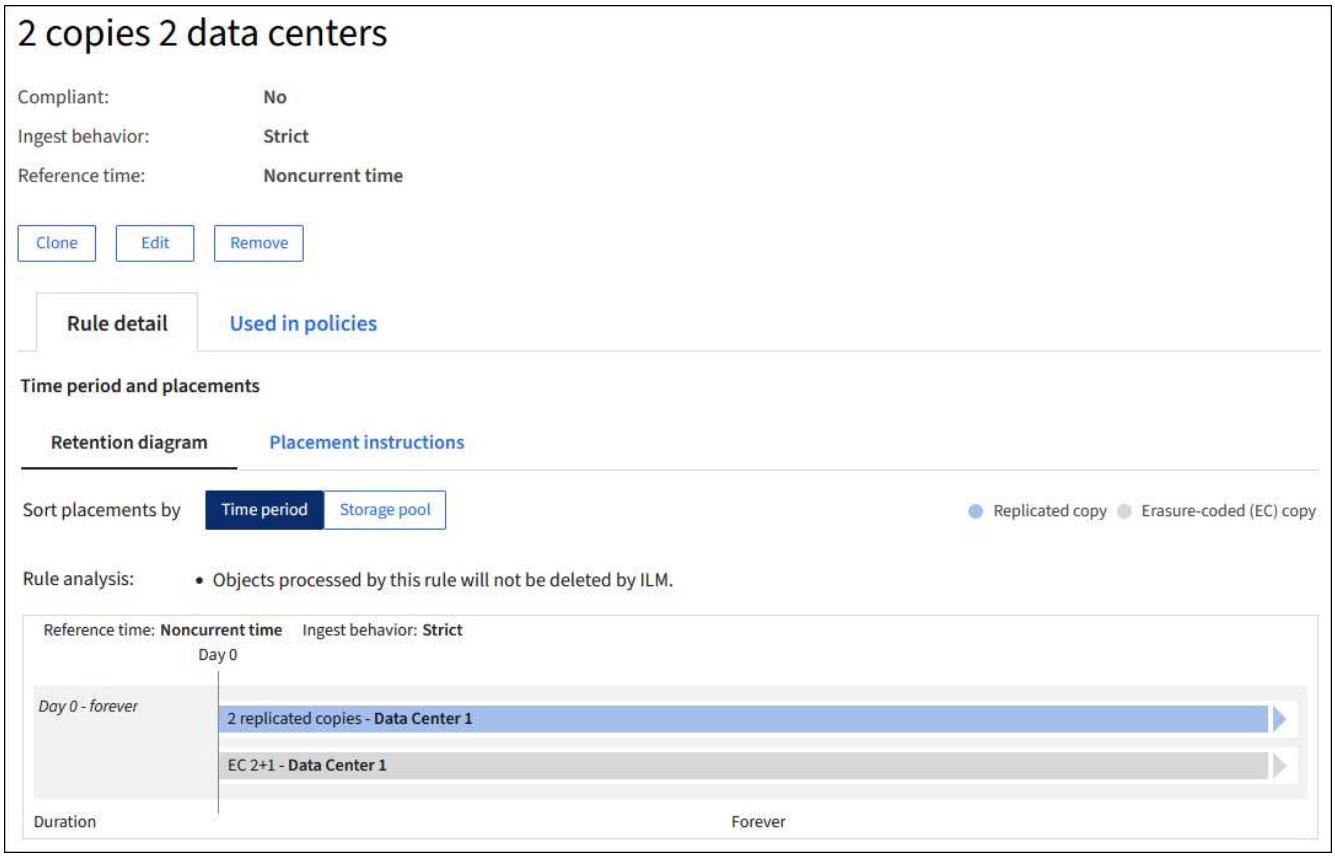
1. Selezionare **ILM** > **Policy**.
2. Selezionare la casella di controllo relativa al criterio inattivo che si desidera rimuovere.

3. Selezionare **Rimuovi**.

Visualizza i dettagli della regola ILM

Per visualizzare i dettagli di una regola ILM, inclusi il diagramma di conservazione e le istruzioni di posizionamento della regola:

1. Selezionare **ILM** > **regole**.
2. Selezionare il nome della regola di cui si desidera visualizzare i dettagli. Esempio:



Inoltre, è possibile utilizzare la pagina dei dettagli per clonare, modificare o rimuovere una regola. Non è possibile modificare o rimuovere una regola se utilizzata in alcun criterio.

Clonare una regola ILM

È possibile clonare una regola esistente se si desidera creare una nuova regola che utilizzi alcune delle impostazioni della regola esistente. Se è necessario modificare una regola utilizzata in qualsiasi criterio, è necessario clonare la regola e apportare le modifiche al clone. Una volta apportate le modifiche al clone, è possibile rimuovere la regola originale dal criterio e sostituirla con la versione modificata, se necessario.

> Non è possibile clonare una regola ILM se è stata creata utilizzando StorageGRID versione 10.2 o precedente.

Fasi

1. Selezionare **ILM** > **regole**.
2. Selezionare la casella di controllo della regola da clonare, quindi selezionare **Clone**. In alternativa,

selezionare il nome della regola, quindi selezionare **Clone** dalla pagina dei dettagli della regola.

3. Aggiornare la regola clonata seguendo i passaggi per Modifica di una regola ILM e "Utilizzo di filtri avanzati nelle regole ILM".

   Quando si clonano una regola ILM, è necessario immettere un nuovo nome.

Modificare una regola ILM

Potrebbe essere necessario modificare una regola ILM per modificare un filtro o un'istruzione di posizionamento.

Non è possibile modificare una regola se utilizzata in qualsiasi criterio ILM. È possibile clonare la regolaapportare tutte le modifiche necessarie alla copia clonata.

> 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.

Fasi

1. Selezionare **ILM** > **regole**.
2. Verificare che la regola che si desidera modificare non sia utilizzata in alcun criterio ILM.
3. Se la regola che si desidera modificare non è in uso, selezionare la casella di controllo corrispondente e selezionare **azioni** > **Modifica**. In alternativa, selezionare il nome della regola, quindi selezionare **Modifica** nella pagina dei dettagli della regola.
4. Completare i passaggi della procedura guidata Modifica regola ILM. Se necessario, seguire i passi per "Creazione di una regola ILM" e "Utilizzo di filtri avanzati nelle regole ILM".

   Quando si modifica una regola ILM, non è possibile modificarne il nome.

Rimuovere una regola ILM

Per mantenere gestibile l'elenco delle regole ILM correnti, rimuovi tutte le regole ILM che non sei in grado di utilizzare.

Fasi

Per rimuovere una regola ILM attualmente utilizzata in un criterio attivo:

1. Clonazione della policy.
2. Rimuovere la regola ILM dal clone dei criteri.
3. Salvare, simulare e attivare il nuovo criterio per assicurarsi che gli oggetti siano protetti come previsto.
4. Passare alla procedura per la rimozione di una regola ILM attualmente utilizzata in un criterio inattivo.

Per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo:

1. Selezionare il criterio inattivo.
2. Rimuovere la regola ILM dal criterio o rimuovere il criterio.
3. Passare alla procedura per la rimozione di una regola ILM non attualmente utilizzata.

Per rimuovere una regola ILM attualmente non utilizzata:

1. Selezionare **ILM** > **regole**.
2. Verificare che la regola che si desidera rimuovere non venga utilizzata in alcun criterio.
3. Se la regola che si desidera rimuovere non è in uso, selezionarla e scegliere **azioni** > **Rimuovi**. È possibile selezionare più regole e rimuoverle tutte contemporaneamente.
4. Selezionare **Sì** per confermare che si desidera rimuovere la regola ILM.

