Gestisci gli oggetti con ILM

StorageGRID software

NetApp
July 23, 2026

Sommario

Gestisci gli oggetti con ILM

Gestisci gli oggetti con ILM in StorageGRID

Le regole di gestione del ciclo di vita delle informazioni (ILM) in una policy ILM indicano a StorageGRID come creare e distribuire copie dei dati degli oggetti e come gestire queste copie nel tempo.

Informazioni su queste istruzioni

La progettazione e l'implementazione di regole e politiche ILM richiedono un'attenta pianificazione. Devi comprendere i requisiti operativi, la topologia del tuo sistema StorageGRID, le esigenze di protezione degli oggetti e i tipi di storage disponibili. Poi devi decidere come vuoi che i diversi tipi di oggetti vengano copiati, distribuiti e archiviati.

Usa queste istruzioni per:

- Scopri StorageGRID ILM, incluso "come funziona ILM durante l'intero ciclo di vita di un oggetto".
- Scopri come configurare "pool di storage", "Pool di storage cloud" e "Regole ILM".
- Scopri come "creare, simulare e attivare una policy ILM" proteggere i dati degli oggetti su uno o più siti.
- Scopri come "Gestisci gli oggetti con S3 Object Lock" ti aiuta a garantire che gli oggetti in specifici bucket S3 non vengano eliminati o sovrascritti per un periodo di tempo specificato.

Saperne di più

Per saperne di più, guarda questi video:

Panoramica delle regole ILM

Panoramica delle policy ILM

ILM e ciclo di vita degli oggetti

Come funziona ILM durante il ciclo di vita di un oggetto in StorageGRID

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

- **Ingestione**: L'ingestione inizia quando un'applicazione client S3 stabilisce una connessione per salvare un oggetto nel sistema StorageGRID e termina quando StorageGRID restituisce al client un messaggio di "ingestione riuscita". I dati dell'oggetto vengono protetti durante l'ingestione applicando immediatamente le istruzioni ILM (posizionamento sincrono) oppure creando copie intermedie e applicando le istruzioni ILM in un secondo momento (dual commit), a seconda di come sono stati specificati i requisiti ILM.
- **Gestione delle copie**: Dopo aver creato il numero e il tipo di copie di oggetti specificati nelle istruzioni di posizionamento dell'ILM, StorageGRID gestisce le posizioni degli oggetti e li protegge dalla perdita.
  - **Scansione e valutazione ILM**: StorageGRID analizza continuamente l'elenco degli oggetti memorizzati nella griglia e verifica se le copie correnti soddisfano i requisiti ILM. Quando sono necessari tipi, numeri o posizioni diverse di copie di oggetti, StorageGRID crea, elimina o sposta le

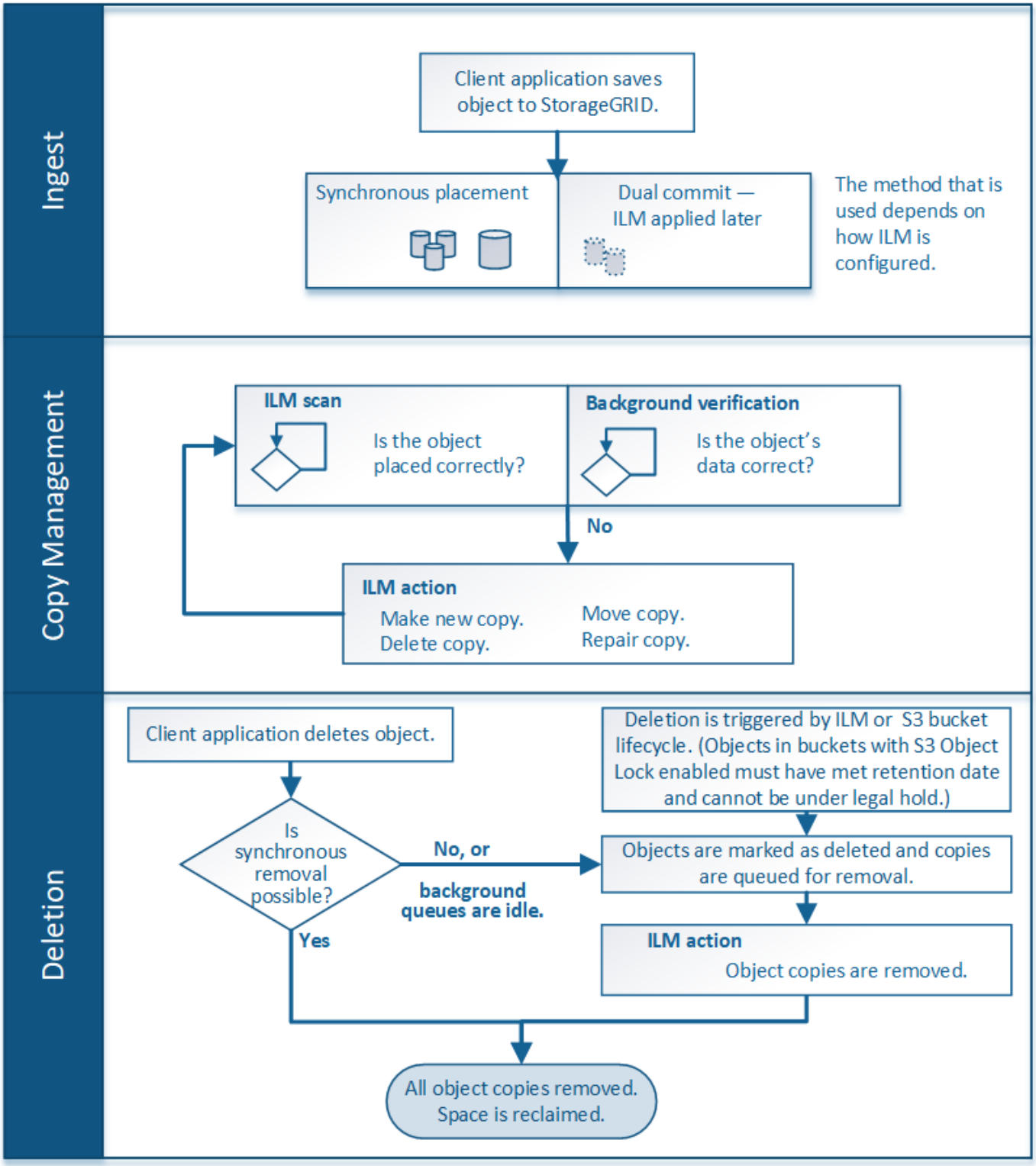
copie secondo necessità.

  - **Verifica in background**: StorageGRID esegue continuamente la verifica in background per controllare l'integrità dei dati degli oggetti. Se viene rilevato un problema, StorageGRID crea automaticamente una nuova copia dell'oggetto o un frammento di oggetto sostitutivo con codifica di cancellazione in una posizione che soddisfa i requisiti ILM correnti. Vedi "Verifica l'integrità dell'oggetto".

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

> Gli oggetti in un bucket con S3 Object Lock abilitato non possono essere eliminati se sono soggetti a un blocco legale o se è stata specificata una retain-until-date non ancora raggiunta.

Il diagramma riassume come funziona ILM durante il ciclo di vita di un oggetto.



Come vengono ingeriti gli oggetti

Opzioni di ingestione ILM in StorageGRID

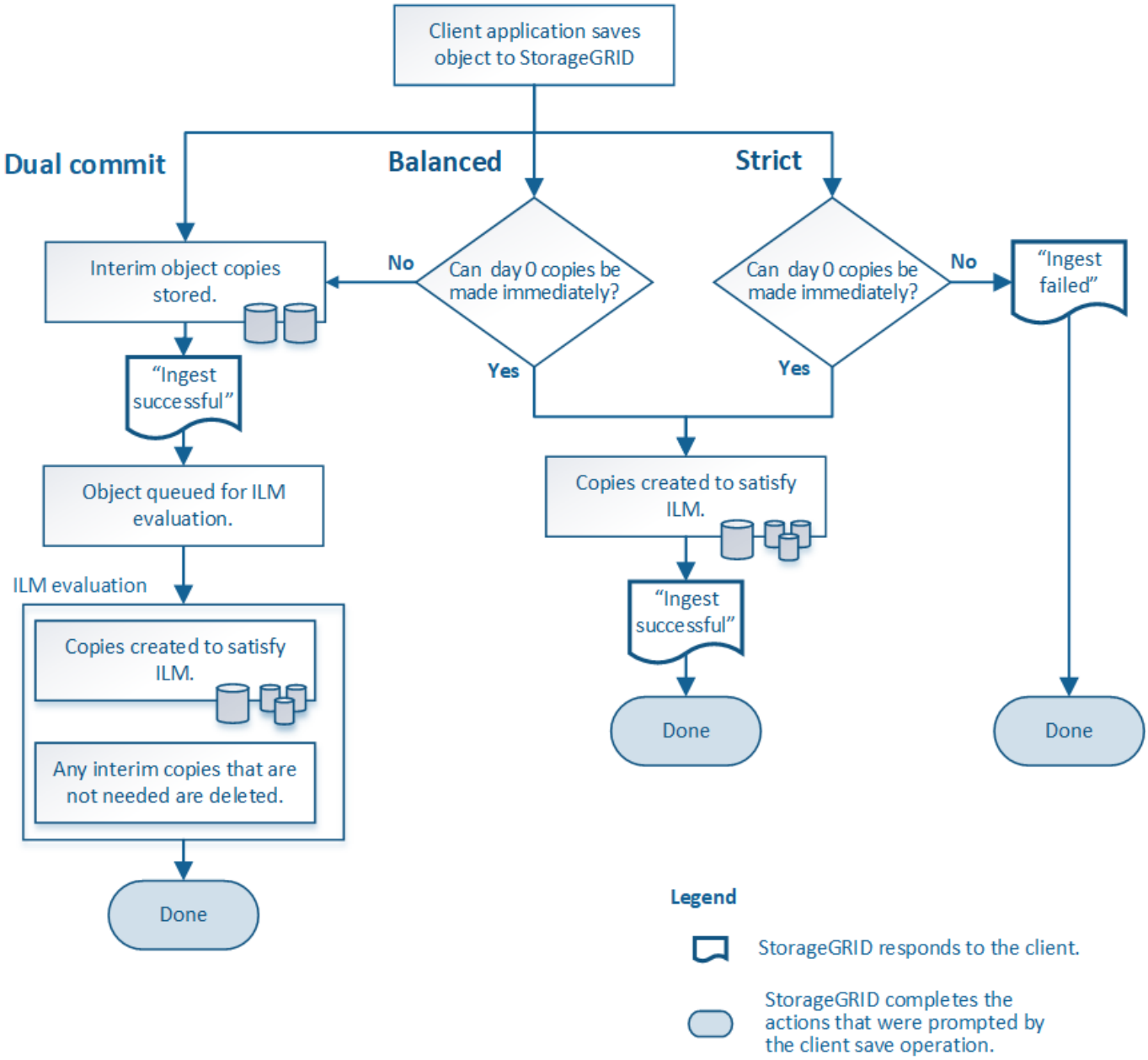
Quando crei una regola ILM, specifichi una delle tre opzioni per proteggere gli oggetti in fase di acquisizione: Dual commit, Strict o Balanced.

A seconda della tua scelta, StorageGRID crea copie provvisorie e mette in coda gli oggetti per una successiva

valutazione ILM, oppure utilizza il posizionamento sincrono e crea immediatamente le copie per soddisfare i requisiti ILM.

Diagramma di flusso delle opzioni di ingestione

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



Commit doppio

Quando selezioni l'opzione Dual commit, StorageGRID crea immediatamente copie provvisorie dell'oggetto su due diversi Storage Node e restituisce al client un messaggio di "ingest successful". L'oggetto viene messo in coda per la valutazione ILM e le copie che rispettano le istruzioni di posizionamento della regola vengono create successivamente. Se la policy ILM non può essere elaborata immediatamente dopo il dual commit, la protezione dalla perdita del sito potrebbe richiedere tempo per essere raggiunta.

Usa l'opzione Dual commit in entrambi questi casi:

- Stai usando regole ILM multi-sito e la latenza di ingest dei client è la tua considerazione principale. Quando usi il Dual commit, devi assicurarti che la tua grid possa eseguire il lavoro aggiuntivo di creazione e rimozione delle copie dual-commit se queste non soddisfano l'ILM. Nello specifico:
  - Il carico sulla grid deve essere sufficientemente basso da evitare un accumulo di ILM.
  - La griglia deve disporre di risorse hardware in eccesso (IOPS, CPU, memoria, larghezza di banda di rete e così via).
- Stai usando regole ILM multi-sito e la connessione WAN tra i siti di solito ha elevata latenza o larghezza di banda limitata. In questo scenario, usare l'opzione Dual commit può aiutare a prevenire i timeout del client. Prima di scegliere l'opzione Dual commit, dovresti testare l'applicazione client con carichi di lavoro realistici.

Bilanciato (impostazione predefinita)

Quando selezioni l'opzione Bilanciata, StorageGRID utilizza anche il posizionamento sincrono durante l'ingest e crea immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. A differenza dell'opzione Rigorosa, se StorageGRID non può creare immediatamente tutte le copie, utilizza invece Dual commit. Se la policy ILM utilizza posizionamenti su più siti e non è possibile ottenere una protezione immediata dalla perdita del sito, viene attivato l'avviso **ILM placement unachievable**.

Usa l'opzione Balanced per ottenere la migliore combinazione di protezione dei dati, prestazioni della grid e successo dell'ingest. Balanced è l'opzione predefinita nella procedura guidata di creazione delle regole ILM.

Rigoroso

Quando selezioni l'opzione Rigorosa, StorageGRID utilizza il posizionamento sincrono durante l'ingest e crea immediatamente tutte le copie degli oggetti specificate nelle istruzioni di posizionamento della regola. L'ingest non riesce se StorageGRID non può creare tutte le copie, ad esempio perché una posizione di storage richiesta non è temporaneamente disponibile. Devi riprovare l'operazione dal client.

Utilizza l'opzione Rigorosa se hai un requisito operativo o normativo che ti impone di archiviare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potresti dover utilizzare l'opzione Rigorosa e un filtro avanzato Location Constraint per garantire che gli oggetti non vengano mai archiviati in determinati data center.

Vedi "Esempio 5: Regole e policy ILM per Strict ingest behavior".

Vantaggi, svantaggi e limitazioni delle opzioni di ingestione ILM in StorageGRID

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 aiutarti a decidere quale selezionare per una regola ILM.

Per una panoramica delle opzioni di ingest, vedi "Opzioni di ingest".

Vantaggi delle opzioni Bilanciata e Rigorosa

Rispetto al Dual 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 vengono protetti immediatamente come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per proteggere da un'ampia varietà di condizioni di errore, incluso il guasto di più posizioni di storage. Il dual commit può proteggere solo dalla perdita di una singola copia locale.

- **Funzionamento della grid più efficiente**: ogni oggetto viene elaborato una sola volta, al momento dell'ingestione. Poiché il sistema StorageGRID non ha bisogno di tracciare o eliminare copie intermedie, il carico di elaborazione è inferiore e viene consumato meno spazio nel database.
- **(Bilanciato) Consigliato**: L'opzione Bilanciato offre un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Bilanciato a meno che non sia richiesto un comportamento di ingest rigoroso o che la grid soddisfi tutti i criteri per l'utilizzo del Dual commit.
- **(Rigorosa) Certezza sulla posizione degli oggetti**: L'opzione Rigorosa garantisce che gli oggetti vengano memorizzati immediatamente in base alle istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni Bilanciata e Rigorosa

Rispetto alla modalità Dual commit, le opzioni Balanced e Strict presentano alcuni svantaggi:

- **Tempi di acquisizione client più lunghi**: I tempi di acquisizione client potrebbero essere più lunghi. Quando usi le opzioni Balanced o Strict, il messaggio "acquisizione riuscita" non viene restituito al client finché non vengono creati e archiviati tutti i frammenti codificati con cancellazione o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano la loro posizione finale molto più velocemente.
- **(Rigoroso) Tassi di errore di acquisizione più elevati**: Con l'opzione Rigoroso, l'acquisizione fallisce ogni volta che StorageGRID non riesce a creare immediatamente tutte le copie specificate nella regola ILM. Potresti riscontrare tassi elevati di errore di acquisizione se una posizione di storage richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia degli oggetti tra i siti.
- **(Rigoroso) Il posizionamento degli oggetti caricati in più parti su S3 potrebbe non essere quello previsto in alcune circostanze**: Con Rigoroso, ti aspetti che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'ingestione fallisca. Tuttavia, con un caricamento in più parti su S3, ILM viene valutato per ogni parte dell'oggetto durante l'ingestione e per l'oggetto nel suo complesso al termine del caricamento in più parti. Nelle seguenti circostanze questo potrebbe comportare posizionamenti diversi da quelli che ti aspetti:
  - **Se ILM cambia durante un caricamento multipart su S3**: Poiché ogni parte viene posizionata in base alla regola attiva al momento dell'acquisizione, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento multipart. In questi casi, l'acquisizione dell'oggetto non fallisce. Invece, qualsiasi parte non posizionata correttamente viene messa in coda per una rivalutazione da parte di ILM e spostata nella posizione corretta in un secondo momento.
  - **Quando le regole ILM filtrano in base alle dimensioni**: Quando valuti ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non alle dimensioni dell'oggetto. Questo significa che parti di un oggetto possono essere archiviate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo insieme. Per esempio, se una regola specifica che tutti gli oggetti da 10 GB o più vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, durante l'ingestione ogni parte da 1 GB di un caricamento multipart in 10 parti viene archiviata in DC2. Quando ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Rigoroso) L'ingest non fallisce quando i tag dell'oggetto o i metadati vengono aggiornati e non è possibile effettuare i nuovi posizionamenti richiesti**: Con Rigoroso, ti aspetti che gli oggetti vengano posizionati come descritto dalla regola ILM oppure che l'ingest fallisca. Tuttavia, quando aggiorni i metadati o i tag per un oggetto già memorizzato nella grid, l'oggetto non viene reinserito. Questo significa che eventuali modifiche al posizionamento dell'oggetto attivate dall'aggiornamento non vengono applicate immediatamente. Le modifiche al posizionamento vengono applicate quando ILM viene rivalutato dai normali processi ILM in background. Se non è possibile apportare le modifiche di posizionamento richieste (ad esempio, perché una nuova posizione richiesta non è disponibile), l'oggetto aggiornato mantiene il suo posizionamento attuale finché non è possibile apportare le modifiche.

Limitazioni al posizionamento degli oggetti con le opzioni Balanced e Strict

Le opzioni Bilanciato o Rigoroso non possono essere utilizzate per le regole ILM che presentano una qualsiasi di queste istruzioni di posizionamento:

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

Queste restrizioni esistono perché StorageGRID non può effettuare copie sincrone in un Cloud Storage Pool e un'ora di creazione definita dall'utente potrebbe corrispondere al presente.

Come le regole ILM e la coerenza interagiscono per influenzare la protezione dei dati

Sia la regola ILM che la scelta di coerenza influiscono sul modo in cui gli oggetti vengono protetti. 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 l'archiviazione di un oggetto influisce sul posizionamento iniziale dei metadati. Poiché StorageGRID richiede l'accesso sia ai dati sia ai metadati per soddisfare le richieste dei client, la selezione di livelli di protezione corrispondenti per la coerenza e il comportamento di acquisizione può offrire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

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

- **Tutti**: Tutti i nodi ricevono immediatamente i metadati dell'oggetto oppure la richiesta fallirà.
- **Strong-global**: Garantisce la coerenza read-after-write per tutte le richieste client su tutti i siti. Quando la semantica del quorum è configurata, si applicano i seguenti comportamenti:
  - Consente la tolleranza ai guasti del sito per le richieste dei client quando le griglie hanno tre o più siti. Le griglie con due siti non avranno la tolleranza ai guasti del sito.
  - Le seguenti operazioni S3 non andranno a buon fine se un sito non è disponibile:
    - DeleteBucketEncryption
    - PutBucketBranch
    - PutBucketEncryption
    - PutBucketVersioning
    - PutObjectLegalHold
    - PutObjectLockConfiguration
    - PutObjectRetention

  Se necessario, puoi "Configura la semantica del quorum di StorageGRID per una strong-global consistency".
- **Strong-site**: i metadati degli oggetti vengono distribuiti immediatamente agli altri nodi del sito. Garantisce la coerenza read-after-write per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write**: Garantisce la coerenza read-after-write per i nuovi oggetti e la coerenza finale per gli aggiornamenti degli oggetti. Offre elevata disponibilità e garanzie di protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile**: Fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i

bucket S3, usalo solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente 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". Dovresti capire i vantaggi e le limitazioni prima di cambiare il valore predefinito.

Esempio di come la coerenza e le regole ILM possono interagire

Supponiamo che tu abbia una griglia a tre siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM**: Crea tre copie dell'oggetto, una nel sito locale e una in ciascun sito remoto. Usa il comportamento di acquisizione rigoroso.
- **Coerenza**: Forte-globale (i metadati degli oggetti vengono distribuiti immediatamente a più siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID crea tutte e tre le copie dell'oggetto e distribuisce i metadati a più siti prima di restituire conferma al client.

L'oggetto è completamente protetto dalla perdita al momento della ricezione del messaggio di avvenuta acquisizione. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto che dei metadati dell'oggetto esistono comunque nei siti remoti. L'oggetto è completamente recuperabile dagli altri siti.

Se invece usi la stessa regola ILM e la coerenza strong-site, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati nei siti remoti, ma prima che i metadati dell'oggetto vengano distribuiti lì. In questo caso, il livello di protezione dei metadati dell'oggetto non corrisponde al livello di protezione dei dati dell'oggetto. Se il sito locale viene perso poco dopo l'ingestione, i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

La relazione tra coerenza e regole ILM può essere complessa. Contatta NetApp se hai bisogno di assistenza.

Informazioni correlate

"Esempio 5: Regole e policy ILM per Strict ingest behavior"

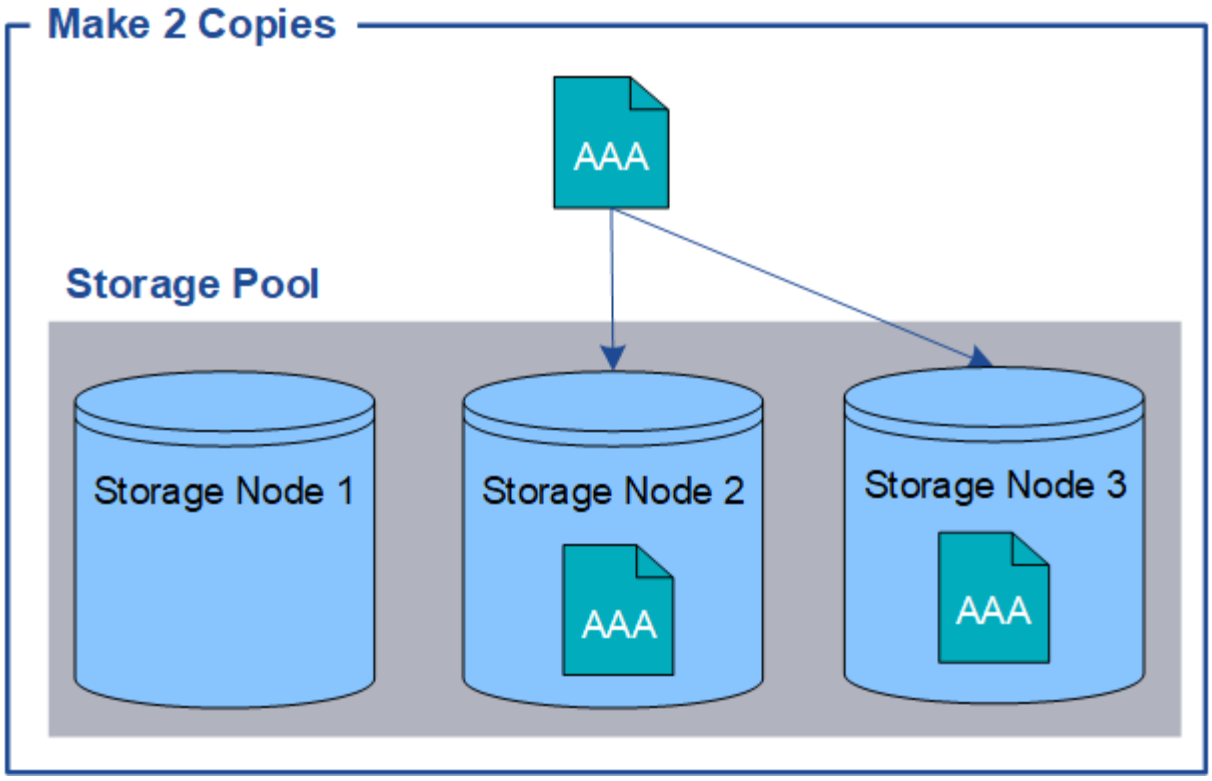
Come vengono memorizzati gli oggetti (replica o erasure coding)

Scopri la replica in StorageGRID

La replica è uno dei due metodi utilizzati da StorageGRID per memorizzare i dati degli oggetti (l'altro metodo è la codifica di cancellazione). Quando gli oggetti corrispondono a una regola ILM che utilizza la replica, il sistema crea copie esatte dei dati degli oggetti e le memorizza sui nodi di Storage.

Quando configuri una regola ILM per creare copie replicate, specifichi quante copie devono essere create, dove devono essere collocate e per quanto tempo devono essere conservate in ciascuna posizione.

Nell'esempio seguente, la regola ILM specifica che due copie replicate di ciascun oggetto devono essere inserite in un pool di storage che contiene tre Storage Nodes.



Quando StorageGRID associa gli oggetti a questa regola, crea due copie dell'oggetto, posizionando ciascuna copia su un diverso Storage Node nel pool di storage. Le due copie possono essere posizionate su due qualsiasi dei tre Storage Node disponibili. In questo caso, la regola ha posizionato le copie dell'oggetto sui Storage Node 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato se uno qualsiasi dei nodi nel pool di storage dovesse guastarsi.

> StorageGRID può memorizzare una sola copia replicata di un oggetto su ciascun Storage Node. Se la tua grid include tre Storage Node e crei una regola ILM a 4 copie, verranno create solo tre copie, una per ciascun Storage Node. L'avviso **ILM placement unachievable** viene attivato per indicare che la regola ILM non è stata applicata completamente.

Informazioni correlate

- "Cos'è la codifica di cancellazione"
- "Cos'è un pool di storage"
- "Abilita la protezione dalla perdita del sito tramite replica e erasure coding"

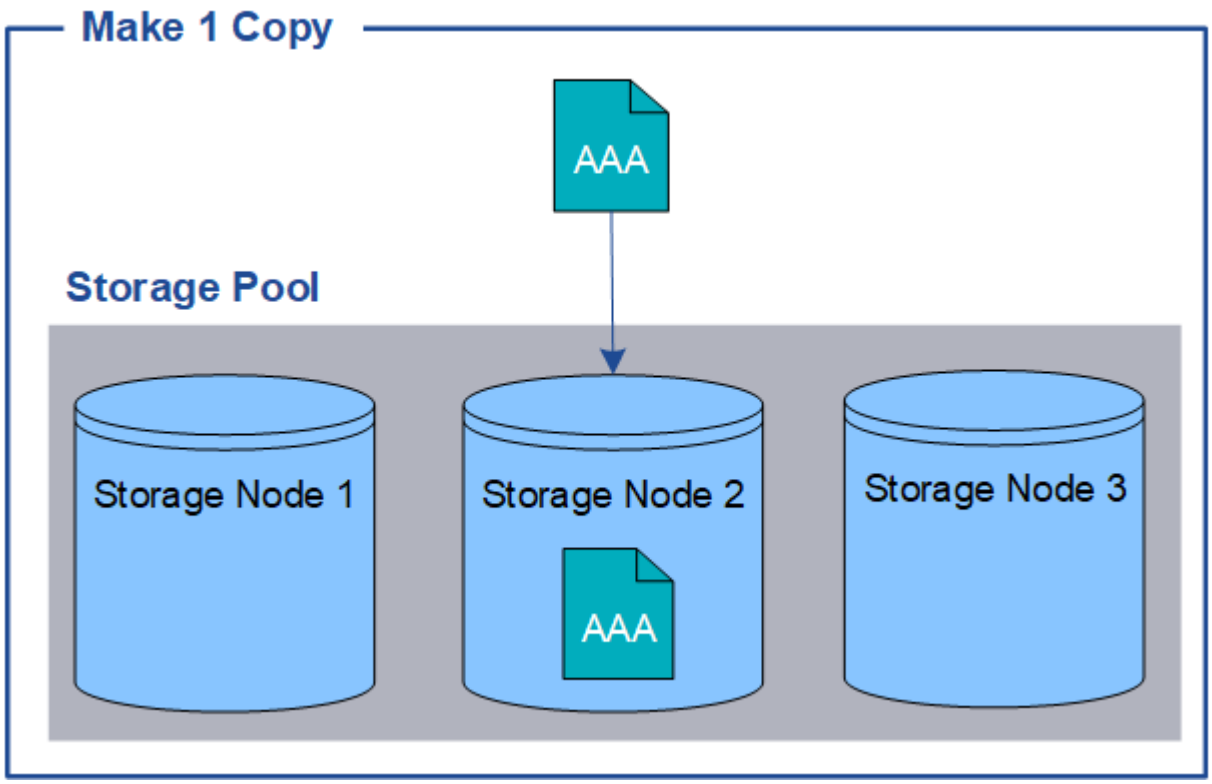
Rischi della replica a copia singola in StorageGRID

Quando crei una regola ILM per generare copie replicate, dovresti sempre specificare almeno due copie per qualsiasi periodo di tempo nelle istruzioni di posizionamento.

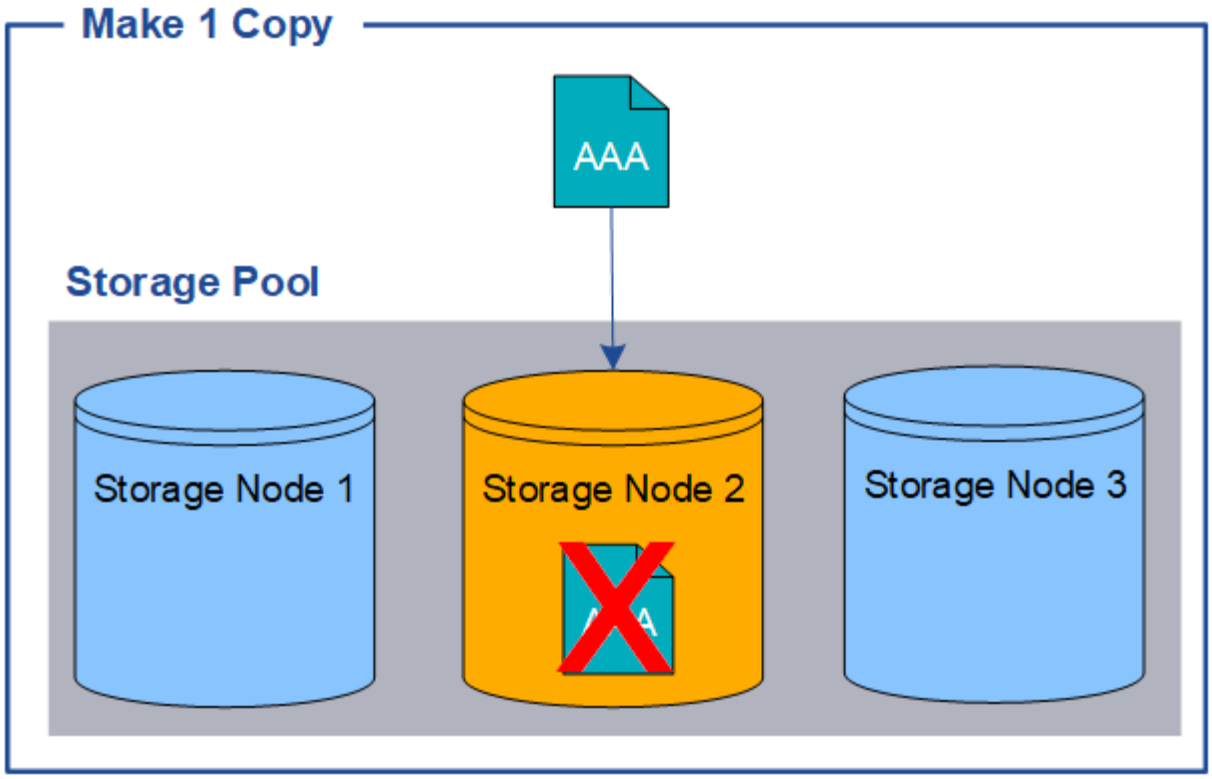
> Non usare una regola ILM che crea solo una copia replicata per qualsiasi periodo di tempo. Se esiste solo una copia replicata di un oggetto, quell'oggetto viene perso se un Storage Node si guasta o ha un errore significativo. Perderai anche temporaneamente l'accesso all'oggetto durante le procedure di manutenzione come gli upgrade.

Nell'esempio seguente, la regola ILM "Crea 1 copia" specifica che una copia replicata di un oggetto deve essere inserita in un pool di storage contenente tre Storage Node. Quando viene acquisito un oggetto che

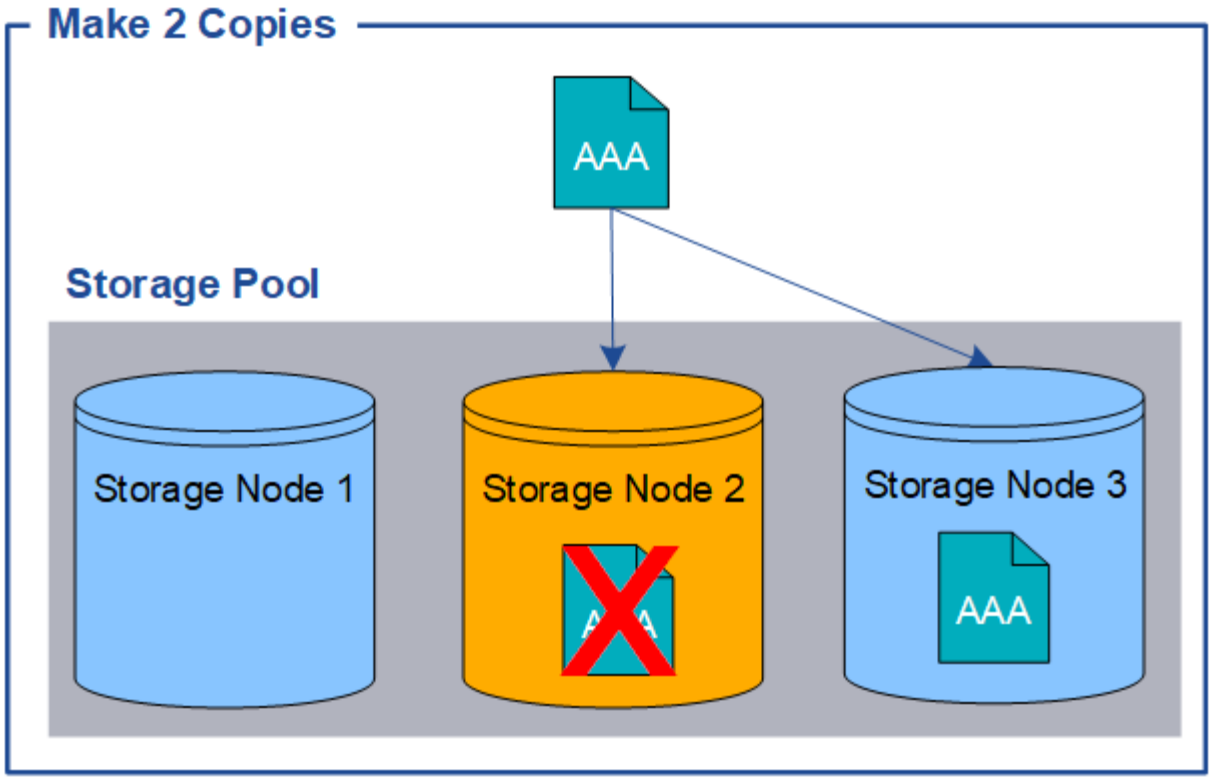
corrisponde a questa regola, StorageGRID ne inserisce una singola copia su un solo Storage Node.



Quando una regola ILM crea solo una copia replicata di un oggetto, l'oggetto diventa inaccessibile quando il Storage Node non è disponibile. In questo esempio, perderai temporaneamente l'accesso all'oggetto AAA ogni volta che il Storage Node 2 è offline, ad esempio durante un aggiornamento o un'altra procedura di manutenzione. Perderai completamente l'oggetto AAA se il Storage Node 2 si guasta.



Per evitare di perdere i dati degli oggetti, dovresti sempre creare almeno due copie di tutti gli oggetti che vuoi proteggere con la replica. Se esistono due o più copie, puoi comunque accedere all'oggetto se un nodo di storage si guasta o va offline.



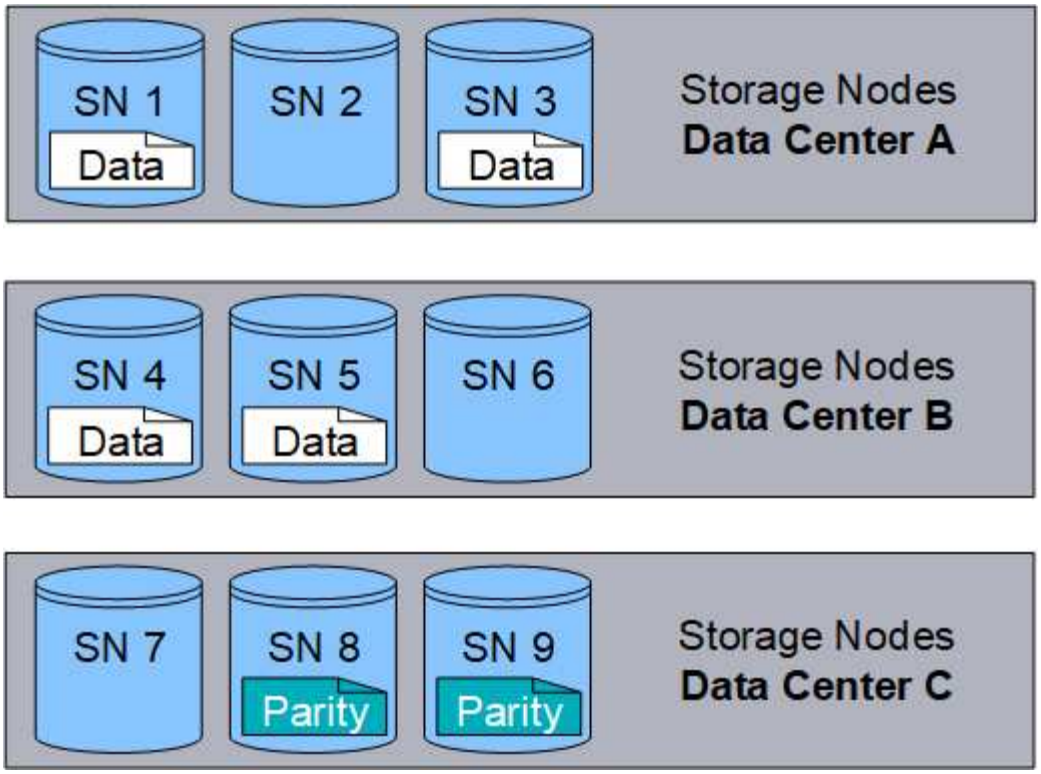
Scopri la codifica di cancellazione in StorageGRID

La codifica di cancellazione è uno dei due metodi che StorageGRID utilizza per memorizzare i dati degli oggetti (l'altro metodo è la replica). Quando gli oggetti corrispondono a una regola ILM che utilizza la codifica di cancellazione, questi vengono suddivisi in frammenti di dati, vengono calcolati ulteriori frammenti di parità e ciascun frammento viene memorizzato su un diverso Storage Node.

