Gestire gli oggetti con ILM

StorageGRID software

NetApp
December 03, 2025

Sommario

Gestire gli oggetti con ILM

Gestire gli oggetti con ILM

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 tali copie nel tempo.

Informazioni su queste istruzioni

La progettazione e l'implementazione delle regole e delle politiche ILM richiedono un'attenta pianificazione. È necessario comprendere i requisiti operativi, la topologia del sistema StorageGRID , le esigenze di protezione degli oggetti e i tipi di storage disponibili. Quindi, è necessario stabilire come si desidera che i diversi tipi di oggetti vengano copiati, distribuiti e archiviati.

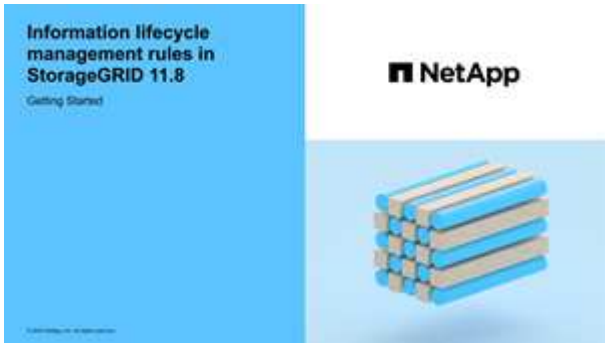
Utilizzare queste istruzioni per:

- Scopri di più su StorageGRID ILM, incluso"come funziona l'ILM durante tutta la vita di un oggetto" .
- Scopri come configurare"pool di stoccaggio" ,"Pool di archiviazione cloud" , E"Regole ILM" .
- Impara come"creare, simulare e attivare una politica ILM" che proteggerà i dati degli oggetti su uno o più siti.
- Impara come"gestire gli oggetti con S3 Object Lock" , che aiuta a garantire che gli oggetti in bucket S3 specifici non vengano eliminati o sovrascritti per un periodo di tempo specificato.

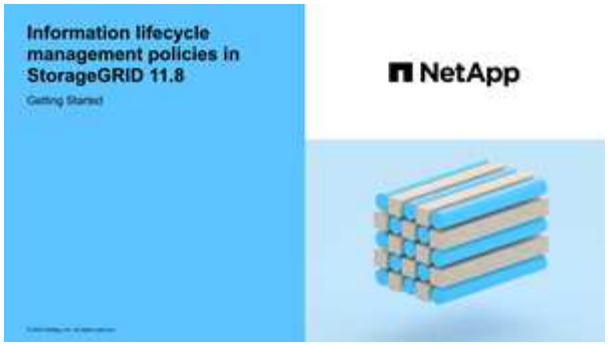
Saperne di più

Per saperne di più, guarda questi video:

- "Video: panoramica delle regole ILM" .



- "Video: Panoramica delle politiche ILM"