Visualizza metriche ILM

È possibile visualizzare le metriche per ILM, ad esempio il numero di oggetti nella coda e il tasso di valutazione. È possibile monitorare queste metriche per determinare le performance del sistema. Una grande coda o un tasso di valutazione 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 eccessivo o che esistono condizioni anomale.

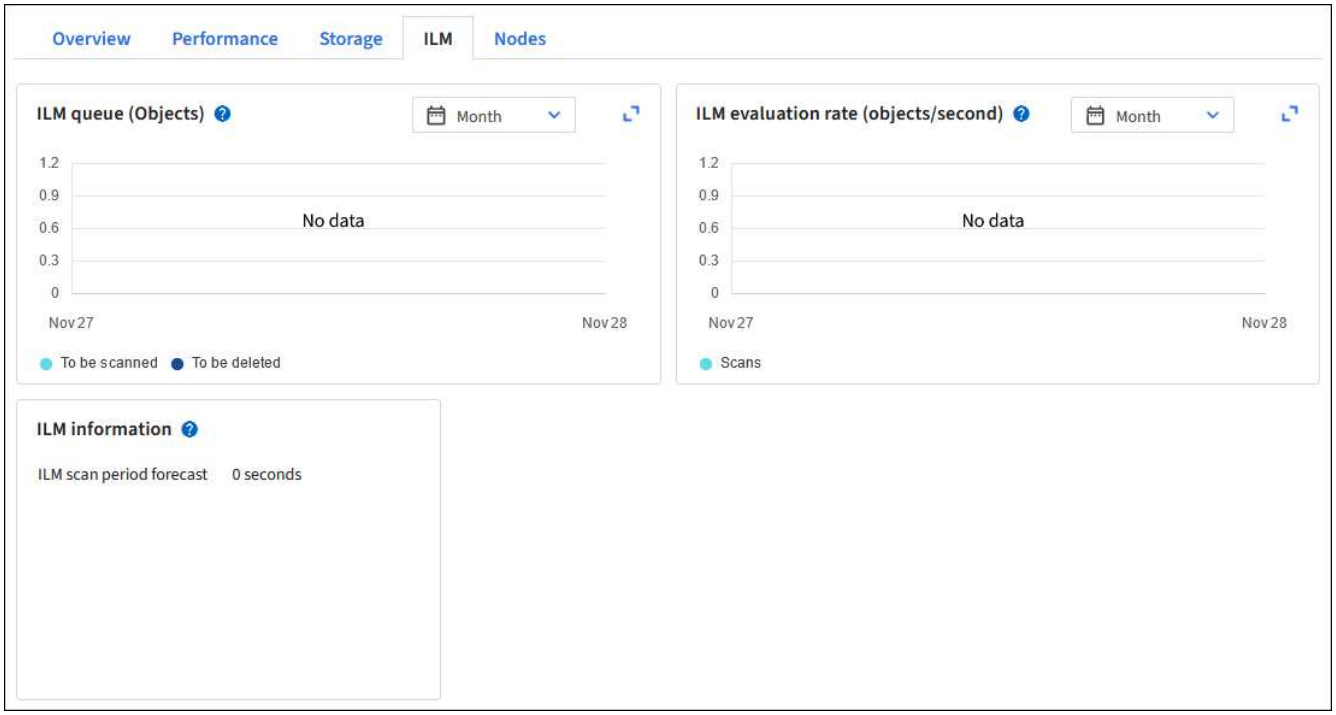
Fasi

1. Selezionare **Dashboard** > **ILM**.

   Poiché la dashboard può essere personalizzata, la scheda ILM potrebbe non essere disponibile.

2. Monitorare le metriche nella scheda ILM.

   È possibile selezionare il punto interrogativo per visualizzare una descrizione degli elementi nella scheda ILM.



USA blocco oggetti S3

Gestire gli oggetti con S3 Object Lock

In qualità di amministratore di rete, è possibile attivare il blocco oggetti S3 per il sistema

StorageGRID e implementare un criterio ILM conforme per garantire che gli oggetti in specifici bucket S3 non vengano cancellati o sovrascritti per un periodo di tempo specificato.

Che cos'è il blocco oggetti S3?

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

Quando l'impostazione blocco oggetto S3 globale è abilitata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza blocco oggetto S3 abilitato. Se un bucket ha S3 Object Lock attivato, è necessario il controllo della versione del bucket e viene attivato automaticamente.

Un bucket senza blocco oggetti S3 può avere solo oggetti senza impostazioni di conservazione specificate. Nessun oggetto acquisito avrà impostazioni di conservazione.

Un bucket con blocco oggetti S3 può avere oggetti con e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con blocco oggetto S3 e conservazione predefinita configurata può avere caricato oggetti con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, poiché l'impostazione di conservazione non è stata configurata a livello di oggetto.

In effetti, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurata la conservazione predefinita. Gli oggetti esistenti senza impostazioni di conservazione degli oggetti rimangono invariati.

Modalità di conservazione

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

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

Impostazioni di conservazione per le versioni degli oggetti

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

- **Modalità di conservazione**: Conformità o governance.

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

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

Per informazioni dettagliate sulle impostazioni dell'oggetto, vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

Impostazione di conservazione predefinita per i bucket

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

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

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

Vedere "Creare un bucket S3" e "Aggiorna la conservazione predefinita del blocco oggetti S3".

Confronto tra blocco oggetti S3 e conformità legacy

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

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

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

	Blocco oggetti S3	Compliance (legacy)
In che modo la funzionalità è abilitata a livello globale?	Da Grid Manager, selezionare **CONFIGURATION** > **System** > **S3 Object Lock**.	Non più supportato.

	Blocco oggetti S3	Compliance (legacy)
In che modo è abilitata la funzione per un bucket?	Gli utenti devono attivare il blocco oggetti S3 quando creano un nuovo bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3.	Non più supportato.
La versione del bucket è supportata?	Sì. La versione del bucket è obbligatoria e viene attivata automaticamente quando il blocco oggetti S3 è attivato per il bucket.	No
Come viene impostata la conservazione degli oggetti?	Gli utenti possono impostare un periodo di conservazione fino alla data di scadenza per ciascuna versione dell'oggetto oppure impostare un periodo di conservazione predefinito per ciascun bucket.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
È possibile modificare il periodo di conservazione?	• In modalità compliance, è possibile aumentare il periodo di conservazione fino alla data di una versione a oggetti, ma non ridurlo mai. • In modalità governance, gli utenti con autorizzazioni speciali possono ridurre o persino rimuovere le impostazioni di conservazione di un oggetto.	Il periodo di conservazione di un bucket può essere aumentato ma non ridotto.
Dove viene controllata la conservazione legale?	Gli utenti possono porre un blocco legale o revocare un blocco legale per qualsiasi versione di oggetto nel bucket.	Un blocco legale viene posizionato sul bucket e influisce su tutti gli oggetti nel bucket.

	Blocco oggetti S3	Compliance (legacy)
Quando è possibile eliminare gli oggetti?	• In modalità compliance, è possibile eliminare una versione dell'oggetto dopo aver raggiunto la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale. • In modalità governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale.	È possibile eliminare un oggetto dopo la scadenza del periodo di conservazione, presupponendo che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere cancellati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	No

S3 attività di blocco degli oggetti

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.

> L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più in base a connettività di rete, stato dei nodi e operazioni Cassandra.

Gli elenchi seguenti per gli amministratori di grid e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzione blocco oggetti S3.