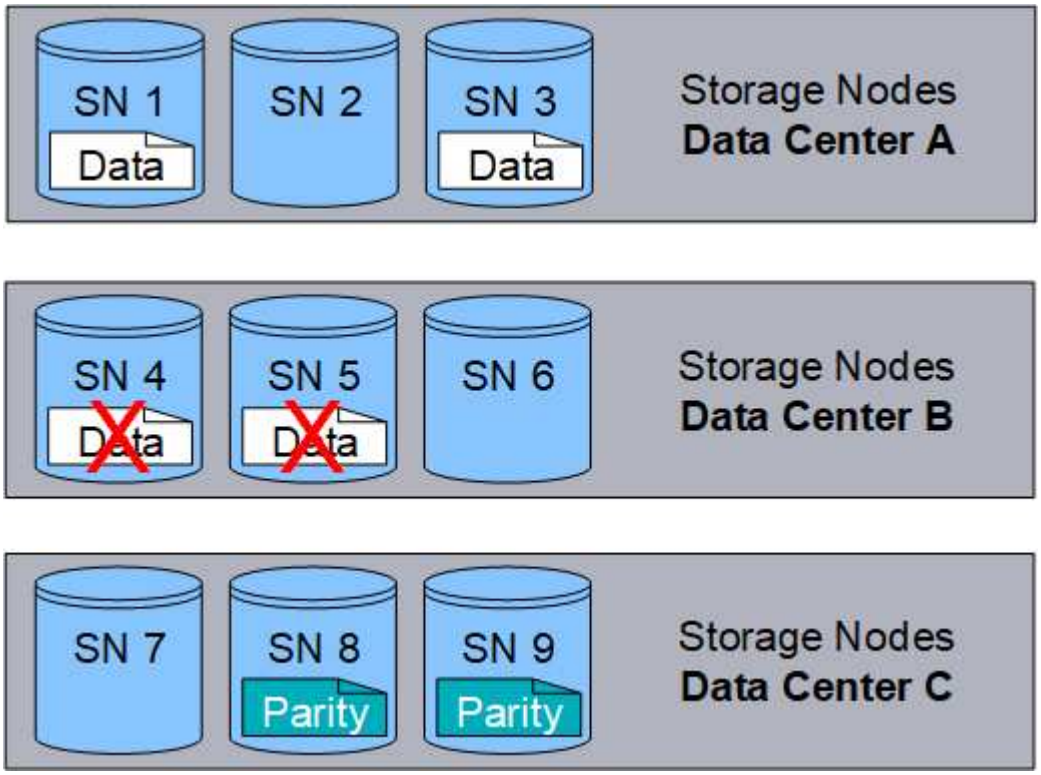
Quando accedi a un oggetto, questo viene ricostruito utilizzando i frammenti memorizzati. Se un frammento di dati o di parità risulta danneggiato o perso, l'algoritmo di codifica di cancellazione può ricreare quel frammento utilizzando un sottoinsieme dei frammenti di dati e di parità rimanenti.

Quando crei regole ILM, StorageGRID crea profili di codifica di cancellazione che supportano tali regole. Puoi visualizzare un elenco di profili di codifica di cancellazione, "rinominare un profilo di erasure-coding", oppure "Disattiva un profilo di codifica di cancellazione se non è attualmente utilizzato in nessuna regola ILM".

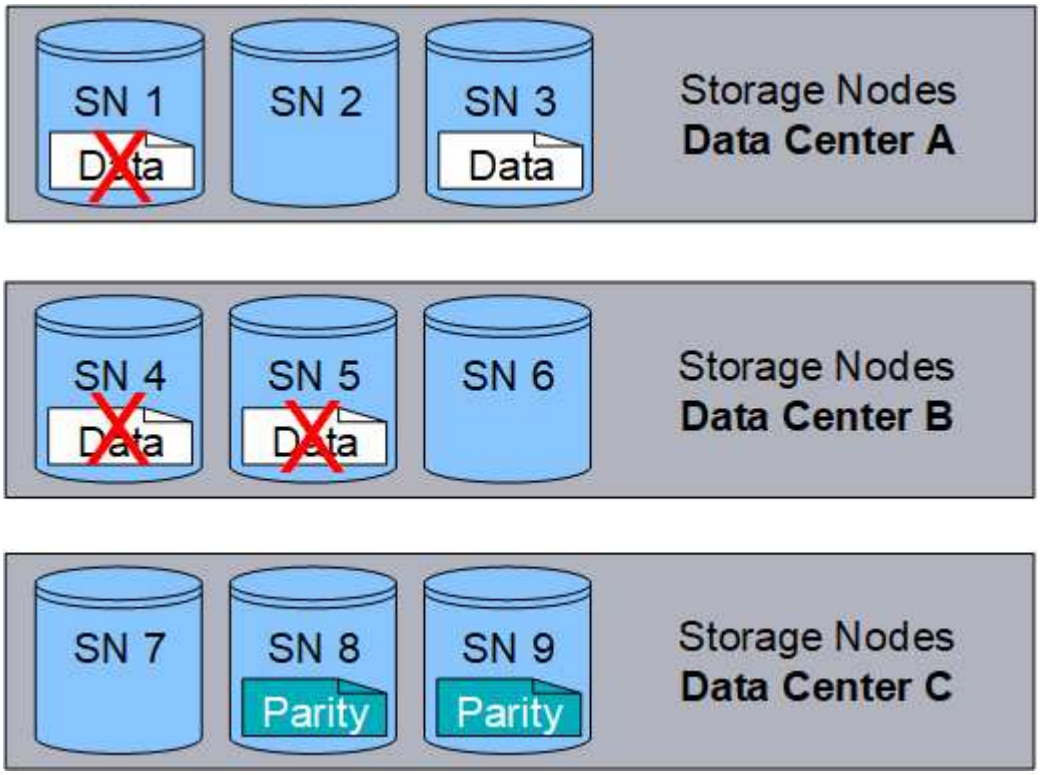
L'esempio seguente illustra l'utilizzo di un algoritmo di codifica di cancellazione sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di codifica di cancellazione 4+2. Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e da questi vengono calcolati due frammenti di parità. Ciascuno dei sei frammenti viene memorizzato su un nodo diverso in tre siti di data center per garantire la protezione dei dati in caso di guasti ai nodi o perdita di un sito.



Lo schema di codifica di cancellazione 4+2 può essere configurato in vari modi. Ad esempio, puoi configurare un pool di storage che contiene sei Storage Node. Per "protezione dalla perdita del sito", puoi usare un pool di storage che contiene tre siti con tre Storage Node in ciascun sito. Un oggetto può essere recuperato finché almeno quattro dei sei frammenti (dati o parità) rimangono disponibili. Si possono perdere fino a due frammenti senza perdere i dati dell'oggetto. Se un intero sito viene perso, l'oggetto può comunque essere recuperato o riparato, finché tutti gli altri frammenti rimangono accessibili.



Se perdi più di due Storage Node, l'oggetto non è recuperabile.



Informazioni correlate

- "Che cos'è la replicazione"
- "Cos'è un pool di storage"
- "Cosa sono gli schemi di codifica a cancellazione"
- "Rinomina un profilo di codifica di cancellazione"
- "Disattiva un profilo di codifica di cancellazione"

Scopri gli schemi di codifica di cancellazione in StorageGRID

Gli schemi di codifica a cancellazione controllano quanti frammenti di dati e quanti frammenti di parità vengono creati per ciascun oggetto.

Quando crei o modifichi una regola ILM, selezioni uno schema di erasure coding disponibile. StorageGRID crea automaticamente gli schemi di erasure coding in base a quanti Storage Node e siti compongono il pool di storage che vuoi usare.

Protezione dei dati

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

I `k + m = n`frammenti sono distribuiti tra `n`Storage Nodes per fornire la protezione dei dati come segue:

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

La migliore protezione dei dati è garantita dallo schema di codifica di cancellazione con la più alta tolleranza ai

guasti di nodi o volumi all'interno di un pool di storage.

Overhead dello storage

L'overhead dello storage di uno schema di codifica a cancellazione si calcola dividendo il numero di frammenti di parità (`m` per il numero di frammenti di dati (`k`. Puoi usare l'overhead dello storage per calcolare quanto spazio su disco richiede ciascun oggetto codificato a cancellazione:

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

Ad esempio, se memorizzi un oggetto da 10 MB utilizzando lo schema 4+2 (che presenta un overhead dello storage del 50%), l'oggetto consuma 15 MB di grid storage. Se memorizzi lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (che presenta un overhead dello storage del 33%), l'oggetto consuma circa 13,3 MB.

Seleziona lo schema di codifica di cancellazione con il valore totale più basso di `k+m` che soddisfa le tue esigenze. Gli schemi di codifica di cancellazione con un numero inferiore di frammenti sono più efficienti dal punto di vista computazionale perché:

- Vengono creati e distribuiti (o recuperati) meno frammenti per ogni oggetto
- Mostrano prestazioni migliori perché la dimensione del frammento è maggiore
- Possono richiedere l'aggiunta di un minor numero di nodi in un"espansione quando è necessario più storage"

Linee guida per i pool di storage

Quando selezioni il pool di storage da usare per una regola che creerà una copia con codifica di cancellazione, segui queste linee guida per i pool di storage:

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

  > Non puoi usare la codifica di cancellazione se il pool di storage include due siti.

  - Schemi di codifica di cancellazione per pool di storage contenenti tre o più siti
  - Schemi di codifica a cancellazione per pool di storage a sito singolo
- Non usare un pool di storage che includa il sito All Sites.
- Il pool di storage dovrebbe includere almeno *k+m* `+1` Storage Nodes in grado di memorizzare dati oggetto.

  > I nodi di archiviazione possono essere configurati durante l'installazione per contenere dati degli oggetti e metadati ("nodo di archiviazione combinato"), solo metadati degli oggetti o solo dati degli oggetti. Per ulteriori informazioni, consulta "Tipi di nodi di archiviazione".

  Il numero minimo di Storage Node richiesti è `k+m`. Tuttavia, avere almeno un Storage Node aggiuntivo può aiutare a prevenire errori di acquisizione o arretrati ILM se un Storage Node richiesto non è temporaneamente disponibile.

Schemi di codifica di cancellazione per pool di storage contenenti tre o più siti

La tabella seguente descrive gli schemi di codifica di cancellazione attualmente supportati da StorageGRID per i pool di storage che includono tre o più siti. Tutti questi schemi offrono protezione in caso di perdita di un sito. Un sito può andare perso e l'oggetto sarà comunque accessibile.

Per gli schemi di codifica di cancellazione che forniscono protezione dalla perdita del sito, il numero consigliato di nodi di archiviazione nel pool di storage supera `k+m +1` perché ogni sito richiede un minimo di tre nodi di archiviazione.

Schema di codifica a cancellazione (*k*+*m*)	Numero minimo di siti distribuiti	Numero consigliato di Storage Node in ciascun sito	Numero totale consigliato di Storage Node	Protezione contro la perdita del 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 Storage Node per sito. Per utilizzare lo schema 7+5, ogni sito richiede un minimo di quattro Storage Node. Si consiglia di utilizzare cinque Storage Node per sito.

Quando scegli uno schema di codifica di cancellazione che offre la protezione del sito, bilancia 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.
- **Tolleranza ai guasti**: La tolleranza ai guasti aumenta con un maggior numero di segmenti di parità (ovvero, quando `m` ha un valore più elevato.)
- **Traffico di rete**: Durante il ripristino da guasti, l'utilizzo di uno schema con più frammenti (ovvero, un totale più elevato per `k+m`) crea più traffico di rete.
- **Overhead dello storage**: Gli schemi con un overhead maggiore richiedono più spazio di storage per oggetto.

Ad esempio, quando decidi tra uno schema 4+2 e uno schema 6+3 (entrambi con overhead dello storage del 50%), scegli lo schema 6+3 se hai bisogno di una tolleranza ai guasti aggiuntiva. Scegli invece lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, scegli il 4+2 perché ha un numero totale di frammenti inferiore.

Se non sei sicuro di quale schema utilizzare, seleziona 4+2 o 6+3 oppure contatta il supporto tecnico.

Schemi di codifica a cancellazione per pool di storage a sito singolo

Un pool di storage con un solo sito supporta tutti gli schemi di codifica di cancellazione definiti per tre o più siti, a condizione che il sito disponga di un numero sufficiente di Storage Node.

Il numero minimo di Storage Node richiesti è `k+m`, ma è consigliato un pool di storage con `k+m +1` Storage Node. Ad esempio, lo schema di erasure-coding 2+1 richiede un pool di storage con un minimo di tre Storage Node, ma è consigliato utilizzarne quattro.

Schema di codifica a cancellazione (*k*+*m*)	Numero minimo di Storage Node	Numero consigliato di Storage Node	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 in StorageGRID

Prima di decidere se utilizzare la replica o la codifica di cancellazione per proteggere i dati degli oggetti dalla perdita, dovresti capire i vantaggi, gli svantaggi e i requisiti della codifica di cancellazione.

Vantaggi della codifica a cancellazione

Rispetto alla replica, la codifica a cancellazione offre maggiore affidabilità, disponibilità ed efficienza di archiviazione.

- **Affidabilità**: Misurata dal numero di guasti simultanei che possono essere sostenuti senza perdita di dati.
  - Replicazione: più copie identiche degli oggetti sono memorizzate su nodi diversi e in siti diversi.
  - Codifica di cancellazione: un oggetto viene codificato in frammenti di dati e di parità e distribuito su molti nodi e siti. Questa dispersione offre protezione sia dai guasti del sito che del nodo.

- **Disponibilità**: la possibilità di recuperare gli oggetti se i nodi di archiviazione si guastano o diventano inaccessibili. Rispetto alla replica, la codifica di cancellazione offre una maggiore disponibilità a costi di storage comparabili.
- **Efficienza di archiviazione**: a parità di disponibilità e affidabilità, gli oggetti con codifica di cancellazione utilizzano meno spazio su disco rispetto agli oggetti replicati. Ad esempio, un oggetto da 10 MB replicato su due siti occupa 20 MB di spazio su disco (due copie), mentre un oggetto con codifica di cancellazione su tre siti con uno schema di codifica di cancellazione 6+3 occupa solo 15 MB di spazio su disco.

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

Svantaggi della codifica di cancellazione

Rispetto alla replicazione, la codifica a cancellazione presenta i seguenti svantaggi:

- A seconda dello schema di codifica di cancellazione, si consiglia un numero maggiore di Storage Node e siti. Al contrario, se replichi i dati degli oggetti, ti serve solo un Storage Node per ogni copia. Vedi "Schemi di codifica di cancellazione per pool di storage contenenti tre o più siti" e "Schemi di codifica a cancellazione per pool di storage a sito singolo".
- Aumento dei costi e della complessità delle espansioni di storage. Per espandere una deployment che utilizza la replica, devi aggiungere capacità di storage in ogni posizione in cui vengono create copie di oggetti. Per espandere una deployment che utilizza la codifica di cancellazione, devi considerare sia lo schema di codifica di cancellazione in uso sia quanto sono pieni i nodi di storage esistenti. Ad esempio, se aspetti che i nodi esistenti siano pieni al 100%, devi aggiungere almeno `k+m` nodi di storage, ma se espandi quando i nodi esistenti sono pieni al 70%, puoi aggiungere due nodi per sito e comunque massimizzare la capacità di storage utilizzabile. Per ulteriori informazioni, vedi "${post_edited_translations.segment}".
- L'utilizzo della codifica di cancellazione su siti geograficamente distribuiti comporta un aumento delle latenze di recupero. I frammenti di un oggetto codificato con codifica di cancellazione e distribuito su siti remoti richiedono più tempo per essere recuperati tramite connessioni WAN rispetto a un oggetto replicato e disponibile localmente (nello stesso sito a cui si connette il client).
- Quando usi la codifica di cancellazione su siti distribuiti geograficamente, c'è un maggiore utilizzo del traffico di rete WAN per i recuperi e le riparazioni, soprattutto per gli oggetti recuperati frequentemente o per le riparazioni di oggetti tramite connessioni di rete WAN.
- Quando usi la codifica di cancellazione tra siti, il throughput massimo degli oggetti diminuisce drasticamente man mano che la latenza di rete tra i siti aumenta. Questa diminuzione è il risultato di una riduzione del throughput di rete TCP, che influisce sulla rapidità con cui il sistema StorageGRID può memorizzare e recuperare i frammenti degli oggetti.
- Maggiore utilizzo delle risorse di calcolo.

Quando utilizzare la codifica di cancellazione

Usa la codifica di cancellazione per i seguenti requisiti:

- Oggetti di dimensioni superiori a 1 MB.

> La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non usare la codifica di cancellazione per oggetti più piccoli di 200 KB per evitare l'overhead della gestione di frammenti codificati molto piccoli.

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

Come StorageGRID determina la conservazione degli oggetti

StorageGRID offre opzioni sia agli amministratori della griglia che ai singoli tenant per specificare per quanto tempo conservare gli oggetti. In generale, le istruzioni di conservazione fornite da un tenant hanno la precedenza su quelle fornite dall'amministratore della griglia.

Come gli utenti tenant controllano la conservazione degli oggetti

Gli utenti tenant possono utilizzare questi metodi per controllare per quanto tempo i loro oggetti vengono conservati in StorageGRID:

- Se l'impostazione globale S3 Object Lock è abilitata per la grid, gli utenti tenant S3 possono creare bucket con S3 Object Lock abilitato e poi selezionare un **periodo di conservazione predefinito** per ciascun bucket.
- Se l'impostazione globale di S3 Object Lock è abilitata per la grid, gli utenti tenant S3 possono creare bucket con S3 Object Lock abilitato e poi usare l'API REST S3 per specificare retain-until-date e legal hold per ogni versione dell'oggetto aggiunta a quel bucket.
  - Una versione di un oggetto soggetta a blocco legale non può essere eliminata in alcun modo.
  - Prima che venga raggiunta la retain-until-date di una versione di un oggetto, tale versione non può essere eliminata in alcun modo.
  - Gli oggetti nei bucket con S3 Object Lock abilitato vengono conservati da ILM "per sempre". Tuttavia, dopo il raggiungimento della data di conservazione, una versione dell'oggetto può essere eliminata su richiesta del client o alla scadenza del ciclo di vita del bucket. Vedi "Gestisci gli oggetti con S3 Object Lock".
- Gli utenti tenant S3 possono aggiungere una configurazione del ciclo di vita ai propri bucket che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID memorizza un oggetto fino alla data o al numero di giorni specificati nell'azione di scadenza, a meno che il client non elimini prima l'oggetto. Vedi "Crea configurazione del ciclo di vita S3".
- Un client S3 può inviare una richiesta di eliminazione di un oggetto. StorageGRID dà sempre la priorità alle richieste di eliminazione del client rispetto al ciclo di vita del bucket S3 o all'ILM quando determina se eliminare o conservare un oggetto.

Come gli amministratori della griglia controllano la conservazione degli oggetti

Gli amministratori della griglia possono utilizzare questi metodi per controllare la conservazione degli oggetti:

- Imposta un periodo massimo di conservazione S3 Object Lock per ogni tenant. Poi, gli utenti del tenant possono impostare un periodo di conservazione predefinito per ciascuno dei loro bucket. Il periodo massimo di conservazione viene applicato anche a tutti i nuovi oggetti ingeriti per quel bucket (retain-until-

date dell'oggetto).

- Crea istruzioni di posizionamento ILM per controllare per quanto tempo gli oggetti vengono conservati. Quando gli oggetti vengono abbinati da una regola ILM, StorageGRID li memorizza fino allo scadere dell'ultimo periodo di tempo nella regola ILM. Gli oggetti vengono conservati a tempo indeterminato se nelle istruzioni di posizionamento è specificato "forever".
- Indipendentemente da chi controlla per quanto tempo vengono conservati gli oggetti, le impostazioni ILM controllano quali tipi di copie degli oggetti (replicate o con codifica di cancellazione) vengono memorizzate e dove si trovano le copie (Storage Nodes o Cloud Storage Pools).

Come interagiscono il ciclo di vita del bucket S3 e ILM

Quando il ciclo di vita di un bucket S3 è configurato, le azioni di scadenza del ciclo di vita sovrascrivono la policy ILM per gli oggetti che corrispondono al filtro del ciclo di vita. Di conseguenza, un oggetto potrebbe essere conservato nella grid anche dopo che tutte le istruzioni ILM per il posizionamento dell'oggetto sono scadute.

Esempi di conservazione degli oggetti

Per comprendere meglio le interazioni tra S3 Object Lock, le impostazioni del ciclo di vita del bucket, le richieste di eliminazione del client e ILM, considera i seguenti esempi.

Esempio 1: il ciclo di vita S3 mantiene gli oggetti più a lungo di ILM

ILM

Conserva due copie per 1 anno (365 giorni)

Ciclo di vita del bucket

Gli oggetti scadono dopo 2 anni (730 giorni)

Risultato

StorageGRID conserva 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 specifica che gli oggetti devono essere conservati più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento di ILM per determinare il numero e il tipo di copie da memorizzare. In questo esempio, due copie dell'oggetto continueranno a essere memorizzate in StorageGRID dal giorno 366 al giorno 730.

Esempio 2: il ciclo di vita del bucket S3 fa scadere gli oggetti prima di ILM

ILM

Conserva due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Gli oggetti scadono dopo 1 anno (365 giorni)

Risultato

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

Esempio 3: L'eliminazione da parte del client sovrascrive ciclo di vita e ILM

ILM

Archivia due copie sui nodi di StorageGRID "per sempre"

Ciclo di vita del bucket

Gli oggetti scadono dopo 2 anni (730 giorni)

Richiesta di eliminazione del client

Emesso il giorno 400

Risultato

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

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

Blocco oggetto S3

La data di conservazione fino a per una versione dell'oggetto è il 31-03-2026. Non è attivo alcun blocco legale.

Regola ILM conforme

Archivia due copie sui nodi di StorageGRID "per sempre"

Richiesta di eliminazione del client

Emesso il 31/03/2024

Risultato

StorageGRID non eliminerà la versione dell'oggetto perché la retain-until-date è ancora a 2 anni di distanza.

Come StorageGRID elimina gli oggetti

StorageGRID può eliminare gli oggetti sia in risposta diretta a una richiesta del client sia automaticamente a seguito della scadenza del ciclo di vita di un bucket S3 o dei requisiti della policy ILM. Comprendere i diversi modi in cui gli oggetti possono essere eliminati e come StorageGRID gestisce le richieste di eliminazione può aiutarti a gestire gli oggetti in modo più efficace.

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

- Eliminazione sincrona: quando StorageGRID riceve una richiesta di eliminazione da un client, tutte le copie dell'oggetto vengono rimosse immediatamente. Il client viene informato che l'eliminazione è avvenuta con successo dopo che le copie sono state rimosse.
- 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 che l'eliminazione è avvenuta con successo. Le copie degli oggetti vengono rimosse in seguito tramite l'elaborazione ILM in background.

Quando elimini oggetti, StorageGRID utilizza il metodo che ottimizza le prestazioni di eliminazione, riduce al minimo i potenziali accumuli di eliminazioni in sospeso e libera spazio il più rapidamente possibile.

La tabella riassume quando StorageGRID utilizza ciascun metodo.

Metodo per eseguire la cancellazione	Quando usato
Gli oggetti vengono messi in coda per la cancellazione	Quando **una qualsiasi** delle seguenti condizioni è vera: • La cancellazione automatica dell'oggetto è stata attivata da uno dei seguenti eventi: ◦ È stata raggiunta la data di scadenza o il numero di giorni previsto nella configurazione del ciclo di vita per un bucket S3. ◦ Trascorre l'ultimo periodo di tempo specificato in una regola ILM. **Nota:** Gli oggetti in un bucket con S3 Object Lock abilitato non possono essere eliminati se sono soggetti a un blocco legale o se è stata specificata una data di conservazione non ancora raggiunta. • Un client S3 richiede la cancellazione e si verifica una o più di queste condizioni: ◦ Non puoi eliminare le copie entro 30 secondi perché, ad esempio, la posizione di un 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 i client S3 effettuano richieste di eliminazione, StorageGRID inizia aggiungendo oggetti alla coda di eliminazione. Poi passa all'eliminazione sincrona. Assicurarsi che la coda di eliminazione in background abbia oggetti da elaborare permette a StorageGRID di gestire le eliminazioni in modo più efficiente, soprattutto per i client con bassa concorrenza, aiutando a prevenire l'accumulo di richieste di eliminazione da parte dei client.

Tempo necessario per eliminare gli oggetti

Il modo in cui StorageGRID elimina gli oggetti può influire su come il sistema sembra funzionare:

- Quando StorageGRID esegue la cancellazione sincrona, StorageGRID può impiegare fino a 30 secondi per restituire un risultato al client. Ciò significa che la cancellazione può sembrare più lenta, anche se in realtà le copie vengono rimosse più rapidamente rispetto a quando StorageGRID mette in coda gli oggetti per la cancellazione.
- Se monitori attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, potresti notare che la velocità di eliminazione sembra rallentare dopo che un certo numero di oggetti è stato eliminato. Questo cambiamento si verifica quando StorageGRID passa dall'accodare gli oggetti per l'eliminazione all'eseguire l'eliminazione sincrona. L'apparente riduzione della velocità di eliminazione non significa che le copie degli oggetti vengano rimosse più lentamente. Al contrario, indica che in media lo spazio viene ora liberato più rapidamente.

Se devi eliminare un gran numero di oggetti e la tua priorità è liberare spazio rapidamente, valuta la possibilità di utilizzare una richiesta client per eliminare gli oggetti anziché eliminarli tramite ILM o altri metodi. In generale, lo spazio viene liberato più velocemente quando l'eliminazione viene eseguita dai client perché StorageGRID può utilizzare l'eliminazione sincrona.

Il tempo necessario per liberare spazio dopo l'eliminazione di un oggetto dipende da diversi fattori:

- Indica se le copie degli oggetti vengono rimosse in modo sincrono o se vengono messe in coda per la rimozione successiva (per le richieste di eliminazione da parte del client).
- Altri fattori includono il numero di oggetti nella griglia o la disponibilità delle risorse della griglia quando le copie degli oggetti vengono messe in coda per la rimozione (sia per le eliminazioni client che per altri metodi).

Come vengono eliminati gli oggetti versionati di S3

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

Quando gli oggetti sono versionati, le richieste di eliminazione dell'oggetto non eliminano la versione corrente dell'oggetto e non liberano spazio. Al contrario, una richiesta di eliminazione dell'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 dell'oggetto diventa un marcatore di eliminazione 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 tale oggetto restituiscono 404 NotFound. Tuttavia, poiché i dati dell'oggetto non corrente non sono stati rimossi, le richieste che specificano una versione non corrente dell'oggetto possono avere esito positivo.

Se un client elimina una versione di un oggetto con un ID di versione da un "bucket branch", StorageGRID nasconde l'esistenza della versione dell'oggetto ma non crea un delete marker nel branch bucket. Se un client elimina un oggetto senza un ID di versione da un branch bucket, StorageGRID crea un delete marker nel branch bucket secondo il comportamento standard di S3.

Per liberare spazio quando elimini oggetti con versioni o per rimuovere i marcatori di eliminazione, usa uno dei seguenti metodi:

- **Richiesta client S3**: specifica l'ID della versione dell'oggetto nella richiesta S3 DELETE Object (`DELETE /object?versionId=ID`). Tieni presente che questa richiesta rimuove solo le copie dell'oggetto per la versione specificata (le altre versioni continuano a occupare spazio).
- **Bucket lifecycle**: Usa l'azione `NoncurrentVersionExpiration` nella configurazione del ciclo di vita del bucket. Quando viene raggiunto il numero di NoncurrentDays specificato, StorageGRID rimuove definitivamente tutte le copie delle versioni non correnti degli oggetti. Queste versioni degli oggetti non possono essere recuperate.

  L'azione `NewerNoncurrentVersions` nella configurazione del ciclo di vita del bucket specifica il numero di versioni non correnti conservate in un bucket S3 versionato. Se ci sono più versioni non correnti di quante ne `NewerNoncurrentVersions` specifica, StorageGRID rimuove le versioni più vecchie quando il valore NoncurrentDays è trascorso. La soglia `NewerNoncurrentVersions` sostituisce le regole del ciclo di vita fornite da ILM, il che significa che un oggetto non corrente con una versione entro la soglia `NewerNoncurrentVersions` viene conservato se ILM ne richiede l'eliminazione.

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

- **ILM**: "Clona una policy attiva" e aggiungi due regole ILM alla nuova policy:
  - Prima regola: usa "Tempo non corrente" come tempo di riferimento per abbinare le versioni non

correnti dell'oggetto. In "Passaggio 1 (Inserisci i dettagli) della procedura guidata Crea una regola ILM", seleziona **Sì** alla domanda "Applica questa regola solo alle versioni non correnti dell'oggetto (nei bucket S3 con versioning abilitato)?"

- Seconda regola: usa **Ingest time** per corrispondere alla versione corrente. La regola "Noncurrent time" deve comparire nella policy sopra la regola **Ingest time**.

  Per rimuovere i marcatori di eliminazione degli oggetti scaduti, usa 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 marcatore di eliminazione corrente è scaduto (non ci sono versioni non correnti).

- **Elimina oggetti nel bucket**: Usa il tenant manager per "elimina tutte le versioni degli oggetti"eliminare oggetti, inclusi i marcatori di eliminazione, da un bucket.

Quando un oggetto versionato viene eliminato, StorageGRID crea un marcatore di eliminazione di zero byte come versione corrente dell'oggetto. Tutti gli oggetti e i marcatori di eliminazione devono essere rimossi prima che sia possibile eliminare un bucket versionato.

- I marcatori di eliminazione creati in StorageGRID 11.7 o versioni precedenti possono essere rimossi solo tramite richieste client S3, non vengono rimossi da ILM, dalle regole del ciclo di vita del bucket o dalle operazioni di eliminazione degli oggetti nel bucket.
- I marcatori di eliminazione da un bucket creato in StorageGRID 11.8 o versioni successive possono essere rimossi da ILM, dalle regole del ciclo di vita del bucket, dalle operazioni di eliminazione di oggetti nel bucket o da un'eliminazione esplicita tramite client S3.

Informazioni correlate

- "${post_edited_translations.segment}"
- "Esempio 4: Regole e policy ILM per gli oggetti versionati S3"

Crea e assegna gradi di storage in StorageGRID

I livelli di storage identificano il tipo di storage utilizzato da un Storage Node. Puoi creare livelli di storage se vuoi che le regole ILM posizionino determinati oggetti su determinati Storage Node.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

Quando installi StorageGRID, il livello di storage **Default** viene assegnato automaticamente a ogni Storage Node nel tuo sistema. Se necessario, puoi definire livelli di storage personalizzati e assegnarli a Storage Node diversi.

L'utilizzo di livelli di storage personalizzati consente di creare pool di storage ILM che contengono solo un tipo specifico di Storage Node. Ad esempio, potresti voler archiviare determinati oggetti sui tuoi Storage Node più veloci, come gli appliance di storage all-flash StorageGRID.

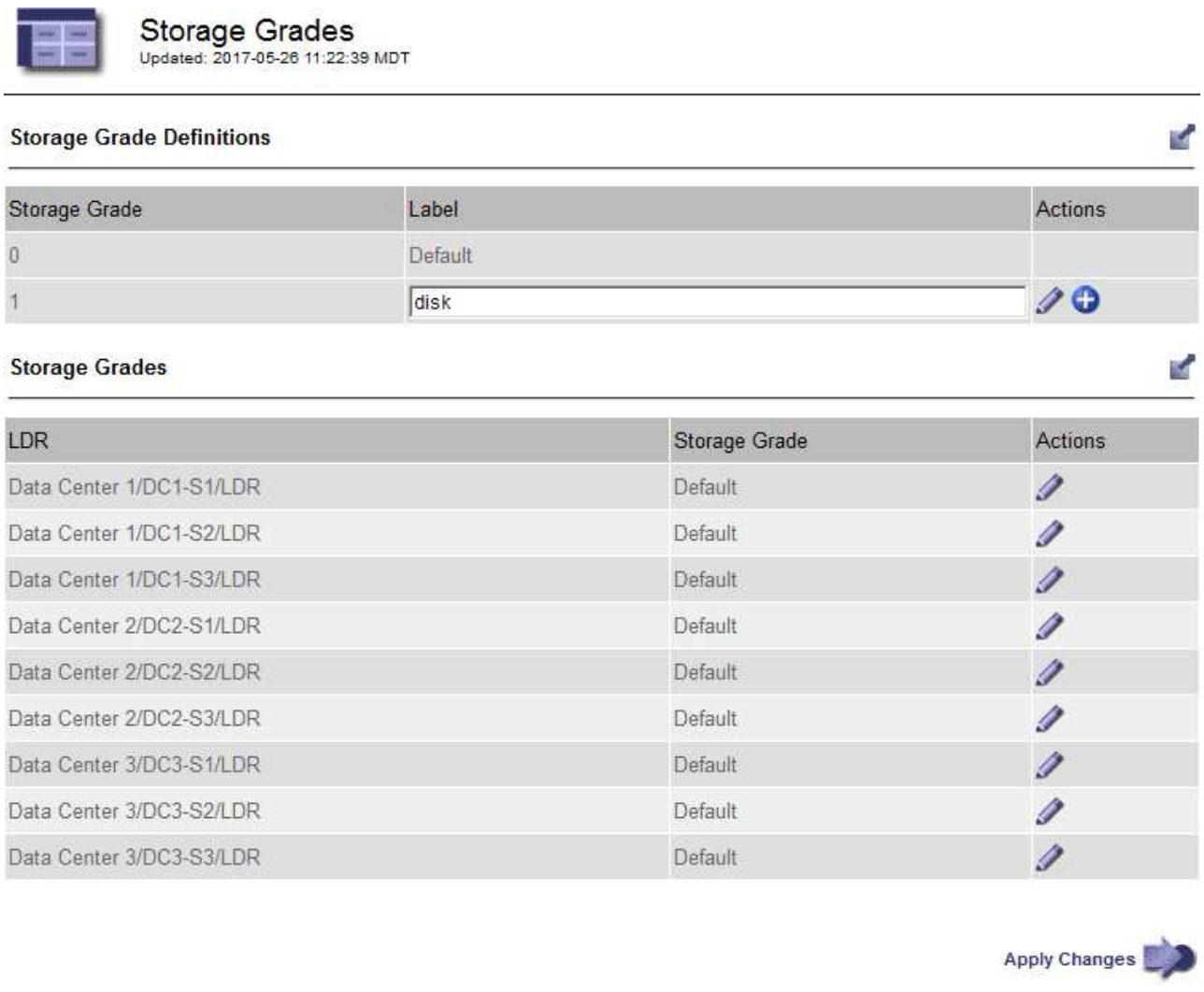
Ai nodi di storage che contengono solo metadati non puoi assegnare un livello di storage. Per ulteriori informazioni, consulta "Tipi di nodi di archiviazione".

Se il livello di storage non è un problema (ad esempio, tutti i nodi di storage sono identici), puoi saltare questa procedura e usare la selezione **includes all storage grades** per il livello di storage quando "creare pool di storage". Usando questa selezione, il pool di storage includerà ogni nodo di storage nel sito, indipendentemente dal suo livello di storage.

> Non creare più livelli di storage del necessario. Ad esempio, non creare un livello di storage per ogni Storage Node. Assegna invece ciascun livello di storage a due o più nodi. I livelli di storage assegnati a un solo nodo possono causare ritardi nell'ILM se quel nodo diventa non disponibile.

Passaggi

1. Seleziona **ILM** > **Gradi di storage**.
2. Definisci livelli di storage personalizzati:
   a. Per ogni livello di storage personalizzato che vuoi aggiungere, seleziona **Inserisci** per aggiungere una riga.
   b. Inserisci un'etichetta descrittiva.



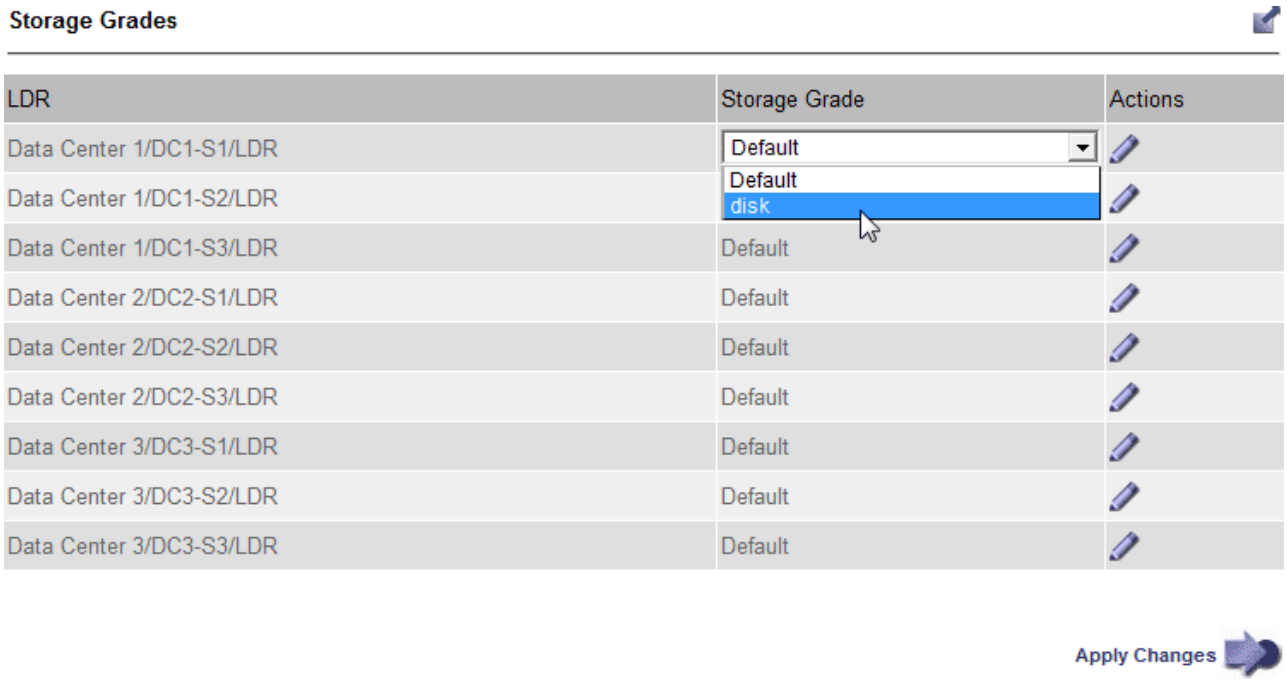
   c. Seleziona **Applica modifiche**.
   d. Facoltativamente, se devi modificare un'etichetta salvata, seleziona **Modifica** e seleziona **Applica modifiche**.

Non puoi eliminare i storage grades.

3. Assegna nuovi storage grade ai Storage Node:

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

   b. Seleziona il livello di storage appropriato dall'elenco.



Assegna un livello di storage a un determinato Storage Node una sola volta. Un Storage Node ripristinato dopo un errore mantiene il livello di storage assegnato in precedenza. Non cambiare questa assegnazione dopo l'attivazione della policy ILM. Se l'assegnazione viene cambiata, i dati vengono archiviati in base al nuovo livello di storage.

   a. Seleziona **Applica modifiche**.

Usa i pool di storage

Scopri i pool di storage in StorageGRID

Un pool di storage è un raggruppamento logico di Storage Nodes.

Quando installi StorageGRID, viene creato automaticamente un pool di storage per ogni sito. Puoi configurare pool di storage aggiuntivi in base alle tue esigenze di storage.

I nodi di storage possono essere configurati durante l'installazione per contenere dati degli oggetti e metadati ("nodo di storage combinato"), solo metadati degli oggetti o solo dati degli oggetti. I nodi di storage contenenti solo metadati non possono essere utilizzati nei pool di storage. Per ulteriori informazioni, consulta "Tipi di nodi di archiviazione".

I pool di storage hanno due attributi:

- **Livello di archiviazione**: Per i nodi di archiviazione, le prestazioni relative dello storage sottostante.
- **Sito**: Il data center in cui archivierai gli oggetti.

I pool di storage vengono utilizzati nelle regole ILM per determinare dove vengono archiviati i dati degli oggetti e il tipo di storage utilizzato. Quando configuri le regole ILM per la replica, selezioni uno o più pool di storage.