ILM e ciclo di vita degli oggetti

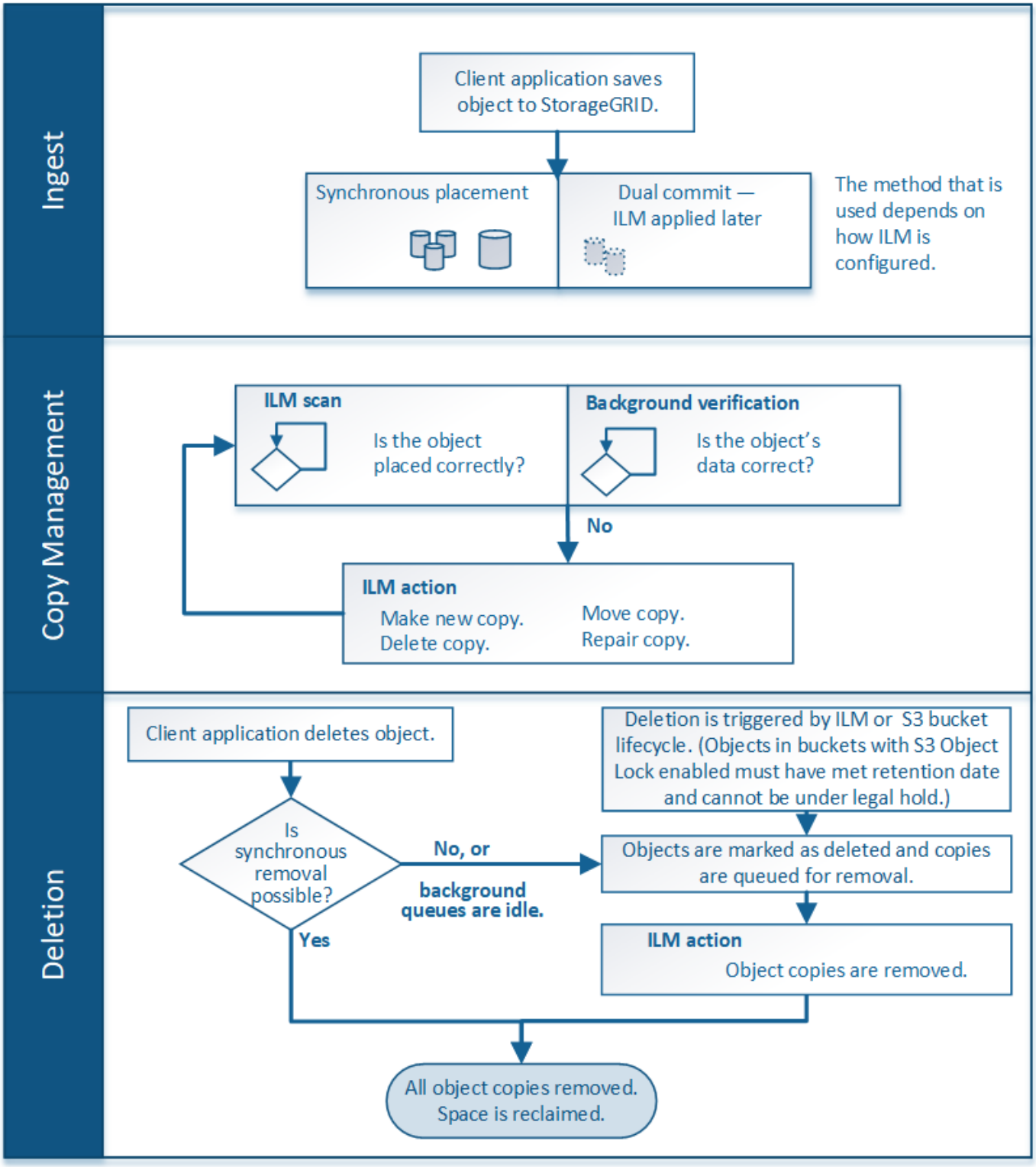
Come funziona l'ILM durante la vita di un oggetto

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.

- **Ingest**: 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 "ingest riuscito". I dati degli oggetti vengono protetti durante l'acquisizione applicando immediatamente le istruzioni ILM (posizionamento sincrono) oppure creando copie provvisorie e applicando ILM in un secondo momento (doppio commit), a seconda di come sono stati specificati i requisiti ILM.
- **Gestione delle copie**: dopo aver creato il numero e il tipo di copie degli oggetti specificati nelle istruzioni di posizionamento dell'ILM, StorageGRID gestisce le posizioni degli oggetti e li protegge dalla perdita.
  - **Scansione e valutazione ILM**: StorageGRID esegue continuamente la scansione dell'elenco degli oggetti archiviati 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 in base alle necessità.
  - **Verifica in background**: StorageGRID esegue costantemente 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 codice di cancellazione in una posizione che soddisfa i requisiti ILM correnti. Vedere "Verificare l'integrità dell'oggetto" .
- **Eliminazione oggetto**: la gestione di un oggetto termina quando tutte le copie vengono rimosse dal sistema StorageGRID . Gli oggetti possono essere rimossi a seguito di una richiesta di eliminazione da parte di un client, oppure a seguito di un'eliminazione da parte di ILM o causata dalla scadenza del ciclo di vita di un bucket S3.