Amministratore di grid

- Attiva l'impostazione blocco oggetti S3 globale per l'intero sistema StorageGRID.
- Assicurarsi che i criteri ILM (Information Lifecycle Management) siano *conformi*, ovvero che soddisfino la "Requisiti dei bucket con blocco oggetti S3 abilitato".
- Se necessario, consentire a un tenant di utilizzare la modalità di conservazione Compliance. In caso contrario, è consentita solo la modalità Governance.
- In base alle necessità, imposta il periodo di conservazione massimo per un tenant.

Utente tenant

- Esaminare le considerazioni per bucket e oggetti con blocco oggetto S3.
- Se necessario, contattare l'amministratore della griglia per abilitare l'impostazione blocco oggetti S3 globale e impostare le autorizzazioni.
- Crea bucket con blocco oggetti S3 abilitato.
- Facoltativamente, configurare le impostazioni di conservazione predefinite per un bucket:

    - Modalità di conservazione predefinita: Governance o conformità, se consentita dall'amministratore della griglia.
    - Periodo di conservazione predefinito: Deve essere minore o uguale al periodo di conservazione massimo impostato dall'amministratore di rete.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e impostare facoltativamente la conservazione specifica degli oggetti:
    - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore del grid.
    - Mantieni fino alla data: Deve essere minore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per il blocco oggetti S3

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

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

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

Requisiti per le regole ILM conformi

Se si desidera attivare l'impostazione blocco oggetto S3 globale, è necessario verificare che la regola predefinita in tutti i criteri ILM attivi sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con blocco oggetti S3 attivato e di tutti i bucket esistenti con conformità legacy attivata:

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

Requisiti per le policy ILM

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

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

"Esempio di un criterio ILM conforme per il blocco degli oggetti S3"

Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.
- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Impossibile attivare il blocco oggetti S3 per un bucket esistente.
- Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket. Non puoi disattivare il blocco oggetti S3 o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione e un periodo di conservazione predefiniti per ciascun bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di proprie impostazioni di conservazione. È possibile eseguire l'override di queste impostazioni predefinite specificando una modalità di conservazione e conservarla fino alla data per ogni versione dell'oggetto al momento del caricamento.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con blocco oggetti S3 attivato.
- La replica di CloudMirror non è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure le impostazioni di conservazione per ciascuna versione dell'oggetto. È possibile specificare le impostazioni di conservazione a livello di oggetto utilizzando l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

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

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

1. **Acquisizione oggetto**

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

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

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

2. **Conservazione ed eliminazione degli oggetti**

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

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

Informazioni correlate

- "Creare un bucket S3"
- "Aggiorna la conservazione predefinita del blocco oggetti S3"
- "Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
- "Esempio 7: Policy ILM conforme per il blocco oggetti S3"

Attiva il blocco oggetti S3 a livello globale

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

Prima di iniziare

- Si dispone di "Autorizzazione di accesso root".
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai esaminato il flusso di lavoro S3 Object Lock e hai compreso le considerazioni.
- La regola predefinita nel criterio ILM attivo è conforme. Per ulteriori informazioni, vedere "Creare una regola ILM predefinita" .

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.

Rivedere le impostazioni di conformità dei tenant esistenti dopo aver attivato l'impostazione blocco oggetto S3 globale. Quando si attiva questa impostazione, le impostazioni di blocco degli oggetti S3 per tenant dipendono dalla release di StorageGRID al momento della creazione del tenant.

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

Fasi

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

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

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

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

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

   Quando si seleziona **OK**:

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

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

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

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

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

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Per risolvere questo errore, attenersi alla seguente procedura:

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

Informazioni correlate

- "Utilizzare un account tenant"
- "UTILIZZARE L'API REST S3"
- "Ripristino e manutenzione"

Esempio di regole e policy ILM

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 un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

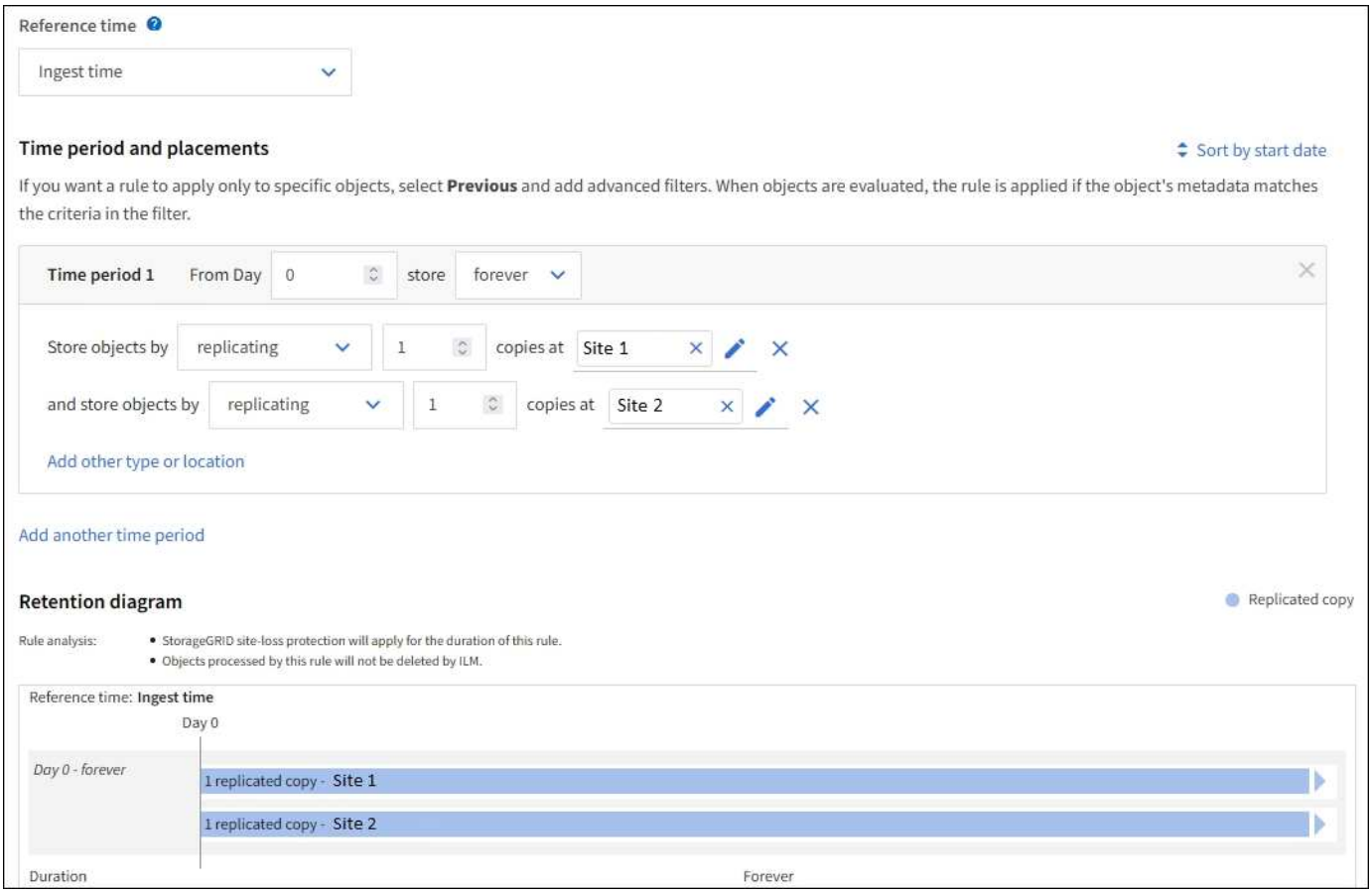
ILM regola 1 per esempio 1: Copia dei dati degli oggetti in due siti

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due siti.