Linee guida per la configurazione del pool di storage in StorageGRID

Configura e utilizza i pool di storage per proteggerti dalla perdita di dati distribuendo i dati su più siti. Le copie replicate e le copie con codifica di cancellazione richiedono configurazioni diverse per i pool di storage.

Vedi "Esempi di abilitazione della protezione dalla perdita del sito tramite replica e codifica di cancellazione".

Linee guida per tutti i pool di storage

- Mantieni le configurazioni dei pool di storage il più semplici possibile. Non creare più pool di storage del necessario.
- Crea pool di storage con il maggior numero possibile di nodi. Ogni pool di storage dovrebbe contenere due o più nodi. Un pool di storage con un numero insufficiente di nodi può causare backlog di ILM se un nodo diventa non disponibile.
- Evita di creare o utilizzare pool di storage sovrapposti (che contengono uno o più degli stessi nodi). Se i pool di storage si sovrappongono, più di una copia dei dati degli oggetti potrebbe essere salvata sullo stesso nodo.
- In generale, non usare il pool di storage All Storage Nodes (StorageGRID 11.6 e versioni precedenti) o il sito All Sites. Questi elementi vengono aggiornati automaticamente per includere eventuali nuovi siti che aggiungi durante un'espansione, il che potrebbe non essere il comportamento che desideri.

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

- Per la protezione dalla perdita del sito tramite "replicazione", specifica uno o più pool di storage specifici del sito in "Istruzioni di posizionamento per ciascuna 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 ogni sito garantisce che le copie replicate degli oggetti vengano posizionate esattamente dove ti aspetti (ad esempio, una copia di ogni oggetto in ogni sito per la protezione dalla perdita del sito).

- Se aggiungi un sito in un'espansione, crea un nuovo pool di storage che contenga solo il nuovo sito. Quindi, "aggiornare le regole ILM" per controllare quali oggetti vengono archiviati 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 Storage Node), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Devi assicurarti che i pool di storage selezionati non contengano gli stessi Storage Node.

Linee guida per i pool di storage utilizzati per le copie con codifica di cancellazione

- Per la protezione dalla perdita di siti tramite "erasure coding", crea pool di storage composti da almeno tre siti. Se un pool di storage include solo due siti, non puoi usare quel pool di storage per la codifica di

cancellazione. Non sono disponibili schemi di codifica di cancellazione per un pool di storage con due siti.

- Il numero di Storage Nodes e siti contenuti nel pool di storage determina quali "schemi di codifica a cancellazione" sono disponibili.
- Se possibile, un pool di storage dovrebbe includere più del numero minimo di Storage Node richiesto dallo schema di erasure-coding che scegli. Ad esempio, se usi uno schema di erasure-coding 6+3, devi avere almeno nove Storage Node. Tuttavia, è consigliato avere almeno uno Storage Node aggiuntivo per sito.
- Distribuisci i nodi di archiviazione tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di codifica di cancellazione 6+3, configura un pool di storage che includa almeno tre nodi di archiviazione in tre siti.
- Se hai requisiti di throughput elevati, non è consigliato utilizzare un pool di storage che include più siti se la latenza di rete tra i siti è superiore a 100 ms. Man mano che la latenza aumenta, la velocità con cui StorageGRID può creare, posizionare e recuperare frammenti di oggetti diminuisce drasticamente a causa della riduzione del throughput di rete TCP.

  La diminuzione del throughput influisce sulle velocità massime raggiungibili di acquisizione e recupero degli oggetti (quando si seleziona Balanced o Strict come comportamento di acquisizione) o potrebbe causare arretrati nella coda ILM (quando si seleziona Dual commit come comportamento di acquisizione). Vedi "Comportamento di ingest delle regole ILM".

> Se la griglia include un solo sito, non puoi utilizzare il pool di storage All Storage Nodes (StorageGRID 11.6 e versioni precedenti) o il sito All Sites in un profilo di codifica di cancellazione. Questo comportamento impedisce che il profilo diventi non valido se aggiungi un secondo sito.

Protezione dalla perdita del sito con pool di storage in StorageGRID

Se la tua implementazione di StorageGRID include più di un sito, puoi utilizzare la replica e la codifica di cancellazione con pool di storage opportunamente configurati per abilitare la protezione dalla perdita di siti.

La replicazione e la codifica di cancellazione richiedono diverse configurazioni dei pool di storage:

- Per utilizzare la replica per la protezione dalla perdita di siti, usa i pool di storage specifici del sito che vengono creati automaticamente durante l'installazione di StorageGRID. Poi crea regole ILM con "istruzioni di posizionamento" che specificano più pool di storage, così che una copia di ogni oggetto venga posizionata in ogni sito.
- Per utilizzare la codifica di cancellazione per la protezione dalla perdita del sito, "crea pool di storage costituiti da più siti". Crea quindi regole ILM che utilizzano un pool di storage composto da più siti e qualsiasi schema di codifica di cancellazione disponibile.

> Quando configuri la tua distribuzione StorageGRID per la protezione dalla perdita del sito, devi anche tenere conto degli effetti di "opzioni di ingest" e "coerenza".

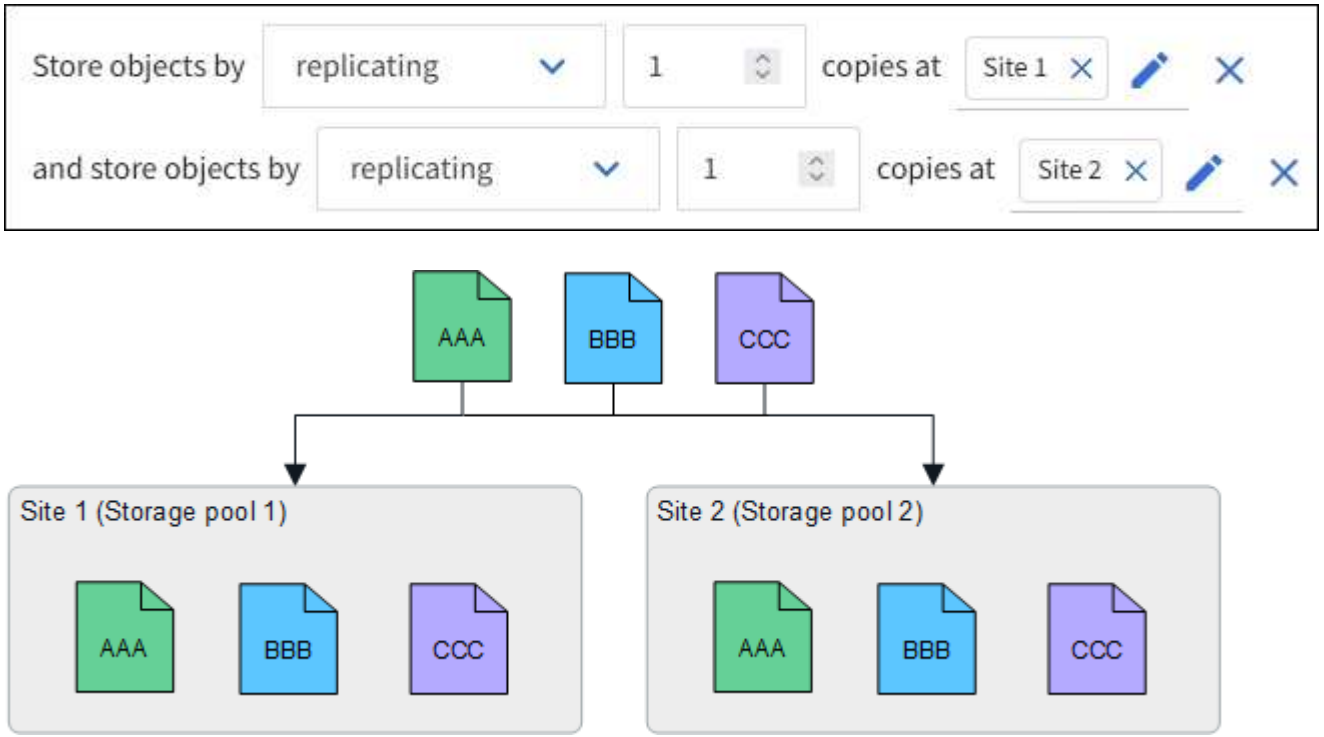
Esempio di replica

Per impostazione predefinita, viene creato un pool di storage per ogni sito durante l'installazione di StorageGRID. Avere pool di storage costituiti da un solo sito ti permette di configurare regole ILM che usano la replica per la protezione dalla perdita del sito. In questo esempio:

- Il pool di storage 1 contiene Site 1

- Il pool di storage 2 contiene Site 2
- La regola ILM contiene due posizionamenti:
  - Archivia gli oggetti replicando 1 copia nel Site 1
  - Archivia gli oggetti replicando 1 copia nel Sito 2

Posizionamenti delle regole ILM:



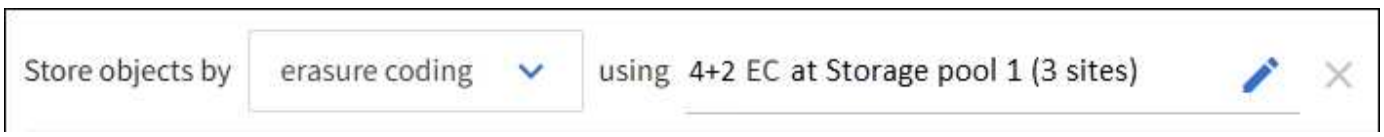
Se uno dei siti viene perso, le copie degli oggetti sono disponibili nell'altro sito.

Esempio di codifica di cancellazione

Disporre di pool di storage composti da più di un sito per pool di storage consente di configurare regole ILM che utilizzano la codifica di cancellazione per la protezione dalla perdita del sito. In questo esempio:

- Il pool di storage 1 contiene i siti da 1 a 3
- La regola ILM contiene un posizionamento: memorizza gli oggetti tramite codifica di cancellazione utilizzando uno schema EC 4+2 nello storage pool 1, che contiene tre siti

Posizionamenti delle regole ILM:



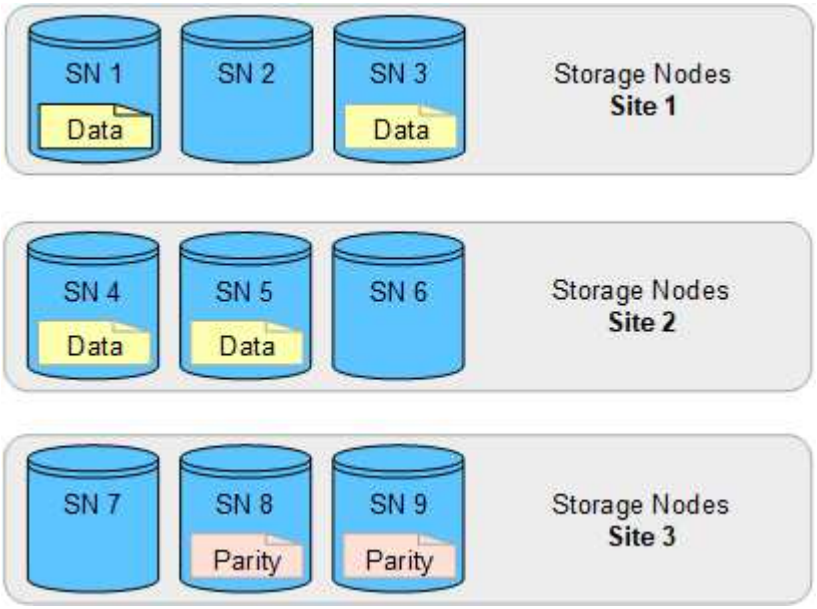
In questo esempio:

- 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.

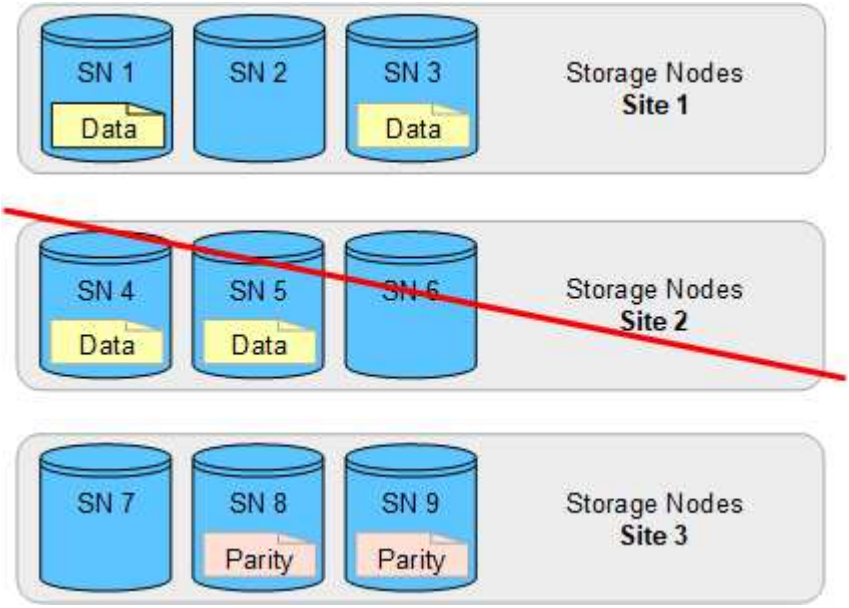
- Ciascuno dei sei frammenti è memorizzato su un nodo diverso in tre siti di data center per garantire la protezione dei dati in caso di guasti ai nodi o perdita di sito.

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

Regola ILM che utilizza lo schema di codifica a cancellazione 4+2:



Se un sito viene perso, i dati possono comunque essere recuperati:



Crea un pool di storage in StorageGRID

Crei pool di storage per determinare dove il sistema StorageGRID memorizza i dati degli oggetti e il tipo di storage utilizzato. Ogni pool di storage include uno o più siti e uno o più livelli di storage.

> Quando installi StorageGRID 12.0 su una nuova griglia, i pool di storage vengono creati automaticamente per ogni sito. Tuttavia, se inizialmente hai installato StorageGRID 11.6 o una versione precedente, i pool di storage non vengono creati automaticamente per ogni sito.

Se vuoi creare Cloud Storage Pools per archiviare i dati degli oggetti al di fuori del tuo sistema StorageGRID, consulta la "Informazioni sull'utilizzo dei Cloud Storage Pools".

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- Hai esaminato le linee guida per la creazione di pool di storage.

Informazioni su questa attività

I pool di storage determinano dove vengono memorizzati i dati degli oggetti. Il numero di pool di storage di cui hai bisogno dipende dal numero di siti nella tua grid e dai tipi di copie che vuoi: replicate o con erasure coding.

- Per la replica e la codifica di cancellazione a sito singolo, crea un pool di storage per ogni sito. Ad esempio, se desideri archiviare copie di oggetti replicati in tre siti, crea tre pool di storage.
- Per la codifica di cancellazione in tre o più siti, crea un pool di storage che includa una voce per ogni sito. Ad esempio, se vuoi codificare con cancellazione gli oggetti su tre siti, crea un solo pool di storage.

> Non includere il sito Tutti i siti in un pool di storage che verrà utilizzato in un profilo di codifica di cancellazione. Aggiungi invece una voce separata al pool di storage per ogni sito che memorizzerà dati codificati per la cancellazione. Vedi questo passaggio per un esempio.

- Se hai più di un grado di storage, non creare un pool di storage che includa diversi gradi di storage in un unico sito. Vedi "Linee guida per la creazione di pool di storage".

Passaggi

1. Seleziona **ILM** > **pool di storage**.

   La scheda Pool di storage elenca tutti i pool di storage definiti.

   > Per le nuove installazioni di StorageGRID 11.6 o versioni precedenti, il pool di storage All Storage Nodes viene aggiornato automaticamente ogni volta che aggiungi nuovi siti di data center. Non usare questo pool nelle regole ILM.

2. Per creare un nuovo pool di storage, seleziona **Crea**.
3. Inserisci un nome univoco per il pool di storage. Usa un nome che sia facile da identificare quando configuri i profili di erasure coding e le regole ILM.
4. Dal menu a discesa **Site**, seleziona un sito per questo pool di storage.

   Quando selezioni un sito, il numero di Storage Node nella tabella viene aggiornato automaticamente.

   In generale, non usare il sito All Sites in nessun pool di storage. Le regole ILM che utilizzano un pool di storage All Sites posizionano gli oggetti in qualsiasi sito disponibile, dandoti meno controllo sul posizionamento degli oggetti. Inoltre, un pool di storage All Sites utilizza immediatamente i Storage Nodes in un nuovo sito, il che potrebbe non essere il comportamento che ti aspetti.

5. Dall'elenco a discesa **Livello di archiviazione**, seleziona il tipo di archiviazione che verrà utilizzato se una

regola ILM utilizza questo pool di storage.

Il livello di storage, *include tutti i livelli di storage*, comprende tutti i Storage Node nel sito selezionato. Se hai creato livelli di storage aggiuntivi per i Storage Node nella tua grid, questi sono elencati nel menu a tendina.

6. Se vuoi usare il pool di storage in un profilo di codifica di cancellazione multisito, seleziona **Aggiungi altri nodi** per aggiungere una voce per ogni sito al pool di storage.

   Ricevi un avviso se aggiungi più di una voce con diversi livelli di archiviazione per un sito.

   Per rimuovere una voce, seleziona l'icona di eliminazione ✕.

7. Quando sei soddisfatto delle tue selezioni, seleziona **Salva**.

   Il nuovo pool di storage viene aggiunto all'elenco.

Visualizza i dettagli del pool di storage in StorageGRID

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

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Passaggi

1. Seleziona **ILM** > **pool di storage**.

   La tabella dei pool di storage include le seguenti informazioni per ciascun pool di storage che include Storage Nodes:

   - **Nome**: Il nome univoco visualizzato del pool di storage.
   - **Numero di nodi**: Il numero di nodi nel pool di storage.
   - **Utilizzo dello spazio di archiviazione**: la percentuale dello spazio totale utilizzabile che è stata utilizzata per i dati degli oggetti su questo nodo. Questo valore non include i metadati degli oggetti.
   - **Capacità totale**: la dimensione del pool di storage, che corrisponde alla quantità totale di spazio utilizzabile per i dati degli oggetti per tutti i nodi del pool di storage.
   - **Utilizzo ILM**: Come viene attualmente utilizzato il pool di storage. Un pool di storage potrebbe non essere utilizzato oppure potrebbe essere usato in una o più regole ILM, profili di erasure coding o entrambi.

2. Per visualizzare i dettagli di uno specifico pool di storage, seleziona il suo nome.

   Viene visualizzata la pagina dei dettagli del pool di storage.

3. Consulta la scheda **Nodi** per informazioni sui nodi di storage inclusi nel pool di storage.

   La tabella include le seguenti informazioni per ciascun nodo:

   - Nome nodo

- Nome sito
- grado di storage
- Utilizzo dello storage: la % dello spazio totale utilizzabile per i dati degli oggetti che è stata usata per lo Storage Node.

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

4. Visualizza la scheda **Utilizzo ILM** per vedere se il pool di storage è attualmente utilizzato in qualche regola ILM o profilo di erasure coding.
5. Facoltativamente, vai alla **pagina delle regole ILM** per scoprire e gestire le regole che utilizzano il pool di storage.

   Vedi la "Istruzioni per lavorare con le regole ILM".

Modifica un pool di storage in StorageGRID

Puoi modificare un pool di storage per cambiarne il nome o per aggiornare siti e livelli di storage.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- Hai esaminato il "linee guida per la creazione di pool di storage".
- Se prevedi di modificare un pool di storage utilizzato da una regola nella policy ILM attiva, hai considerato come le tue modifiche influenzeranno il posizionamento dei dati degli oggetti.

Informazioni su questa attività

Se aggiungi un nuovo sito o livello di storage a un pool di storage utilizzato nella policy ILM attiva, tieni presente che i nodi di storage nel nuovo sito o livello di storage non verranno utilizzati automaticamente. Per forzare StorageGRID a usare un nuovo sito o livello di storage, devi attivare una nuova policy ILM dopo aver salvato il pool di storage.

Passaggi

1. Seleziona **ILM** > **pool di storage**.
2. Seleziona la casella di controllo per il pool di storage che vuoi modificare.

   Non puoi modificare il pool di storage All Storage Nodes (StorageGRID 11.6 e versioni precedenti).

3. Seleziona **Modifica**.
4. Se necessario, cambia il nome del pool di storage.
5. Se necessario, seleziona altri siti e livelli di storage.

   Non puoi modificare il sito o il livello di storage se il pool di storage viene utilizzato in un profilo di erasure-coding e la modifica renderebbe lo schema di erasure-coding non valido. Ad esempio, se un pool di storage utilizzato in un profilo di erasure-coding attualmente include un livello di storage con un solo sito, non puoi utilizzare un livello di storage con due siti perché la modifica renderebbe lo schema di erasure-

coding non valido.

> Aggiungere o rimuovere siti da un pool di storage esistente non sposterà alcun dato già codificato con cancellazione. Se vuoi spostare i dati esistenti dal sito, devi creare un nuovo pool di storage e un nuovo profilo EC per ricodificare i dati.

6. Seleziona **Salva**.

Dopo aver finito

Se hai aggiunto un nuovo sito o un nuovo livello di storage a un pool di storage utilizzato nella policy ILM attiva, attiva una nuova policy ILM per forzare StorageGRID a usare il nuovo sito o il nuovo livello di storage. Ad esempio, clona la tua policy ILM esistente e poi attiva il clone. Vedi "Lavora con le regole ILM e le policy ILM".

Rimuovere un pool di storage in StorageGRID

Puoi rimuovere un pool di storage che non viene utilizzato.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Tu hai il "autorizzazioni di accesso richieste".

Passaggi

1. Seleziona **ILM** > **pool di storage**.
2. Guarda la colonna "Utilizzo ILM" nella tabella per capire se puoi rimuovere il pool di storage.

   Non puoi rimuovere un pool di storage se viene utilizzato in una regola ILM o in un profilo di erasure coding. Se necessario, seleziona **storage pool name** > **ILM usage** per vedere dove viene utilizzato il pool di storage.

3. Se il pool di storage che vuoi rimuovere non è in uso, seleziona la casella di controllo.
4. Seleziona **Rimuovi**.
5. Seleziona **OK**.

Usa i Cloud Storage Pool

Scopri i Cloud Storage Pool in StorageGRID

Un pool di cloud storage ti permette di usare ILM per spostare i dati degli oggetti al di fuori del sistema StorageGRID. Ad esempio, potresti voler spostare oggetti a cui accedi raramente verso cloud storage a costo inferiore, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive in Microsoft Azure Blob storage. Oppure, potresti voler mantenere un backup cloud degli oggetti StorageGRID per migliorare il disaster recovery.

Dal punto di vista dell'ILM, un Cloud Storage Pool è simile a un pool di storage. Per archiviare oggetti in entrambe le posizioni, selezioni il pool quando crei le istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di storage sono costituiti da Storage Nodes all'interno del sistema StorageGRID, un Cloud Storage Pool è costituito da un bucket esterno (S3) o da un container (Azure Blob storage).

La tabella confronta i pool di storage con i Cloud Storage Pools e mostra le high-level somiglianze e differenze.

	Pool di storage	Pool di storage cloud
Come lo crei?	Utilizzando l'opzione **ILM** > **Storage pools** in Grid Manager.	Utilizzando l'opzione **ILM** > **Storage pools** > **Cloud Storage Pools** in Grid Manager. Devi configurare il bucket o il container esterno prima di poter creare il Cloud Storage Pool.
Quanti pool puoi creare?	Illimitato.	Fino a 10.
Dove sono memorizzati gli oggetti?	Su uno o più nodi di storage all'interno di StorageGRID.	In un bucket Amazon S3, in un container Azure Blob storage o in Google Cloud esterno al sistema StorageGRID. Se il pool di cloud storage è un bucket Amazon S3: • Puoi configurare facoltativamente un ciclo di vita del bucket per trasferire gli oggetti in storage a basso costo e a lungo termine, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema storage esterno deve supportare la classe di storage Glacier e l'API S3 RestoreObject. • Puoi creare Cloud Storage Pools da usare con AWS Commercial Cloud Services (C2S), che supportano la AWS Secret Region. Se il Cloud Storage Pool è un container Azure Blob storage, StorageGRID sposta l'oggetto al livello Archive. **Nota:** In generale, non configurare la gestione del ciclo di vita di Azure Blob storage per il container utilizzato per un Cloud Storage Pool. RestoreObject operazioni sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nelle policy ILM attive.	Una regola ILM nelle policy ILM attive.
Quale metodo di protezione dei dati usi?	Replica o erasure coding.	Replicazione.

	Pool di storage	Pool di storage cloud
Quante copie di ciascun oggetto sono consentite?	Molteplici.	Una copia nel Cloud Storage Pool e, facoltativamente, una o più copie in StorageGRID. **Nota:** Non puoi archiviare un oggetto in più di un Cloud Storage Pool contemporaneamente.
Quali sono i vantaggi?	Gli oggetti sono accessibili rapidamente in qualsiasi momento.	Storage a basso costo. **Nota**: I dati di FabricPool non possono essere suddivisi in livelli nei Cloud Storage Pools.

Ciclo di vita di un oggetto pool di storage cloud in StorageGRID

Prima di implementare i Cloud Storage Pool, rivedi il ciclo di vita degli oggetti che sono archiviati in ciascun tipo di Cloud Storage Pool.

S3: Ciclo di vita di un oggetto Cloud Storage Pool

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un S3 Cloud Storage Pool.

> "Glacier" si riferisce sia alla classe di storage Glacier che alla classe di storage Glacier Deep Archive, con un'eccezione: la classe di storage Glacier Deep Archive non supporta il tier di ripristino Expedited. Sono supportati solo i recuperi Bulk o Standard.

> La piattaforma Google Cloud (GCP) supporta il recupero di oggetti da storage a lungo termine senza richiedere un'operazione POST Restore.

1. **Oggetto memorizzato in StorageGRID**

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

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

     > Se vuoi trasferire gli oggetti, devi creare una configurazione del ciclo di vita per il bucket S3 esterno e devi usare una soluzione storage che implementa la classe di storage Glacier e supporta 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 migrato allo storage Glacier, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel pool di storage cloud S3. La richiesta specifica per quanti giorni la copia deve essere disponibile nel pool di storage cloud e il livello di accesso ai dati da utilizzare per l'operazione di ripristino (Expedited, Standard o Bulk). Quando viene raggiunta la data di scadenza della copia recuperabile, la copia viene automaticamente riportata a 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 inviando una richiesta RestoreObject. Invece, la copia locale può essere recuperata direttamente tramite una richiesta GetObject.

5. **Oggetto recuperato**

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

Azure: Ciclo di vita di un oggetto pool di storage cloud

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un pool di storage cloud di Azure.

1. **Oggetto memorizzato in StorageGRID**

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

2. **Oggetto spostato nel pool di storage cloud di Azure**

   Quando l'oggetto viene abbinato a una regola ILM che utilizza un pool di storage cloud Azure come posizione di collocazione, StorageGRID sposta l'oggetto nel container Azure Blob storage esterno specificato dal Cloud Storage Pool.

3. **Oggetto trasferito al livello Archivio (stato non recuperabile)**

   Subito dopo aver spostato l'oggetto nel pool di storage cloud di Azure, StorageGRID passa automaticamente l'oggetto al livello Archive di Azure Blob storage.

4. **Oggetto ripristinato dal livello Archive**

   Se un oggetto è stato spostato nel livello Archivio, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel pool di storage Azure Cloud Storage Pool.

   Quando StorageGRID riceve la RestoreObject, sposta temporaneamente l'oggetto nel livello Cool di Azure Blob storage. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID riporta l'oggetto al livello Archive.

   > Se una o più copie dell'oggetto esistono anche sui nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso Archive inviando una richiesta RestoreObject. Invece, puoi recuperare direttamente la copia locale usando una richiesta GetObject.

5. **Oggetto recuperato**

   Una volta che un oggetto è stato ripristinato nel pool di storage cloud di Azure, l'applicazione client può inviare una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

"${post_edited_translations.segment}"

Casi d'uso del Cloud Storage Pool in StorageGRID

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

Esegui il backup dei dati di StorageGRID in una posizione esterna

Puoi usare un Cloud Storage Pool per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, puoi utilizzare i dati degli oggetti nel Cloud Storage Pool per soddisfare le richieste dei client. Tuttavia, potresti dover inviare una richiesta S3 RestoreObject per accedere alla copia di backup dell'oggetto nel Cloud Storage Pool.

I dati degli oggetti in un Cloud Storage Pool possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un errore del volume di storage o dello Storage Node. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sullo Storage Node ripristinato.

Per implementare una soluzione di backup:

1. Crea un singolo Cloud Storage Pool.
2. Configura una regola ILM che memorizza simultaneamente copie degli oggetti sui Storage Node (come copie replicate o con codifica di cancellazione) e una singola copia dell'oggetto nel Cloud Storage Pool.
3. Aggiungi la regola alla tua policy ILM. Poi, simula e attiva la policy.

Sposta i dati di livello da StorageGRID a una posizione esterna

Puoi usare un Cloud Storage Pool per memorizzare oggetti al di fuori del sistema StorageGRID. Ad esempio, supponi di avere un gran numero di oggetti che devi conservare, ma prevedi di accedervi raramente, se mai. Puoi usare un Cloud Storage Pool per spostare gli oggetti in uno storage a costo inferiore e liberare spazio in StorageGRID.

Per implementare una soluzione di tiering:

1. Crea un singolo Cloud Storage Pool.
2. Configura una regola ILM che sposta gli oggetti usati raramente dai Storage Node al Cloud Storage Pool.
3. Aggiungi la regola alla tua policy ILM. Poi, simula e attiva la policy.

Gestisci più endpoint cloud

Puoi configurare più endpoint di Cloud Storage Pool se vuoi eseguire il tiering o il backup dei dati degli oggetti su più cloud. I filtri nelle tue regole ILM ti permettono di specificare quali oggetti vengono archiviati in ciascun Cloud Storage Pool. Ad esempio, potresti voler archiviare gli oggetti di alcuni tenant o bucket in Amazon S3 Glacier e gli oggetti di altri tenant o bucket in Azure Blob storage. Oppure, potresti voler spostare i dati tra

Amazon S3 Glacier e Azure Blob storage.

> Quando usi più endpoint di Cloud Storage Pool, tieni presente che un oggetto può essere archiviato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 Cloud Storage Pools.
2. Configura le regole ILM per archiviare i dati degli oggetti appropriati al momento opportuno in ciascun Cloud Storage Pool. Ad esempio, archivia gli oggetti del bucket A nel Cloud Storage Pool A e gli oggetti del bucket B nel Cloud Storage Pool B. Oppure, archivia gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e poi spostali nel Cloud Storage Pool B.
3. Aggiungi le regole alla tua policy ILM. Poi, simula e attiva la policy.

Requisiti e limiti del pool di storage cloud in StorageGRID

Se hai intenzione di usare un Cloud Storage Pool per spostare oggetti fuori dal sistema StorageGRID, devi esaminare le considerazioni per la configurazione e l'utilizzo dei Cloud Storage Pool.

Considerazioni generali

- In generale, l'archiviazione cloud di tipo archivio, come Amazon S3 Glacier o Azure Blob storage, è un posto economico dove memorizzare dati a oggetti. Tuttavia, i costi per recuperare i dati dall'archiviazione cloud di tipo archivio sono relativamente alti. Per ottenere il costo complessivo più basso, devi considerare quando e quanto spesso accederai agli oggetti nel Cloud Storage Pool. Si consiglia di usare un Cloud Storage Pool solo per contenuti a cui pensi di accedere raramente.
- L'uso di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva per recuperare un oggetto dal target del Cloud Storage Pool.
- Gli oggetti con S3 Object Lock abilitato non possono essere inseriti nei Cloud Storage Pools.
- Le seguenti combinazioni di piattaforma, autenticazione e protocollo con S3 Object lock non sono supportate per i Cloud Storage Pools:
  - **Piattaforme**: Google Cloud Platform e Azure
  - **Tipi di autenticazione**: Accesso anonimo
  - **Protocollo**: HTTP

Considerazioni sulle porte utilizzate per i Cloud Storage Pools

Per garantire che le regole ILM possano spostare oggetti da e verso il Cloud Storage Pool specificato, devi configurare la rete o le reti che contengono i Storage Node del sistema. Devi assicurarti che le seguenti porte possano comunicare con il Cloud Storage Pool.

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

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

Puoi specificare una porta diversa quando crei o modifichi un Cloud Storage Pool.

Se usi un proxy server non trasparente, devi anche "configurare un proxy storage" consentire l'invio di messaggi a endpoint esterni, come un endpoint su internet.

Considerazioni sui costi

L'accesso allo storage nel cloud tramite un Cloud Storage Pool richiede la connettività di rete al cloud. Devi considerare il costo dell'infrastruttura di rete che userai per accedere al cloud e predisporla in modo appropriato, in base alla quantità di dati che prevedi di spostare tra StorageGRID e il cloud usando il Cloud Storage Pool.

Quando StorageGRID si connette all'endpoint esterno del Cloud Storage Pool, invia diverse richieste per monitorare la connettività e assicurarsi di poter eseguire le operazioni richieste. Sebbene queste richieste comportino dei costi aggiuntivi, il costo del monitoraggio di un Cloud Storage Pool dovrebbe rappresentare solo una piccola frazione del costo complessivo dell'archiviazione degli oggetti in S3 o Azure.

Potrebbero essere sostenuti costi più significativi se devi spostare oggetti da un endpoint esterno del Cloud Storage Pool a StorageGRID. Gli oggetti potrebbero essere spostati nuovamente in StorageGRID in uno di questi casi:

- L'unica copia dell'oggetto si trova in un Cloud Storage Pool e decidi di archiviare l'oggetto in StorageGRID invece. In questo caso, riconfiguri le tue regole e policy ILM. Quando avviene la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal Cloud Storage Pool. StorageGRID crea quindi localmente il numero specificato di copie replicate o con codifica di cancellazione. Dopo che l'oggetto viene spostato di nuovo in StorageGRID, la copia nel Cloud Storage Pool viene eliminata.
- Gli oggetti vengono persi a causa di un errore del nodo di archiviazione. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di archiviazione ripristinato.

> Quando gli oggetti vengono spostati di nuovo su StorageGRID da un Cloud Storage Pool, StorageGRID invia più richieste all'endpoint del Cloud Storage Pool per ciascun oggetto. Prima di spostare un numero elevato di oggetti, contatta il supporto tecnico per ottenere aiuto nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket del Cloud Storage Pool

Le policy per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono concedere a StorageGRID l'autorizzazione a spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto da Glacier storage quando necessario e altro ancora. Idealmente, StorageGRID dovrebbe avere accesso con controllo completo al bucket (`s3:*`; tuttavia, se ciò non è possibile, la policy del 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

Il movimento degli oggetti tra StorageGRID e il bucket S3 esterno specificato nel Cloud Storage Pool è controllato dalle regole ILM e dalle policy ILM attive in StorageGRID. Al contrario, il trasferimento degli oggetti dal bucket S3 esterno specificato nel Cloud Storage Pool ad Amazon S3 Glacier o S3 Glacier Deep Archive (o a una soluzione storage che implementa la classe di storage Glacier) è controllato dalla configurazione del ciclo di vita di quel bucket.

Se vuoi trasferire oggetti dal Cloud Storage Pool, devi creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e devi usare una soluzione storage che implementa la classe di storage Glacier e supporta l'API S3 RestoreObject.

Ad esempio, supponi di voler fare in modo che tutti gli oggetti spostati da StorageGRID al Cloud Storage Pool vengano trasferiti immediatamente in Amazon S3 Glacier storage. Dovresti creare una configurazione del ciclo di vita sul bucket S3 esterno che specifichi una sola azione (**Transition**) 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 sposterebbe tutti gli oggetti bucket su Amazon S3 Glacier il giorno stesso della loro creazione (ovvero, il giorno in cui vengono spostati da StorageGRID al Cloud Storage Pool).

> Quando configuri il ciclo di vita del bucket esterno, non usare mai le azioni **Scadenza** per definire quando gli oggetti scadono. Le azioni di scadenza fanno sì che il sistema storage esterno elimini gli oggetti scaduti. Se in seguito provi ad accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non verrà trovato.

Se vuoi migrare gli oggetti nel Cloud Storage Pool verso S3 Glacier Deep Archive (invece che verso Amazon S3 Glacier), specifica `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tieni però presente che non puoi usare il livello `Expedited` per ripristinare oggetti da S3 Glacier Deep Archive.

Azure: considerazioni per il tier Access

Quando configuri un account di archiviazione Azure, puoi impostare il livello di accesso predefinito su Hot o Cool. Quando crei un account di archiviazione da usare con un Cloud Storage Pool, dovresti usare il livello Hot come livello predefinito. Anche se StorageGRID imposta immediatamente il livello su Archive quando sposta gli oggetti nel Cloud Storage Pool, usare l'impostazione predefinita Hot garantisce che non ti venga addebitato un costo di eliminazione anticipata per gli oggetti rimossi dal livello Cool prima dei 30 giorni minimi.

Azure: la gestione del ciclo di vita non è supportata

Non usare la gestione del ciclo di vita di Azure Blob storage 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

"${post_edited_translations.segment}"

Pool di storage cloud e replica CloudMirror in StorageGRID

Quando inizi a utilizzare Cloud Storage Pools, potrebbe essere utile comprendere le somiglianze e le differenze tra Cloud Storage Pools e il servizio di replica CloudMirror di StorageGRID.

	Pool di storage cloud	servizio di replica CloudMirror
Qual è lo scopo principale?	Funge da destinazione di archiviazione. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure una copia aggiuntiva. Cioè, invece di conservare due copie in sede, puoi conservarne una in StorageGRID e inviarne una al Cloud Storage Pool.	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 si configura?	Definito nello stesso modo dei pool di storage, usando il Grid Manager o la Grid Management API. Puoi selezionarlo come destinazione di posizionamento in una regola ILM. Mentre un pool di storage è costituito da un gruppo di Storage Node, un Cloud Storage Pool viene definito usando un endpoint S3 o Azure remoto (indirizzo IP, credenziali e così via).	Un utente tenant "configura la replica CloudMirror" definisce un endpoint CloudMirror (indirizzo IP, credenziali e così via) usando il Tenant Manager o l'API S3. Dopo che l'endpoint CloudMirror è stato configurato, qualsiasi bucket di proprietà di quell'account tenant può essere configurato per puntare all'endpoint CloudMirror.
Chi è responsabile della configurazione?	Di solito, un amministratore della grid	Di solito, un tenant
${post_edited_translations.segment}	• Qualsiasi infrastruttura S3 compatibile (inclusi Amazon S3) • Livello Archive di Azure Blob • ${post_edited_translations.segment}	• Qualsiasi infrastruttura S3 compatibile (inclusi Amazon S3) • ${post_edited_translations.segment}

	Pool di storage cloud	servizio di replica CloudMirror
Cosa fa sì che gli oggetti vengano spostati verso la destinazione?	Una o più regole ILM nelle policy ILM attive. Le regole ILM definiscono quali oggetti StorageGRID sposta nel Cloud Storage Pool e quando gli oggetti vengono spostati.	L'azione di inserire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti già presenti nel bucket di origine prima che il bucket fosse configurato con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come recuperi gli oggetti?	Le applicazioni devono inviare richieste a StorageGRID per recuperare gli oggetti che sono stati spostati in un Cloud Storage Pool. Se l'unica copia di un oggetto è stata trasferita nell'archivio, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia replicata nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto effettuando richieste sia a StorageGRID che alla destinazione S3. Ad esempio, supponi di usare la replica CloudMirror per replicare oggetti verso un'organizzazione partner. Il partner può usare le proprie applicazioni per leggere o aggiornare oggetti direttamente dalla destinazione S3. Non è necessario usare StorageGRID.
Puoi leggere direttamente dalla destinazione?	No. Gli oggetti spostati in un Cloud Storage Pool sono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero dal Cloud Storage Pool).	Sì, perché la copia speculare è una copia indipendente.
Cosa succede se un oggetto viene eliminato dalla sorgente?	L'oggetto viene inoltre eliminato dal Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto eliminato non esiste più nel bucket StorageGRID, ma continua a esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.
Come accedi agli oggetti dopo un disastro (StorageGRID non operativo)?	I nodi StorageGRID non funzionanti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie presenti nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, quindi puoi accedervi direttamente prima che i nodi StorageGRID vengano ripristinati.