> Gli oggetti in un bucket in cui è abilitato il blocco degli oggetti S3 non possono essere eliminati se sono soggetti a conservazione legale o se è stata specificata una data di conservazione fino a quando non è stata ancora rispettata.

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



Come vengono ingeriti gli oggetti

Opzioni di acquisizione

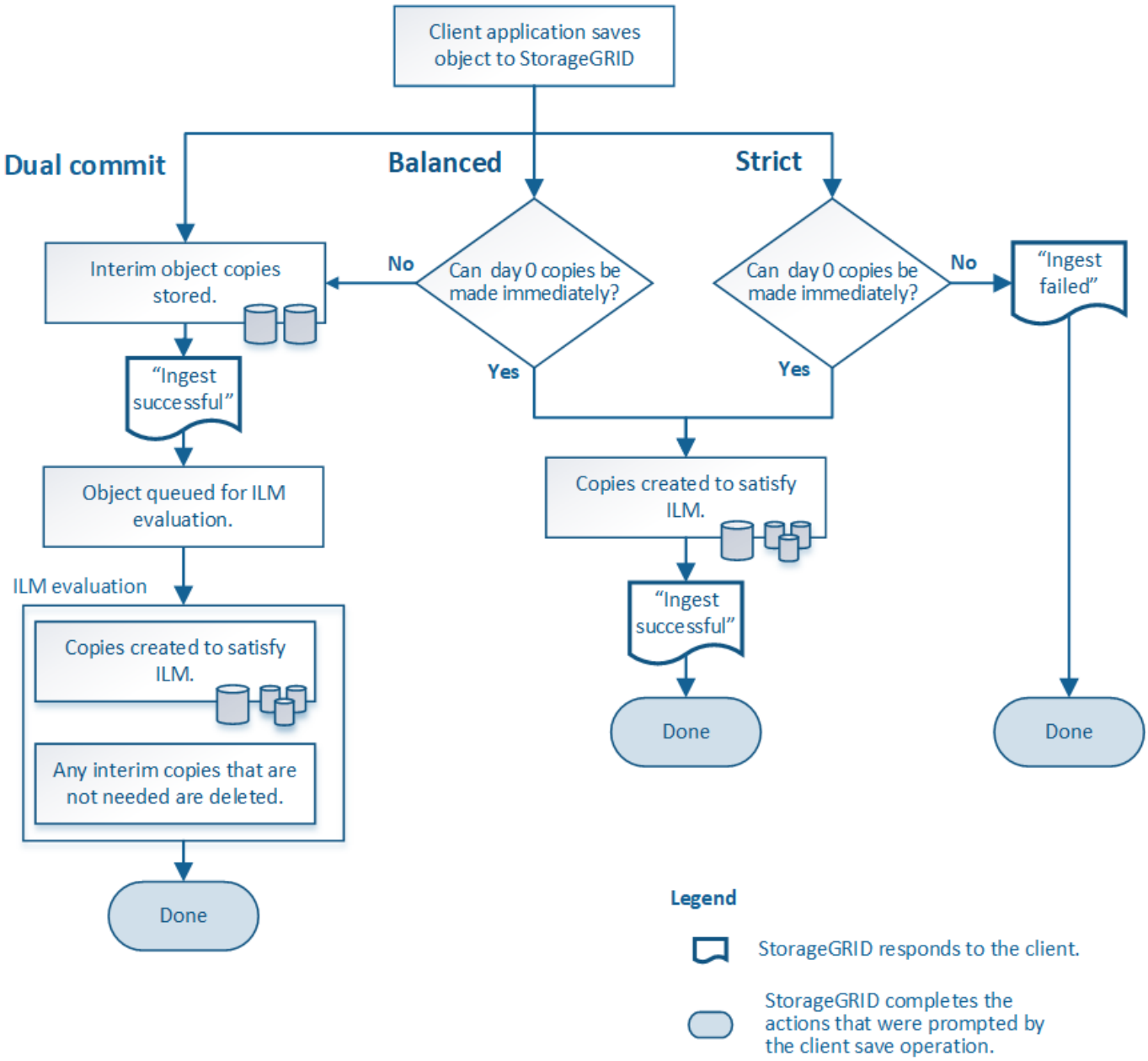
Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Doppio commit, Rigoroso o Bilanciato.