Definizione della regola	Valore di esempio
Pool di storage one-site	Due pool di storage, ciascuno contenente diversi siti, denominati Sito 1 e Sito 2.
Nome della regola	Due copie di due siti
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 al giorno per sempre, conservare una copia replicata nel sito 1 e una copia replicata nel sito 2.

La sezione analisi delle regole del diagramma di conservazione riporta:

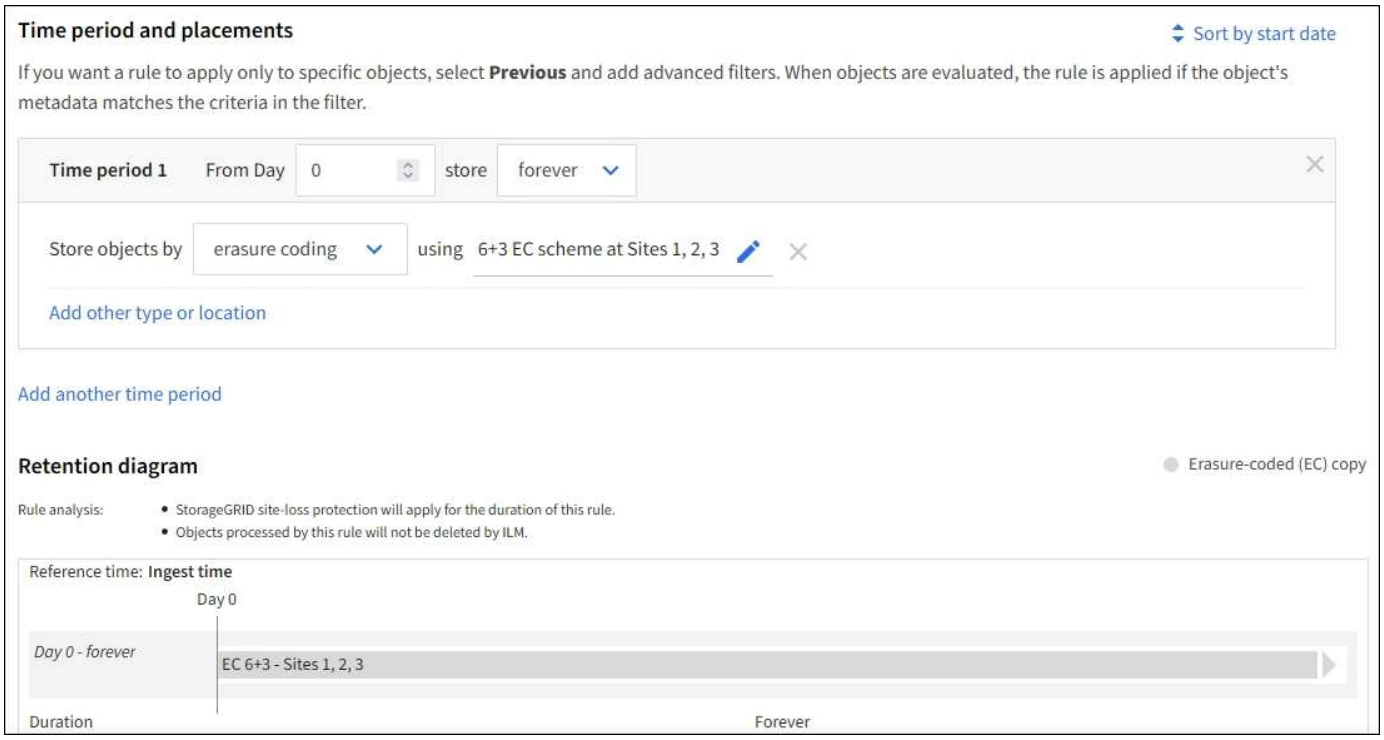
- La protezione contro la perdita di sito di StorageGRID verrà applicata per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola non verranno eliminati da ILM.



Regola ILM 2 per l'esempio 1: Profilo di erasure coding con abbinamento bucket

Questa regola ILM di esempio utilizza un profilo di erasure coding e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene memorizzato.

Definizione della regola	Valore di esempio
Pool di storage con più siti	• Un pool di storage in tre siti (siti 1, 2, 3) • Utilizzare uno schema di erasure coding 6+3
Nome della regola	Record finanziari di S3 Bucket
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Per gli oggetti nel bucket S3 denominato Finance-records, creare una copia con erasure coding nel pool specificato dal profilo di erasure coding. Conserva questa copia per sempre.

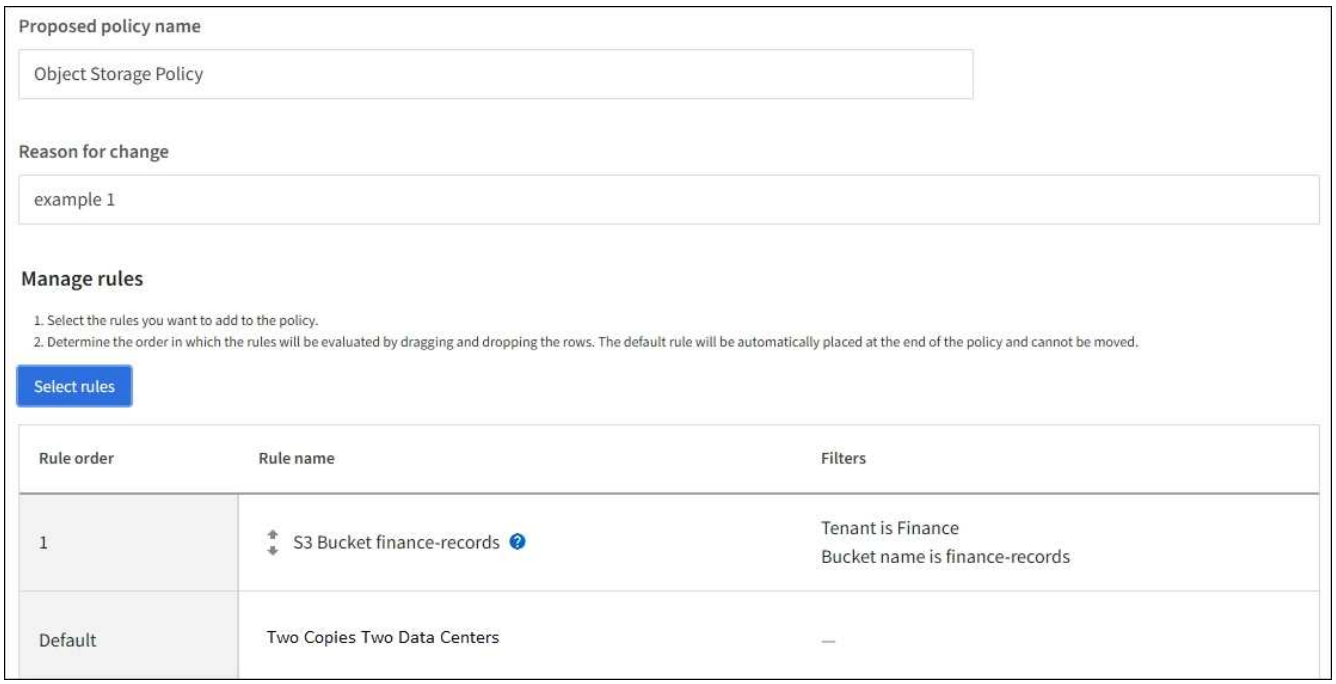


Politica ILM ad esempio 1

In pratica, la maggior parte delle policy ILM è semplice, anche se il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse.