Crea un pool di storage cloud in StorageGRID

Un cloud storage pool specifica un singolo bucket Amazon S3 esterno o un altro cloud provider compatibile con S3 oppure un container Azure Blob storage.

Quando crei un Cloud Storage Pool, specifichi il nome e la posizione del bucket o container esterno che StorageGRID userà per archiviare gli oggetti, il tipo di cloud provider (Amazon S3/GCP o Azure Blob storage)

e le informazioni di cui StorageGRID ha bisogno per accedere al bucket o container esterno.

StorageGRID convalida il Cloud Storage Pool non appena lo salvi, quindi devi assicurarti che il bucket o container specificato nel Cloud Storage Pool esista e sia raggiungibile.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Tu hai il "autorizzazioni di accesso richieste".
- Hai esaminato il "Considerazioni sui Cloud Storage Pool".
- Il bucket o container a cui fa riferimento il Cloud Storage Pool esiste già e hai il informazioni sull'endpoint del servizio.
- Per accedere al bucket o container, hai l'informazioni sull'account per il tipo di autenticazione che sceglierai.

Passaggi

1. Seleziona **ILM** > **Storage pools** > **Cloud Storage Pools**.
2. Seleziona **Crea**, quindi inserisci le seguenti informazioni:

Campo	Descrizione
Nome del cloud storage pool	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Usa un nome che sia facile da identificare quando configuri le regole ILM.
Tipo di provider	Quale cloud provider utilizzerai per questo Cloud Storage Pool? • **Amazon S3/GCP**: Seleziona questa opzione per un Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o un altro provider compatibile con S3. • **Azure Blob Storage**
Bucket o container	Il nome del bucket S3 esterno o container Azure. Non puoi modificare questo valore dopo che il Cloud Storage Pool è stato salvato.

3. In base al tipo di provider selezionato, inserisci le informazioni sull'endpoint del servizio.

Amazon S3/GCP

a. Per il protocollo, seleziona HTTPS o HTTP.

> Non usare connessioni HTTP per dati sensibili.

b. Inserisci il nome host. Esempio:

`s3-aws-region.amazonaws.com`

c. Seleziona lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tenta di rilevare automaticamente quale stile di URL utilizzare, in base alle informazioni fornite. Ad esempio, se specifichi un indirizzo IP, StorageGRID utilizzerà un URL in stile percorso. Seleziona questa opzione solo se non sai quale stile specifico utilizzare.
Stile virtual-hosted	Utilizza un URL in stile virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del domain name. Esempio: `https://bucket-name.s3.company.com/key-name`
Stile path	Utilizza un URL in formato percorso per accedere al bucket. Gli URL in formato percorso includono il nome del bucket alla fine. Esempio: `https://s3.company.com/bucket-name/key-name` **Nota:** L'opzione URL in formato percorso non è consigliata e verrà deprecata in una versione futura di StorageGRID.

d. Facoltativamente, inserisci il numero di porta oppure usa la porta predefinita: 443 per HTTPS o 80 per HTTP.

Azure Blob Storage

a. Utilizzando uno dei seguenti formati, inserisci l'URI dell'endpoint del servizio.

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

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

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

4. Seleziona **Continua**. Quindi seleziona il tipo di autenticazione e inserisci le informazioni richieste per l'endpoint del Cloud Storage Pool:

Chiave di accesso

Per Amazon S3/GCP o altri cloud provider compatibili con S3

a. **ID chiave di accesso**: Inserisci l'ID della chiave di accesso per l'account che possiede il bucket esterno.
b. **Chiave di accesso segreta**: Inserisci la chiave di accesso segreta.

IAM Roles Anywhere

Per il servizio AWS IAM Roles Anywhere

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

a. **Regione di AWS IAM Roles Anywhere**: Seleziona la regione per il pool di storage cloud. Ad esempio, `us-east-1`.
b. **URN dell'ancora di fiducia**: Inserisci l'URN dell'ancora di fiducia che convalida le richieste di credenziali STS a breve termine. Può essere una CA root o intermedia.
c. **URN del profilo**: Inserisci l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia considerato attendibile.
d. **URN del ruolo**: Inserisci l'URN del ruolo IAM che può essere assunto da chiunque sia considerato affidabile.
e. **Durata della sessione**: Inserisci la durata delle credenziali di sicurezza temporanee e della sessione del ruolo. Inserisci almeno 15 minuti e non più di 12 ore.
f. **Certificato CA del server** (facoltativo): uno o più certificati CA attendibili, in formato PEM, per verificare il server IAM Roles Anywhere. Se omesso, il server non viene verificato.
g. **Certificato dell'entità finale**: la chiave pubblica, in formato PEM, del certificato X509 firmato dall'ancora di fiducia. 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 delle credenziali temporanee**: Inserisci l'URL completo che StorageGRID userà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati al tuo account C2S.
b. **Certificato CA del server**: Seleziona **Sfoglia** e carica il certificato CA che StorageGRID utilizzerà per verificare il server CAP. Il certificato deve essere codificato in formato PEM ed essere rilasciato da un'autorità di certificazione (CA) governativa appropriata.
c. **Certificato client**: Seleziona **Sfoglia** e carica il certificato che StorageGRID utilizzerà per identificarsi al server CAP. Il certificato client deve essere codificato in formato PEM, rilasciato da un'autorità di certificazione (CA) governativa appropriata e deve consentire l'accesso al tuo account C2S.
d. **Chiave privata del client**: Seleziona **Sfoglia** e carica la chiave privata codificata in formato PEM per il certificato client.
e. Se la chiave privata del client è crittografata, inserisci la passphrase per decrittare la chiave privata del client. Altrimenti, lascia il campo **Passphrase della chiave privata del client** vuoto.

Se il certificato client deve essere crittografato, usa il formato tradizionale per la crittografia. Il formato crittografato PKCS #8 non è supportato.

Azure Blob Storage

Solo per Azure Blob Storage, solo Chiave condivisa

a. **Nome account**: Inserisci il nome dell'account di storage che possiede il container esterno
b. **Chiave account**: Inserisci la chiave segreta per l'account di storage

Puoi usare il portale di Azure per trovare questi valori.

Anonimo

Non sono richieste ulteriori informazioni.

5. Seleziona **Continua**. Quindi scegli il tipo di verifica del server che desideri utilizzare:

Opzione	Descrizione
Usa i certificati CA root in Storage Node OS	Usa i certificati Grid CA installati sul sistema operativo per proteggere le connessioni.
Usa un certificato CA personalizzato	Utilizza un certificato CA personalizzato. Seleziona **Sfoglia** e carica il certificato codificato in formato PEM.
Non verificare il certificato	Selezionando questa opzione, le connessioni TLS al pool di storage cloud non sono sicure.

6. Seleziona **Salva**.

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

   - Verifica che il bucket o container e l'endpoint del servizio esistano e che siano raggiungibili utilizzando le credenziali che hai specificato.
   - Scrive un file di marcatura nel bucket o container per identificarlo come Cloud Storage Pool. Non rimuovere mai questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

     Se la convalida del pool di storage cloud non riesce, ricevi un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, potrebbe essere segnalato un errore se c'è un problema con il certificato o se il bucket o container che hai specificato non esiste già.

7. Se si verifica un errore, consulta la "Istruzioni per la risoluzione dei problemi relativi ai Cloud Storage Pools" e risolvi eventuali problemi, poi prova a salvare di nuovo il Cloud Storage Pool.

Visualizza i dettagli del pool di storage cloud in StorageGRID

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

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Passaggi

1. Seleziona **ILM** > **Storage pools** > **Cloud Storage Pools**.

   La tabella Cloud Storage Pools include le seguenti informazioni per ciascun Cloud Storage Pool che include Storage Nodes:

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

2. Per visualizzare i dettagli di uno specifico cloud storage pool, seleziona il suo nome.

   Viene visualizzata la pagina dei dettagli del pool.

3. Consulta la scheda **Autenticazione** per scoprire il tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Consulta la scheda **Verifica server** per informazioni dettagliate sulla verifica, modificare la verifica, scaricare un nuovo certificato o copiare il PEM del certificato.
5. Consulta la scheda **Utilizzo ILM** per verificare se il Cloud Storage Pool viene attualmente utilizzato in qualche regola ILM o profilo di erasure-coding.
6. Facoltativamente, vai alla **pagina delle regole ILM** per "scopri e gestisci qualsiasi regola" che usano il Cloud Storage Pool.

Modifica un pool di storage cloud in StorageGRID

Puoi modificare un pool di storage cloud per cambiarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non puoi cambiare il bucket S3 o il container Azure per un pool di storage cloud.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- Hai esaminato il "Considerazioni sui Cloud Storage Pool".

Passaggi

1. Seleziona **ILM** > **Storage pools** > **Cloud Storage Pools**.

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

2. Seleziona la casella di controllo corrispondente al Cloud Storage Pool che vuoi modificare, poi seleziona **Azioni** > **Modifica**.

In alternativa, seleziona il nome del Cloud Storage Pool, quindi seleziona **Modifica**.

3. Se necessario, modifica il nome del Cloud Storage Pool, l'endpoint del servizio, le credenziali per l'autenticazione o il metodo di verifica del certificato.

   > Non puoi cambiare il tipo di provider, il bucket S3 o il container Azure per un pool di storage cloud.

   Se in precedenza hai caricato un certificato server o client, puoi espandere la sezione **Dettagli certificato** per visualizzare il certificato attualmente in uso.

4. Seleziona **Salva**.

   Quando salvi un Cloud Storage Pool, StorageGRID verifica che il bucket o container e l'endpoint del servizio esistano e che siano raggiungibili utilizzando le credenziali che hai specificato.

   Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore. Ad esempio, potrebbe essere segnalato un errore in caso di errore relativo al certificato.

   Consulta le istruzioni per "Risoluzione dei problemi relativi ai Cloud Storage Pools", risolvi il problema e poi prova a salvare nuovamente il Cloud Storage Pool.

Rimuovere un Cloud Storage Pool in StorageGRID

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

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Tu hai il "autorizzazioni di accesso richieste".

Se necessario, usa ILM per spostare i dati degli oggetti

Se il Cloud Storage Pool che vuoi rimuovere contiene dati oggetto, devi usare ILM per spostare i dati in una posizione diversa. Ad esempio, puoi spostare i dati nei Storage Node della tua grid o in un altro Cloud Storage Pool.

Passaggi

1. Seleziona **ILM** > **Storage pools** > **Cloud Storage Pools**.
2. Consulta la colonna Utilizzo ILM nella tabella per determinare se puoi rimuovere il Cloud Storage Pool.

   Non puoi rimuovere un pool di storage cloud se viene utilizzato in una regola ILM o in un profilo di erasure coding.

3. Se stai utilizzando il Cloud Storage Pool, seleziona * *cloud storage pool name** > **ILM usage**.
4. "Clona ogni regola ILM"che attualmente inserisce gli oggetti nel Cloud Storage Pool che vuoi rimuovere.
5. Determina dove vuoi spostare gli oggetti esistenti gestiti da ciascuna regola che hai clonato.

   Puoi utilizzare uno o più pool di storage oppure un Cloud Storage Pool diverso.

6. Modifica ciascuna delle regole che hai clonato.

Per il passaggio 2 della procedura guidata Crea regola ILM, seleziona la nuova posizione dal campo **copies at**.

7. "Crea una nuova policy ILM" e sostituisci ciascuna delle vecchie regole con una regola clonata.
8. Attiva la nuova policy.
9. Attendi che ILM rimuova gli oggetti dal Cloud Storage Pool e li sposti nella nuova posizione.

Elimina il pool di storage cloud

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

Prima di iniziare

- Hai rimosso tutte le regole ILM che potrebbero aver utilizzato il pool.
- Hai confermato che il bucket S3 o il container Azure non contiene alcun oggetto.

  Si verifica un errore se provi a rimuovere un pool di storage cloud se contiene oggetti. Vedi "Risolvi i problemi dei pool di storage cloud".

> Quando crei un Cloud Storage Pool, StorageGRID scrive un file di marcatura nel bucket o container per identificarlo come Cloud Storage Pool. Non rimuovere questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

Passaggi

1. Seleziona **ILM** > **Storage pools** > **Cloud Storage Pools**.
2. Se nella colonna "Utilizzo ILM" viene indicato che il Cloud Storage Pool non è in uso, seleziona la casella di controllo.
3. Seleziona **Azioni** > **Rimuovi**.
4. Seleziona **OK**.

Risoluzione dei problemi dei pool di storage cloud in StorageGRID

Segui questi passaggi per la risoluzione dei problemi per risolvere gli errori che potresti incontrare durante la creazione, la modifica o l'eliminazione di un Cloud Storage Pool.

${post_edited_translations.segment}

StorageGRID esegue un semplice controllo di integrità su ogni Cloud Storage Pool leggendo l'oggetto noto `x-ntap-sgws-cloud-pool-uuid` per assicurarsi che il Cloud Storage Pool sia accessibile e funzioni correttamente. Quando StorageGRID rileva un errore sull'endpoint, esegue un controllo di integrità ogni minuto da ciascun Storage Node. Quando l'errore viene risolto, i controlli di integrità si interrompono. Se un controllo di integrità rileva un problema, viene mostrato un messaggio nella colonna Last error della tabella Cloud Storage Pools nella pagina Storage pools.

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

Inoltre, viene attivato un avviso di **Errore di connettività del Cloud Storage Pool** se il controllo di integrità rileva che si sono verificati uno o più nuovi errori del Cloud Storage Pool negli ultimi 5 minuti. Se ricevi una notifica email per questo avviso, vai alla pagina Storage pools (seleziona **ILM** > **Storage pools**), esamina i

messaggi di errore nella colonna Last error e fai riferimento alle linee guida per la risoluzione dei problemi riportate di seguito.

Verifica se l'errore è stato risolto

Dopo aver risolto eventuali problemi sottostanti, puoi verificare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, seleziona l'endpoint e seleziona **Cancella errore**. Un messaggio di conferma indica che StorageGRID ha cancellato l'errore per il Cloud Storage Pool.

Se il problema di fondo è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema di fondo non è stato risolto (o se si verifica un errore diverso), il messaggio di errore verrà visualizzato nella colonna "Ultimo errore" entro pochi minuti.

Errore: Controllo di integrità non riuscito. Errore dall'endpoint

Potresti riscontrare questo errore quando abiliti S3 Object Lock con conservazione predefinita per il tuo bucket Amazon S3 dopo aver iniziato a utilizzarlo per un Cloud Storage Pool. Questo errore si verifica quando l'operazione PUT non ha un'intestazione HTTP con un valore di checksum del payload come `Content-MD5`. Questo valore di intestazione è richiesto da AWS per le operazioni PUT nei bucket con S3 Object Lock abilitato.

Per risolvere questo problema, segui i passaggi in "Modifica un pool di archiviazione cloud" senza apportare modifiche. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag S3 Object Lock sulla configurazione dell'endpoint del Cloud Storage Pool.

Errore: questo Cloud Storage Pool contiene contenuti imprevisti

Potresti riscontrare questo errore quando tenti di creare, modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se il bucket o container include il `x-ntap-sgws-cloud-pool-uuid` file marker, ma quel file non ha il campo metadati con l'UUID previsto.

In genere, vedrai questo errore solo se stai creando un nuovo Cloud Storage Pool e un'altra istanza di StorageGRID sta già utilizzando lo stesso Cloud Storage Pool.

Prova uno di questi passaggi per risolvere il problema:

- Se stai configurando un nuovo Cloud Storage Pool e il bucket contiene il file `x-ntap-sgws-cloud-pool-uuid` e ulteriori chiavi di oggetti simili al seguente esempio, crea un nuovo bucket e usa questo nuovo bucket invece.

  Esempio di chiave oggetto aggiuntiva: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Se il `x-ntap-sgws-cloud-pool-uuid` file è l'unico oggetto nel bucket, elimina questo file.

Se questi passaggi non si applicano al tuo caso, contatta il supporto.

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

Potresti riscontrare questo errore nelle seguenti circostanze:

- Quando provi a creare o modificare un Cloud Storage Pool.
- Quando selezioni una combinazione di piattaforma, autenticazione o protocollo non supportata con S3 Object Lock durante la configurazione di un nuovo Cloud Storage Pool. Vedi "Considerazioni sui Cloud

Storage Pool".

Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di scrivere nel Cloud Storage Pool.

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

- Se il messaggio di errore contiene `Get *url*: EOF`, verifica che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi HTTP per un container o un bucket che richiede HTTPS.
- Se il messaggio di errore contiene `Get *url*: net/http: request canceled while waiting for connection`, verifica che la configurazione di rete consenta ai nodi di Storage di accedere all'endpoint del servizio utilizzato per il Cloud Storage Pool.
- Se l'errore è dovuto a una piattaforma, un'autenticazione o un protocollo non supportati, passa a una configurazione supportata con S3 Object Lock e prova a salvare nuovamente il nuovo Cloud Storage Pool.
- Per tutti gli altri messaggi di errore dell'endpoint, prova una o più delle seguenti soluzioni:
  - Crea un container o un bucket esterno con lo stesso nome che hai inserito per il Cloud Storage Pool e prova a salvare nuovamente il nuovo Cloud Storage Pool.
  - Correggi il nome del container o del bucket che hai specificato per il Cloud Storage Pool e prova a salvare di nuovo il nuovo Cloud Storage Pool.

Errore: impossibile analizzare il certificato CA

Potresti riscontrare questo errore quando provi a creare o modificare un Cloud Storage Pool. L'errore si verifica se StorageGRID non riesce a interpretare il certificato che hai inserito durante la configurazione del Cloud Storage Pool.

Per risolvere il problema, controlla il certificato CA che hai fornito per eventuali problemi.

Errore: non è stato trovato un Cloud Storage Pool con questo ID

Potresti riscontrare questo errore quando tenti di modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se l'endpoint restituisce una risposta 404, che può significare una delle seguenti:

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

Prova uno o più di questi passaggi per risolvere il problema:

- Controlla che l'utente associato alla chiave di accesso configurata abbia le autorizzazioni necessarie.
- Modifica il Cloud Storage Pool con credenziali che hanno le autorizzazioni richieste.
- Se le autorizzazioni sono corrette, contatta il supporto.

Errore: Impossibile verificare il contenuto del pool di storage cloud. Errore dall'endpoint

Potresti riscontrare questo errore quando tenti di eliminare un Cloud Storage Pool. Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di leggere il contenuto del bucket del Cloud Storage Pool.

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

Errore: in questo bucket sono già stati inseriti oggetti

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Non puoi eliminare un Cloud Storage Pool se contiene dati che sono stati spostati lì da ILM, dati che erano nel bucket prima che tu configurassi il Cloud Storage Pool, o dati che sono stati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

Prova uno o più di questi passaggi per risolvere il problema:

- Segui le istruzioni per riportare gli oggetti in StorageGRID in "Ciclo di vita di un oggetto Cloud Storage Pool".
- Se sei certo che gli oggetti rimanenti non siano stati inseriti nel Cloud Storage Pool da ILM, elimina manualmente gli oggetti dal bucket.

> Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbero essere stati inseriti da ILM. Se in seguito provi ad accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non verrà trovato.

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

Potresti riscontrare questo errore se hai 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 proxy server esterno non riesce a raggiungere l'endpoint del Cloud Storage Pool. Ad esempio, il DNS server potrebbe non essere in grado di risolvere il nome host oppure potrebbe esserci un problema di rete esterno.

Prova uno o più di questi passaggi per risolvere il problema:

- Verifica le impostazioni del cloud storage pool (**ILM** > **storage pool**).
- Controlla la configurazione di rete del proxy server di storage.

Errore: il certificato X.509 è fuori dal periodo di validità

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Questo errore si verifica quando l'autenticazione richiede un certificato X.509 per garantire che il Cloud Storage Pool esterno corretto venga convalidato e che il pool esterno sia vuoto prima che la configurazione del Cloud Storage Pool venga eliminata.

Prova questi passaggi per correggere il problema:

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

Informazioni correlate

"Ciclo di vita di un oggetto Cloud Storage Pool"

Gestisci i profili di codifica di cancellazione in StorageGRID

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

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Tu hai il "autorizzazioni di accesso richieste".

Visualizza i dettagli del profilo di erasure-coding

Puoi visualizzare i dettagli di un profilo di codifica di cancellazione per determinarne lo stato, lo schema di codifica di cancellazione utilizzato e altre informazioni.

Passaggi

1. Seleziona **Configurazione** > **Sistema** > **Codifica di cancellazione**.
2. Seleziona il profilo. Viene visualizzata la pagina dei dettagli del profilo.
3. Facoltativamente, puoi visualizzare la scheda Regole ILM per un elenco delle regole ILM che utilizzano il profilo e delle policy ILM che utilizzano tali regole.
4. Facoltativamente, puoi visualizzare la scheda Storage Nodes per vedere i dettagli su ciascun Storage Node nel pool di storage del profilo, come il sito in cui si trova e l'utilizzo dello storage.

Rinomina un profilo di codifica di cancellazione

Potresti voler rinominare un profilo di erasure-coding per rendere più evidente cosa fa il profilo.

Passaggi

1. Seleziona **Configurazione** > **Sistema** > **Codifica di cancellazione**.
2. Seleziona il profilo che desideri rinominare.
3. Seleziona **Rinomina**.
4. Inserisci un nome univoco per il profilo di erasure-coding.

   Il nome del profilo di codifica di cancellazione viene aggiunto al nome del pool di storage nell'istruzione di posizionamento per una regola ILM.

   > I nomi dei profili di codifica di cancellazione devono essere univoci. Si verifica un errore di convalida se usi il nome di un profilo esistente, anche se quel profilo è stato disattivato.

5. Seleziona **Salva**.

Disattiva un profilo di codifica di cancellazione

Puoi disattivare un profilo di codifica di cancellazione se non prevedi più di utilizzarlo e se il profilo non è attualmente utilizzato in alcuna regola ILM.

> Conferma che non siano in corso operazioni di riparazione dei dati con codifica di cancellazione o procedure di decommission. Viene visualizzato un messaggio di errore se provi a disattivare un profilo di codifica di cancellazione mentre una di queste operazioni è in corso.

Informazioni su questa attività

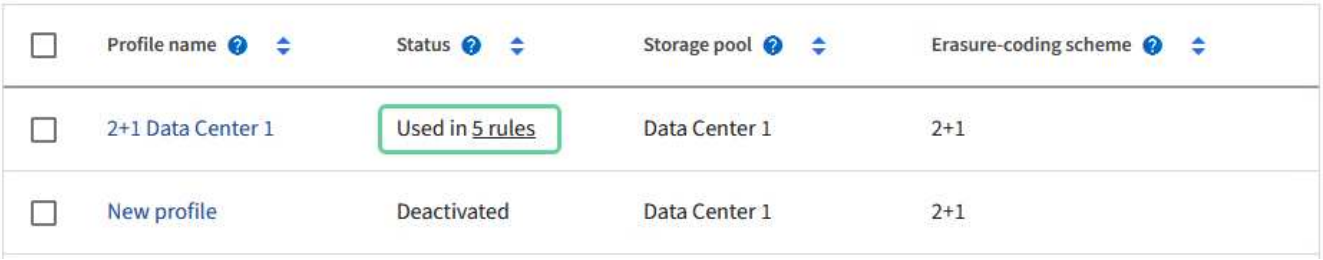
StorageGRID impedisce di disattivare un profilo di codifica di cancellazione se è vera una delle seguenti condizioni:

- Il profilo di erasure coding è attualmente utilizzato in una regola ILM.
- Il profilo di codifica di cancellazione non viene più utilizzato in nessuna regola ILM, ma i dati oggetto e i frammenti di parità relativi al profilo esistono ancora.

Passaggi

1. Seleziona **Configurazione** > **Sistema** > **Codifica di cancellazione**.
2. Nella scheda Attivo, controlla la colonna **Stato** per verificare che il profilo di erasure-coding che desideri disattivare non sia utilizzato in alcuna regola ILM.

   Non puoi disattivare un profilo di codifica di cancellazione se viene utilizzato in una 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, segui questi passaggi:
   a. Seleziona **ILM** > **Regole**.
   b. Seleziona ciascuna regola ed esamina il diagramma di conservazione per determinare se la regola utilizza il profilo di erasure-coding che vuoi disattivare.
   c. Se la regola ILM utilizza il profilo di codifica di cancellazione che vuoi disattivare, verifica se la regola viene utilizzata in qualche criterio ILM.
   d. Completa i passaggi aggiuntivi nella tabella, in base a dove viene utilizzato il profilo di codifica di cancellazione.

Dove è stato utilizzato il profilo?	**Ulteriori passaggi da eseguire prima di disattivare il profilo**	**Consulta queste istruzioni aggiuntive**
Mai utilizzato in alcuna regola ILM	Non sono necessari ulteriori passaggi. Continua con questa procedura.	*Nessuno*
In una regola ILM che non è mai stata utilizzata in nessuna policy ILM	i. Modifica o elimina tutte le regole ILM interessate. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di erasure-coding. ii. Proseguire con questa procedura.	"Lavora con le regole ILM e le policy ILM"

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Consulta queste istruzioni aggiuntive
In una regola ILM che è attualmente in una policy ILM attiva	i. Clona la policy. ii. Rimuovi la regola ILM che utilizza il profilo di erasure coding. iii. Aggiungi una o più nuove regole ILM per garantire che gli oggetti siano protetti. iv. Salva, simula e attiva la nuova policy. v. Attendi che la nuova policy venga applicata e che gli oggetti esistenti vengano spostati nelle nuove posizioni in base alle nuove regole che hai aggiunto. **Nota:** A seconda del numero di oggetti e delle dimensioni del tuo sistema StorageGRID, potrebbero essere necessarie settimane o addirittura mesi perché le operazioni ILM spostino gli oggetti nelle nuove posizioni, in base alle nuove regole ILM. Sebbene tu possa tentare di disattivare un profilo di codifica di cancellazione anche se è ancora associato ai dati, l'operazione di disattivazione non andrà a buon fine. Un messaggio di errore ti informerà se il profilo non è ancora pronto per essere disattivato. vi. Modifica o elimina la regola che hai rimosso dalla policy. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di erasure-coding. vii. Proseguire con questa procedura.	"Crea una policy ILM" "Lavora con le regole ILM e le policy ILM"
In una regola ILM che è attualmente in una policy ILM	i. Modifica la policy. ii. Rimuovi la regola ILM che utilizza il profilo di erasure coding. iii. Aggiungi una o più nuove regole ILM per garantire che tutti gli oggetti siano protetti. iv. Salva la policy. v. Modifica o elimina la regola che hai rimosso dalla policy. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di erasure-coding. vi. Proseguire con questa procedura.	"Crea una policy ILM" "Lavora con le regole ILM e le policy ILM"

e. Aggiorna la pagina Profili di codifica di cancellazione per assicurarti che il profilo non venga utilizzato in una regola ILM.

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

visualizzata la finestra di dialogo Disattiva profilo di codifica di cancellazione.

> Puoi selezionare più profili da disattivare contemporaneamente, purché nessun profilo sia utilizzato in nessuna regola.

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

Risultati

- Se StorageGRID è in grado di disattivare il profilo di codifica di cancellazione, il suo stato è Disattivato. Non puoi più selezionare questo profilo per nessuna regola ILM. Non puoi riattivare un profilo disattivato.
- Se StorageGRID non riesce a disattivare il profilo, viene visualizzato un messaggio di errore. Ad esempio, viene visualizzato un messaggio di errore se i dati degli oggetti sono ancora associati a questo profilo. Potresti dover aspettare diverse settimane prima di riprovare la procedura di disattivazione.

Configura le regioni S3 per StorageGRID

Le regole ILM possono filtrare gli oggetti in base alle regioni opzionali in cui vengono creati i bucket S3, permettendoti di archiviare oggetti provenienti da regioni diverse in posizioni di storage diverse.

Se vuoi usare una regione di un bucket S3 come filtro in una regola, devi prima creare le regioni che possono essere usate dai bucket nel tuo sistema.

> Non puoi cambiare la regione di un bucket dopo che il bucket è stato creato.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

Quando crei un bucket S3, puoi specificare che venga creato in una regione specifica. Specificare una regione permette di posizionare il bucket geograficamente vicino ai suoi utenti, il che può aiutare a ottimizzare la latenza, minimizzare i costi e soddisfare i requisiti normativi.

Quando crei una regola ILM, potresti voler usare la regione associata a un bucket S3 come filtro avanzato. Ad esempio, puoi progettare una regola che si applica solo agli oggetti nei bucket S3 creati nella `us-west-2` regione. Puoi quindi specificare che le copie di quegli oggetti vengano posizionate sui Storage Node in un sito data center all'interno di quella regione per ottimizzare la latenza.

Quando configuri le regioni, segui queste linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati appartenere alla regione `us-east-1`.
- Devi creare le regioni usando Grid Manager prima di poter specificare una regione non predefinita quando crei bucket tramite Tenant Manager o Tenant Management API, oppure con l'elemento di richiesta LocationConstraint per le richieste API S3 PUT Bucket. Si verifica un errore se una richiesta PUT Bucket utilizza una regione che non è stata definita in StorageGRID.
- Devi usare il nome esatto della regione quando crei il bucket S3. I nomi delle regioni distinguono tra maiuscole e minuscole. I caratteri validi sono numeri, lettere e trattini.

EU non è considerato un alias per eu-west-1. Se vuoi usare la regione EU o eu-west-1, devi usare il nome esatto.

- Non puoi eliminare o modificare una regione se viene utilizzata in una regola assegnata a qualsiasi policy (attiva o inattiva).
- Se usi una regione non valida come filtro avanzato in una regola ILM, non puoi aggiungere quella regola a una policy.

  Una regione non valida può verificarsi se usi una regione come filtro avanzato in una regola ILM ma poi la elimini, oppure se usi l'API Grid Management per creare una regola specificando una regione che non hai definito.

- Se elimini una regione dopo averla utilizzata per creare un bucket S3, dovrai aggiungere nuovamente la regione se vorrai usare il filtro avanzato Location Constraint per trovare oggetti in quel bucket.

Passaggi

1. Seleziona **ILM** > **Regioni**.

   Viene visualizzata la pagina Regions.

2. Seleziona la scheda **Tutte le regioni** o **Regione predefinita**.

Tutte le regioni

La scheda **Tutte le regioni** elenca le regioni attualmente definite, inclusa la regione predefinita.

> Non puoi rimuovere o modificare la regione predefinita nella scheda **Tutte le regioni**. Usa la scheda **Regione predefinita** per cambiare la regione predefinita.

a. Per aggiungere una regione, seleziona **Aggiungi un'altra regione**.
b. Inserisci il nome di una regione che vuoi usare quando crei i bucket S3.

   Devi usare esattamente questo nome di regione come elemento LocationConstraint della richiesta quando crei il bucket S3 corrispondente.

c. Per rimuovere un'area non utilizzata, seleziona l'icona di eliminazione ✕.

   Viene visualizzato un messaggio di errore se provi a rimuovere una regione attualmente utilizzata in una qualsiasi policy (attiva o inattiva).

d. Quando hai finito di apportare modifiche, seleziona **Salva**.

   Ora puoi selezionare queste regioni dalla sezione Filtri avanzati nel passaggio 1 della procedura guidata Crea regola ILM. Vedi "Usa filtri avanzati nelle regole ILM".

Regione predefinita

La scheda **Regione predefinita** mostra la regione predefinita attualmente definita, che puoi modificare.

a. Per modificare la regione predefinita, seleziona il nome della regione dalle opzioni disponibili nell'elenco a discesa **Regione predefinita**.
b. Seleziona **Salva**.

Crea regola ILM

Scopri le regole ILM in StorageGRID

Per gestire gli oggetti, crei un insieme di regole di gestione del ciclo di vita delle informazioni (ILM) e le organizzi in una policy ILM.

Ogni oggetto inserito nel sistema viene valutato in base alla policy attiva. Quando una regola della policy corrisponde ai metadati di un oggetto, le istruzioni contenute nella regola determinano le azioni che StorageGRID intraprende per copiare e archiviare tale oggetto.

> I metadati degli oggetti non sono gestiti dalle regole ILM. Al contrario, i metadati degli oggetti vengono memorizzati in un database Cassandra, in quello che viene chiamato un archivio di metadati. Tre copie dei metadati degli oggetti vengono mantenute automaticamente in ogni sito per proteggere i dati dalla perdita.

Elementi di una regola ILM

Una regola ILM ha tre elementi:

- **Criteri di filtraggio**: 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. Ogni regola può includere una sequenza di istruzioni di posizionamento per modificare nel tempo il numero, il tipo e la posizione delle copie degli oggetti. Quando il periodo di tempo per un posizionamento scade, le istruzioni del posizionamento successivo vengono applicate automaticamente dalla successiva valutazione ILM.
- **Comportamento di acquisizione**: Il comportamento di acquisizione di una regola ti permette di scegliere come vengono protetti gli oggetti filtrati dalla regola durante l'ingestione (quando un client S3 salva un oggetto nella grid).

Filtro delle regole ILM

Quando crei una regola ILM, specifichi dei 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 (predefinita) regola in una policy ILM. La regola predefinita fornisce istruzioni di storage per gli oggetti che non corrispondono ai filtri di un'altra regola.

- I filtri di base ti permettono di applicare regole diverse a gruppi di oggetti ampi e distinti. Questi filtri ti permettono di applicare una regola a specifici tenant, a specifici bucket S3 o a entrambi.

  I filtri di base offrono un modo semplice per applicare regole diverse a un gran numero di oggetti. Ad esempio, i dati finanziari della tua azienda potrebbero dover essere archiviati per soddisfare i requisiti normativi, mentre i dati del reparto marketing potrebbero dover essere archiviati per facilitare le operazioni quotidiane. Dopo aver creato account tenant separati per ciascun reparto o dopo aver separato i dati dei diversi reparti in bucket S3 distinti, puoi facilmente creare una regola che si applica a tutti i dati finanziari e una seconda regola che si applica a tutti i dati di marketing.

- I filtri avanzati offrono un controllo granulare. Puoi creare filtri per selezionare gli oggetti in base alle seguenti proprietà degli oggetti:
  - Tempo di ingestione
  - Ultimo accesso
  - Tutto o parte del nome dell'oggetto (Key)
  - Vincolo di posizione (solo S3)
  - Dimensione dell'oggetto
  - Metadati utente
  - Etichetta oggetto (solo S3)

Puoi filtrare gli oggetti in base a criteri molto specifici. Ad esempio, gli oggetti archiviati dal reparto di diagnostica per immagini di un ospedale potrebbero essere utilizzati frequentemente quando hanno meno di 30 giorni e raramente in seguito, mentre gli oggetti che contengono informazioni sulle visite dei pazienti potrebbero dover essere copiati nel reparto di fatturazione presso la sede centrale della rete sanitaria. Puoi creare filtri che identificano ciascun tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag degli oggetti S3 o a qualsiasi altro criterio pertinente, e poi creare regole separate per archiviare ciascun set di oggetti in modo appropriato.

Puoi combinare i filtri come preferisci all'interno di un'unica regola. Ad esempio, il reparto marketing potrebbe voler archiviare i file immagine di grandi dimensioni in modo diverso rispetto ai dati dei fornitori, mentre il reparto Human Resources potrebbe aver bisogno di archiviare i dati del personale relativi a una specifica area geografica e le informazioni sulle policy in un'unica posizione centrale. In questo caso puoi creare regole che filtrano per tenant account per separare i dati di ciascun reparto, utilizzando i filtri in ogni regola per identificare il tipo specifico di oggetti a cui la regola si applica.

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. Ciascuna istruzione di posizionamento si applica a un singolo periodo di tempo.

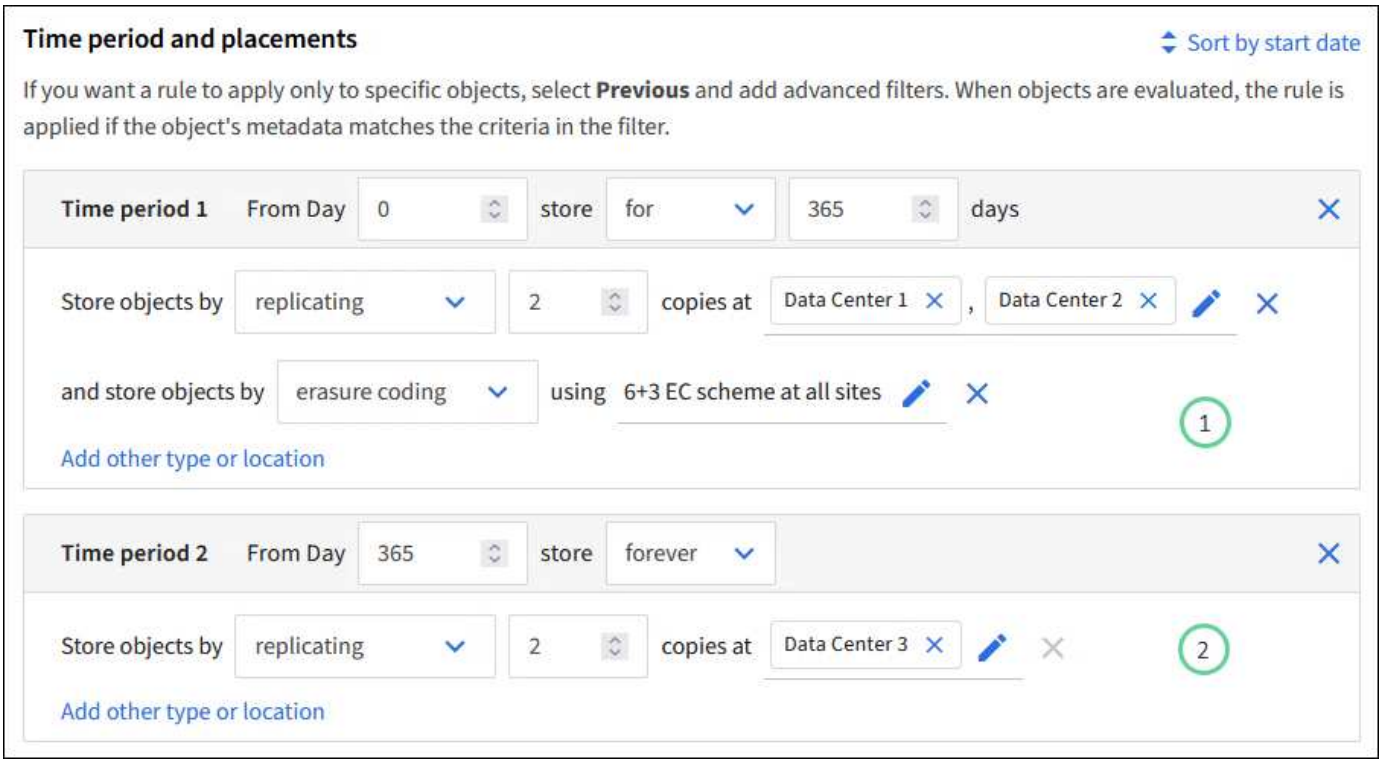
Quando crei le istruzioni di posizionamento:

- Inizi specificando il tempo di riferimento, che determina quando iniziano le istruzioni di posizionamento. Il tempo di riferimento può essere il momento in cui un oggetto viene acquisito, quando vi si accede, quando un oggetto con versione diventa non corrente oppure un momento definito dall'utente.
- Successivamente, specifichi quando il posizionamento avrà effetto, rispetto al tempo di riferimento. Ad esempio, un posizionamento potrebbe iniziare il giorno 0 e continuare per 365 giorni, rispetto al momento in cui l'oggetto è stato acquisito.
- Infine, specifichi il tipo di copie (replica o codifica di cancellazione) e la posizione in cui vengono memorizzate. Ad esempio, potresti voler memorizzare due copie replicate in due siti diversi.