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

valutazione ILM, oppure utilizza il posizionamento sincrono ed esegue immediatamente copie per soddisfare i requisiti ILM.

Diagramma di flusso delle opzioni di acquisizione

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



Doppio impegno

Quando si seleziona l'opzione Dual commit, StorageGRID esegue immediatamente copie provvisorie degli oggetti su due diversi nodi di archiviazione e restituisce al client un messaggio di "ingest riuscito". L'oggetto viene messo in coda per la valutazione ILM e in seguito vengono create copie che soddisfano le istruzioni di posizionamento della regola. Se la policy ILM non può essere elaborata immediatamente dopo il doppio commit, la protezione contro la perdita del sito potrebbe richiedere del tempo.

Utilizzare l'opzione Dual commit in uno di questi casi:

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

Bilanciato (predefinito)

Quando si seleziona l'opzione Bilanciato, StorageGRID utilizza anche il posizionamento sincrono durante l'acquisizione ed esegue immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. A differenza dell'opzione Strict, se StorageGRID non riesce a effettuare 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 contro la perdita del sito, viene attivato l'avviso **Posizionamento ILM non realizzabile**.

Utilizzare l'opzione Bilanciata per ottenere la migliore combinazione di protezione dei dati, prestazioni della griglia e successo dell'acquisizione. Bilanciato è l'opzione predefinita nella procedura guidata Crea regola ILM.

Rigoroso

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

Utilizzare l'opzione Rigorosa se si ha un requisito operativo o normativo che impone di archiviare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potrebbe essere necessario utilizzare l'opzione Rigorosa e un filtro avanzato Vincolo di posizione per garantire che gli oggetti non vengano mai archiviati in determinati data center.

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

Vantaggi, svantaggi e limitazioni delle opzioni di ingestione

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 acquisizione, vedere"Opzioni di acquisizione" .

Vantaggi delle opzioni Bilanciata e Rigorosa

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

- **Maggiore sicurezza dei dati**: i dati degli oggetti vengono immediatamente protetti come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per proteggere da un'ampia gamma di condizioni di errore, incluso l'errore di più di una posizione di archiviazione. Il doppio commit può

proteggere solo dalla perdita di una singola copia locale.

- **Funzionamento della griglia più efficiente**: ogni oggetto viene elaborato una sola volta, quando viene acquisito. Poiché il sistema StorageGRID non ha bisogno di tracciare o eliminare copie provvisorie, il carico di elaborazione è inferiore e viene consumato meno spazio nel database.
- **(Bilanciato) Consigliato**: l'opzione Bilanciata garantisce un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Bilanciata, a meno che non sia richiesto un comportamento di ingestione rigoroso o che la griglia soddisfi tutti i criteri per l'utilizzo del commit doppio.
- **(Rigorosa) Certezza sulla posizione degli oggetti**: l'opzione Rigorosa garantisce che gli oggetti vengano immediatamente archiviati secondo le istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni Bilanciata e Rigorosa