Un tipico criterio ILM per un grid multi-sito potrebbe includere regole ILM come le seguenti:

- Al momento dell'acquisizione, è possibile memorizzare tutti gli oggetti appartenenti al bucket S3 citato `finance-records` in un pool storage contenente tre siti. Utilizzare la codifica di cancellazione 6+3.
- 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 nel sito 1 e una copia nel sito 2.



Informazioni correlate

- "Utilizzare i criteri ILM"
- "Creare policy ILM"

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 un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 2: Utilizzare EC per oggetti superiori a 1 MB

In questo esempio, la cancellazione della regola ILM codifica gli oggetti superiori a 1 MB.

> L'erasure coding è più adatto per oggetti superiori a 1 MB. 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.

Definizione della regola	Valore di esempio
Nome della regola	Solo oggetti EC > 1 MB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB
Posizionamenti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre 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 regola è la regola predefinita per il criterio. Poiché la prima regola filtra tutti gli oggetti superiori a 1 MB, questa regola si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Nessuno
Posizionamenti	Dal giorno 0 al giorno per sempre, conservare una copia replicata nel sito 1 e una copia replicata nel sito 2.

Criterio ILM per esempio 2: Utilizzare EC per oggetti superiori a 1 MB

Questo esempio di policy ILM include due regole ILM:

- La prima regola di cancellazione codifica tutti gli oggetti superiori a 1 MB.
- La seconda regola ILM (predefinita) crea due copie replicate. Poiché gli oggetti superiori a 1 MB sono stati filtrati dalla regola 1, la regola 2 si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine

È possibile utilizzare le regole e i criteri di esempio seguenti per garantire che le immagini di dimensioni superiori a 1 MB siano sottoposte a erasure coding e che vengano create due copie di immagini di dimensioni inferiori.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

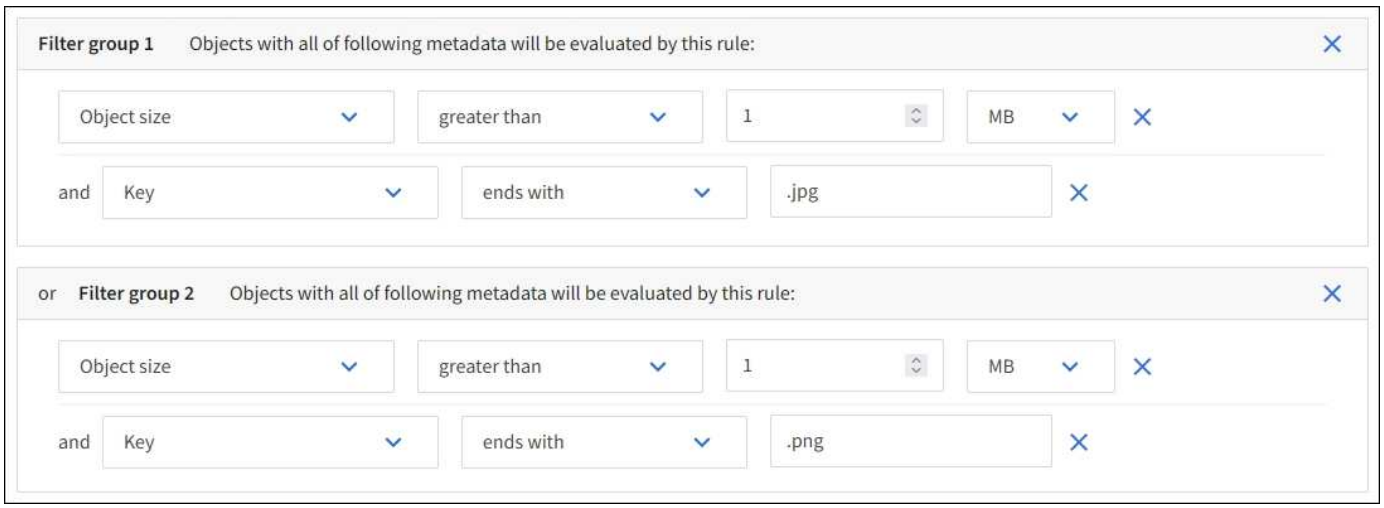
ILM regola 1 per esempio 3: Utilizzare EC per file di immagini superiori a 1 MB

Questa regola ILM di esempio utilizza il filtraggio avanzato per codificare tutti i file di immagine con dimensioni superiori a 1 MB.

> L'erasure coding è più adatto per oggetti superiori a 1 MB. 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.

Definizione della regola	Valore di esempio
Nome della regola	File immagine EC > 1 MB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB
Filtri avanzati per Key	• Termina con .jpg • Termina con .png

Definizione della regola	Valore di esempio
Posizionamenti	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 ai file .jpg e .png che sono superiori a 1 MB.

Regola ILM 2 per esempio 3: Creare 2 copie replicate per tutti i file di immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file di immagine più piccoli devono essere replicati. Poiché la prima regola del criterio ha già trovato corrispondenza tra file di immagine superiori a 1 MB, questa regola si applica ai file di immagine di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	2 copie per i file immagine
Tempo di riferimento	Tempo di acquisizione
Filtri avanzati per Key	• Termina con .jpg • Termina con .png
Posizionamenti	Creare 2 copie replicate in due pool di storage

Policy ILM per esempio 3: Migliore protezione per i file di immagine

Questo esempio di policy ILM include tre regole:

- La prima regola di cancellazione codifica tutti i file di immagine superiori a 1 MB.
- La seconda regola consente di creare due copie dei file immagine rimanenti (ovvero, immagini di dimensioni pari o inferiori a 1 MB).
- La regola predefinita si applica a tutti gli oggetti rimanenti (ovvero a tutti i file non immagine).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

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

Se si dispone di un bucket S3 con versione abilitata, è possibile gestire le versioni non correnti degli oggetti includendo regole nel criterio ILM che utilizzano "tempo non corrente" come tempo di riferimento.

> Se si specifica un tempo di conservazione limitato per gli oggetti, questi verranno eliminati in modo permanente una volta raggiunto il periodo di tempo. Assicurarsi di comprendere per quanto tempo gli oggetti verranno conservati.

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 un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

> Per eseguire la simulazione dei criteri ILM su una versione non corrente di un oggetto, è necessario conoscere l'UUID o il CBID della versione dell'oggetto. Per trovare UUID e CBID, utilizzare "ricerca dei metadati degli oggetti" mentre l'oggetto è ancora corrente.

Informazioni correlate

"Modalità di eliminazione 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 siti 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 costituito da diversi data center, denominati Sito 1, Sito 2 e Sito 3.
Nome della regola	Tre copie dieci anni