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

- Per posizionare oggetti in più posizioni durante un singolo periodo di tempo, seleziona **Aggiungi altro tipo o posizione** per aggiungere più di una riga per quel periodo di tempo.
- Per posizionare gli oggetti in posizioni diverse in periodi di tempo diversi, seleziona **Aggiungi un altro periodo di tempo** per aggiungere il periodo successivo. Quindi, specifica una o più righe all'interno del periodo di tempo.

L'esempio mostra due istruzioni di posizionamento nella pagina Definisci posizionamenti della procedura guidata Crea regola ILM.



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

- La prima riga crea due copie replicate dell'oggetto in due siti di data center.
- La seconda riga crea una copia con codifica di cancellazione 6+3 utilizzando tutti i siti del data center.

La seconda istruzione di collocazione (2) crea due copie dopo un anno e conserva tali copie per sempre.

Quando definisci l'insieme di istruzioni di posizionamento per una regola, devi assicurarti che almeno un'istruzione di posizionamento inizi al giorno 0, che non ci siano interruzioni tra i periodi di tempo che hai definito e che l'ultima istruzione di posizionamento continui all'infinito o finché non ti servono più copie di oggetti.

Alla scadenza di ciascun periodo di tempo definito nella regola, vengono applicate le istruzioni di posizionamento dei contenuti per il periodo successivo. Vengono create nuove copie degli oggetti e quelle non necessarie vengono eliminate.

Comportamento di ingest delle regole ILM

Il comportamento di acquisizione controlla se le copie degli oggetti vengono posizionate immediatamente secondo le istruzioni della regola oppure se vengono create copie provvisorie e le istruzioni di posizionamento vengono applicate in un secondo momento. Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Bilanciato**: StorageGRID tenta di creare tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono create copie intermedie e il client riceve una notifica di successo. Le copie specificate nella regola ILM vengono create quando possibile.
- **Rigoroso**: Tutte le copie specificate nella regola ILM devono essere effettuate prima che il successo venga restituito al client.
- **Dual commit**: StorageGRID crea immediatamente copie provvisorie dell'oggetto e restituisce successo al

client. Le copie specificate nella regola ILM vengono create quando possibile.

Informazioni correlate

- "Opzioni di ingest"
- "Vantaggi, svantaggi e limitazioni delle opzioni di ingest"
- "Come interagiscono la coerenza e le regole ILM per influire sulla protezione dei dati"

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applica solo agli oggetti appartenenti al tenant A.
- Crea due copie replicate di questi oggetti e conserva 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 finché non vengono eliminati da una richiesta di eliminazione da parte del client o alla scadenza del ciclo di vita del bucket.
- Usa l'opzione Bilanciata per il comportamento di acquisizione: l'istruzione di posizionamento su due siti viene applicata non appena il tenant A salva un oggetto in StorageGRID, a meno che non sia possibile creare immediatamente entrambe le copie richieste.

  Ad esempio, se il Sito 2 non è raggiungibile quando il tenant A salva un oggetto, StorageGRID creerà due copie provvisorie sui nodi di storage del Sito 1. Non appena il Sito 2 diventa disponibile, StorageGRID creerà la copia richiesta in quel sito.

Informazioni correlate

- "Cos'è un pool di storage"
- "Cos'è un pool di storage cloud"

Accedi alla procedura guidata Crea una regola ILM in StorageGRID

Le regole ILM ti permettono di gestire il posizionamento dei dati degli oggetti nel tempo. Per creare una regola ILM, usi la procedura guidata "Crea una regola ILM".

> Se vuoi creare la regola ILM predefinita per una policy, segui "Istruzioni per creare una regola ILM predefinita" invece.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- Se vuoi specificare a quali tenant account si applica questa regola, hai "Autorizzazione account tenant" o conosci l'ID dell'account per ciascun account.
- Se vuoi che la regola filtri gli oggetti in base ai metadati dell'ultimo accesso, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati dal bucket S3.
- Hai configurato tutti i Cloud Storage Pools che intendi utilizzare. Vedi "Crea Cloud Storage Pool".
- Hai familiarità con il "opzioni di ingest".
- Se devi creare una regola conforme da utilizzare con S3 Object Lock, hai familiarità con "requisiti per S3 Object Lock".

- Facoltativamente, hai guardato il video:

  Panoramica delle regole ILM

Informazioni su questa attività

Quando crei le regole ILM:

- Considera la topologia del sistema StorageGRID e le configurazioni di storage.
- Considera quali tipi di copie di oggetti vuoi creare (replicate o codificate con cancellazione) e il numero di copie di ciascun oggetto richieste.
- Determina quali tipi di metadati degli oggetti vengono utilizzati nelle applicazioni che si connettono al sistema StorageGRID. Le regole ILM filtrano gli oggetti in base ai loro metadati.
- Valuta dove vuoi che vengano collocate le copie degli oggetti nel tempo.
- Decidi quale opzione di ingest utilizzare (Balanced, Strict o Dual commit).

Passaggi

1. Seleziona **ILM** > **Regole**.
2. Seleziona **Crea**. "Passaggio 1 (Inserisci i dettagli)"Viene visualizzata la procedura guidata Crea una regola ILM.

Inserisci dettagli e filtri per una regola ILM di StorageGRID

Il passaggio **Inserisci dettagli** della procedura guidata Crea una regola ILM ti permette di inserire un nome e una descrizione per la regola e di definire i filtri per la regola.

Inserire una descrizione e definire i filtri per la regola sono opzionali.

Informazioni su questa attività

Quando valuti un oggetto rispetto a una "Regola ILM" regola, 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. Puoi progettare una regola da applicare a tutti gli oggetti oppure specificare filtri di base, come uno o più tenant o nomi di bucket, o filtri avanzati, come la dimensione dell'oggetto o i metadati utente.

Passaggi

1. Inserisci un nome univoco per la regola nel campo **Name**.
2. Facoltativamente, inserisci una breve descrizione della regola nel campo **Descrizione**.

   Dovresti descrivere lo scopo o la funzione della regola così potrai riconoscerla in seguito.

3. Facoltativamente, seleziona uno o più account tenant S3 a cui applicare questa regola. Se questa regola si applica a tutti i tenant, lascia vuoto questo campo.

   Se non hai l'autorizzazione di accesso Root o l'autorizzazione per gli account tenant, non puoi selezionare i tenant dall'elenco. Invece, inserisci il tenant ID o inserisci più ID come stringa separata da virgole.

4. Facoltativamente, specifica i bucket S3 a cui si applica questa regola.

   Se è selezionata l'opzione **si applica a tutti i bucket** (impostazione predefinita), la regola si applica a tutti i bucket S3.

5. Per i tenant S3, puoi selezionare **Sì** per applicare la regola solo alle versioni precedenti degli oggetti nei bucket S3 in cui è abilitato il versioning.

   Se selezioni **Sì**, "Tempo non corrente" verrà selezionato automaticamente per Tempo di riferimento in "Passaggio 2 della procedura guidata Crea una regola ILM".

   > Il tempo non corrente si applica solo agli oggetti S3 nei bucket con versioning abilitato. Vedi "Operazioni sui bucket, PutBucketVersioning" e "Gestisci gli oggetti con S3 Object Lock".

   Puoi usare questa opzione per ridurre l'impatto dello storage degli oggetti con versioni, filtrando le versioni degli oggetti non correnti. Vedi "Esempio 4: Regole e policy ILM per gli oggetti versionati S3".

6. Facoltativamente, seleziona **Aggiungi un filtro avanzato** per specificare filtri aggiuntivi.

   Se non configuri il filtro avanzato, la regola si applica a tutti gli oggetti che corrispondono ai filtri di base. Per ulteriori informazioni sul filtro avanzato, vedi Usa filtri avanzati nelle regole ILM e Specifica più tipi di metadati e valori.

7. Seleziona **Continua**. "Fase 2 (Definisci i posizionamenti)" della procedura guidata Crea una regola ILM viene visualizzata.

Usa filtri avanzati nelle regole ILM

Il filtraggio avanzato ti permette di creare regole ILM che si applicano solo a oggetti specifici in base ai loro metadati. Quando imposti il filtraggio avanzato per una regola, selezioni il tipo di metadato che vuoi confrontare, scegli un operatore e specifichi un valore per il metadato. Quando gli oggetti vengono valutati, la regola ILM viene applicata solo a quegli oggetti che hanno metadati corrispondenti al filtro avanzato.

La tabella mostra i tipi di metadati che puoi specificare nei filtri avanzati, gli operatori che puoi usare per ciascun tipo di metadati e i valori dei metadati previsti.

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di ingestione	• è • non è • è prima • è il o prima • è dopo • è il o dopo	Data e ora in cui hai caricato l'oggetto. **Nota:** Per evitare problemi di risorse durante l'attivazione di una nuova policy ILM, puoi usare il filtro avanzato "Tempo di acquisizione" in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Imposta il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore per assicurarti che gli oggetti esistenti non vengano spostati inutilmente.

Tipo di metadati	Operatori supportati	Valore dei metadati
Chiave	• uguale • non è uguale • contiene • non contiene • inizia con • non inizia con • termina con • non finisce con	Tutta o parte di una chiave oggetto S3 univoca. Ad esempio, potresti voler abbinare oggetti che terminano con `.txt` o iniziano con `test-object/`.
Ultimo accesso	• è • non è • è prima • è il o prima • è dopo • è il o dopo	Data e ora dell'ultimo recupero (lettura o visualizzazione) dell'oggetto. **Nota:** Se vuoi "usa l'ultimo orario di accesso" come filtro avanzato, devi abilitare gli aggiornamenti dell'ora dell'ultimo accesso per il bucket S3.
Vincolo di posizione (solo S3)	• uguale • non è uguale	La regione in cui è stato creato un bucket S3. Usa **ILM** > **Regioni** per definire le regioni che vengono mostrate. **Nota:** Il valore us-east-1 corrisponde agli oggetti nei bucket creati nella regione us-east-1 e anche agli oggetti nei bucket per cui non è specificata alcuna regione. Vedi "Configura le regioni S3".
Dimensione dell'oggetto	• uguale • non è uguale • meno di • minore o uguale a • maggiore di • maggiore o uguale a	La dimensione dell'oggetto. La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non usare la codifica di cancellazione per oggetti più piccoli di 200 KB per evitare l'overhead della gestione di frammenti codificati molto piccoli.

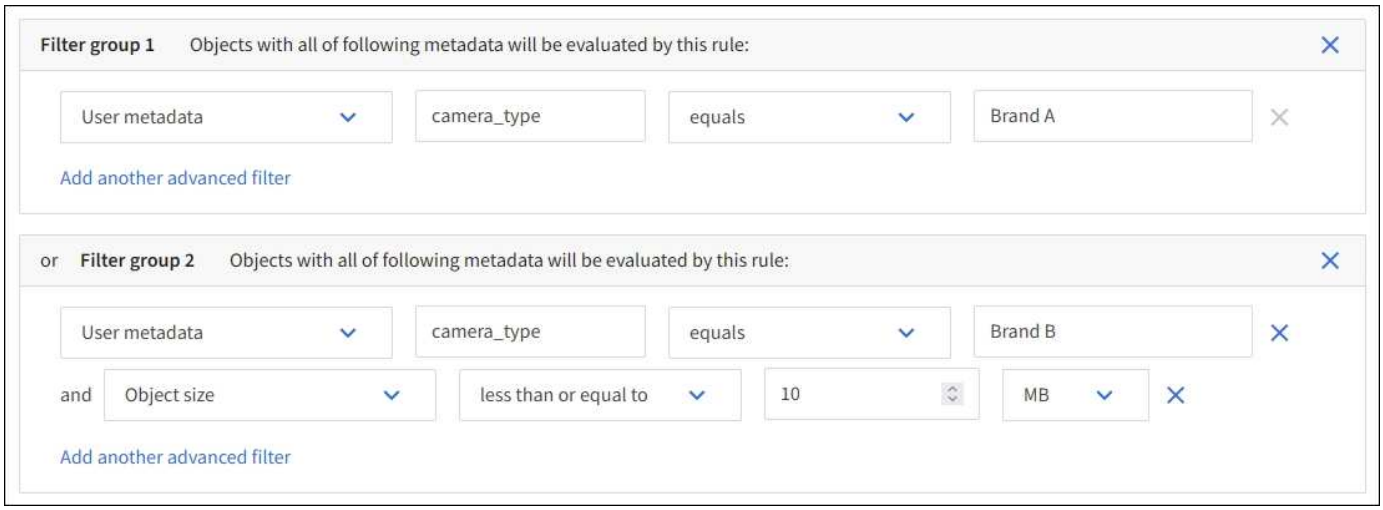
Tipo di metadati	Operatori supportati	Valore dei metadati
Metadati utente	• contiene • termina con • uguale • esiste • inizia con • non contiene • non finisce con • non è uguale • non esiste • non inizia con	Coppia chiave-valore, dove **User metadata name** è la chiave e **Metadata value** è il valore.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

Specifica più tipi di metadati e valori

Quando definisci un filtro avanzato, puoi specificare più tipi di metadati e più valori di metadati. Ad esempio, se vuoi che una regola corrisponda a oggetti di dimensioni comprese tra 10 MB e 100 MB, devi selezionare il tipo di metadati **Object size** e specificare due valori di metadati.

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

L'utilizzo di più voci ti permette di avere un controllo preciso su quali oggetti vengono abbinati. Nell'esempio seguente, la regola si applica agli oggetti che hanno Brand A o Brand B come valore del metadato utente camera_type. Tuttavia, la regola si applica solo a quegli oggetti Brand B che sono più piccoli di 10 MB.



Definisci le istruzioni di posizionamento per una regola StorageGRID ILM

La fase **Definisci posizionamenti** della procedura guidata Crea regola ILM ti permette di definire le istruzioni di posizionamento che determinano per quanto tempo gli oggetti vengono conservati, il tipo di copie (replicate o con codifica di cancellazione), la posizione di archiviazione e il numero di copie.

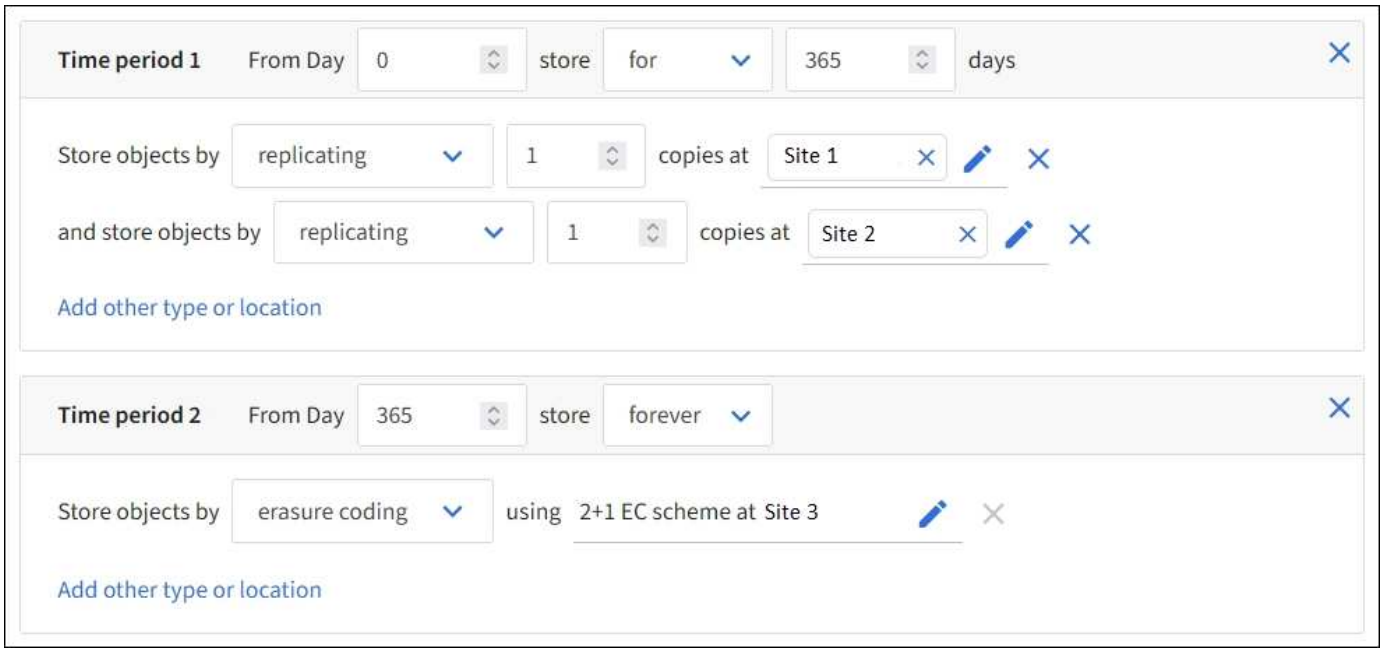
Le schermate mostrate sono esempi. I risultati potrebbero variare a seconda della versione di StorageGRID.

Informazioni su 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 usi più istruzioni, i periodi di tempo devono essere contigui e almeno un'istruzione deve iniziare dal giorno 0. Le istruzioni possono continuare per sempre o fino a quando non ti servono più copie di oggetti.

Ogni istruzione di posizionamento può avere più righe se vuoi creare diversi tipi di copie o usare posizioni diverse durante quel periodo.

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 con codifica di cancellazione 2+1 e salvata in un solo sito.



Passaggi

1. Per **Tempo di riferimento**, seleziona il tipo di tempo da usare quando calcoli l'ora di inizio di un'istruzione di posizionamento.

Opzione	Descrizione
Tempo di ingestione	L'ora in cui l'oggetto è stato acquisito.
Ultimo accesso	L'ultima volta che l'oggetto è stato recuperato (letto o visualizzato). Per utilizzare questa opzione, devi abilitare gli aggiornamenti all'ora dell'ultimo accesso per il bucket S3. Consulta "Usa l'ora dell'ultimo accesso nelle regole ILM".
Ora di creazione definita dall'utente	Un orario specificato nei metadati definiti dall'utente.
Tempo non corrente	"Tempo non corrente" viene selezionato automaticamente se hai selezionato **Sì** alla domanda "Applica questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con versioning abilitato)?" in "Passaggio 1 della procedura guidata Crea una regola ILM".

   Se vuoi creare una regola *conforme*, devi selezionare **Tempo di acquisizione**. Consulta "Gestisci gli oggetti con S3 Object Lock".

2. Nella sezione **Periodo di tempo e collocazioni**, inserisci un orario di inizio e una durata per il primo periodo di tempo.

   Ad esempio, potresti voler specificare dove archiviare gli oggetti per il primo anno (*A partire dal giorno 0, archivia per 365 giorni*). Almeno un'istruzione deve iniziare dal giorno 0.

3. Se vuoi creare copie replicate:

a. Dall'elenco a discesa **Archivia oggetti per**, seleziona **replicazione**.

b. Seleziona il numero di copie che vuoi fare.

   Viene visualizzato un avviso se imposti il numero di copie su 1. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Consulta "Perché non dovresti usare la replica a copia singola".

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

   - Aumenta il numero di copie per il periodo di tempo.
   - Aggiungi copie ad altri pool di storage o a un Cloud Storage Pool.
   - Seleziona **codifica di cancellazione** invece di **replicazione**.

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

c. Nel campo **copie in**, seleziona i pool di storage che vuoi aggiungere.

   Se specifichi un solo pool di storage, tieni presente che StorageGRID può memorizzare solo una copia replicata di un oggetto su qualsiasi Storage Node. Se la tua grid include tre Storage Node e selezioni 4 come numero di copie, verranno create solo tre copie: una per ciascun Storage Node.

   L'avviso **Impossibile posizionare ILM** viene attivato per indicare che la regola ILM non può essere applicata completamente.

   Se specifichi più di un pool di storage, tieni a mente queste regole:

   - Il numero di copie non può essere superiore al numero di pool di storage.
   - Se il numero di copie è uguale al numero di pool di storage, una copia dell'oggetto viene memorizzata 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 ingest, e poi il sistema distribuisce le copie rimanenti per mantenere bilanciato l'utilizzo del disco tra i pool, assicurando che nessun sito riceva più di una copia di un oggetto.
   - Se i pool di storage si sovrappongono (contengono gli stessi Storage Node), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di storage All Storage Nodes (StorageGRID 11.6 e versioni precedenti) e un altro pool di storage.

4. Se vuoi creare una copia con codifica di cancellazione:

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

      > La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non usare la codifica di cancellazione per oggetti più piccoli di 200 KB per evitare l'overhead della gestione di frammenti codificati molto piccoli.

   b. Se non hai aggiunto un filtro per le dimensioni dell'oggetto con un valore superiore a 200 KB, seleziona **Precedente** per tornare al passaggio 1. Quindi, seleziona **Aggiungi un filtro avanzato** e imposta un filtro **Dimensioni oggetto** con un valore qualsiasi superiore a 200 KB.

   c. Seleziona il pool di storage che desideri aggiungere e lo schema di codifica di cancellazione che vuoi usare.

      La posizione di archiviazione per una copia con codifica di cancellazione include il nome dello schema

di codifica di cancellazione, seguito dal nome del pool di storage.

Gli schemi di codifica di cancellazione disponibili sono limitati dal numero di nodi di archiviazione nel pool di storage che selezioni. Un badge `Recommended` appare accanto agli schemi che forniscono o il "migliore protezione o il più basso overhead dello storage".

5. Facoltativamente:
   a. Seleziona **Aggiungi altro tipo o posizione** per creare copie aggiuntive in posizioni diverse.
   b. Seleziona **Aggiungi un altro periodo di tempo** per aggiungere periodi di tempo diversi.

> L'eliminazione degli oggetti avviene in base alle seguenti impostazioni:
>
> - Gli oggetti vengono eliminati automaticamente al termine dell'ultimo periodo di tempo, a meno che un altro periodo di tempo non termini con **forever**.
> - A seconda delle "impostazioni del periodo di conservazione del bucket e del tenant" impostazioni, gli oggetti potrebbero non essere eliminati anche se il periodo di conservazione ILM termina.

6. Se vuoi archiviare oggetti in un Cloud Storage Pool:
   a. Nell'elenco a discesa **Archivia oggetti per**, seleziona **replicazione**.
   b. Seleziona il campo **copie in**, quindi seleziona un Cloud Storage Pool.

      Quando usi i Cloud Storage Pools, tieni a mente queste regole:

      - Non puoi selezionare più di un Cloud Storage Pool in una singola istruzione di posizionamento. Allo stesso modo, non puoi selezionare un Cloud Storage Pool e un pool di storage nella stessa istruzione di posizionamento.
      - Puoi memorizzare solo una copia di un oggetto in qualsiasi Cloud Storage Pool. Viene visualizzato un messaggio di errore se imposti **Copies** su 2 o più.
      - Non puoi archiviare più di una copia di un oggetto contemporaneamente in un Cloud Storage Pool. Viene visualizzato un messaggio di errore se più posizionamenti che utilizzano un Cloud Storage Pool hanno date sovrapposte o se più righe nello stesso posizionamento utilizzano un Cloud Storage Pool.
      - Puoi archiviare un oggetto in un Cloud Storage Pool mentre lo stesso oggetto viene archiviato come copie replicate o con codifica di cancellazione in StorageGRID. Tuttavia, devi includere più di una riga nell'istruzione di posizionamento per il periodo di tempo, così puoi specificare il numero e i tipi di copie per ciascuna posizione.

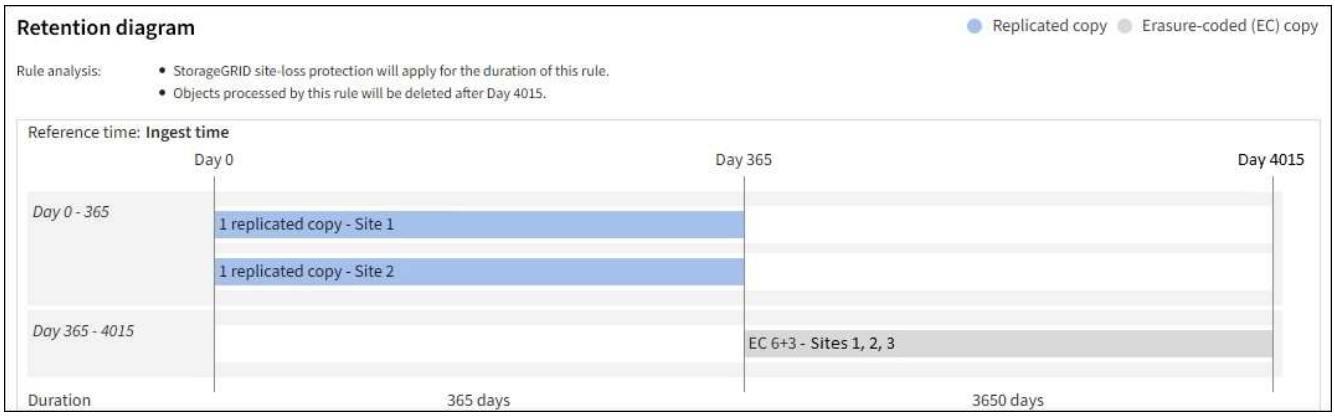
7. Nel diagramma di retention, conferma le istruzioni di posizionamento.

   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 ulteriori 10 anni, una copia con codifica di cancellazione 6+3 verrà salvata in tre siti. Dopo un totale di 11 anni, gli oggetti verranno eliminati da StorageGRID.

   La sezione di analisi delle regole del diagramma di retention afferma:

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

     Fai riferimento a "Attiva la protezione contro la perdita del sito."



8. Seleziona **Continua**. "Passaggio 3 (Seleziona il comportamento di ingestione)" Viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare l'orario dell'ultimo accesso nelle regole ILM di StorageGRID

Puoi usare l'ora dell'ultimo accesso come data di riferimento in una regola ILM. Ad esempio, potresti voler lasciare gli oggetti visualizzati negli ultimi tre mesi sui nodi di storage locali, mentre sposti gli oggetti che non sono stati visualizzati di recente in una posizione remota. Puoi anche usare l'ora dell'ultimo accesso come filtro avanzato se vuoi che una regola ILM si applichi solo agli oggetti a cui si è avuto accesso per l'ultima volta in una data specifica.

Informazioni su questa attività

Prima di utilizzare l'ora dell'ultimo accesso in una regola ILM, valuta le seguenti considerazioni:

- Quando usi l'ora dell'ultimo accesso come riferimento, tieni presente che la modifica dell'ora dell'ultimo accesso di un oggetto non attiva immediatamente una valutazione ILM. Al contrario, le posizioni dell'oggetto vengono valutate e l'oggetto viene spostato, se necessario, quando ILM in background valuta l'oggetto. Questo potrebbe richiedere due settimane o più dopo che l'oggetto è stato accesso.

  Tieni conto di questa latenza quando crei regole ILM basate sull'ora dell'ultimo accesso ed evita posizionamenti che utilizzano periodi di tempo brevi (meno di un mese).

- Quando usi l'ora dell'ultimo accesso come filtro avanzato o come tempo di riferimento, devi abilitare gli aggiornamenti dell'ora dell'ultimo accesso per i bucket S3. Puoi usare "${post_edited_translations.segment}" o "API di gestione tenant".

> Gli aggiornamenti dell'ora dell'ultimo accesso sono disabilitati per impostazione predefinita per i bucket S3.

> Tieni presente che l'attivazione degli aggiornamenti dell'ora dell'ultimo accesso può ridurre le prestazioni, soprattutto nei sistemi con oggetti di piccole dimensioni. L'impatto sulle prestazioni 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 aggiornamenti dell'ora dell'ultimo accesso sono disabilitati	Se l'ora dell'ultimo accesso viene aggiornata quando sono abilitati gli aggiornamenti dell'ora dell'ultimo accesso
Richiesta di recupero di un oggetto, del relativo access control list o dei relativi metadati	No	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì
Richiesta di copiare un oggetto da un bucket a un altro	• No, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completamento di un caricamento in più parti	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Selezionare il comportamento di acquisizione per una regola StorageGRID ILM

Il passaggio **Seleziona comportamento di acquisizione** della procedura guidata Crea regola ILM ti permette di scegliere come vengono protetti gli oggetti filtrati da questa regola mentre vengono acquisiti.

Informazioni su questa attività

StorageGRID può creare copie provvisorie e mettere in coda gli oggetti per una successiva valutazione ILM, oppure può creare copie per soddisfare immediatamente le istruzioni di posizionamento della regola.

Passaggi

1. Seleziona "comportamento di ingest" da usare.

   Per ulteriori informazioni, vedi "Vantaggi, svantaggi e limitazioni delle opzioni di ingest".

   > Non puoi usare l'opzione Bilanciata o Rigorosa se la regola utilizza uno di questi posizionamenti:
   >
   > - Un Cloud Storage Pool al giorno 0
   > - Un Cloud Storage Pool quando la regola utilizza un'ora di creazione definita dall'utente come ora di riferimento
   >
   > Vedi "Esempio 5: Regole e policy ILM per Strict ingest behavior".

2. Seleziona **Create**.

   La regola ILM viene creata. La regola non diventa attiva finché non viene aggiunta a un "Policy ILM" e quel criterio non viene attivato.

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

Crea una regola ILM predefinita in StorageGRID

Prima di creare una policy ILM, devi creare una regola predefinita per inserire nella policy tutti gli oggetti non corrispondenti a un'altra regola. La regola predefinita non può usare alcun filtro. Deve essere applicata a tutti i tenant, a tutti i bucket e a tutte le versioni degli oggetti.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

La regola predefinita è l'ultima regola ad essere valutata in una policy 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 nella policy.

In questo esempio di policy, la prima regola si applica solo agli oggetti appartenenti a test-tenant-1. La regola predefinita, che è l'ultima, si applica agli oggetti appartenenti a tutti gli altri tenant account.

Quando crei la regola predefinita, tieni presenti questi requisiti:

- La regola predefinita verrà automaticamente inserita come ultima regola quando la aggiungi a una policy.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita deve essere applicata a tutte le versioni dell'oggetto.
- La regola predefinita dovrebbe creare copie replicate.

Non usare come regola predefinita per una policy una regola che crea copie con codifica di cancellazione. Le regole di codifica di cancellazione dovrebbero usare un filtro avanzato per impedire che gli oggetti più piccoli vengano codificati con la codifica di cancellazione.

- In generale, la regola predefinita dovrebbe conservare gli oggetti per sempre.
- Se usi (o prevedi di abilitare) l'impostazione globale S3 Object Lock, la regola predefinita deve essere conforme.

Passaggi

1. Seleziona **ILM** > **Regole**.
2. Seleziona **Create**.

   Viene visualizzato il passaggio 1 (Inserisci i dettagli) della procedura guidata Crea regola ILM.

3. Inserisci un nome univoco per la regola nel campo **Nome regola**.
4. Facoltativamente, inserisci una breve descrizione della regola nel campo **Descrizione**.
5. Lascia vuoto il campo **Account tenant**.

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

6. Lascia l'opzione "Si applica a tutti i bucket" selezionata nel menu a tendina "Nome del bucket".

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

7. Mantieni la risposta predefinita, **No**, alla domanda "Applica questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con versioning abilitato)?"
8. Non aggiungere filtri avanzati.

   La regola predefinita non può specificare alcun filtro.

9. Seleziona **Next**.

   Viene visualizzato il passaggio 2 (Definisci i posizionamenti).

10. Per il tempo di riferimento, seleziona qualsiasi opzione.

    Se hai mantenuto la risposta predefinita, **No**, alla domanda "Applica questa regola solo alle versioni precedenti dell'oggetto?" Il tempo non corrente non sarà incluso nell'elenco a discesa. La regola predefinita deve applicarsi a tutte le versioni dell'oggetto.

11. Specifica le istruzioni di posizionamento per la regola predefinita.
    - La regola predefinita dovrebbe conservare gli oggetti per sempre. Viene visualizzato un avviso quando attivi una nuova policy 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 usare come regola predefinita per una policy una regola che crea copie con codifica di cancellazione. Le regole di codifica di cancellazione dovrebbero includere il filtro avanzato **Dimensione oggetto (MB) superiore a 200 KB** per impedire che oggetti più piccoli vengano codificati con la cancellazione.

- Se usi (o hai intenzione di abilitare) l'impostazione globale S3 Object Lock, la regola predefinita deve essere conforme:
  - Devi creare almeno due copie replicate dell'oggetto o una copia con codifica di cancellazione.
  - Queste copie devono esistere sui nodi di archiviazione per tutta la durata di ogni riga delle istruzioni di posizionamento.
  - Non puoi salvare copie di oggetti in un Cloud Storage Pool.
  - Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando l'Ingest time come orario di riferimento.
  - Almeno una riga delle istruzioni per il posizionamento deve essere "per sempre".

12. Guarda il diagramma di conservazione per confermare le tue istruzioni di posizionamento.
13. Seleziona **Continue**.

    Viene visualizzato il passaggio 3 (Seleziona il comportamento di ingest).

14. Seleziona l'opzione di ingest da utilizzare e seleziona **Crea**.

Gestisci le policy ILM

Scopri le policy ILM in StorageGRID

Una policy di gestione del ciclo di vita delle informazioni (ILM) è un insieme ordinato di regole ILM che determina come il sistema StorageGRID gestisce i dati degli oggetti nel tempo.

> Una policy ILM configurata in modo errato può causare una perdita di dati irreversibile. Prima di attivare una policy ILM, esaminala attentamente, verifica le relative regole ILM e poi simula la policy ILM. Assicurati sempre che la policy ILM funzioni come previsto.

Criterio ILM predefinito

Quando installi StorageGRID e aggiungi siti, viene creata automaticamente una policy ILM predefinita, come segue:

- Se la tua griglia contiene un solo sito, la policy predefinita include una regola predefinita che replica due copie di ciascun oggetto in quel sito.
- Se la tua griglia contiene più di un sito, la regola predefinita replica una copia di ciascun oggetto in ogni sito.

Se i criteri predefiniti non soddisfano i requisiti di archiviazione, puoi creare le tue regole e i tuoi criteri. Vedi "Crea una regola ILM" e "Crea una policy ILM".

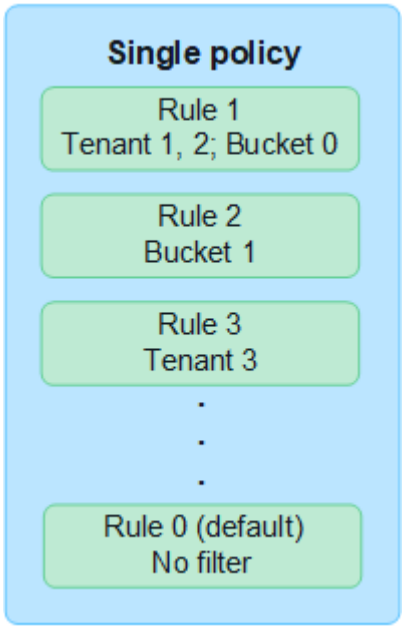
Una o più policy ILM attive?

Puoi avere una o più policy ILM attive contemporaneamente.

Una policy

Se la griglia utilizzerà uno schema di protezione dei dati semplice con poche regole specifiche per tenant e bucket, utilizza una singola policy ILM attiva. Le regole ILM possono contenere filtri per gestire bucket o tenant

diversi.



Quando hai solo una policy e i requisiti di un tenant cambiano, devi creare una nuova policy ILM o clonare la policy esistente per applicare le modifiche, simulare e poi attivare la nuova policy ILM. Le modifiche alla policy ILM potrebbero comportare spostamenti di oggetti che potrebbero richiedere molti giorni e causare latenza.

Più policy

Per offrire diverse opzioni di qualità del servizio ai tenant, puoi avere più di una policy attiva contemporaneamente. Ogni policy può gestire tenant, bucket S3 e oggetti specifici. Quando applichi o modifichi una policy per un set specifico di tenant o oggetti, le policy applicate ad altri tenant e oggetti non vengono influenzate.

Tag delle policy ILM

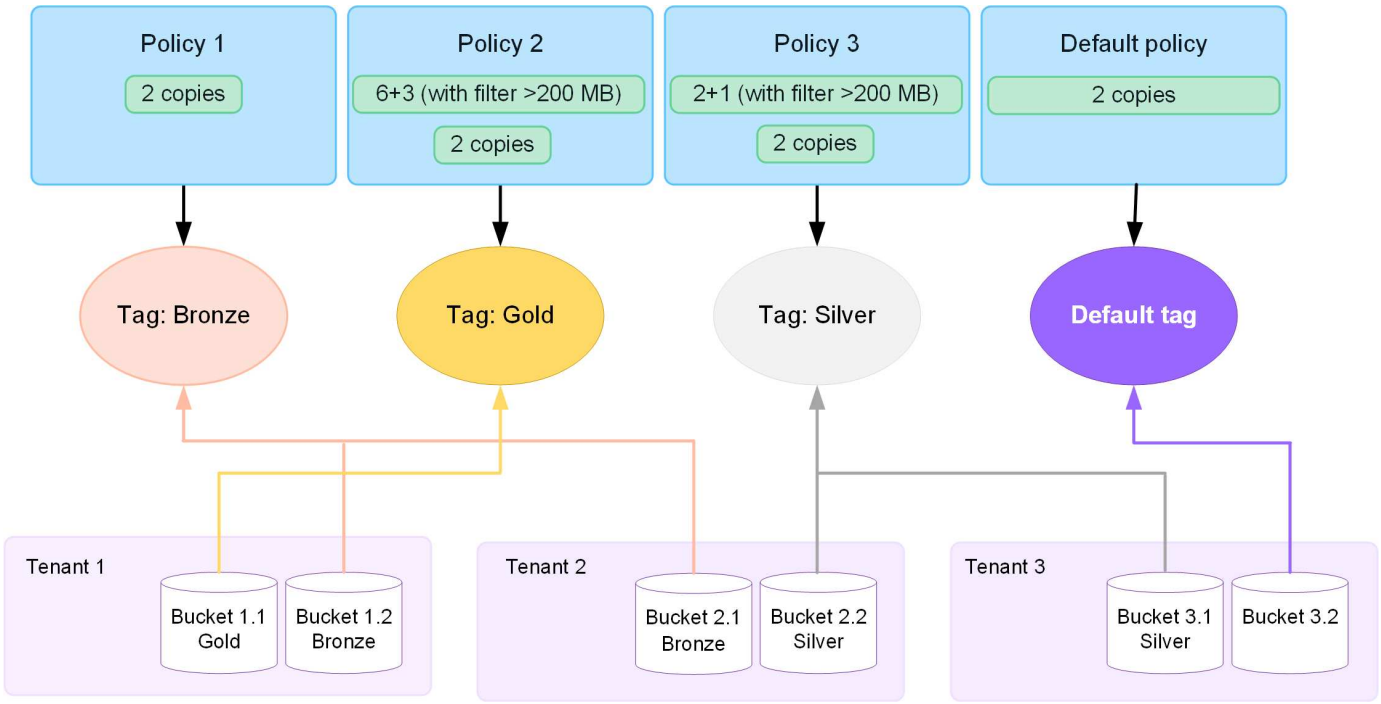
Se desideri consentire ai tenant di passare facilmente da un criterio di protezione dei dati all'altro per singolo bucket, utilizza più criteri ILM con i *tag dei criteri ILM*. Assegni ciascun criterio ILM a un tag, quindi i tenant applicano un tag a un bucket per applicare il criterio a quel bucket. Puoi impostare i tag dei criteri ILM solo sui bucket S3.

Ad esempio, potresti avere tre tag denominati Gold, Silver e Bronze. Puoi assegnare una policy ILM a ciascun tag, in base a quanto a lungo e dove quella policy memorizza gli oggetti. I tenant possono scegliere quale policy utilizzare etichettando i propri bucket. Un bucket etichettato Gold è gestito dalla policy Gold e riceve il livello Gold di protezione dei dati e di prestazioni.

Puoi "crea un massimo di 10 tag di policy" per la tua griglia.

Tag predefinito della policy ILM

Un tag di policy ILM predefinito viene creato automaticamente quando installi StorageGRID. Ogni grid deve avere una policy attiva assegnata al tag Default. La policy predefinita si applica a qualsiasi bucket S3 senza tag.



In che modo una policy ILM valuta gli oggetti?