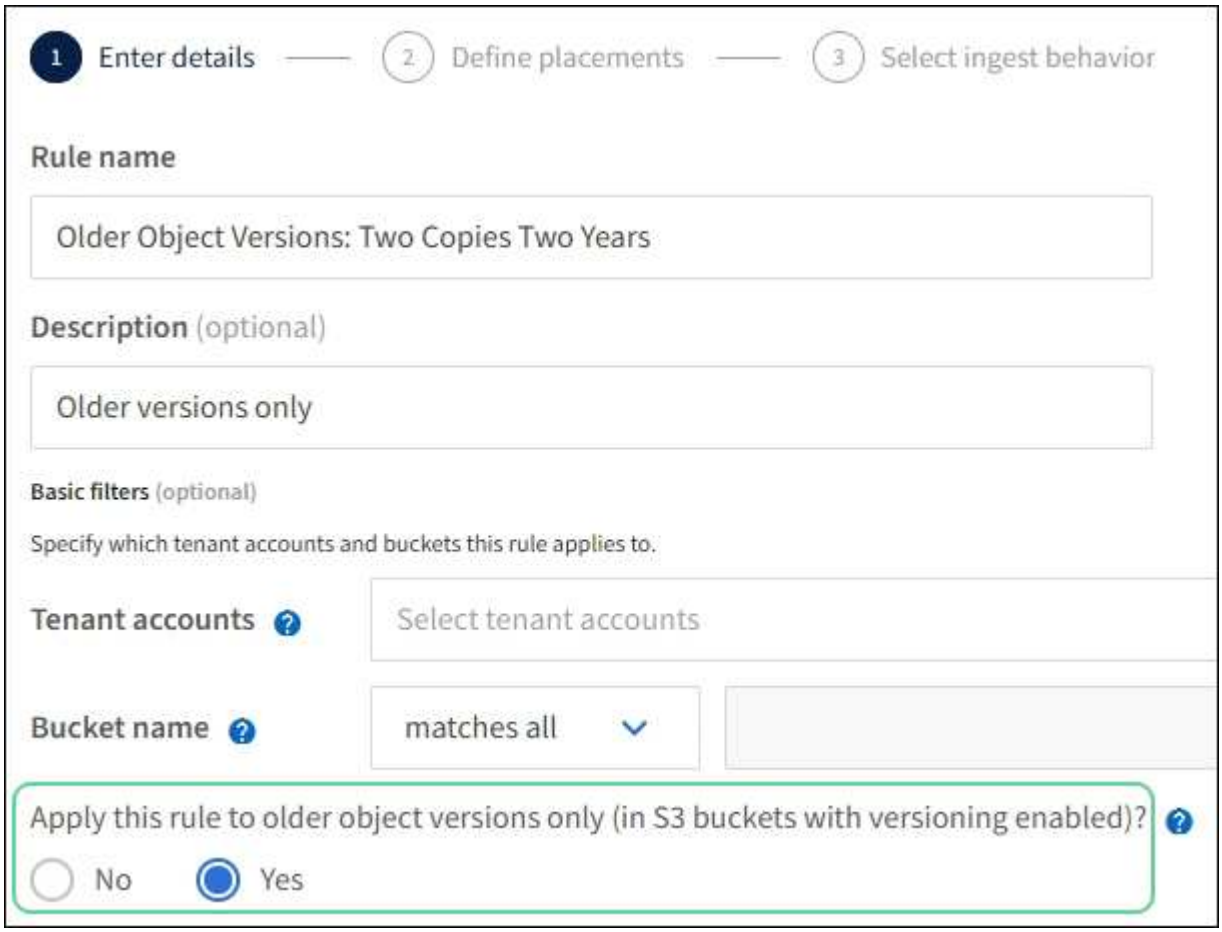
Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva tre copie replicate per 10 anni (3,652 giorni), una nel sito 1, una nel sito 2 e una nel sito 3. Alla fine dei 10 anni, eliminare tutte le copie dell'oggetto.

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.

Per creare una regola che utilizza "ora non corrente" come ora di riferimento, selezionare **Sì** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?" Nel passaggio 1 (immettere i dettagli) della procedura guidata Crea una regola ILM. Quando si seleziona **Sì**, viene automaticamente selezionata l'opzione *ora non corrente* per l'ora di riferimento e non è possibile selezionare un'ora di riferimento diversa.



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, sito 1 e sito 2.
Nome della regola	Versioni non correnti: Due copie per due anni
Tempo di riferimento	Ora non corrente Selezionato automaticamente quando si seleziona **Sì** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?" Nella procedura guidata Crea una regola ILM.
Posizionamenti	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 nel sito 1 e una nel sito 2. 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 l'ora non corrente come ora di riferimento devono essere visualizzate nel criterio ILM prima delle regole applicabili 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 "tempo non corrente" devono essere visualizzate nel criterio prima delle regole che si applicano alla versione dell'oggetto corrente. In caso contrario, le versioni degli oggetti non correnti non verranno mai abbinate alla regola "tempo non corrente".

- Al momento dell'acquisizione, creare tre copie replicate e memorizzare una copia in ciascuno dei tre siti. 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).
- La seconda regola corrisponde alla versione corrente dell'oggetto. Quando la versione corrente dell'oggetto è stata archiviata per 10 anni, il processo ILM aggiunge un marcatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente "non corrente". La prossima volta che si verifica la valutazione ILM, questa versione non corrente corrisponde alla prima regola. Di conseguenza, la copia del sito 3 viene eliminata e le due copie del sito 1 e del sito 2 vengono memorizzate per altri 2 anni.

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 un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

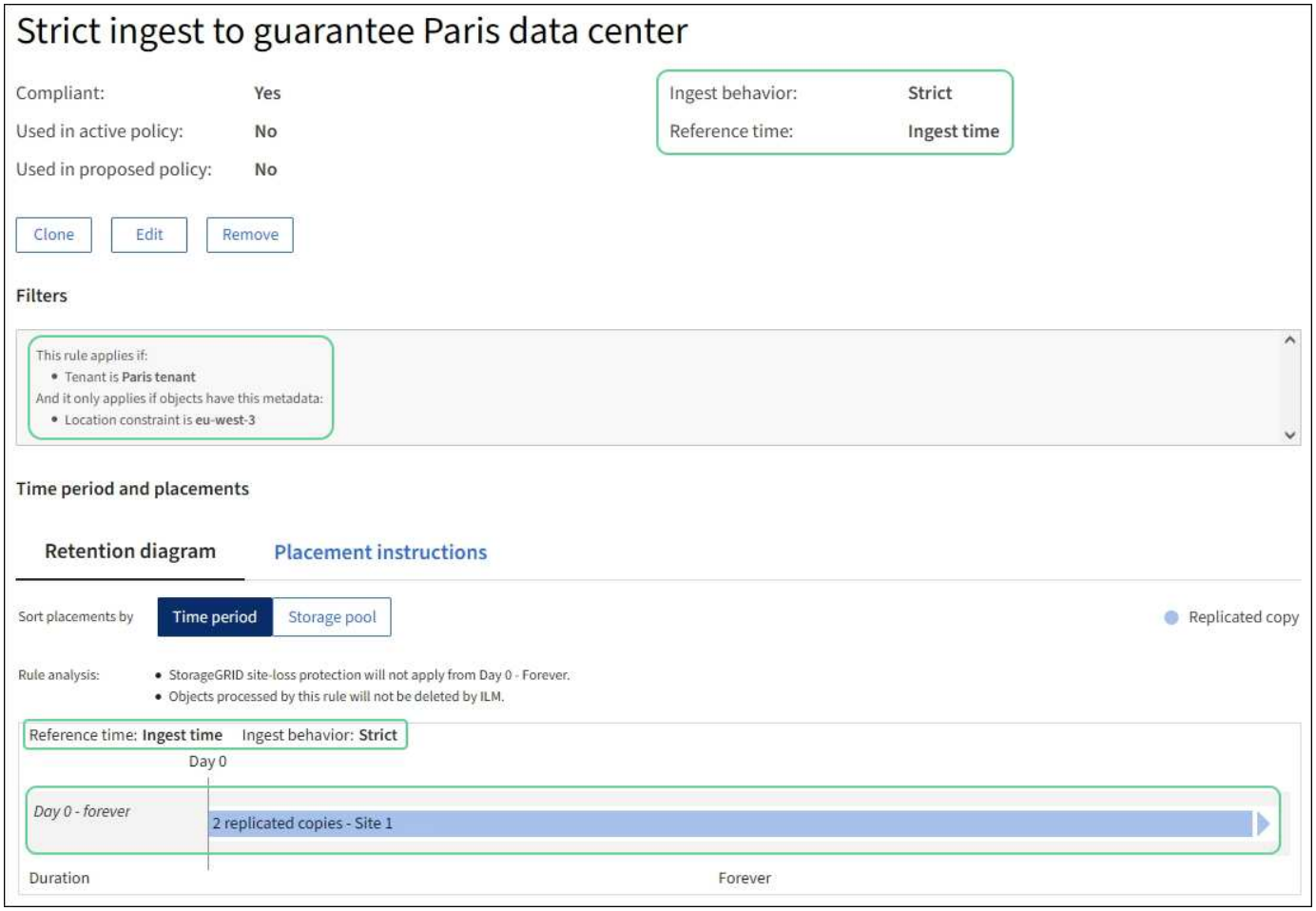
- "Opzioni di acquisizione"
- "Create ILM rule (Crea regola ILM): Selezionare il comportamento di acquisizione"