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

Quando i client salvano oggetti in StorageGRID, gli oggetti vengono valutati rispetto all'insieme ordinato di regole ILM nella policy, come segue:

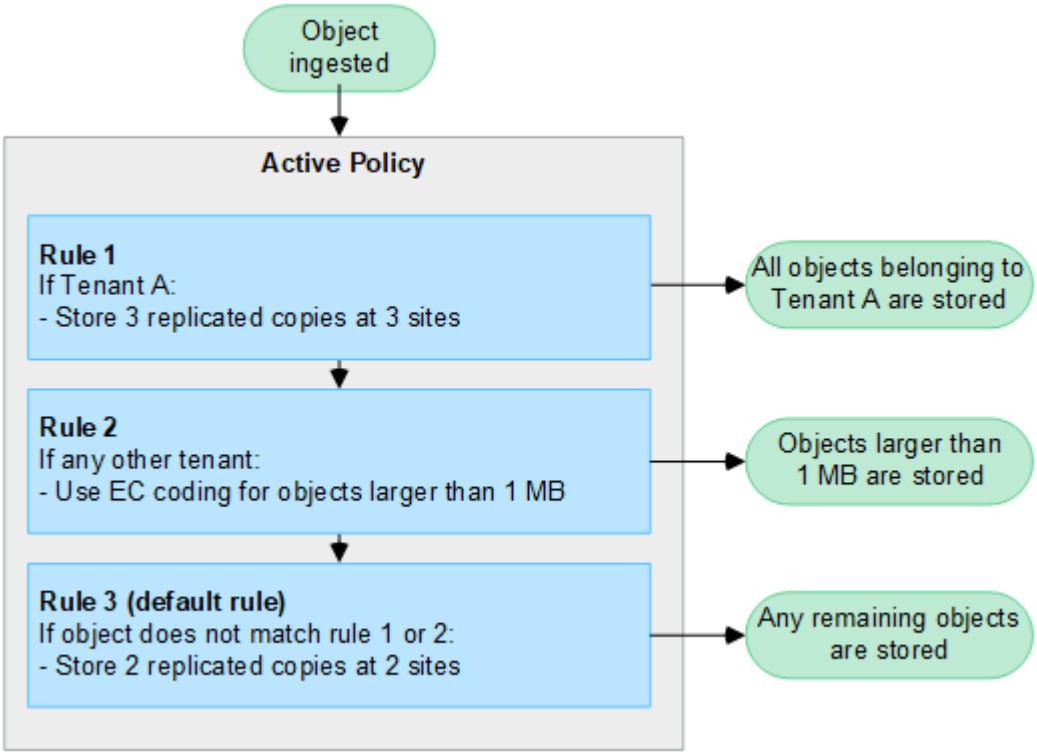
1. Se i filtri della prima regola nella policy corrispondono a un oggetto, l'oggetto viene acquisito secondo il comportamento di ingestione di quella regola e memorizzato secondo le istruzioni di posizionamento di quella regola.
2. Se i filtri della prima regola non corrispondono all'oggetto, l'oggetto viene valutato rispetto a ciascuna regola successiva della policy fino a quando non viene trovata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di acquisizione e posizionamento della regola predefinita nella policy. La regola predefinita è l'ultima regola in una policy. 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 filtri avanzati.

Esempio di policy ILM

Ad esempio, una policy 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.
  - Conserva questi oggetti come tre copie replicate in tre siti.
  - Gli oggetti appartenenti ad altri tenant non vengono abbinati dalla Regola 1, quindi vengono valutati in base alla Regola 2.
- **Regola 2: Codifica di cancellazione per oggetti superiori a 1 MB**
  - Abbina 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 agli oggetti di 1 MB o più piccoli, quindi questi oggetti vengono valutati in base alla Regola 3.
- **Regola 3: 2 copie 2 centri dati** (default)
    - È l'ultima regola predefinita della policy. Non utilizza filtri.
    - Crea due copie replicate di tutti gli oggetti non corrispondenti alla Regola 1 o alla Regola 2 (oggetti non appartenenti al Tenant A che sono di dimensioni pari o inferiori a 1 MB).



Cosa sono le policy attive e inattive?

Ogni sistema StorageGRID deve avere almeno una policy ILM attiva. Se vuoi avere più di una policy ILM attiva, crea dei tag di policy ILM e assegna una policy a ciascun tag. I tenant applicano quindi i tag ai bucket S3. La policy predefinita viene applicata a tutti gli oggetti nei bucket a cui non è stato assegnato un tag di policy.

Quando crei per la prima volta una policy ILM, selezioni una o più regole ILM e le disponi in un ordine specifico. Dopo aver simulato la policy per confermarne il comportamento, la attivi.

Quando attivi una policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando vengono implementate le regole ILM della nuova policy.

Se attivi più criteri ILM contemporaneamente e i tenant applicano tag di criterio ai bucket S3, gli oggetti in ciascun bucket vengono gestiti in base al criterio assegnato al tag.

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

Considerazioni per la creazione di una policy ILM

- Usa solo la policy fornita dal sistema, Baseline 2 copies policy, nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola Make 2 Copies in questa policy utilizza il pool di storage All Storage Nodes,

che contiene tutti i siti. Se il tuo sistema StorageGRID ha più di un sito, due copie di un oggetto potrebbero essere posizionate nello stesso sito.

> Il pool di storage All Storage Nodes viene creato automaticamente durante l'installazione di StorageGRID 11.6 e versioni precedenti. Se aggiorni a una versione successiva di StorageGRID, il pool All Storage Nodes esisterà ancora. Se installi StorageGRID 11.7 o versioni successive come nuova installazione, il pool All Storage Nodes non viene creato.

- Quando progetti una nuova policy, considera tutti i diversi tipi di oggetti che potrebbero essere inseriti nella tua grid. Assicurati che la policy includa regole per abbinare e posizionare questi oggetti come richiesto.
- Mantieni la policy ILM il più semplice possibile. Questo evita situazioni potenzialmente pericolose in cui i dati degli oggetti non sono protetti come previsto quando vengono apportate modifiche al sistema StorageGRID nel tempo.
- Assicurati che le regole nella policy siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, a partire dall'alto. Per esempio, se la prima regola in una policy corrisponde a un oggetto, quell'oggetto non verrà valutato da nessun'altra regola.
- L'ultima regola in ogni policy ILM è la regola ILM predefinita, che non può utilizzare alcun filtro. Se un oggetto non è stato abbinato da un'altra regola, la regola predefinita controlla dove viene posizionato tale oggetto e per quanto tempo viene conservato.
- Prima di attivare una nuova policy, rivedi eventuali modifiche che la policy apporta al posizionamento degli oggetti esistenti. Cambiare la posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Crea policy ILM in StorageGRID

Crea una o più policy ILM per soddisfare i tuoi requisiti di qualità del servizio.

Disporre di una singola policy ILM attiva consente di applicare le stesse regole ILM a tutti i tenant e bucket.

Disporre di più policy ILM attive ti permette di applicare le regole ILM appropriate a specifici tenant e bucket per soddisfare molteplici requisiti di qualità del servizio.

Crea una policy ILM

Informazioni su questa attività

Prima di creare la tua policy, verifica che "policy ILM predefinita" non soddisfi i tuoi requisiti di storage.

> Usa solo le policy fornite dal sistema, 2 copie Policy (per griglie a sito singolo) o 1 Copy per Site (per griglie multisito), nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola predefinita in questa policy utilizza il pool di storage All Storage Nodes, che contiene tutti i siti. Se il tuo sistema StorageGRID ha più di un sito, due copie di un oggetto potrebbero essere posizionate nello stesso sito.

> Se "L'impostazione globale di blocco degli oggetti S3 è stata abilitata" si verifica, devi assicurarti che la policy ILM sia conforme ai requisiti dei bucket che hanno S3 Object Lock abilitato. In questa sezione, segui le istruzioni che menzionano S3 Object Lock abilitato.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".

- Tu hai il "autorizzazioni di accesso richieste".
- Hai "regole ILM create" in base al fatto che S3 Object Lock sia abilitato.

  Blocco oggetti S3 non abilitato

  - Hai "hai creato le regole ILM" che vuoi aggiungere alla policy. Se necessario, puoi salvare una policy, creare regole aggiuntive e poi modificare la policy per aggiungere le nuove regole.
  - Hai "hai creato una regola ILM predefinita" che non contiene alcun filtro.

  Blocco oggetto S3 abilitato

  - Il "L'impostazione globale di blocco degli oggetti S3 è già abilitata" per il sistema StorageGRID.
  - Hai "hai creato le regole ILM conformi e non conformi" che vuoi aggiungere alla policy. Se necessario, puoi salvare una policy, creare regole aggiuntive e poi modificare la policy per aggiungere le nuove regole.
  - Hai "hai creato una regola ILM predefinita" per la policy che è conforme.

- Facoltativamente, hai guardato il video:

Panoramica delle policy ILM

Vedi anche "Usa le policy ILM".

Passaggi

1. Seleziona **ILM** > **Policies**.

   Se l'impostazione globale S3 Object Lock è abilitata, la pagina delle policy ILM indica quali regole ILM sono conformi.

2. Definisci come vuoi creare la policy ILM.

   Crea una nuova policy

   a. Seleziona **Crea policy**.

   Clona la policy esistente

   a. Seleziona la casella di controllo per il criterio da cui vuoi iniziare, poi seleziona **Clona**.

   Modifica la policy esistente

   a. Se una policy è inattiva, puoi modificarla. Seleziona la casella di controllo corrispondente alla policy inattiva da cui vuoi iniziare, poi seleziona **Modifica**.

3. Nel campo **Policy name**, inserisci un nome univoco per la policy.
4. Facoltativamente, nel campo **Motivo della modifica**, inserisci il motivo per cui stai creando una nuova policy.
5. Per aggiungere regole alla policy, seleziona **Seleziona regole**. Seleziona il nome di una regola per visualizzarne le impostazioni.

   Se stai clonando una policy:

- Le regole utilizzate dalla policy che stai clonando sono selezionate.
- Se la policy che stai clonando utilizzava regole senza filtri che non erano la regola predefinita, ti viene richiesto di rimuovere tutte tranne una di queste regole.
- Se la regola predefinita utilizzava un filtro, ti verrà chiesto di selezionare una nuova regola predefinita.
- Se la regola predefinita non era l'ultima, puoi spostare la regola alla fine della nuova policy.

Blocco oggetti S3 non abilitato

a. Seleziona una regola predefinita per la policy. Per creare una nuova regola predefinita, seleziona **pagina Regole ILM**.

   La regola predefinita si applica a tutti gli oggetti che non corrispondono ad altre regole della policy. La regola predefinita non può usare filtri e viene sempre valutata per ultima.

   > Non usare la regola "Make 2 Copies" come regola predefinita per una policy. La regola "Make 2 Copies" utilizza un singolo pool di storage, All Storage Nodes, che contiene tutti i siti. Se il tuo sistema StorageGRID ha più di un sito, due copie di un oggetto potrebbero essere posizionate nello stesso sito.

Blocco oggetto S3 abilitato

a. Seleziona una regola predefinita per la policy. Per creare una nuova regola predefinita, seleziona **pagina Regole ILM**.

   L'elenco delle regole contiene solo le regole conformi e non utilizza alcun filtro.

   > Non usare la regola "Make 2 Copies" come regola predefinita per una policy. La regola "Make 2 Copies" utilizza un unico pool di storage, All Storage Nodes, che contiene tutti i siti. Se usi questa regola, più copie di un oggetto potrebbero essere posizionate nello stesso sito.

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

   Ad esempio, potresti voler utilizzare un Cloud Storage Pool per memorizzare oggetti in bucket in cui non è abilitato S3 Object Lock.

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

Vedi anche "Esempio 7: Criterio ILM conforme per S3 Object Lock".

6. Quando hai finito di selezionare la regola predefinita, seleziona **Continua**.
7. Nella fase Altre regole, seleziona le altre regole che vuoi aggiungere alla policy. Queste regole utilizzano almeno un filtro (tenant account, nome bucket, filtro avanzato o Noncurrent reference time). Poi seleziona **Select**.

   La finestra "Crea una policy" ora elenca le regole che hai selezionato. La regola predefinita è alla fine, con le altre regole sopra di essa.

Se il blocco degli oggetti S3 è abilitato e hai anche selezionato una regola "predefinita" non conforme, tale regola viene aggiunta come penultima regola nella policy.

> Viene visualizzato un avviso se una regola non conserva gli oggetti per sempre. Quando attivi questa policy, devi confermare che vuoi che StorageGRID elimini gli oggetti quando scadono le istruzioni di posizionamento della regola predefinita (a meno che un ciclo di vita del bucket mantenga gli oggetti per un periodo di tempo più lungo).

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

   Non puoi spostare la regola predefinita. Se S3 Object Lock è abilitato, non puoi spostare nemmeno la regola "default" non conforme, se ne è stata selezionata una.

   > Devi confermare che le regole ILM siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, partendo dall'alto.

9. Se necessario, seleziona **Seleziona regole** per aggiungere o rimuovere regole.
10. Al termine, seleziona **Salva**.
11. Ripeti questi passaggi per creare ulteriori criteri ILM.
12. Simula una policy ILM. Dovresti sempre simulare una policy prima di attivarla per assicurarti che funzioni come previsto.

Simula una policy

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

Prima di iniziare

- Conosci il bucket S3/la chiave dell'oggetto per ogni oggetto che vuoi testare.

Passaggi

1. Utilizzando un client S3 o "Console S3", importa gli oggetti necessari per testare ogni regola.
2. Nella pagina delle policy di ILM, seleziona la casella di controllo corrispondente alla policy, quindi seleziona **Simula**.
3. Nel campo **Oggetto**, inserisci l'S3 `bucket/object-key` per un oggetto di prova. Ad esempio, `bucket-01/filename.png`.
4. Se il versioning S3 è abilitato, puoi inserire facoltativamente un ID di versione per l'oggetto nel campo **ID versione**.
5. Seleziona **Simula**.
6. Nella sezione Risultati della simulazione, conferma che ogni oggetto sia stato abbinato alla regola corretta.
7. Per determinare quale pool di storage o profilo di codifica di cancellazione è attivo, seleziona il nome della regola corrispondente per andare alla pagina dei dettagli della regola.

> Esamina qualsiasi modifica al posizionamento degli oggetti replicati ed erasure-coded esistenti. Cambiare la posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando vengono valutati e implementati i nuovi posizionamenti.

Risultati

Qualsiasi modifica alle regole della policy si rifletterà nei risultati della simulazione e mostrerà la nuova corrispondenza e la corrispondenza precedente. La finestra Simula policy conserva gli oggetti che hai testato finché non selezioni **Cancella tutto** o l'icona di rimozione ✕ per ciascun oggetto nell'elenco dei risultati della simulazione.

Informazioni correlate

"Esempi di simulazioni di policy ILM"

Attiva una policy

Quando attivi una singola nuova policy ILM, gli oggetti esistenti e quelli appena acquisiti sono gestiti da quella policy. Quando attivi più policy, i tag delle policy ILM assegnati ai bucket determinano quali oggetti devono essere gestiti.

Prima di attivare una nuova policy:

1. Simula la policy per confermare che si comporta come ti aspetti.
2. Esamina qualsiasi modifica al posizionamento degli oggetti replicati ed erasure-coded esistenti. Cambiare la posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando vengono valutati e implementati i nuovi posizionamenti.

> ⚠ Gli errori in una policy ILM possono causare una perdita di dati irreversibile.

Informazioni su questa attività

Quando attivi una policy ILM, il sistema distribuisce la nuova policy a tutti i nodi. Tuttavia, la nuova policy attiva potrebbe non entrare effettivamente in vigore finché tutti i nodi della griglia non sono disponibili a ricevere la nuova policy. In alcuni casi, il sistema aspetta a implementare una nuova policy attiva per assicurarsi che gli oggetti della griglia non vengano rimossi accidentalmente. Nello specifico:

- Se apporti modifiche ai criteri che **aumentano la ridondanza o la durabilità dei dati**, tali modifiche vengono implementate immediatamente. Ad esempio, se attivi un nuovo criterio che include una regola a tre copie anziché a due, tale criterio verrà implementato immediatamente perché aumenta la ridondanza.
- Se apporti modifiche ai criteri che **potrebbero ridurre la ridondanza o la durabilità dei dati**, tali modifiche non saranno implementate finché tutti i nodi della griglia non saranno disponibili. Ad esempio, se attivi un nuovo criterio che utilizza una regola a due copie anziché a tre, il nuovo criterio verrà visualizzato nella scheda Criteri attivi ma non avrà effetto finché tutti i nodi non saranno online e disponibili.

Passaggi

Segui i passaggi per attivare una o più policy:

Attiva una policy

Segui questi passaggi se hai una sola policy attiva. Se hai già una o più policy attive e ne stai attivando altre, segui i passaggi per attivare più policy.

1. Quando sei pronto ad attivare una policy, seleziona **ILM** > **Policies**.

   In alternativa, puoi attivare una singola policy dalla pagina **ILM** > **Policy tags**.

2. Nella scheda Criteri, seleziona la casella di controllo corrispondente al criterio che vuoi attivare, quindi seleziona **Attiva**.
3. Segui il passaggio appropriato:
   - Se viene visualizzato un messaggio di avviso che ti chiede di confermare che vuoi attivare il criterio, seleziona **OK**.
   - Se viene visualizzato un messaggio di avviso contenente dettagli sulla policy:
     i. Esamina i dettagli per assicurarti che la policy gestisca i dati come previsto.
     ii. Se la regola predefinita prevede la conservazione degli oggetti per un numero limitato di giorni, consulta il diagramma di conservazione e poi inserisci quel 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, digita **yes** nella casella di testo.
     iv. Seleziona **Attiva policy**.

Attiva più criteri

Per attivare più criteri, devi creare dei tag per i criteri e assegnare un criterio a ciascun tag. Puoi creare un massimo di 10 tag per i criteri per la tua grid.

> Quando si utilizzano più tag di policy, se i tenant riassegnano frequentemente i tag di policy ai bucket, le prestazioni della grid potrebbero risentirne. Se hai tenant non attendibili, valuta di usare solo il tag di policy Default.

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

   > I nomi e le descrizioni dei tag sono visibili ai tenant. Scegli valori che aiutino i tenant a prendere una decisione informata quando selezionano i tag delle policy da assegnare ai loro bucket. Ad esempio, se la policy assegnata eliminerà gli oggetti dopo un certo periodo di tempo, puoi comunicarlo nella descrizione. Non includere informazioni sensibili in questi campi.

4. Seleziona **Crea tag**.
5. Nella tabella dei tag delle policy ILM, usa il menu a tendina per selezionare una policy da assegnare al tag.
6. Se nella colonna Limitazioni della policy compaiono degli avvisi, seleziona **Visualizza dettagli della policy** per esaminare la policy.

7. Assicurati che ogni policy gestisca i dati come previsto.
8. Seleziona **Attiva i criteri assegnati**. Oppure seleziona **Cancella modifiche** per rimuovere l'assegnazione dei criteri.
9. Nella finestra di dialogo Attiva criteri con nuovi tag, esamina le descrizioni di come ogni tag, criterio e regola gestirà gli oggetti. Apporta le modifiche necessarie per garantire che i criteri gestiscano gli oggetti come previsto.
10. Quando sei sicuro di voler attivare i criteri, digita **yes** nella casella di testo, quindi seleziona **Attiva criteri**.

Informazioni correlate

"Esempio 6: Modifica di una policy ILM"

Esempi di simulazioni di policy ILM in StorageGRID

Gli esempi di simulazioni delle policy ILM forniscono linee guida per strutturare e modificare le simulazioni per il tuo ambiente.

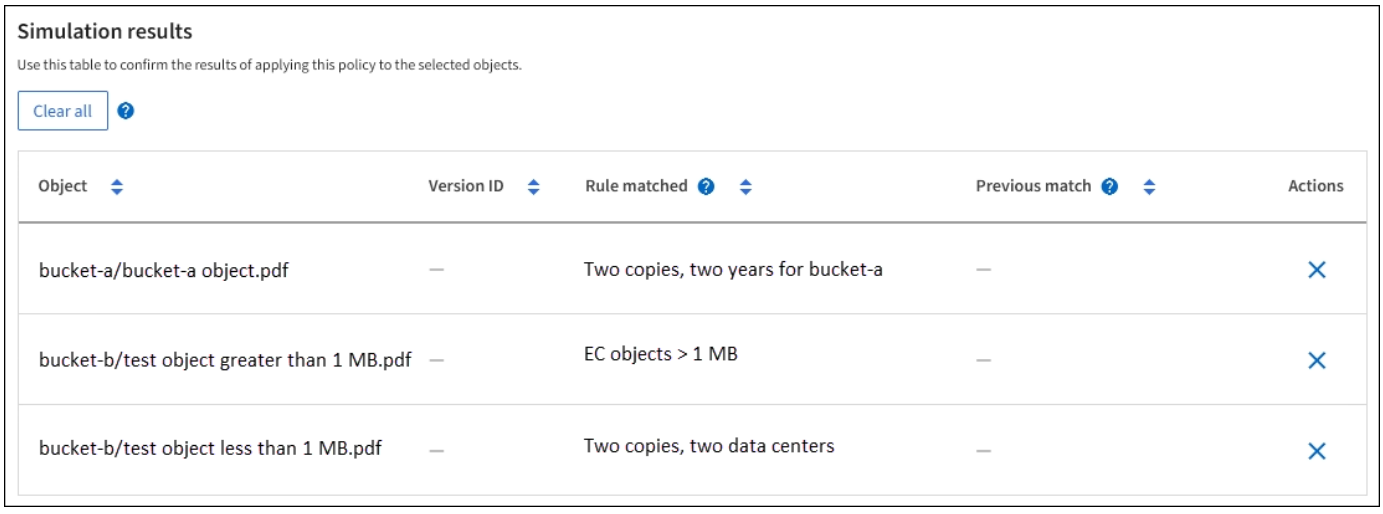
Esempio 1: Verifica le regole durante la simulazione di una policy ILM

Questo esempio descrive come verificare le regole quando si simula una policy.

In questo esempio, la **Example ILM policy** viene simulata sugli 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 in bucket-a.
- La seconda regola, **oggetti EC > 1 MB**, si applica a tutti i bucket ma filtra gli oggetti superiori a 1 MB.
- La terza regola, **Due copie, due data center**, è la regola predefinita. Non include alcun filtro e non utilizza il Noncurrent reference time.

Dopo aver simulato la policy, conferma che a ciascun oggetto sia stata associata la regola corretta.



In questo esempio:

- `bucket-a/bucket-a object.pdf`ha correttamente abbinato la prima regola, che filtra gli oggetti in `bucket-a.

- `bucket-b/test object greater than 1 MB.pdf` è in `bucket-b`, quindi non corrispondeva alla prima regola. Invece, è stato correttamente abbinato dalla seconda regola, che filtra gli oggetti di dimensioni superiori a 1 MB.
- `bucket-b/test object less than 1 MB.pdf`Non corrispondeva ai filtri delle prime due regole, quindi verrà applicata la regola predefinita, che non include filtri.

Esempio 2: Riordina le regole quando simuli una policy ILM

Questo esempio mostra come puoi riordinare le regole per modificare i risultati quando simuli una policy.

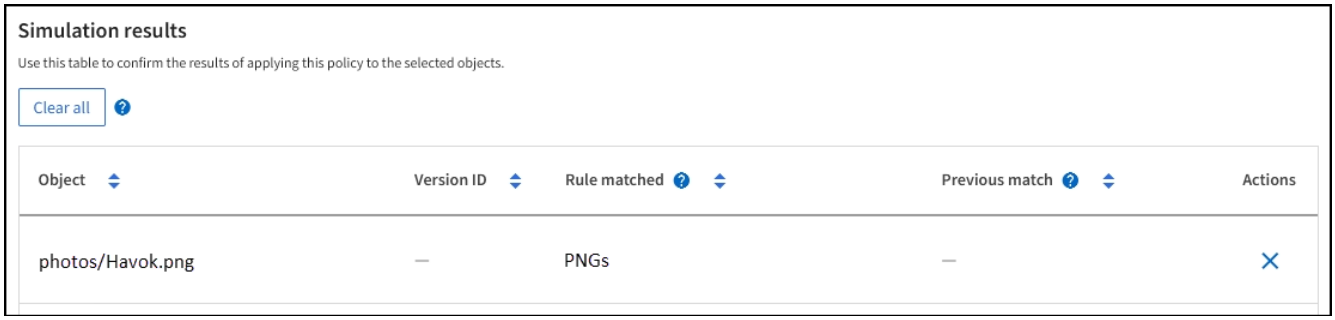
In questo esempio, si sta simulando la policy **Demo**. Questa policy, che ha lo scopo di trovare oggetti che hanno metadati utente series=x-men, include tre regole, come segue:

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

Passaggi

1. Dopo aver aggiunto le regole e salvato i criteri, seleziona **Simula**.
2. Nel campo **Oggetto**, inserisci il bucket S3/la chiave oggetto per un oggetto di test e seleziona **Simula**.

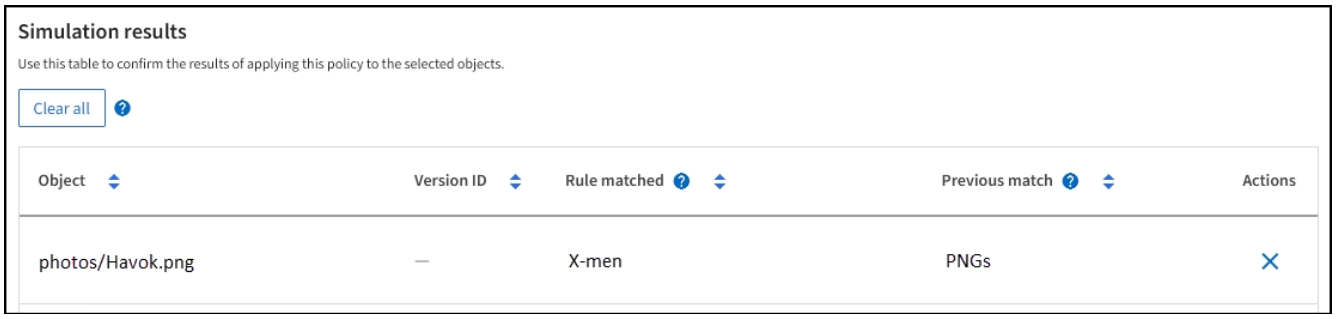
   I risultati della simulazione vengono visualizzati e mostrano che l'oggetto `Havok.png` è stato abbinato dalla regola **PNGs**.



   Tuttavia, `Havok.png` era pensato per testare la regola degli **X-men**.

3. Per risolvere il problema, riordina le regole.
   a. Seleziona **Fine** per chiudere la finestra Simula criteri ILM.
   b. Seleziona **Modifica** per modificare la policy.
   c. Trascina la regola **X-men** in cima all'elenco.
   d. Seleziona **Salva**.
4. Seleziona **Simula**.

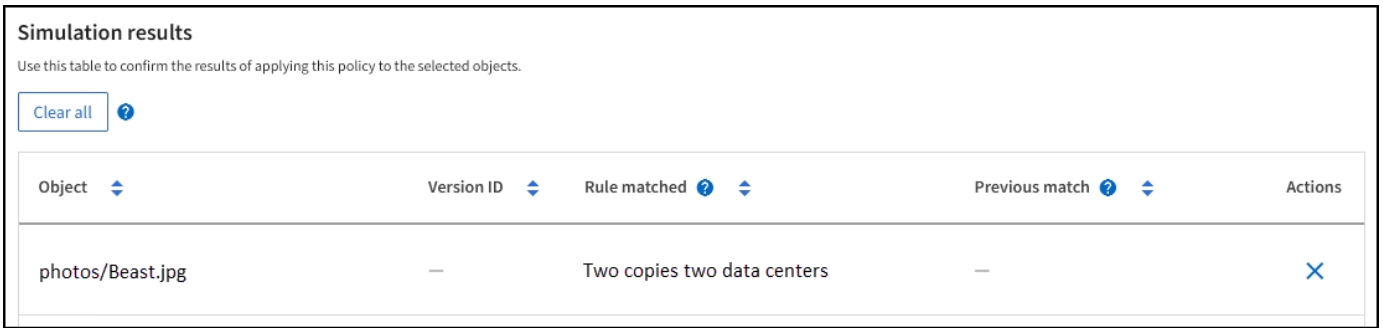
   Gli oggetti che hai testato in precedenza vengono rivalutati in base alla policy aggiornata e vengono mostrati i nuovi risultati della simulazione. Nell'esempio, la colonna "Regola corrispondente" mostra che l' `Havok.png`oggetto ora corrisponde alla regola dei metadati X-men, come previsto. La colonna "Corrispondenza precedente" mostra che la regola PNG corrispondeva all'oggetto nella simulazione precedente.



Esempio 3: Correggi una regola durante la simulazione di una policy ILM

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

In questo esempio, si sta simulando la policy **Demo**. Questa policy è pensata per trovare oggetti che hanno `series=x-men` metadati utente. Tuttavia, si sono verificati risultati inattesi quando hai simulato questa policy sull' `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati X-men, l'oggetto ha corrisposto alla regola predefinita, Due copie due data center.



Quando un oggetto di test non corrisponde alla regola prevista nella policy, devi esaminare ogni regola della policy e correggere eventuali errori.

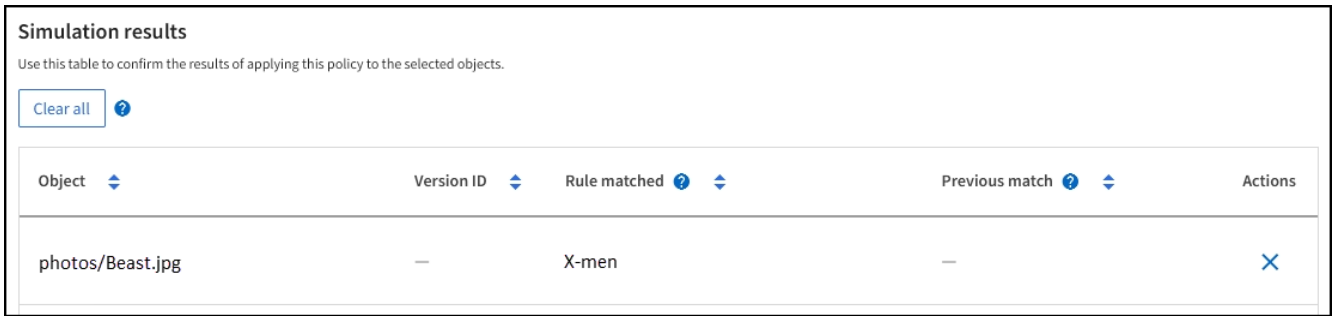
Passaggi

1. Seleziona **Fine** per chiudere la finestra di dialogo Simula policy. Nella pagina dei dettagli della policy, seleziona **Retention diagram**. Quindi seleziona **Espandi tutto** o **Visualizza dettagli** per ogni regola, a seconda delle necessità.
2. Esamina il tenant account della regola, il periodo di riferimento e i criteri di filtraggio.

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

3. Per risolvere l'errore, correggi la regola come segue:
   - Se la regola fa parte della policy, puoi clonare la regola oppure rimuoverla dalla policy e poi modificarla.
   - Se la regola fa parte della policy attiva, devi clonare la regola. Non puoi modificare o rimuovere una regola dalla policy attiva.
4. Esegui di nuovo la simulazione.

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



Gestisci i tag dei criteri ILM in StorageGRID

Puoi visualizzare i dettagli dei tag delle policy ILM, modificare un tag o rimuovere un tag.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Tu hai il "autorizzazioni di accesso richieste".

Visualizza i dettagli del tag di policy ILM

Per visualizzare i dettagli di un tag:

1. Seleziona **ILM** > **Policy tags**.
2. Seleziona il nome della policy dalla tabella. Viene visualizzata la pagina dei dettagli del tag.
3. Nella pagina dei dettagli, visualizza la cronologia precedente delle policy assegnate.
4. Visualizza una policy selezionandola.

Modifica il tag della policy ILM

> I nomi e le descrizioni dei tag sono visibili ai tenant. Scegli valori che aiutino i tenant a prendere una decisione informata quando selezionano i tag delle policy da assegnare ai loro bucket. Ad esempio, se la policy assegnata eliminerà gli oggetti dopo un certo periodo di tempo, puoi comunicarlo nella descrizione. Non includere informazioni sensibili in questi campi.

Per modificare la descrizione di un tag esistente:

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

   In alternativa, seleziona il nome del tag. Viene visualizzata la pagina dei dettagli del tag e puoi selezionare **Modifica** su quella pagina.

3. Modifica la descrizione del tag secondo necessità
4. Seleziona **Salva**.

Rimuovi il tag della policy ILM

Quando rimuovi un tag di policy, a tutti i bucket a cui è assegnato quel tag verrà applicata la policy predefinita.

Per rimuovere un tag:

1. Seleziona **ILM** > **Policy tags**.
2. Seleziona la casella di controllo corrispondente al tag, quindi seleziona **Rimuovi**. Viene visualizzata una finestra di dialogo di conferma.

   In alternativa, seleziona il nome del tag. Viene visualizzata la pagina dei dettagli del tag e puoi selezionare **Rimuovi** in quella pagina.

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

Informazioni correlate

"Scopri come creare tag di policy ILM"

Verifica una policy ILM con la ricerca dei metadati degli oggetti in StorageGRID

Dopo aver attivato una policy ILM, importa oggetti di test rappresentativi nel sistema StorageGRID, quindi esegui una ricerca dei metadati degli oggetti per confermare che le copie vengano create come previsto e posizionate nelle posizioni corrette.

Prima di iniziare

Hai un identificatore di oggetto, che può essere uno dei seguenti:

- **UUID**: L'Universally Unique Identifier dell'oggetto.
- **CBID**: Identificativo univoco dell'oggetto all'interno di StorageGRID. Puoi ottenere il CBID di un oggetto dal registro di audit. Inserisci il CBID tutto in maiuscolo.
- **Bucket S3 e chiave dell'oggetto**: Quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di bucket e chiave dell'oggetto per archiviare e identificare l'oggetto. Se il bucket S3 è versionato e vuoi cercare una versione specifica di un oggetto S3 utilizzando il bucket e la chiave dell'oggetto, hai l'**ID di versione**.

Passaggi

1. Acquisisci l'oggetto.
2. Seleziona **ILM** > **Object metadata lookup**.
3. Inserisci l'identificativo dell'oggetto nel campo **Identifier**. Puoi inserire un UUID, un CBID o una chiave bucket/object-key S3.
4. Facoltativamente, inserisci un ID di versione per l'oggetto (solo S3).
5. Seleziona **Look Up**.

   Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. Questa pagina elenca le seguenti tipologie di informazioni:

   - Metadati di sistema, come l'ID dell'oggetto (UUID), il tipo di risultato (oggetto, indicatore di eliminazione, bucket S3) e la dimensione logica dell'oggetto. Consulta lo screenshot di esempio qui sotto per maggiori dettagli.
   - ${post_edited_translations.segment}
   - Per gli oggetti S3, tutte le coppie chiave-valore dei tag associate all'oggetto.
   - ${post_edited_translations.segment}
   - Per le copie di oggetti con codifica di cancellazione, la posizione di archiviazione 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'identificativo univoco dell'oggetto.
- Per gli oggetti segmentati e gli oggetti composti da più parti, viene visualizzato un elenco dei segmenti dell'oggetto, inclusi gli identificatori dei segmenti e le dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono mostrati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati di sistema interni che non è garantito persistano da una release all'altra.

6. Conferma che l'oggetto sia memorizzato nella posizione o nelle posizioni corrette e che sia il tipo di copia corretto.

   Se l'opzione Audit è abilitata, puoi anche monitorare il registro di controllo per il messaggio ORLM Object Rules Met. Il messaggio di audit ORLM può darti più informazioni sullo stato del processo di valutazione ILM, ma non può darti informazioni sulla correttezza del posizionamento dei dati dell'oggetto o sulla completezza della policy ILM. Devi valutare tu stesso questo aspetto. Per dettagli, vedi "${post_edited_translations.segment}".

Il seguente esempio mostra i risultati della ricerca dei metadati di un oggetto di test S3 archiviato come due copie replicate.

> La seguente screenshot è un esempio. I risultati varieranno a seconda della versione di StorageGRID.

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

"${post_edited_translations.segment}"

Lavora con le policy ILM e le regole ILM in StorageGRID

Poiché le tue esigenze di storage cambiano, potresti dover implementare criteri aggiuntivi o modificare le regole ILM associate a un criterio. Puoi visualizzare le metriche ILM per determinare le prestazioni del sistema.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Visualizza le policy di ILM

Per visualizzare le policy ILM attive e inattive e la cronologia di attivazione delle policy:

1. Seleziona **ILM** > **Policies**.
2. Seleziona **Policies** per visualizzare un elenco delle policies attive e inattive. La tabella elenca il nome di ciascuna policy, i tag a cui è assegnata e se la policy è attiva o inattiva.
3. Seleziona **Cronologia attivazioni** per visualizzare un elenco delle date di inizio e fine attivazione delle policy.
4. Seleziona un nome di policy per visualizzarne i dettagli.

> Se visualizzi i dettagli di una policy il cui stato è Modificato o Eliminato, viene visualizzato un messaggio che spiega che stai visualizzando la versione della policy che era attiva per il periodo di tempo specificato e che da allora è stata modificata o eliminata.

Modifica una policy ILM

Puoi modificare solo una policy inattiva. Se vuoi modificare una policy attiva, disattivala oppure crea un clone e modifica il clone.

Per modificare una policy:

1. Seleziona **ILM** > **Policies**.
2. Seleziona la casella di controllo corrispondente alla policy che vuoi modificare, poi seleziona **Modifica**.
3. Modifica la policy seguendo le istruzioni in "${post_edited_translations.segment}".
4. Simula la policy prima di riattivarla.

> Una policy ILM configurata in modo errato può causare una perdita di dati irreversibile. Prima di attivare una policy ILM, esaminala attentamente, verifica le relative regole ILM e poi simula la policy ILM. Assicurati sempre che la policy ILM funzioni come previsto.

Clona una policy ILM

Per clonare una policy ILM:

1. Seleziona **ILM** > **Policies**.
2. Seleziona la casella di controllo corrispondente al criterio che vuoi clonare, poi seleziona **Clona**.
3. Crea una nuova policy partendo dalla policy che hai clonato seguendo le istruzioni in "${post_edited_translations.segment}".

> Una policy ILM configurata in modo errato può causare una perdita di dati irreversibile. Prima di attivare una policy ILM, esaminala attentamente, verifica le relative regole ILM e poi simula la policy ILM. Assicurati sempre che la policy ILM funzioni come previsto.