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
Filtro avanzato	Il vincolo di posizione equivale a eu-West-3
Pool di storage	Sito 1 (Parigi)
Nome della regola	Un ingest rigoroso per garantire il data center di Parigi
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre nel sito 1 (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
Filtro avanzato	*Non specificato*
Pool di storage	Sito 1 (Parigi) e sito 2 (Stati Uniti)
Nome della regola	2 copie di 2 data center
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre in due data center

Definizione della regola	Valore di esempio
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: Modificare un criterio ILM

Se è necessario modificare la protezione dei dati o aggiungere nuovi siti, è possibile creare e attivare una nuova policy ILM.

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 occorre implementare una nuova policy ILM attiva per memorizzare i dati nel nuovo sito. Per implementare un nuovo criterio attivo, prima "creare un criterio". Successivamente, è necessario "simulare" e quindi "attivare" la nuova policy.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni 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.

Per garantire che un nuovo criterio ILM non influisca sul posizionamento degli oggetti replicati e con erasure coding esistenti, è possibile "Creare una regola ILM con un filtro per l'ora di acquisizione". Ad esempio, **Ingest Time è *attivo o successivo a <date and time>***, in modo che la nuova regola si applichi solo agli oggetti acquisiti in data e ora specificate o successive.

I tipi di modifiche ai criteri ILM che possono influire temporaneamente sulle prestazioni di StorageGRID includono:

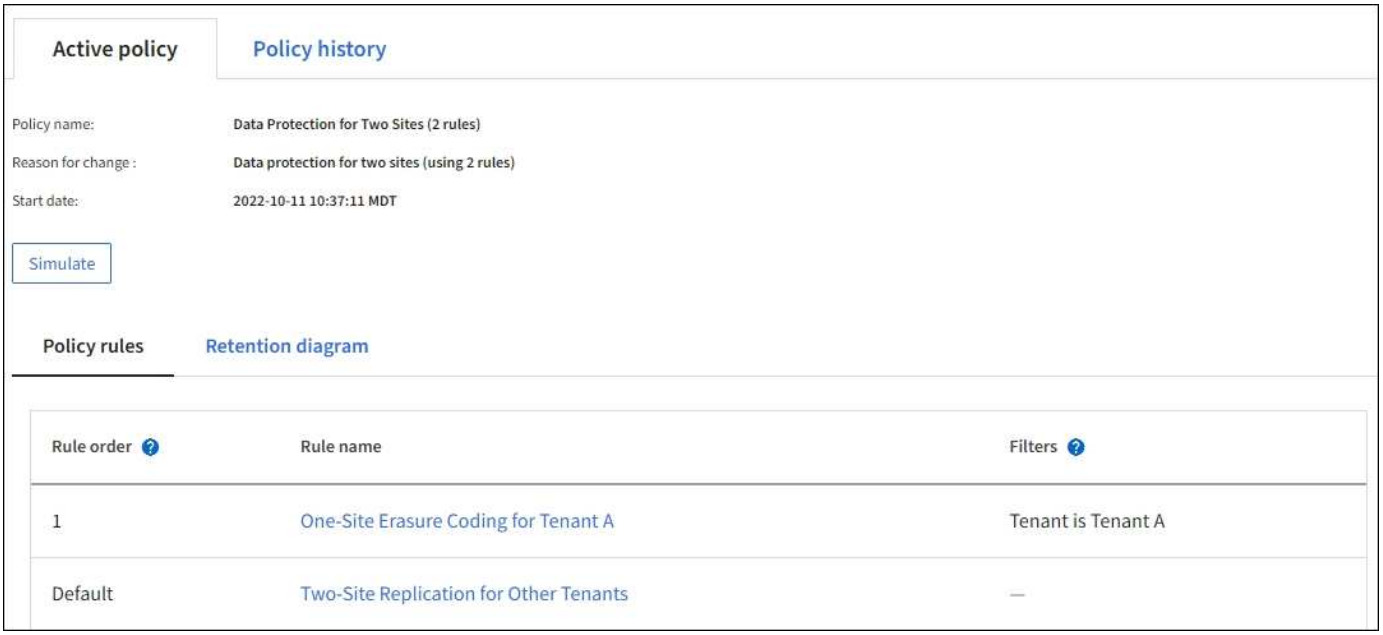
- Applicazione di un profilo di erasure coding diverso agli oggetti esistenti sottoposti a erasure coding.

> StorageGRID considera ogni profilo di erasure coding come univoco e non riutilizza i frammenti di erasure coding 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.

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.

Regola 1: Erasure coding per un sito per il tenant A.

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione one-site per il tenant A.
Account tenant	Tenant A.
Pool di storage	Sito 1
Posizionamenti	2+1 erasure coding in Site 1 dal giorno 0 a per sempre

Regola 2: Replica a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a due siti per altri tenant
Account tenant	Ignorare
Pool di storage	Sito 1 e sito 2
Posizionamenti	Due copie replicate dal giorno 0 a sempre: Una copia nel sito 1 e una nel sito 2.

Criterio ILM per esempio 6: Protezione dei dati in tre siti

In questo esempio, la policy ILM viene sostituita con una nuova policy per un sistema StorageGRID a tre siti.

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore della griglia ha creato due nuovi pool di storage: Un pool di storage per il sito 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 un nuovo criterio ILM, progettato 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 della regola	Codifica di cancellazione a tre siti per il tenant A.
Account tenant	Tenant A.

Definizione della regola	Valore di esempio
Pool di storage	Tutti e 3 i siti (inclusi Sito 1, Sito 2 e Sito 3)
Posizionamenti	2+1 erasure coding in tutti e 3 i siti dal giorno 0 a per sempre

Regola 2: Replica a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a tre siti per altri tenant
Account tenant	Ignorare
Pool di storage	Sito 1, sito 2 e sito 3
Posizionamenti	Tre copie replicate dal giorno 0 a sempre: Una copia presso il sito 1, una copia presso il sito 2 e una copia presso il sito 3.

Attivazione del criterio ILM ad esempio 6

Quando si attiva un nuovo criterio ILM, è possibile spostare gli oggetti esistenti in nuove posizioni o creare nuove copie degli oggetti per gli oggetti esistenti, in base alle istruzioni di posizionamento nelle regole nuove o aggiornate.

> 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

Nel criterio ILM attualmente attivo, per questo esempio, gli oggetti appartenenti al tenant A sono protetti utilizzando la codifica di cancellazione 2+1 nel sito 1. Nella nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti mediante erasure coding 2+1 nei siti 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 sito diverso.
- Gli oggetti esistenti appartenenti al tenant A vengono rivalutati durante il processo di scansione ILM in corso. Poiché le istruzioni di posizionamento dell'ILM utilizzano un nuovo profilo di erasure coding, vengono creati e distribuiti ai tre siti frammenti completamente nuovi e codificati tramite erasure coding.

I frammenti 2+1 esistenti nel sito 1 non vengono riutilizzati. StorageGRID considera ogni profilo di erasure coding come univoco e non riutilizza i frammenti di erasure coding quando viene utilizzato un nuovo profilo.

Cosa succede quando cambiano le istruzioni di replica

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti ad altri tenant sono protetti utilizzando due copie replicate nei pool di storage dei siti 1 e 2. Nella nuova policy ILM, gli oggetti appartenenti ad altri tenant verranno protetti attraverso tre copie replicate nei pool di storage dei siti 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 sito.
- Gli oggetti esistenti appartenenti a questi altri tenant vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie degli oggetti esistenti nei siti 1 e 2 continuano a soddisfare i requisiti di replica della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il sito 3.

Impatto delle performance dell'attivazione di questa policy

Quando il criterio ILM in questo esempio è attivato, le prestazioni generali del sistema StorageGRID saranno temporaneamente influenzate. Per creare nuovi frammenti erasure-coded per gli oggetti esistenti del tenant A e nuove copie replicate nel sito 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 la nuova policy verrà applicata 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 un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

- "Gestire gli oggetti con S3 Object Lock"
- "Creare 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 oggetto e oggetto aggiunta al bucket di record bancari utilizzerà i seguenti valori per le `retain-until-date` impostazioni e `legal hold`.

Impostazione per ciascun oggetto	Valore di esempio
`retain-until-date`	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione oggetto ha una propria `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 bloccato a fini giudiziari, l'oggetto non può essere eliminato anche se `retain-until-date` è stato raggiunto.

Regola ILM 1 per blocco oggetto S3 esempio: Profilo di erasure coding con abbinamento bucket

Questa regola ILM di esempio si applica solo all'account tenant S3 denominato Bank of ABC. Si abbina a qualsiasi oggetto nel `bank-records` bucket e quindi utilizza l'erasure coding per memorizzare l'oggetto sui nodi storage in tre siti di data center utilizzando un profilo di erasure coding 6+3. Questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato: Una copia viene conservata nei nodi di storage dal giorno 0 a per sempre, utilizzando l'ora di inizio come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Compliant Rule (regola conforme): Oggetti EC nel bucket dei record bancari - Bank of ABC

Definizione della regola	Valore di esempio
Account tenant	Banca di ABC
Nome bucket	`bank-records`
Filtro avanzato	Dimensione oggetto (MB) maggiore di 1 **Nota:** questo filtro garantisce che la codifica erasure non venga utilizzata per oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 memorizzare per sempre
Profilo di erasure coding	• 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 della regola	Regola non conforme: Utilizza il Cloud Storage Pool
Account tenant	Non specificato
Nome bucket	Non specificato, ma si applica solo ai bucket che non hanno S3 Object Lock (o la funzionalità Compliance legacy) abilitato.
Filtro 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, non utilizza il tempo di riferimento non corrente e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: Due copie di oggetti vengono conservate sui nodi di storage dal giorno 0 a per sempre, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola di conformità predefinita: Due copie di due data center
Account tenant	Non specificato
Nome bucket	Non specificato
Filtro 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 il criterio.

Aggiungere 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 superiori a 1 MB 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.

Simulare la policy

Dopo aver aggiunto regole al criterio, scelto una regola conforme predefinita e organizzato le altre regole, è necessario simulare il criterio testando gli oggetti dal bucket con blocco oggetti S3 attivato 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 che sono superiori a 1 MB nei record di banco 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 1 MB 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.

Attivare il criterio

Quando si è completamente soddisfatti del fatto che il nuovo criterio protegga i dati degli oggetti come previsto, è possibile attivarlo.

Esempio 8: Priorità per il ciclo di vita dei bucket S3 e la politica ILM

A seconda della configurazione del ciclo di vita, gli oggetti seguono le impostazioni di conservazione del ciclo di vita del bucket S3 o di un criterio ILM.

Esempio di priorità del ciclo di vita dei bucket rispetto alla policy ILM

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le X copie per 50 giorni

Ciclo di vita della benna

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Risultato

- Viene acquisito un oggetto denominato "docs/text". Corrisponde al filtro del ciclo di vita del bucket del prefisso "docs/".
  - Dopo 100 giorni viene creato un marker di eliminazione e "documenti/testo" diventa non corrente.
  - Dopo 5 giorni, un totale di 105 giorni dall'acquisizione, "documenti/testo" viene eliminato.
  - Dopo 95 giorni, per un totale di 200 giorni dall'acquisizione e 100 giorni dalla creazione del marker di eliminazione, il marker di eliminazione scaduto viene eliminato.
- Viene acquisito un oggetto denominato "video/filmato". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
  - Dopo 50 giorni viene creato un marker di eliminazione e "video/filmato" diventa non corrente.
  - Dopo 20 giorni, un totale di 70 giorni dall'acquisizione, "video/film" viene eliminato.
  - Dopo 30 giorni, per un totale di 100 giorni dall'acquisizione e 50 giorni dalla creazione del marker di eliminazione, il marker di eliminazione scaduto viene eliminato.

Esempio di ciclo di vita del bucket che mantiene implicitamente per sempre

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le X copie per 50 giorni

Ciclo di vita della benna

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Risultato

- Viene acquisito un oggetto denominato "docs/text". Corrisponde al filtro del ciclo di vita del bucket del prefisso "docs/".

  L' `Expiration`azione si applica solo ai marcatori di cancellazione scaduti, il che implica mantenere tutto il resto per sempre (a partire da "docs/").

  I marcatori di eliminazione che iniziano con "docs/" vengono rimossi quando diventano scaduti.

- Viene acquisito un oggetto denominato "video/filmato". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
  - Dopo 50 giorni viene creato un marker di eliminazione e "video/filmato" diventa non corrente.
  - Dopo 20 giorni, un totale di 70 giorni dall'acquisizione, "video/film" viene eliminato.
  - Dopo 30 giorni, per un totale di 100 giorni dall'acquisizione e 50 giorni dalla creazione del marker di eliminazione, il marker di eliminazione scaduto viene eliminato.

Esempio di utilizzo del ciclo di vita bucket per duplicare ILM e ripulire i marcatori di eliminazione scaduti

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le copie X per sempre

Ciclo di vita della benna

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Risultato

- Il criterio ILM viene duplicato nel ciclo di vita del bucket.
  - La regola per sempre della policy ILM è progettata per la rimozione manuale degli oggetti e la pulizia delle versioni non correnti dopo 20 giorni. Di conseguenza, la regola del tempo di acquisizione manterrà sempre i marcatori di eliminazione scaduti.
  - Il ciclo di vita del bucket duplica il comportamento del criterio ILM durante l'aggiunta di `"ExpiredObjectDeleteMarker": true`, che rimuove i marcatori di eliminazione una volta scaduti
- Un oggetto viene acquisito. Nessun filtro significa che il ciclo di vita del bucket si applica a tutti gli oggetti e sovrascrive le impostazioni di conservazione ILM.
  - Quando un tenant invia una richiesta di eliminazione di un oggetto, viene creato un marcatore di eliminazione e l'oggetto diventa non corrente.

- Dopo 20 giorni, l’oggetto non corrente viene eliminato e il marker di eliminazione viene scaduto.
- Poco dopo, il marker di eliminazione scaduto viene eliminato.

Informazioni sul copyright

Informazioni sul marchio commerciale