Rimuovi una policy ILM

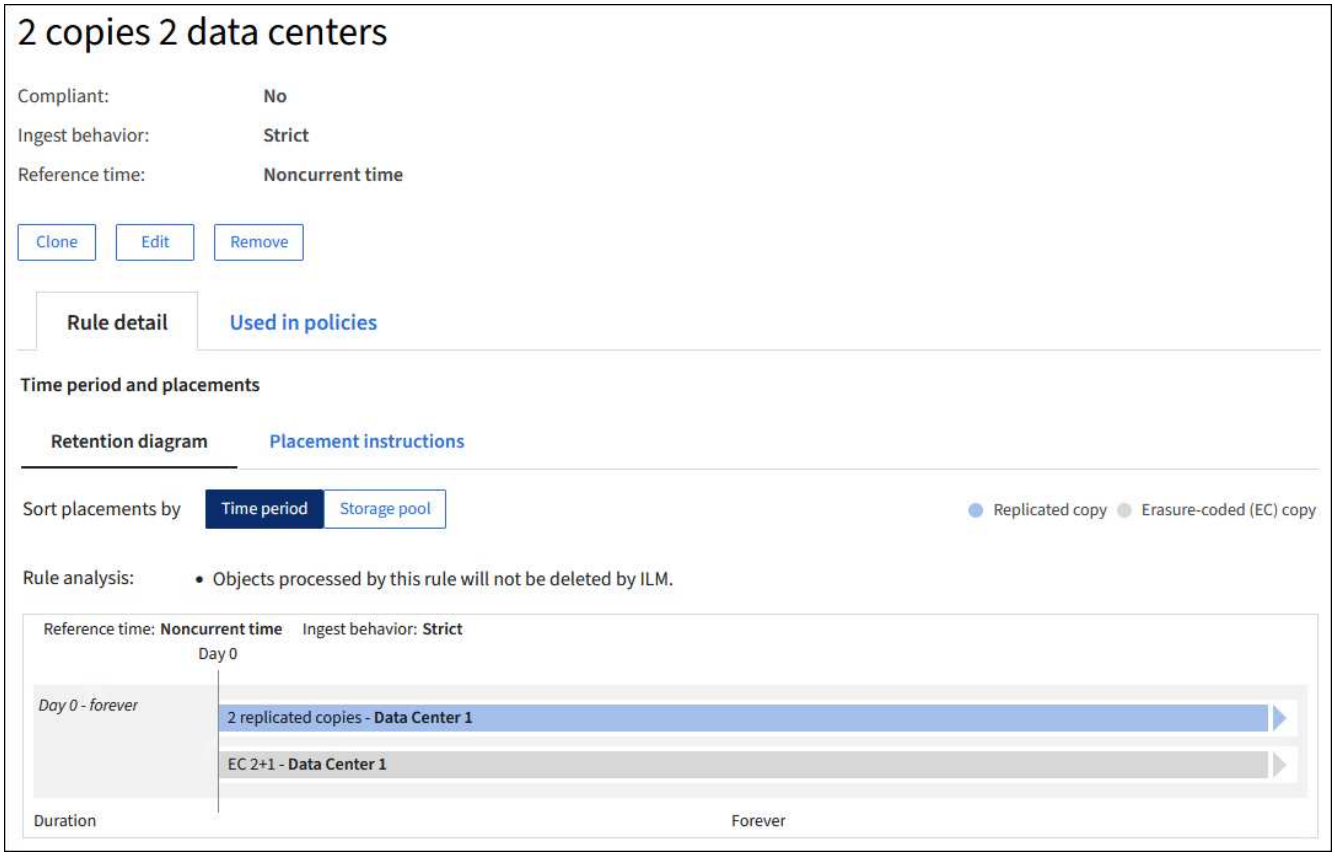
Puoi rimuovere una policy ILM solo se è inattiva. Per rimuovere una policy:

1. Seleziona **ILM** > **Policies**.
2. Seleziona la casella di controllo corrispondente al criterio inattivo che vuoi rimuovere.
3. Seleziona **Rimuovi**.

Visualizza i dettagli della regola ILM

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

1. Seleziona **ILM** > **Regole**.
2. Seleziona il nome della regola di cui desideri visualizzare i dettagli. Esempio:



Inoltre, puoi utilizzare la pagina dei dettagli per clonare, modificare o rimuovere una regola. Non puoi modificare o rimuovere una regola se è utilizzata in una qualsiasi policy.

Clona una regola ILM

Puoi clonare una regola esistente se vuoi creare una nuova regola che utilizza alcune delle impostazioni della regola esistente. Se hai bisogno di modificare una regola utilizzata in una policy, clona invece la regola e apporta le modifiche alla copia. Dopo aver apportato le modifiche alla copia, puoi rimuovere la regola originale dalla policy e sostituirla con la versione modificata, se necessario.

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

Passaggi

1. Seleziona **ILM** > **Regole**.
2. Seleziona la casella di controllo corrispondente alla regola che desideri clonare, quindi seleziona **Clona**. In alternativa, seleziona il nome della regola, quindi seleziona **Clona** dalla pagina dei dettagli della regola.
3. Aggiorna la regola clonata seguendo i passaggi per modifica di una regola ILM e "utilizzare filtri avanzati

nelle regole ILM".

Quando cloni una regola ILM, devi inserire un nuovo nome.

Modifica una regola ILM

Potresti dover modificare una regola ILM per cambiare un filtro o un'istruzione di posizionamento.

Non puoi modificare una regola se viene utilizzata in una policy ILM. Invece, puoi clonare la regola e apportare le modifiche necessarie alla copia clonata.

> Una policy ILM configurata in modo errato può causare una perdita di dati irreversibile. Prima di attivare una policy ILM, esaminala attentamente, verifica le relative regole ILM e poi simula la policy ILM. Assicurati sempre che la policy ILM funzioni come previsto.

Passaggi

1. Seleziona **ILM** > **Regole**.
2. Conferma che la regola che vuoi modificare non sia utilizzata in nessuna policy ILM.
3. Se la regola che vuoi modificare non è in uso, seleziona la casella di controllo della regola e seleziona **Azioni** > **Modifica**. In alternativa, seleziona il nome della regola, poi seleziona **Modifica** nella pagina dei dettagli della regola.
4. Completa i passaggi della procedura guidata Modifica regola ILM. Se necessario, segui i passaggi per "creare una regola ILM" e "utilizzare filtri avanzati nelle regole ILM".

   Quando modifichi una regola ILM, non puoi cambiarne il nome.

Rimuovi una regola ILM

Per mantenere gestibile l'elenco delle regole ILM correnti, rimuovi tutte le regole ILM che probabilmente non utilizzerai.

Passaggi

Per rimuovere una regola ILM attualmente utilizzata in una policy attiva:

1. Clona la policy.
2. Rimuovi la regola ILM dal clone della policy.
3. Salva, simula e attiva la nuova policy per assicurarti che gli oggetti siano protetti come previsto.
4. Vai ai passaggi per rimuovere una regola ILM attualmente utilizzata in una policy inattiva.

Per rimuovere una regola ILM attualmente utilizzata in una policy inattiva:

1. Seleziona la policy inattiva.
2. Rimuovi la regola ILM dalla policy o rimuovi la policy.
3. Vai ai passaggi per rimuovere una regola ILM che non è attualmente in uso.

Per rimuovere una regola ILM attualmente non in uso:

1. Seleziona **ILM** > **Regole**.

2. Verifica che la regola che vuoi rimuovere non sia utilizzata in nessuna policy.
3. Se la regola che desideri rimuovere non è in uso, seleziona la regola e seleziona **Azioni** > **Rimuovi**. Puoi selezionare più regole e rimuoverle tutte contemporaneamente.
4. Seleziona **Sì** per confermare che vuoi rimuovere la regola ILM.

Visualizza metriche ILM

Puoi visualizzare le metriche per ILM, come il numero di oggetti in coda e il tasso di valutazione. Puoi monitorare queste metriche per determinare le prestazioni del sistema. Una coda di grandi dimensioni o un tasso di valutazione elevato potrebbero indicare che il sistema non riesce a tenere il passo con il tasso di acquisizione, che il carico dalle applicazioni client è eccessivo o che esiste una condizione anomala.

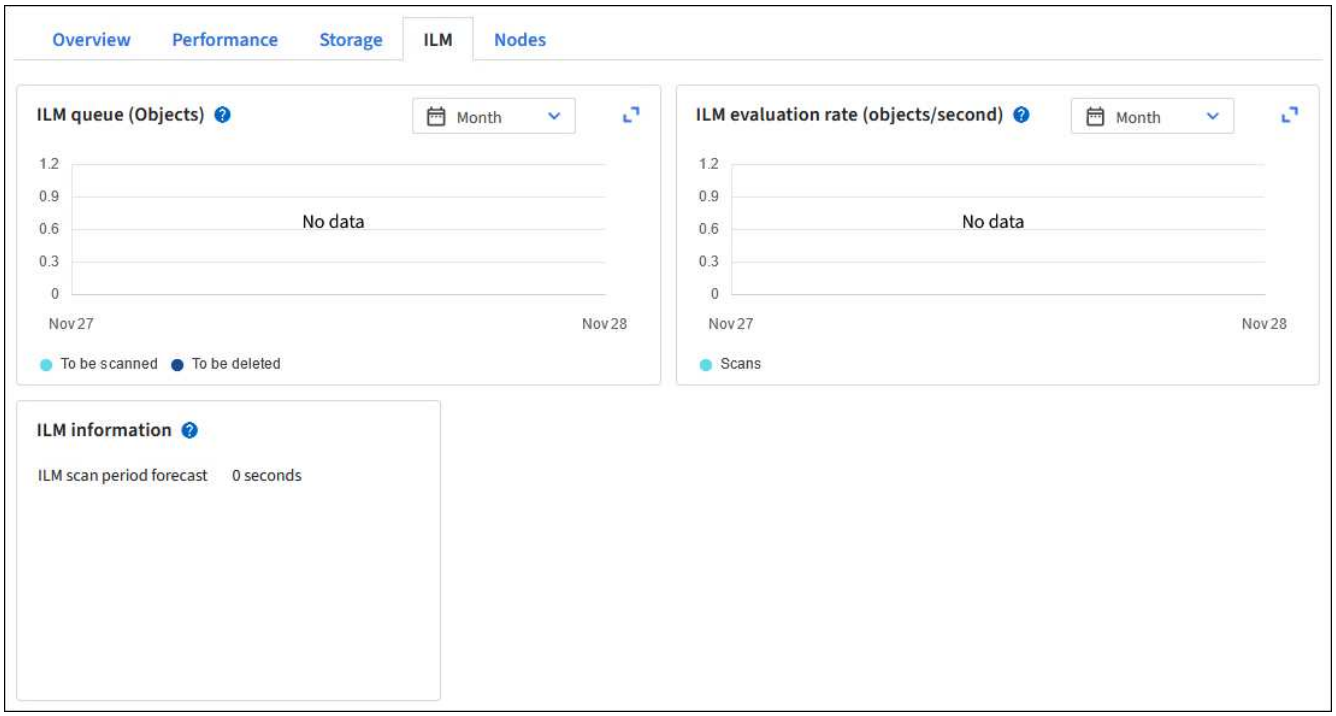
Passaggi

1. Seleziona **Dashboard** > **ILM**.

   Poiché la dashboard è personalizzabile, la scheda ILM potrebbe non essere disponibile.

2. Monitora le metriche nella scheda ILM.

   Puoi selezionare il punto interrogativo per vedere una descrizione degli elementi nella scheda ILM.



Usa il blocco oggetto S3

Come S3 Object Lock protegge gli oggetti in StorageGRID

Come amministratore della griglia, puoi abilitare S3 Object Lock per il tuo sistema StorageGRID e implementare una policy ILM conforme per assicurarti che gli oggetti in specifici bucket S3 non vengano eliminati o sovrascritti per un periodo di tempo specificato.

Che cos'è S3 Object Lock?

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

Quando l'impostazione globale S3 Object Lock è abilitata per un sistema StorageGRID, un tenant account S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock abilitato, il versioning del bucket è obbligatorio e viene abilitato automaticamente.

Un bucket senza S3 Object Lock può contenere solo oggetti per i quali non sono specificate impostazioni di conservazione. Nessun oggetto ingerito avrà impostazioni di conservazione.

Un bucket con S3 Object Lock può contenere oggetti con o senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con S3 Object Lock e periodo di conservazione predefinito configurato può avere oggetti caricati con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, perché l'impostazione di conservazione non è stata configurata a livello di oggetto.

In pratica, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurato il periodo di conservazione predefinito. Gli oggetti esistenti senza impostazioni di conservazione rimangono invariati.

Modalità di retention

La funzionalità S3 Object Lock di StorageGRID supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità sono equivalenti alle modalità di conservazione di Amazon S3.

- In modalità conformità:
  - L'oggetto non può essere eliminato fino al raggiungimento della sua retain-until-date.
  - La data di conservazione dell'oggetto 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 determinate impostazioni di conservazione.
  - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione prevista.
  - Questi utenti possono aumentare, diminuire o rimuovere la retain-until-date di un oggetto.

Impostazioni di conservazione per le versioni degli oggetti

Se crei un bucket con la funzionalità S3 Object Lock abilitata, puoi usare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione**: conformità o governance.
- **Retain-until-date**: Se la retain-until-date di una versione dell'oggetto è nel futuro, l'oggetto può essere recuperato, ma non può essere eliminato.
- **Blocco legale**: L'applicazione di un blocco legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potresti dover applicare un blocco legale a un oggetto che è collegato a un'indagine o a una controversia legale. Un blocco legale non ha una data di scadenza, ma rimane in vigore finché non viene esplicitamente rimosso. I blocchi legali sono indipendenti dalla retain-until-date.

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

Per i dettagli sulle impostazioni dell'oggetto, vedi "Utilizza l'API REST S3 per configurare S3 Object Lock".

Impostazione di conservazione predefinita per i bucket

Se crei un bucket con S3 Object Lock abilitato, puoi facoltativamente specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita**: conformità o governance.
- **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 hanno le proprie impostazioni di conservazione. Gli oggetti esistenti nel bucket non vengono influenzati quando aggiungi o modifichi queste impostazioni predefinite.

Vedi "Crea un bucket S3" e "Aggiorna la conservazione predefinita del blocco oggetto S3".

Confronto tra S3 Object Lock e la Compliance legacy

La funzionalità S3 Object Lock sostituisce la funzionalità Compliance che era disponibile nelle versioni precedenti di StorageGRID. Poiché la funzionalità S3 Object Lock è conforme ai requisiti di Amazon S3, depreca la funzionalità proprietaria Compliance di StorageGRID, che ora viene chiamata "legacy Compliance".

L'impostazione globale di conformità è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione S3 Object Lock viene abilitata automaticamente. Puoi continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non puoi creare nuovi bucket conformi. Per dettagli, vedi "NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5".

Se hai utilizzato la funzione Compliance legacy in una versione precedente di StorageGRID, consulta la tabella seguente per scoprire come si confronta con la funzionalità S3 Object Lock in StorageGRID.

	Blocco oggetto S3	**Conformità (legacy)**
Come abiliti questa funzionalità a livello globale?	Dal Grid Manager, seleziona **Configurazione** > **Sistema** > **S3 Object Lock**.	Non più supportata.
Come abiliti questa funzionalità per un bucket?	Devi abilitare S3 Object Lock quando crei un nuovo bucket utilizzando il Tenant Manager, l'API di gestione del tenant o l'API REST S3.	Non più supportata.
È supportata la gestione delle versioni dei bucket?	Sì. Il versioning del bucket è obbligatorio e viene abilitato automaticamente quando S3 Object Lock è abilitato per il bucket.	No.

	Blocco oggetto S3	Conformità (legacy)
Come imposti la conservazione degli oggetti?	Gli utenti possono impostare una data di conservazione per ogni versione dell'oggetto, oppure possono impostare un periodo di conservazione predefinito per ogni bucket.	Devi 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 conformità, la retain-until-date per una versione di un oggetto può essere aumentata, ma mai diminuita. • 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 mai diminuito.
Dove si controlla il legal hold?	Puoi applicare o rimuovere un blocco legale per qualsiasi versione dell'oggetto nel bucket.	Un sequestro legale viene applicato al bucket e riguarda tutti gli oggetti nel bucket.
Quando puoi eliminare gli oggetti?	• In modalità conformità, una versione di un oggetto può essere eliminata dopo il raggiungimento della retain-until-date, a condizione che l'oggetto non sia soggetto a legal hold. • In modalità governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la sua retain-until-date, a condizione che l'oggetto non sia soggetto a legal hold.	Un oggetto può essere eliminato dopo la scadenza del periodo di conservazione, a condizione che il bucket non sia soggetto a blocco legale. Gli oggetti possono essere eliminati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	No

Flusso di lavoro S3 Object Lock in StorageGRID

Come amministratore della griglia, devi coordinarti strettamente con gli utenti tenant per assicurarti che gli oggetti siano protetti in modo da soddisfare i loro requisiti di conservazione.

L’applicazione delle impostazioni del tenant all’intera griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato dei nodi e delle operazioni di Cassandra.

I seguenti elenchi per gli amministratori della griglia e gli utenti tenant contengono le high-level attività per l’utilizzo della funzionalità S3 Object Lock.

Amministratore della grid

- Abilita l’impostazione globale di S3 Object Lock per l’intero sistema StorageGRID.
- Assicurati che le policy di information lifecycle management (ILM) siano *conformi*; cioè che soddisfino i "requisiti dei bucket con S3 Object Lock abilitato".
- Se necessario, consenti a un tenant di utilizzare Compliance come modalità di conservazione. Altrimenti, è consentita solo la modalità Governance.
- Se necessario, imposta un periodo massimo di conservazione per un tenant.

Utente tenant

- Esamina le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contatta l’amministratore della grid per abilitare l’impostazione globale S3 Object Lock e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, puoi configurare le impostazioni di conservazione predefinite per un bucket:
  - Modalità di conservazione predefinita: Governance o Compliance, se consentita dall’amministratore della grid.
  - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall’amministratore della griglia.
- Utilizza l’applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica per ciascun oggetto:
  - Modalità di conservazione. Governance o Compliance, se consentito dall’amministratore del grid.
  - Data di conservazione: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall’amministratore della griglia.

Requisiti di S3 Object Lock in StorageGRID

Devi esaminare i requisiti per abilitare l’impostazione globale S3 Object Lock, i requisiti per creare regole e policy ILM conformi e le restrizioni che StorageGRID impone ai bucket e agli oggetti che utilizzano S3 Object Lock.

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

- Devi abilitare l’impostazione globale S3 Object Lock usando il Grid Manager o la Grid Management API prima che qualsiasi tenant possa creare un bucket con S3 Object Lock abilitato.
- L’attivazione dell’impostazione globale S3 Object Lock permette a tutti gli account tenant S3 di creare bucket con S3 Object Lock abilitato.
- Dopo che hai attivato l’impostazione globale S3 Object Lock, non puoi disattivarla.
- Non puoi abilitare il blocco globale degli oggetti S3 a meno che la regola predefinita in tutte le policy ILM attive non sia *conforme* (cioè, la regola predefinita deve essere conforme ai requisiti dei bucket con S3 Object Lock abilitato).

- Quando l'impostazione globale S3 Object Lock è abilitata, non puoi creare una nuova policy ILM o attivare una policy ILM esistente a meno che la regola predefinita nella policy sia conforme. Dopo che l'impostazione globale S3 Object Lock è stata abilitata, le pagine delle regole ILM e delle policy ILM indicano quali regole ILM sono conformi.

Requisiti per le regole ILM conformi

Se vuoi abilitare l'impostazione globale S3 Object Lock, devi assicurarti che la regola predefinita in tutte le policy ILM attive sia conforme. Una regola conforme soddisfa i requisiti sia dei bucket con S3 Object Lock abilitato sia di tutti i bucket esistenti che hanno la Compliance legacy abilitata:

- Devi creare almeno due copie replicate dell'oggetto o una copia con codifica di cancellazione.
- Queste copie devono esistere sui nodi di archiviazione per tutta la durata di ogni riga delle istruzioni di posizionamento.
- Non puoi salvare copie di oggetti in un Cloud Storage Pool.
- Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando **Ingest time** come orario di riferimento.
- Almeno una riga delle istruzioni per il posizionamento deve essere "per sempre".

Requisiti per le policy ILM

Quando l'impostazione globale di S3 Object Lock è abilitata, le policy ILM attive e inattive possono includere sia regole conformi che non conformi.

- La regola predefinita in una policy ILM attiva o inattiva deve essere conforme.
- Le regole di non conformità si applicano solo agli oggetti nei bucket che non hanno il blocco degli oggetti S3 abilitato o che non hanno la funzionalità di conformità legacy abilitata.
- Le regole di conformità possono essere applicate agli oggetti in qualsiasi bucket; non è necessario abilitare S3 Object Lock o legacy Compliance per il bucket.

"Esempio di una policy ILM conforme per S3 Object Lock"

Requisiti per i bucket con S3 Object Lock abilitato

- Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID, puoi usare il Tenant Manager, la Tenant Management API o la S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se intendi utilizzare S3 Object Lock, devi abilitarlo quando crei il bucket. Non puoi abilitare S3 Object Lock per un bucket esistente.
- Quando il blocco degli oggetti S3 è abilitato per un bucket, StorageGRID abilita automaticamente il versioning per quel bucket. Non puoi disabilitare il blocco degli oggetti S3 o sospendere il versioning per il bucket.
- Facoltativamente, puoi specificare una modalità di conservazione predefinita e un periodo di conservazione per ogni bucket utilizzando il Tenant Manager, la Tenant Management API o la S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non hanno proprie impostazioni di conservazione. Puoi ignorare queste impostazioni predefinite specificando una modalità di conservazione e una retain-until-date per ogni versione dell'oggetto quando viene caricata.
- La configurazione del ciclo di vita dei bucket è supportata per i bucket con S3 Object Lock abilitato.
- CloudMirror replication non è supportata per i bucket con S3 Object Lock abilitato.

Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato

- Per proteggere una versione di un oggetto, puoi specificare le impostazioni di conservazione predefinite per il bucket oppure puoi specificare le impostazioni di conservazione per ogni versione dell'oggetto. Le impostazioni di conservazione a livello di oggetto possono essere specificate usando l'applicazione client S3 o l'S3 REST API.
- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia una data di conservazione che un'impostazione di legal hold, una sola delle due oppure nessuna delle due. Specificare una data di conservazione o un'impostazione di legal hold per un oggetto protegge solo la versione specificata nella richiesta. Puoi creare nuove versioni dell'oggetto, mentre la versione precedente dell'oggetto rimane bloccata.

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

Ogni oggetto salvato in un bucket con S3 Object Lock abilitato attraversa queste fasi:

1. **Ingestione oggetto**

   Quando una versione di un oggetto viene aggiunta a un bucket che ha S3 Object Lock abilitato, le impostazioni di conservazione vengono applicate come segue:

   - Se per l'oggetto sono specificate delle impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Le impostazioni predefinite del bucket vengono ignorate.
   - Se non vengono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se esistono.
   - Se non vengono 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, sia l'oggetto che tutti i metadati S3 definiti dall'utente sono protetti.

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 di copie degli oggetti e le posizioni di archiviazione sono determinati dalle regole conformi nelle policy ILM attive. Se un oggetto protetto può essere eliminato prima che venga raggiunta la sua retain-until-date dipende dalla sua modalità di conservazione.

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

Informazioni correlate

- "Crea un bucket S3"
- "Aggiorna la conservazione predefinita del blocco oggetto S3"
- "Utilizza l'API REST S3 per configurare S3 Object Lock"
- "Esempio 7: Criterio ILM conforme per S3 Object Lock"

Abilita S3 Object Lock a livello globale in StorageGRID

Se un tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, devi abilitare S3 Object Lock per l'intero sistema StorageGRID. Abilitando l'impostazione globale S3 Object Lock, qualsiasi utente tenant S3 può creare e gestire

bucket e oggetti con S3 Object Lock.

Prima di iniziare

- Hai "Permesso di accesso root".
- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai esaminato il flusso di lavoro S3 Object Lock e ne comprendi le considerazioni.
- Hai confermato che la regola predefinita nella policy ILM attiva è conforme. Consulta "Crea una regola ILM predefinita" per i dettagli.

Informazioni su questa attività

Un amministratore della griglia deve abilitare l'impostazione globale Blocco oggetti S3 per consentire agli utenti del tenant di creare nuovi bucket con Blocco oggetti S3 abilitato. Una volta abilitata, questa impostazione non può essere disabilitata.

Rivedi le impostazioni di conformità dei tenant esistenti dopo aver abilitato l'impostazione globale S3 Object Lock. Quando abiliti questa impostazione, le impostazioni di S3 Object Lock per singolo tenant dipendono dalla versione di StorageGRID in vigore al momento della creazione del tenant.

> ⓘ L'impostazione globale di conformità è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione S3 Object Lock viene abilitata automaticamente. Puoi continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non puoi creare nuovi bucket conformi. Per dettagli, vedi "NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5".

Passaggi

1. Seleziona **Configurazione** > **Sistema** > **S3 Object Lock**.

   Viene visualizzata la pagina delle impostazioni di blocco degli oggetti S3.

2. Seleziona **Abilita S3 Object Lock**.
3. Seleziona **Applica**.

   Viene visualizzata una finestra di dialogo di conferma che ti ricorda che non puoi disabilitare S3 Object Lock dopo che è stato abilitato.

4. Se sei sicuro di voler abilitare in modo permanente S3 Object Lock per l'intero sistema, seleziona **OK**.

   Quando selezioni **OK**:

   - Se la regola predefinita nella policy ILM attiva è conforme, S3 Object Lock è ora abilitato per l'intera griglia e non può essere disabilitato.
   - Se la regola predefinita non è conforme, viene visualizzato un errore. Devi creare e attivare una nuova policy ILM che includa una regola conforme come regola predefinita. Seleziona **OK**. Poi crea una nuova policy, simulala e attivala. Vedi "Crea criteri ILM" per le istruzioni.

Risolvi gli errori di coerenza durante l'aggiornamento delle impostazioni di S3 Object Lock o di Compliance legacy in StorageGRID

Se un sito del data center o più Storage Node in un sito diventano non disponibili, potresti dover aiutare gli utenti tenant S3 ad applicare modifiche alla configurazione di S3 Object

Lock o di Compliance legacy.

Gli utenti tenant che dispongono di bucket con S3 Object Lock (o Compliance legacy) abilitato possono modificare determinate impostazioni. Ad esempio, un utente tenant che utilizza S3 Object Lock potrebbe dover mettere una versione di un oggetto sotto blocco legale.

Quando un utente tenant aggiorna le impostazioni di un bucket S3 o di una versione di oggetto, StorageGRID tenta di aggiornare immediatamente i metadati del bucket o dell'oggetto in tutta la grid. Se il sistema non riesce ad aggiornare i metadati perché un sito del data center o più Storage Node non sono disponibili, restituisce 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, segui questi passaggi:

1. Cerca di rendere nuovamente disponibili tutti i nodi di Storage o i siti il prima possibile.
2. Se non riesci a rendere disponibili un numero sufficiente di Storage Node in ciascun sito, contatta il supporto tecnico, che può aiutarti a recuperare i nodi e a garantire che le modifiche vengano applicate in modo coerente su tutta la grid.
3. Una volta risolto il problema di fondo, ricorda all'utente del tenant di riprovare a modificare la configurazione.

Informazioni correlate

- "Usa un tenant account"
- "${post_edited_translations.segment}"
- "Recupera e mantieni"

Esempi di regole e policy ILM

Regole e policy ILM per la protezione e la conservazione di base degli oggetti in StorageGRID

Puoi usare le seguenti regole e la seguente policy di esempio come punto di partenza quando definisci una policy ILM per soddisfare i tuoi requisiti di protezione e conservazione degli oggetti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per confermare che funzionerà come previsto per proteggere i contenuti dalla perdita.

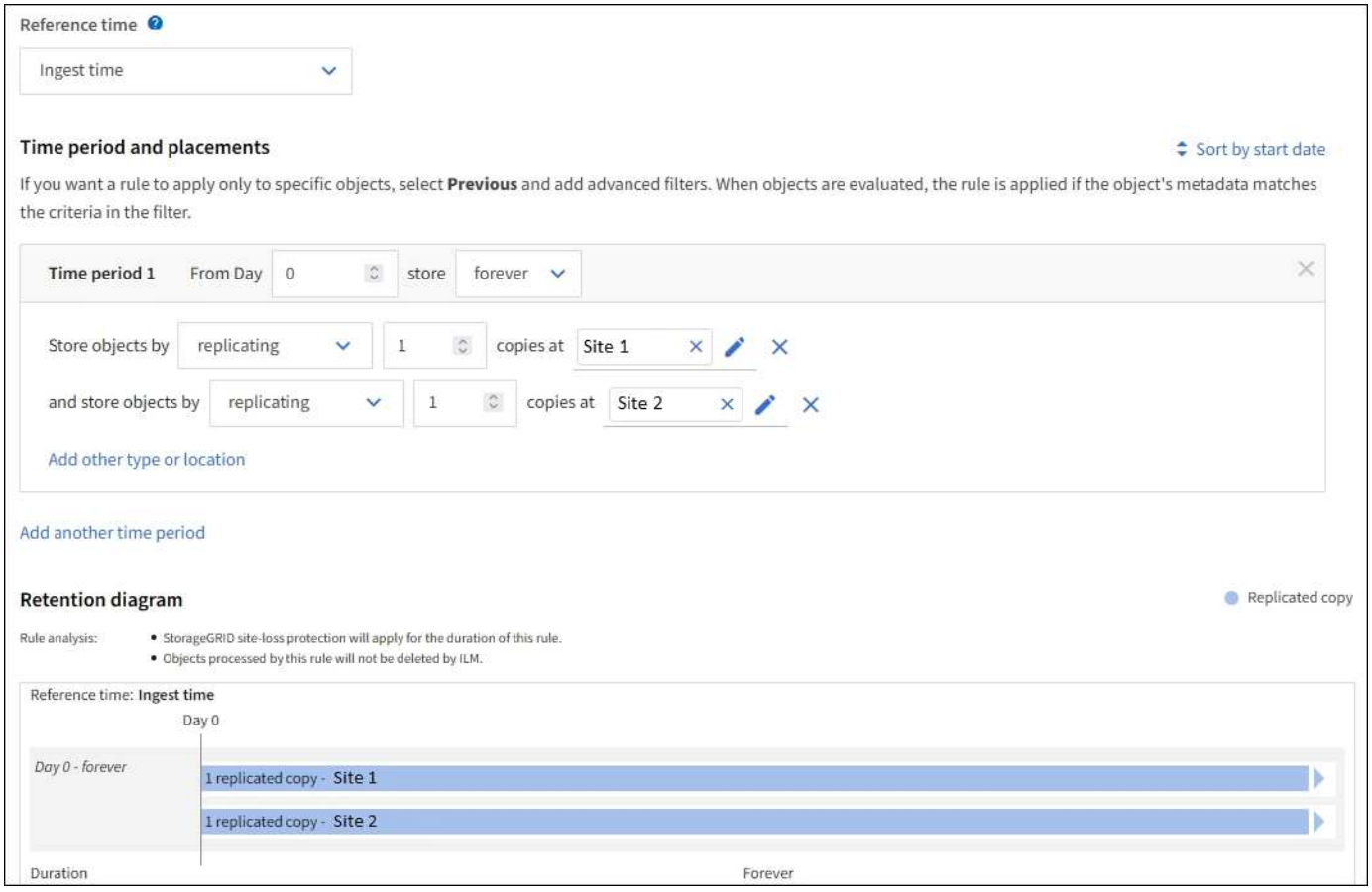
Regola ILM 1 per l'esempio 1: copia i dati dell'oggetto in due siti

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

Definizione della regola	Esempio di valore
Pool di storage in un unico sito	Due pool di storage, ciascuno contenente siti diversi, denominati Site 1 e Site 2.
Nome regola	Due copie due siti
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 in poi, tieni una copia replicata presso il Sito 1 e una copia replicata presso il Sito 2.

La sezione di analisi delle regole del diagramma di retention afferma:

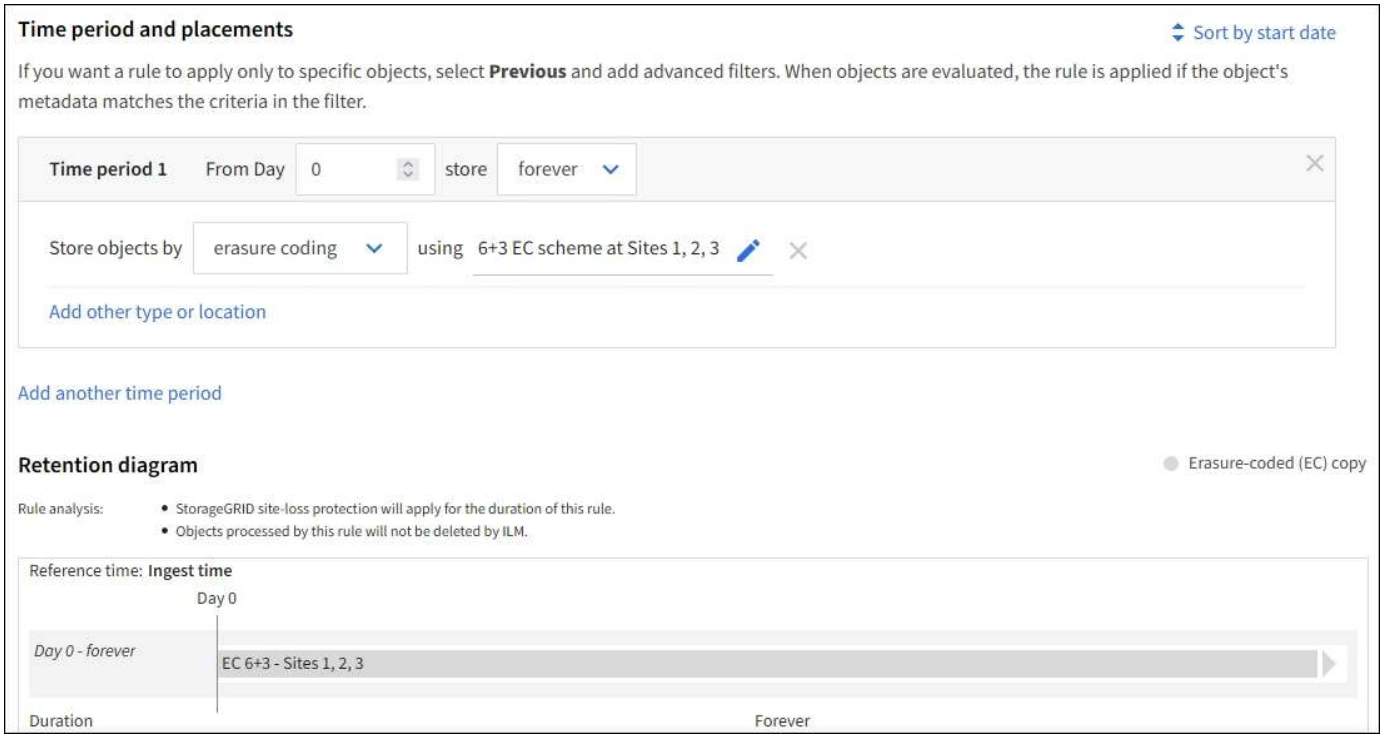
- La protezione contro la perdita di sito di StorageGRID sarà applicata per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola non verranno eliminati da ILM.



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

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

Definizione della regola	Esempio di valore
Pool di storage con più siti	• Un unico pool di storage su tre siti (Siti 1, 2, 3) • Usa lo schema di codifica a cancellazione 6+3
Nome regola	Bucket S3 finance-records
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Per gli oggetti nel bucket S3 denominato finance-records, crea una copia con codifica di cancellazione nel pool specificato dal profilo di codifica di cancellazione. Conserva questa copia per sempre.

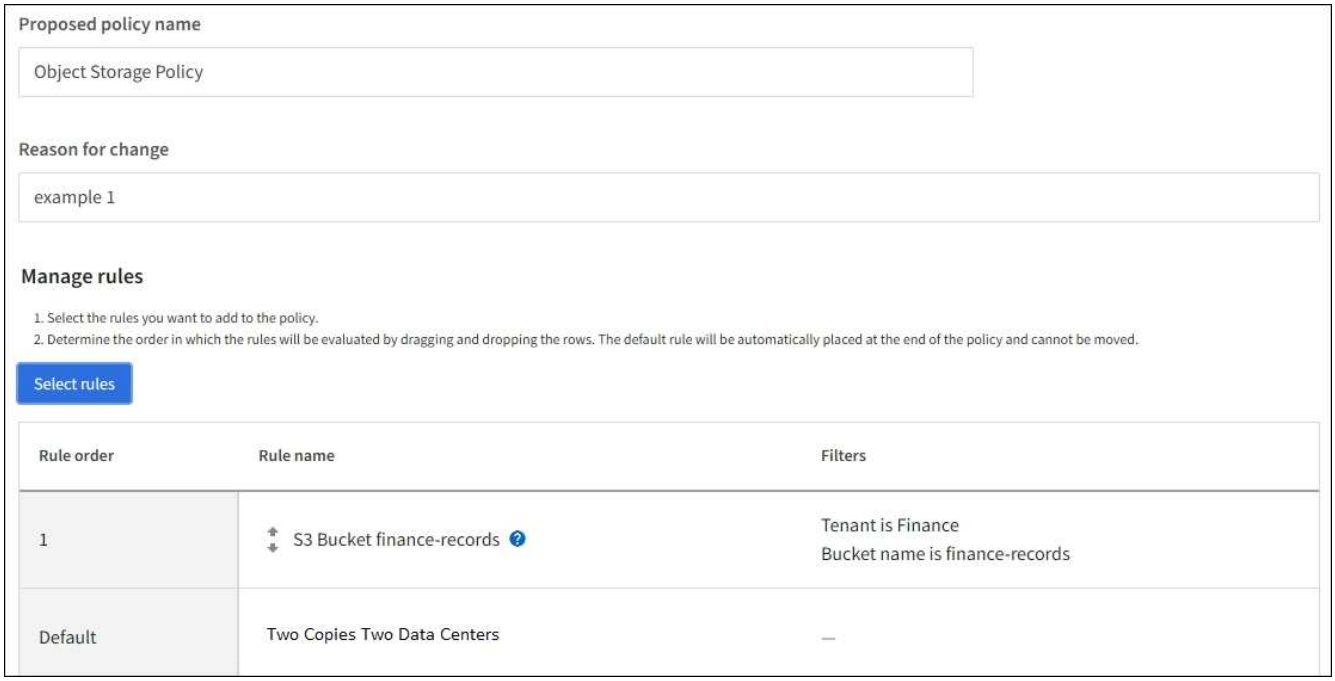


Policy ILM per l'esempio 1

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

Una tipica policy ILM per una grid multisito potrebbe includere regole ILM come le seguenti:

- Al momento dell'ingest, memorizza tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in un pool di storage che contiene tre siti. Usa la codifica di cancellazione 6+3.
- Se un oggetto non corrisponde alla prima regola ILM, usa la regola ILM predefinita della policy, Two Copies Two Data Centers, per archiviare una copia di quell'oggetto nel Sito 1 e una copia nel Sito 2.



Informazioni correlate

- "Usa le policy ILM"
- "${post_edited_translations.segment}"

Regole e policy ILM per il filtraggio delle dimensioni degli oggetti EC in StorageGRID

Puoi usare le seguenti regole e politiche di esempio come punti di partenza per definire una policy ILM che filtra in base alle dimensioni degli oggetti per soddisfare i requisiti EC consigliati.

> Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per confermare che funzionerà come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per l'esempio 2: usa EC per oggetti superiori a 1 MB

Questo esempio di regola ILM applica la codifica di cancellazione agli oggetti di dimensioni superiori a 1 MB.

> La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non usare la codifica di cancellazione per oggetti più piccoli di 200 KB per evitare l'overhead della gestione di frammenti codificati molto piccoli.

Definizione della regola	Esempio di valore
Nome regola	Oggetti EC Only > 1 MB
Tempo di riferimento	Tempo di ingestione

Definizione della regola	Esempio di valore
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB
Posizionamenti	Crea una copia con codifica di cancellazione 2+1 utilizzando tre siti

Regola ILM 2 per l'esempio 2: due copie replicate

Questa regola ILM di esempio crea due copie replicate e non filtra in base alle dimensioni degli oggetti. Questa regola è la regola predefinita per la policy. Poiché la prima regola filtra tutti gli oggetti di dimensioni superiori a 1 MB, questa regola si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Esempio di valore
Nome regola	Due copie replicate
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Nessuno
Posizionamenti	Dal giorno 0 in poi, tieni una copia replicata presso il Sito 1 e una copia replicata presso il Sito 2.

Policy ILM per l'esempio 2: usa EC per oggetti superiori a 1 MB

Questo esempio di policy ILM include due regole ILM:

- La prima regola applica la codifica di cancellazione a 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 pari o inferiori a 1 MB.

Regole e policy ILM per la protezione dei file immagine in StorageGRID

Puoi usare le seguenti regole e policy di esempio per assicurarti che le immagini superiori a 1 MB vengano codificate con cancellazione e che vengano create due copie delle immagini più piccole.

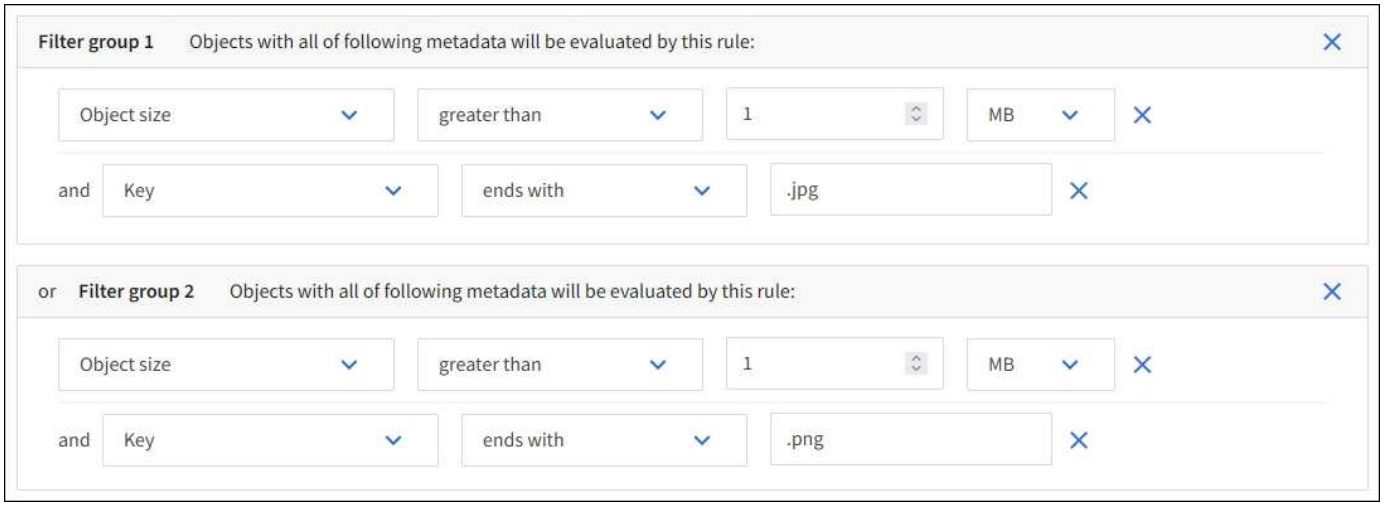
> Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per confermare che funzionerà come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per esempio 3: Usa EC per file immagine superiori a 1 MB

Questo esempio di regola ILM utilizza un filtro avanzato per applicare la codifica di cancellazione a tutti i file immagine di dimensioni superiori a 1 MB.

> La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non usare la codifica di cancellazione per oggetti più piccoli di 200 KB per evitare l'overhead della gestione di frammenti codificati molto piccoli.

Definizione della regola	Esempio di valore
Nome regola	File immagine EC > 1 MB
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB
Filtri avanzati per Key	• Termina con .jpg • Termina con .png
Posizionamenti	Crea una copia con codifica di cancellazione 2+1 utilizzando tre siti



Poiché questa regola è configurata come prima regola nella policy, l'istruzione di posizionamento della codifica di cancellazione si applica solo ai file .jpg e .png di dimensioni superiori a 1 MB.

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

Questa regola ILM di esempio utilizza il filtraggio avanzato per specificare che i file immagine di dimensioni ridotte vengano replicati. Poiché la prima regola della policy ha già individuato i file immagine di dimensioni superiori a 1 MB, questa regola si applica ai file immagine di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Esempio di valore
Nome regola	2 copie per i file immagine

Definizione della regola	Esempio di valore
Tempo di riferimento	Tempo di ingestione
Filtri avanzati per Key	• Termina con .jpg • Termina con .png
Posizionamenti	Crea 2 copie replicate in due pool di storage

Policy ILM per l'esempio 3: migliore protezione per i file immagine

Questo esempio di policy ILM include tre regole:

- La prima regola applica i codici di cancellazione a tutti i file immagine superiori a 1 MB.
- La seconda regola crea due copie di tutti i file immagine rimanenti (cioè immagini che sono di 1 MB o più piccole).
- 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	—

Regole e policy ILM per le versioni non correnti degli oggetti S3 in StorageGRID

Se hai un bucket S3 con la gestione delle versioni abilitata, puoi gestire le versioni non correnti degli oggetti includendo regole nella tua policy ILM che usano "Tempo non corrente" come tempo di riferimento.

> Se specifichi un periodo di conservazione limitato per gli oggetti, questi verranno eliminati definitivamente al termine del periodo stabilito. Assicurati di capire per quanto tempo gli oggetti verranno conservati.

Come mostra questo esempio, puoi controllare la quantità di spazio di archiviazione utilizzata dagli oggetti versionati usando istruzioni di posizionamento diverse per le versioni degli oggetti non correnti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per confermare che funzionerà come previsto per proteggere i contenuti dalla perdita.

Per eseguire la simulazione della policy ILM su una versione non corrente di un oggetto, devi conoscere l'UUID o il CBID della versione dell'oggetto. Per trovare l'UUID e il CBID, usa "ricerca dei metadati dell'oggetto" mentre l'oggetto è ancora corrente.

Informazioni correlate

"Come vengono eliminati gli oggetti"

Regola ILM 1 per esempio 4: Conserva 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 versionati o meno.

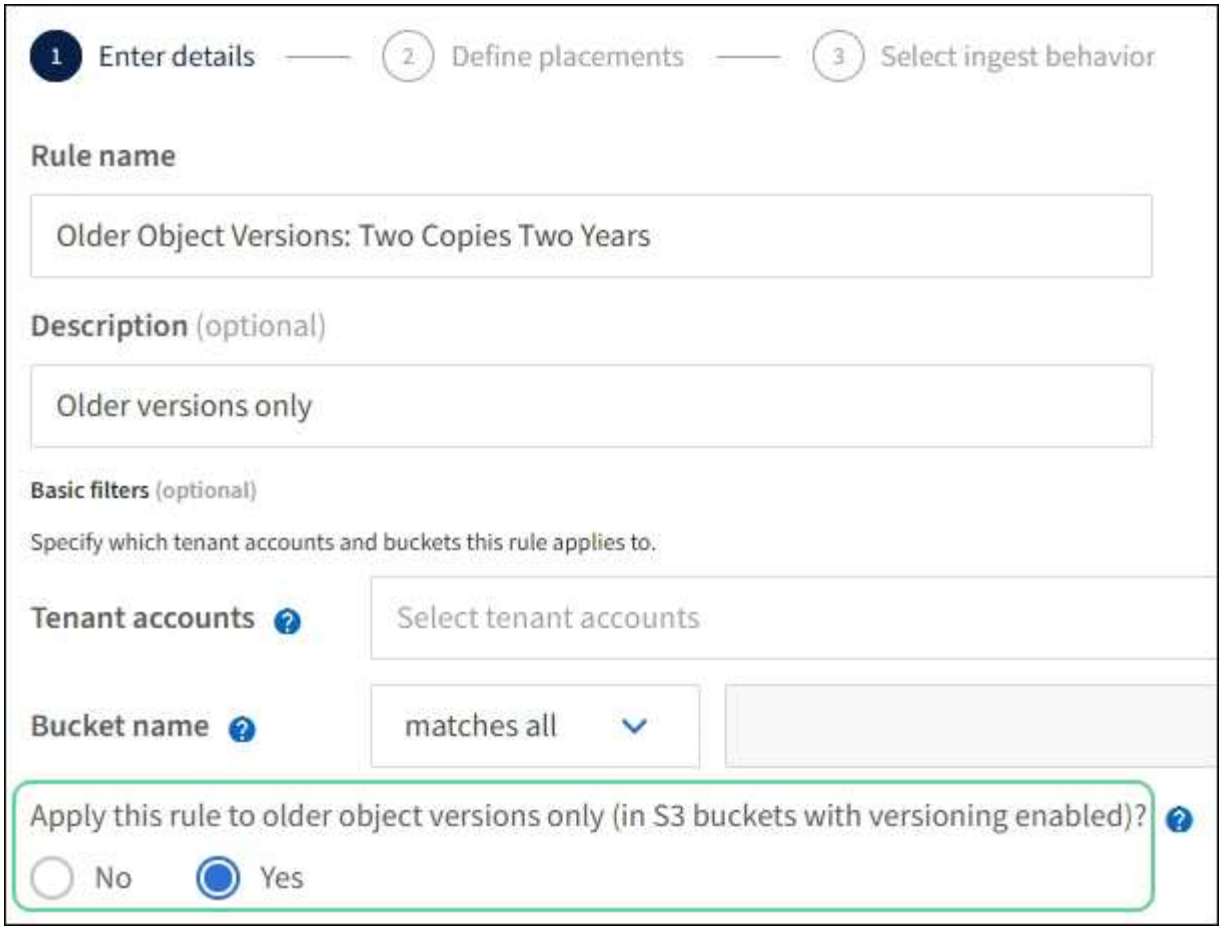
Definizione della regola	Esempio di valore
Pool di storage	Tre pool di archiviazione, ciascuno composto da diversi data center, denominati Site 1, Site 2 e Site 3.
Nome regola	Tre copie dieci anni
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva tre copie replicate per 10 anni (3.652 giorni), una nel Sito 1, una nel Sito 2 e una nel Sito 3. Alla fine dei 10 anni, elimina tutte le copie dell'oggetto.

Regola ILM 2 per l'esempio 4: salva due copie delle versioni non correnti per 2 anni

Questa regola ILM di esempio memorizza due copie delle versioni non correnti di un oggetto versionato S3 per 2 anni.

Poiché la regola ILM 1 si applica a tutte le versioni dell'oggetto, devi creare un'altra regola per filtrare le versioni non correnti.

Per creare una regola che utilizza "Noncurrent time" come tempo di riferimento, seleziona **Sì** alla domanda "Applica questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con versioning abilitato)?" nel passaggio 1 (Inserisci dettagli) della procedura guidata Crea una regola ILM. Quando selezioni **Sì**, *Noncurrent time* viene selezionato automaticamente come tempo di riferimento e non puoi selezionarne uno diverso.



In questo esempio, vengono memorizzate solo due copie delle versioni non correnti e tali copie saranno conservate per due anni.

Definizione della regola	Esempio di valore
Pool di storage	Due pool di archiviazione, ciascuno in un data center diverso, Site 1 e Site 2.
Nome regola	Versioni non correnti: Due copie due anni
Tempo di riferimento	Tempo non corrente Selezionato automaticamente quando selezioni **Sì** alla domanda "Applica questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con versioning abilitato)?" nella procedura guidata Crea una regola ILM.
Posizionamenti	Al giorno 0 rispetto al tempo non corrente (ovvero, a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), conserva due copie replicate delle versioni non correnti dell'oggetto per 2 anni (730 giorni), una in Site 1 e una in Site 2. Alla fine dei 2 anni, elimina le versioni non correnti.

Policy ILM per l'esempio 4: oggetti versionati S3

Se vuoi gestire le versioni precedenti di un oggetto in modo diverso rispetto alla versione corrente, le regole che utilizzano "Tempo non corrente" come tempo di riferimento devono comparire nella policy ILM prima delle regole che si applicano alla versione corrente dell'oggetto.

Una policy ILM per gli oggetti versionati di S3 potrebbe includere regole ILM come le seguenti:

- Tieni le versioni precedenti (non correnti) di ogni oggetto per 2 anni, a partire dal giorno in cui la versione è diventata non corrente.

> Le regole "Tempo non corrente" devono comparire nella policy prima delle regole che si applicano alla versione corrente dell'oggetto. Altrimenti, le versioni non correnti dell'oggetto non verranno mai abbinate dalla regola "Tempo non corrente".

- Al momento dell'acquisizione, crea tre copie replicate e archivia una copia in ciascuno dei tre siti. Tieni le copie della versione corrente dell'oggetto per 10 anni.

Quando simuli la policy di esempio, ti aspetti che gli oggetti di test vengano valutati come segue:

- Qualsiasi versione non corrente di un oggetto verrebbe abbinata dalla prima regola. Se una versione non corrente di un oggetto è più vecchia di 2 anni, viene eliminata definitivamente da ILM (tutte le copie della versione non corrente vengono rimosse dal grid).
- La versione corrente dell'oggetto corrisponde alla seconda regola. Quando la versione corrente dell'oggetto è stata memorizzata per 10 anni, il processo ILM aggiunge un indicatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente "noncurrent". Alla successiva valutazione ILM, questa versione noncurrent viene abbinata alla prima regola. Di conseguenza, la copia presso Site 3 viene eliminata e le due copie presso Site 1 e Site 2 vengono conservate per altri 2 anni.

Regole e policy ILM per il comportamento di acquisizione rigoroso in StorageGRID

Puoi usare un location filter e il comportamento di ingestione Strict in una regola per impedire che gli oggetti vengano salvati in una specifica posizione del data center.

In questo esempio, un tenant con sede a Parigi non vuole archiviare alcuni oggetti al di fuori dell'UE per motivi normativi. Altri oggetti, inclusi tutti gli oggetti provenienti da altri account tenant, possono essere archiviati sia nel data center di Parigi che in quello statunitense.

> Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per confermare che funzionerà come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

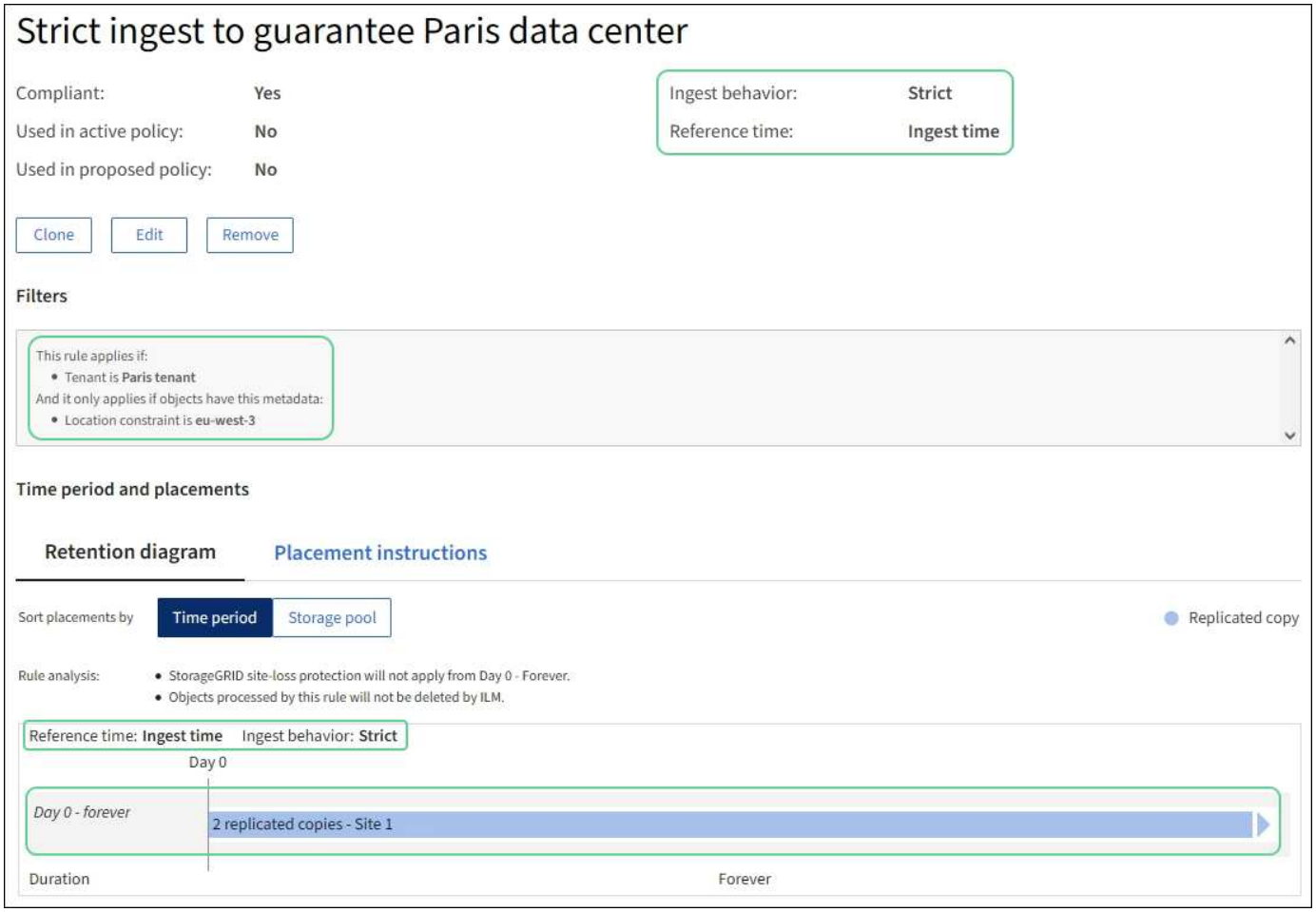
- "Opzioni di ingest"
- "Crea regola ILM: seleziona il comportamento di acquisizione"

Regola ILM 1 per esempio 5: Ingestione rigorosa per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento di acquisizione rigoroso per garantire che gli oggetti salvati da un tenant con sede a Parigi in bucket S3 con la regione impostata su eu-west-3 region (Paris) non vengano mai archiviati nel data center US.

Questa regola si applica agli oggetti che appartengono al tenant Paris e che hanno la regione del bucket S3 impostata su eu-west-3 (Paris).

Definizione della regola	Esempio di valore
Account tenant	tenant di Paris
Filtro avanzato	Vincolo di posizione uguale a eu-west-3
Pool di storage	Sito 1 (Paris)
Nome regola	Ingestione rigorosa per garantire il data center di Parigi
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, tieni per sempre due copie replicate nella Site 1 (Paris)
Comportamento di ingest	Rigoroso. Usa sempre i posizionamenti di questa regola durante l'inserimento. L'inserimento fallisce se non è possibile memorizzare due copie dell'oggetto nel data center di Parigi.



Regola ILM 2 per esempio 5: Ingest bilanciato per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciata per garantire un'efficienza ILM ottimale per tutti gli oggetti non corrispondenti alla prima regola. Due copie di tutti gli oggetti corrispondenti a questa regola verranno memorizzate: una nel data center US e una nel data center di Parigi. Se la regola non può essere soddisfatta immediatamente, le copie provvisorie vengono memorizzate in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi regione.

Definizione della regola	Esempio di valore
Account tenant	Ignora
Filtro avanzato	*Non specificato*
Pool di storage	Sito 1 (Paris) e Sito 2 (US)
Nome regola	2 copie 2 data center
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva per sempre due copie replicate in due data center
Comportamento di ingest	Bilanciato. Gli oggetti che corrispondono a questa regola vengono posizionati secondo le istruzioni di posizionamento della regola stessa, se possibile. Altrimenti, vengono create copie provvisorie in qualsiasi posizione disponibile.

Policy ILM per l'esempio 5: combinare i comportamenti di ingest

L'esempio di policy ILM include due regole che presentano comportamenti di acquisizione differenti.

Una policy ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Archivia gli oggetti appartenenti al tenant Paris e con la regione del bucket S3 impostata su eu-west-3 (Paris) solo nel data center di Parigi. L'acquisizione fallisce se il data center di Parigi non è disponibile.
- Archivia tutti gli altri oggetti (inclusi quelli appartenenti al tenant Paris ma con una regione bucket diversa) sia nel data center statunitense che in quello di Parigi. Crea copie provvisorie in qualsiasi posizione disponibile se non è possibile soddisfare le istruzioni di posizionamento.

Quando simuli la policy di esempio, ti aspetti che gli oggetti di test vengano valutati come segue:

- Tutti gli oggetti che appartengono al tenant Paris e che hanno la regione del bucket S3 impostata su eu-west-3 vengono individuati dalla prima regola e archiviati nel data center di Parigi. Poiché la prima regola utilizza Strict ingest, questi oggetti non vengono mai archiviati nel data center statunitense. Se i Storage Nodes del data center di Parigi non sono disponibili, l'ingestione fallisce.
- Tutti gli altri oggetti vengono abbinati dalla seconda regola, inclusi gli oggetti che appartengono al tenant Paris e che non hanno la regione del bucket S3 impostata su eu-west-3. Una copia di ciascun oggetto viene salvata in ogni data center. Tuttavia, poiché la seconda regola utilizza Balanced ingest, se un data

center non è disponibile, vengono salvate due copie intermedie in una qualsiasi posizione disponibile.

Come la modifica di una policy ILM influisce sulle prestazioni di StorageGRID

Se hai bisogno di modificare la protezione dei dati o aggiungi nuovi siti, puoi creare e attivare una nuova policy ILM.

Prima di modificare una policy, devi capire come le modifiche al posizionamento di ILM possono influire temporaneamente sulle prestazioni complessive di un sistema StorageGRID.

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione ed è necessario implementare una nuova policy ILM attiva per archiviare i dati nel nuovo sito. Per implementare una nuova policy attiva, prima "crea una policy". Dopo, devi "simulare" e poi "attivare" la nuova policy.

> Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per confermare che funzionerà come previsto per proteggere i contenuti dalla perdita.

Come la modifica di una politica ILM influisce sulle prestazioni

Quando attivi una nuova policy ILM, le prestazioni del tuo sistema StorageGRID potrebbero risentirne temporaneamente, soprattutto se le istruzioni di posizionamento della nuova policy richiedono lo spostamento di molti oggetti esistenti in nuove posizioni.

Quando attivi una nuova policy ILM, StorageGRID la usa per gestire tutti gli oggetti, inclusi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, controlla eventuali modifiche al posizionamento degli oggetti replicati e con codifica di cancellazione esistenti. Cambiare la posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando vengono valutati e implementati i nuovi posizionamenti.

Per garantire che una nuova policy ILM non influisca sul posizionamento degli oggetti replicati e codificati per la cancellazione esistenti, puoi "crea una regola ILM con un filtro per il tempo di acquisizione". Ad esempio, **L'ora di inserimento è *uguale o successiva a <date and time>***, così la nuova regola si applica solo agli oggetti inseriti a partire dalla data e ora specificate.

Le tipologie di modifiche alle policy ILM che possono influire temporaneamente sulle prestazioni di StorageGRID includono le seguenti:

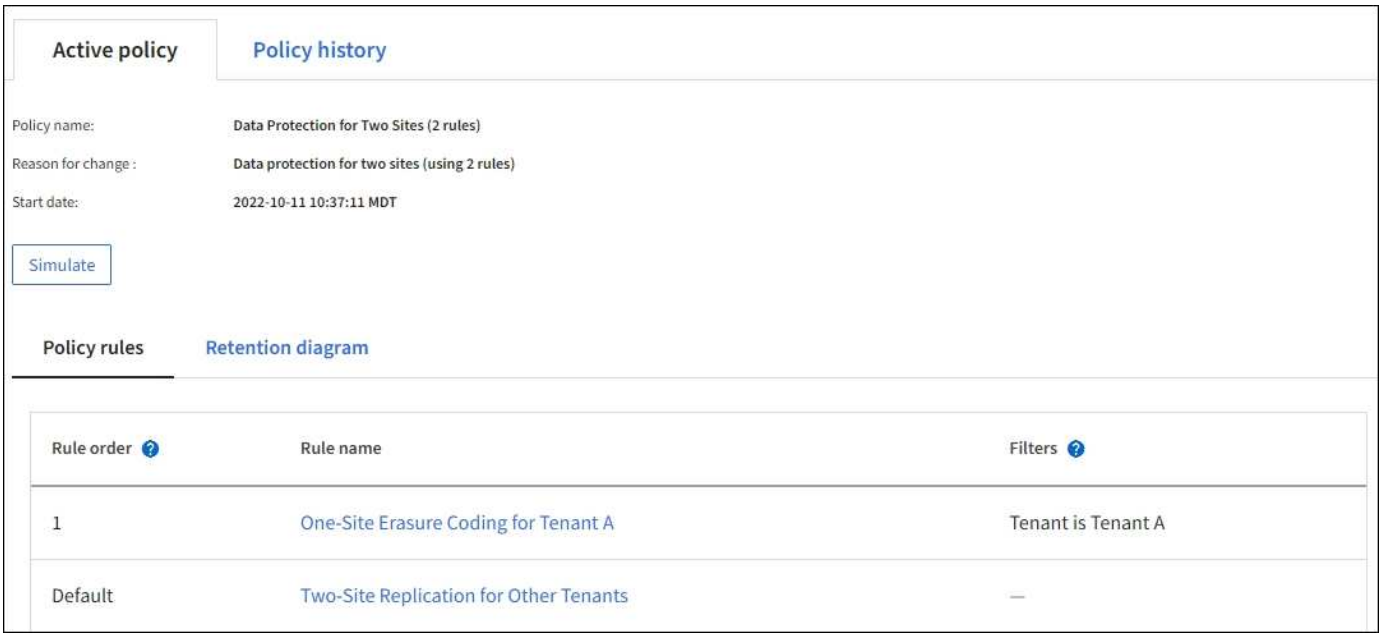
- Applicare un profilo di codifica di cancellazione diverso a oggetti già codificati con questo metodo.

  > StorageGRID considera ogni profilo di codifica di cancellazione come unico e non riutilizza i frammenti di codifica di cancellazione quando viene utilizzato un nuovo profilo.

- Modificare il tipo di copie richieste per gli oggetti esistenti; ad esempio, convertire una grande % di oggetti replicati in oggetti con codifica di cancellazione.
- Spostare copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostare un gran numero di oggetti da o verso un Cloud Storage Pool o da o verso un sito remoto.

Policy ILM attiva per 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 tramite codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti su due siti utilizzando la replica a 2 copie.

Regola 1: Codifica di cancellazione a sito singolo per il tenant A

Definizione della regola	Esempio di valore
Nome regola	Codifica di cancellazione a sito unico per il tenant A
Account tenant	Tenant A
Pool di storage	Sito 1
Posizionamenti	Codifica di cancellazione 2+1 in Site 1 dal giorno 0 per sempre

Regola 2: Replica su due siti per altri tenant

Definizione della regola	Esempio di valore
Nome regola	Replica su due siti per altri tenant
Account tenant	Ignora
Pool di storage	Sito 1 e Sito 2
Posizionamenti	Due copie replicate dal giorno 0 all'infinito: una copia presso Site 1 e una copia presso Site 2.

Politica ILM per l'esempio 6: Protezione dei dati in tre sedi

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 è lo stesso del pool di storage predefinito All Storage Nodes). Poi, l'amministratore ha creato due nuove regole ILM e una nuova policy ILM, progettata per proteggere i dati in tutti e tre i siti.

Quando questa nuova policy ILM viene attivata, gli oggetti appartenenti al Tenant A sono protetti tramite codifica di cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e gli oggetti di dimensioni inferiori appartenenti al Tenant A) sono protetti in tre siti utilizzando la replica a 3 copie.

Regola 1: Codifica di cancellazione a tre siti per il tenant A

Definizione della regola	Esempio di valore
Nome regola	Codifica di cancellazione a tre siti per il tenant A
Account tenant	Tenant A
Pool di storage	Tutti e 3 i siti (include il sito 1, il sito 2 e il sito 3)
Posizionamenti	Codifica di cancellazione 2+1 in tutti e 3 i siti dal giorno 0 per sempre

Regola 2: Replica su tre siti per altri tenant

Definizione della regola	Esempio di valore
Nome regola	Replica su tre siti per altri tenant
Account tenant	Ignora
Pool di storage	Sito 1, Sito 2 e Sito 3
Posizionamenti	Tre copie replicate dal giorno 0 all'infinito: una copia presso il Sito 1, una copia presso il Sito 2 e una copia presso il Sito 3.

Attivare la policy ILM per l'esempio 6

Quando attivi una nuova policy ILM, gli oggetti esistenti potrebbero essere spostati in nuove posizioni oppure potrebbero essere create nuove copie degli oggetti esistenti, in base alle istruzioni di posizionamento contenute nelle regole nuove o aggiornate.

> Gli errori in una policy ILM possono causare una perdita di dati irreversibile. Esamina attentamente e simula la policy prima di attivarla per confermare che funzionerà come previsto.

Quando attivi una nuova policy ILM, StorageGRID la usa per gestire tutti gli oggetti, inclusi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, controlla eventuali modifiche al posizionamento degli oggetti replicati e con codifica di cancellazione esistenti. Cambiare la posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando vengono valutati e implementati i nuovi posizionamenti.

Cosa succede quando cambiano le istruzioni di codifica di cancellazione

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti al Tenant A sono protetti utilizzando la codifica di cancellazione 2+1 presso il Sito 1. Nella nuova policy ILM, gli oggetti appartenenti al Tenant A saranno protetti utilizzando la codifica di cancellazione 2+1 presso i Siti 1, 2 e 3.

Quando viene attivata la nuova policy 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. Poi, 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 ILM utilizzano un nuovo profilo di erasure coding, vengono creati frammenti di erasure coding completamente nuovi e distribuiti ai tre siti.

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 presso i siti 1 e 2. Nella nuova policy ILM, gli oggetti appartenenti ad altri tenant saranno protetti utilizzando tre copie replicate nei pool di storage presso i siti 1, 2 e 3.

Quando viene attivata la nuova policy ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso da Tenant A acquisisce un nuovo oggetto, StorageGRID crea tre copie e ne salva una in ciascun 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 presso il Site 1 e il Site 2 continuano a soddisfare i requisiti di replica della nuova regola ILM, StorageGRID deve creare una sola nuova copia dell'oggetto per il Site 3.

Impatto sulle prestazioni dell'attivazione di questa policy

Quando la policy ILM in questo esempio viene attivata, le prestazioni complessive di questo sistema StorageGRID saranno temporaneamente influenzate. Saranno necessari livelli di risorse di grid superiori alla norma per creare nuovi frammenti con codifica di cancellazione per gli oggetti esistenti del tenant A e nuove copie replicate nel sito 3 per gli oggetti esistenti degli altri tenant.

A seguito della modifica della policy ILM, le richieste di lettura e scrittura dei client potrebbero temporaneamente presentare latenze superiori alla norma. Le latenze torneranno ai livelli normali una volta che le istruzioni di posizionamento saranno completamente implementate sulla griglia.

Per evitare problemi di risorse durante l'attivazione di una nuova policy ILM, puoi usare il filtro avanzato "Tempo di acquisizione" in qualsiasi regola che potrebbe cambiare la posizione di un gran numero di oggetti

esistenti. Imposta il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore per assicurarti che gli oggetti esistenti non vengano spostati inutilmente.

> Contatta il supporto tecnico se hai bisogno di rallentare o aumentare la velocità con cui gli oggetti vengono elaborati dopo una modifica della policy ILM.

Criterio ILM conforme per S3 Object Lock in StorageGRID

Puoi usare il bucket S3, le regole ILM e la policy ILM di questo esempio come punto di partenza quando definisci una policy ILM per soddisfare i requisiti di protezione degli oggetti e di periodo di conservazione per gli oggetti nei bucket con S3 Object Lock abilitato.

> Se nelle versioni precedenti di StorageGRID hai utilizzato la funzionalità di Compliance legacy, puoi usare questo esempio anche per gestire i bucket esistenti che hanno la funzionalità di Compliance legacy abilitata.

> Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per confermare che funzionerà come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

- "Gestisci gli oggetti con S3 Object Lock"
- "Crea una policy ILM"

Bucket e oggetti per l'esempio di S3 Object Lock

In questo esempio, un tenant account S3 denominato Bank of ABC ha utilizzato il Tenant Manager per creare un bucket con S3 Object Lock abilitato per archiviare record bancari critici.

Definizione di bucket	Esempio di valore
Nome account tenant	Bank of ABC
Nome bucket	registri bancari
Regione del bucket	us-east-1 (predefinito)

Ogni oggetto e versione di oggetto aggiunto al bucket bank-records utilizzerà i seguenti valori per `retain-until-date` e `legal hold` impostazioni.

Impostazione per ciascun oggetto	Esempio di valore
`retain-until-date`	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione dell'oggetto ha la propria `retain-until-date`impostazione. Questa impostazione può essere aumentata, ma non diminuita.

Impostazione per ciascun oggetto	Esempio di valore
`legal hold`	"OFF" (Non in vigore) È possibile applicare o rimuovere un blocco legale su qualsiasi versione di un oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è soggetto a un blocco legale, non può essere eliminato anche se il `retain-until-date` è stato raggiunto.

Regola ILM 1 per l'esempio di S3 Object Lock: profilo di erasure-coding con corrispondenza del bucket

Questa regola ILM di esempio si applica solo al tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto nel `bank-records` bucket e quindi utilizza la codifica di cancellazione per memorizzare l'oggetto sui Storage Node in tre siti di data center utilizzando un profilo di codifica di cancellazione 6+3. Questa regola soddisfa i requisiti dei bucket con S3 Object Lock abilitato: una copia viene conservata sui Storage Node dal giorno 0 per sempre, utilizzando l'ora di ingest come tempo di riferimento.

Definizione della regola	Esempio di valore
Nome regola	Norma di conformità: Oggetti EC nel bucket bank-records - Bank of ABC
Account tenant	Bank of ABC
Nome bucket	`bank-records`
Filtro avanzato	Dimensione oggetto (MB) maggiore di 1 **Nota:** Questo filtro garantisce che la codifica di cancellazione non venga utilizzata per oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Esempio di valore
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 conserva per sempre
Profilo di erasure coding	• Crea una copia con codifica di cancellazione sui nodi di archiviazione in tre siti di data center • Utilizza lo schema di codifica a cancellazione 6+3

Regola ILM 2 per S3 Object Lock: esempio di regola non conforme

Questa regola ILM di esempio inizialmente memorizza due copie replicate degli oggetti 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 verrà applicata agli oggetti nei bucket con S3 Object Lock abilitato.

Definizione della regola	Esempio di valore
Nome regola	Regola non conforme: utilizzare il pool di storage cloud
Account tenant	Non specificato
Nome bucket	Non specificato, ma si applicherà solo ai bucket che non hanno S3 Object Lock (o la funzionalità Compliance legacy) abilitato.
Filtro avanzato	Non specificato

Definizione della regola	Esempio di valore
Tempo di riferimento	Tempo di ingestione
Posizionamenti	• Il giorno 0, mantieni due copie replicate sui nodi di storage nel Data Center 1 e nel Data Center 2 per 365 giorni • Dopo 1 anno, conserva una copia replicata in un Cloud Storage Pool per sempre

Regola ILM 3 per l'esempio di S3 Object Lock: regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti nei pool di storage in due data center. Questa regola conforme è progettata per essere la regola predefinita nella policy ILM. Non include alcun filtro, non utilizza il tempo di riferimento Noncurrent e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: due copie degli oggetti vengono mantenute sui Storage Node dal giorno 0 per sempre, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Esempio di valore
Nome regola	Regola di conformità predefinita: Due copie due centri dati
Account tenant	Non specificato
Nome bucket	Non specificato
Filtro avanzato	Non specificato

Definizione della regola	Esempio di valore
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 in poi, mantieni 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 una policy ILM che protegga efficacemente tutti gli oggetti nel tuo sistema, inclusi quelli nei bucket con S3 Object Lock abilitato, devi selezionare le regole ILM che soddisfano i requisiti di storage per tutti gli oggetti. Poi devi simulare e attivare la policy.

Aggiungi le regole alla policy

In questo esempio, la policy ILM include tre regole ILM, nel seguente ordine:

1. Una regola conforme che utilizza la codifica di cancellazione per proteggere oggetti di dimensioni superiori a 1 MB in un bucket specifico con S3 Object Lock abilitato. Gli oggetti sono archiviati sui Storage Node dal giorno 0 per sempre.
2. Una regola non conforme che crea due copie replicate di un oggetto sui Storage Node per un anno e poi sposta una copia dell'oggetto in un Cloud Storage Pool per sempre. Questa regola non si applica ai bucket con S3 Object Lock abilitato perché utilizza un Cloud Storage Pool.
3. La regola conforme predefinita che crea due copie replicate di oggetti sui Storage Node dal giorno 0 per sempre.

Simula la policy

Dopo aver aggiunto le regole alla policy, scelto una regola conforme predefinita e organizzato le altre regole, dovresti simulare la policy testando oggetti dal bucket con S3 Object Lock abilitato e da altri bucket. Ad esempio, quando simuli la policy di esempio, ti aspetteresti che gli oggetti di test vengano valutati come segue:

- La prima regola corrisponderà solo agli oggetti di test di dimensioni superiori a 1 MB presenti nel bucket bank-records per il tenant Bank of ABC.
- La seconda regola corrisponderà a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri tenant account.
- La regola predefinita corrisponde a questi oggetti:
  - Oggetti di dimensioni pari o inferiori a 1 MB nel bucket bank-records per il tenant Bank of ABC.
  - Oggetti in qualsiasi altro bucket per cui è abilitato S3 Object Lock per tutti gli altri account tenant.

Attiva la policy

Quando sei completamente sicuro che la nuova policy protegge i dati degli oggetti come previsto, puoi attivarla.

Come il ciclo di vita del bucket S3 e la policy ILM interagiscono in StorageGRID

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

Esempio di ciclo di vita del bucket che ha la priorità sulla policy ILM

Policy ILM

- Regola basata su un riferimento temporale non corrente: al giorno 0, tieni X copie per 20 giorni
- Regola basata sul riferimento temporale di acquisizione (impostazione predefinita): al giorno 0, conserva X copie per 50 giorni

Ciclo di vita del bucket

```
"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 con prefisso "docs/".
  - Dopo 100 giorni viene creato un delete-marker e "docs/text" diventa noncurrent.
  - Dopo 5 giorni, per un totale di 105 giorni dall'ingestione, "docs/text" viene eliminata.
  - Dopo 95 giorni, ovvero 200 giorni dall'ingest e 100 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.
- È stato acquisito un oggetto denominato "video/movie". Non corrisponde al filtro e utilizza la policy di conservazione ILM.
  - Dopo 50 giorni viene creato un indicatore di eliminazione e "video/movie" diventa non corrente.
  - Dopo 20 giorni, per un totale di 70 giorni dall'ingest, "video/movie" viene eliminato.
  - Dopo 30 giorni, per un totale di 100 giorni dall'ingest e 50 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.

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

Policy ILM

- Regola basata su un riferimento temporale non corrente: al giorno 0, tieni X copie per 20 giorni
- Regola basata sul riferimento temporale di acquisizione (impostazione predefinita): al giorno 0, conserva X copie per 50 giorni

Ciclo di vita del bucket

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

Risultato

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

  L' `Expiration`azione si applica solo ai marcatori di eliminazione 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 scadono.

- È stato acquisito un oggetto denominato "video/movie". Non corrisponde al filtro e utilizza la policy di conservazione ILM.
  - Dopo 50 giorni viene creato un indicatore di eliminazione e "video/movie" diventa non corrente.
  - Dopo 20 giorni, per un totale di 70 giorni dall'ingest, "video/movie" viene eliminato.
  - Dopo 30 giorni, per un totale di 100 giorni dall'ingest e 50 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.

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

Policy ILM

- Regola basata su un riferimento temporale non corrente: al giorno 0, tieni X copie per 20 giorni
- Regola basata sul riferimento del tempo di acquisizione (predefinito): al giorno 0, conserva X copie per sempre

Ciclo di vita del bucket

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

Risultato

- La policy ILM viene duplicata nel ciclo di vita del bucket.
  - La regola "per sempre" della policy ILM è progettata per rimuovere manualmente gli oggetti ed eliminare le versioni non correnti dopo 20 giorni. Di conseguenza, la regola "tempo di acquisizione" manterrà per sempre i delete marker scaduti.
  - Il ciclo di vita del bucket duplica il comportamento della policy ILM aggiungendo `"ExpiredObjectDeleteMarker": true`, che rimuove i marcatori di eliminazione una volta scaduti
- Un oggetto viene ingerito. Nessun filtro significa che il ciclo di vita del bucket si applica a tutti gli oggetti e sovrascrive le impostazioni di conservazione di ILM.
  - Quando un tenant invia una richiesta di eliminazione di un oggetto, viene creato un delete-marker e l'oggetto diventa non corrente.
  - Dopo 20 giorni, l'oggetto non corrente viene eliminato e il delete-marker scade.
  - Poco dopo, il marcatore di eliminazione scaduto viene eliminato.

Informazioni sul copyright

Informazioni sul marchio commerciale