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

- **Ingestione client più lunga**: le latenze di acquisizione client potrebbero essere più lunghe. Quando si utilizzano le opzioni Bilanciato o Rigoroso, il messaggio "ingest riuscito" non viene restituito al client finché non vengono creati e archiviati tutti i frammenti codificati in modo da essere cancellati o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano la loro collocazione finale molto più rapidamente.
- **(Rigoroso) Maggiori tassi di errore di acquisizione**: con l'opzione Rigorosa, l'acquisizione fallisce ogni volta che StorageGRID non riesce a effettuare immediatamente tutte le copie specificate nella regola ILM. Si potrebbero verificare alti tassi di errore di acquisizione se una posizione di archiviazione richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia di oggetti tra siti.
- **(Rigoroso) In alcune circostanze, i posizionamenti dei caricamenti multiparte S3 potrebbero non essere quelli previsti**: con Rigoroso, ci si aspetta che gli oggetti vengano posizionati come descritto dalla regola ILM oppure che l'acquisizione non vada a buon fine. Tuttavia, con un caricamento multiparte S3, l'ILM viene valutato per ogni parte dell'oggetto mentre viene acquisito e per l'oggetto nel suo complesso quando il caricamento multiparte viene completato. Nelle seguenti circostanze, ciò potrebbe comportare posizionamenti diversi da quelli previsti:
  - **Se ILM cambia mentre è in corso un caricamento multiparte S3**: poiché ogni parte viene posizionata in base alla regola attiva al momento dell'acquisizione della parte, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. In questi casi l'acquisizione dell'oggetto non fallisce. Invece, qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e successivamente spostata nella posizione corretta.
  - **Quando le regole ILM filtrano in base alle dimensioni**: quando si valuta ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non in base alle dimensioni dell'oggetto. Ciò significa che parti di un oggetto possono essere archiviate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, al momento dell'acquisizione ogni parte da 1 GB di un caricamento multiparte da 10 parti viene archiviata in DC2. Quando l'ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Rigoroso) L'inserimento non fallisce quando i tag degli oggetti o i metadati vengono aggiornati e non è possibile effettuare nuovi posizionamenti richiesti**: con Rigoroso, ci si aspetta che gli oggetti vengano posizionati come descritto dalla regola ILM oppure che l'inserimento fallisca. Tuttavia, quando si aggiornano i metadati o i tag per un oggetto già archiviato nella griglia, l'oggetto non viene reinserito. Ciò significa che le modifiche al posizionamento degli oggetti attivate dall'aggiornamento non vengono apportate immediatamente. Le modifiche al posizionamento vengono apportate quando l'ILM viene rivalutato tramite i normali processi ILM in background. Se non è possibile apportare le modifiche di posizionamento richieste (ad esempio perché una posizione appena richiesta non è disponibile), l'oggetto aggiornato mantiene la sua posizione attuale finché non saranno possibili le modifiche di posizionamento.

Limitazioni sul posizionamento degli oggetti con le opzioni Bilanciato e Rigoroso

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

- Posizionamento in un Cloud Storage Pool al giorno 0.
- Posizionamenti in un pool di archiviazione cloud quando la regola ha un orario di creazione definito dall'utente come orario di riferimento.

Queste restrizioni esistono perché StorageGRID non può creare copie sincrone su un Cloud Storage Pool e un orario di creazione definito dall'utente potrebbe essere risolto nel presente.

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

Sia la regola ILM che la scelta della 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 quando un oggetto viene archiviato influisce sul posizionamento iniziale dei metadati degli oggetti. Poiché StorageGRID richiede l'accesso sia ai dati che ai metadati di un oggetto per soddisfare le richieste dei client, la selezione di livelli di protezione corrispondenti per la coerenza e il comportamento di acquisizione può garantire 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, altrimenti la richiesta non andrà a buon fine.
- **Strong-global**: i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti. Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.
- **Strong-site**: i metadati degli oggetti vengono immediatamente distribuiti agli altri nodi del sito. Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
- **Lettura dopo nuova scrittura**: garantisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e 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, utilizzare 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 inesistenti). Non supportato per i bucket S3 FabricPool .

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

Esempio di come la coerenza e le regole ILM possono interagire

Supponiamo di avere una griglia a due siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM**: creare due copie dell'oggetto, una nel sito locale e una in un sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **coerenza**: Strong-global (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie dell'oggetto e

distribuisce i metadati a entrambi i siti prima di restituire l'esito positivo al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione corretta del messaggio. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto sia dei metadati dell'oggetto sono ancora presenti nel sito remoto. L'oggetto è completamente recuperabile.

Se invece si utilizzasse la stessa regola ILM e la coerenza del sito forte, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati sul sito remoto, ma prima che i metadati dell'oggetto vengano distribuiti lì. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso subito dopo l'acquisizione, anche i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

L'interrelazione tra coerenza e regole ILM può essere complessa. Se hai bisogno di assistenza, contatta NetApp .

Informazioni correlate

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

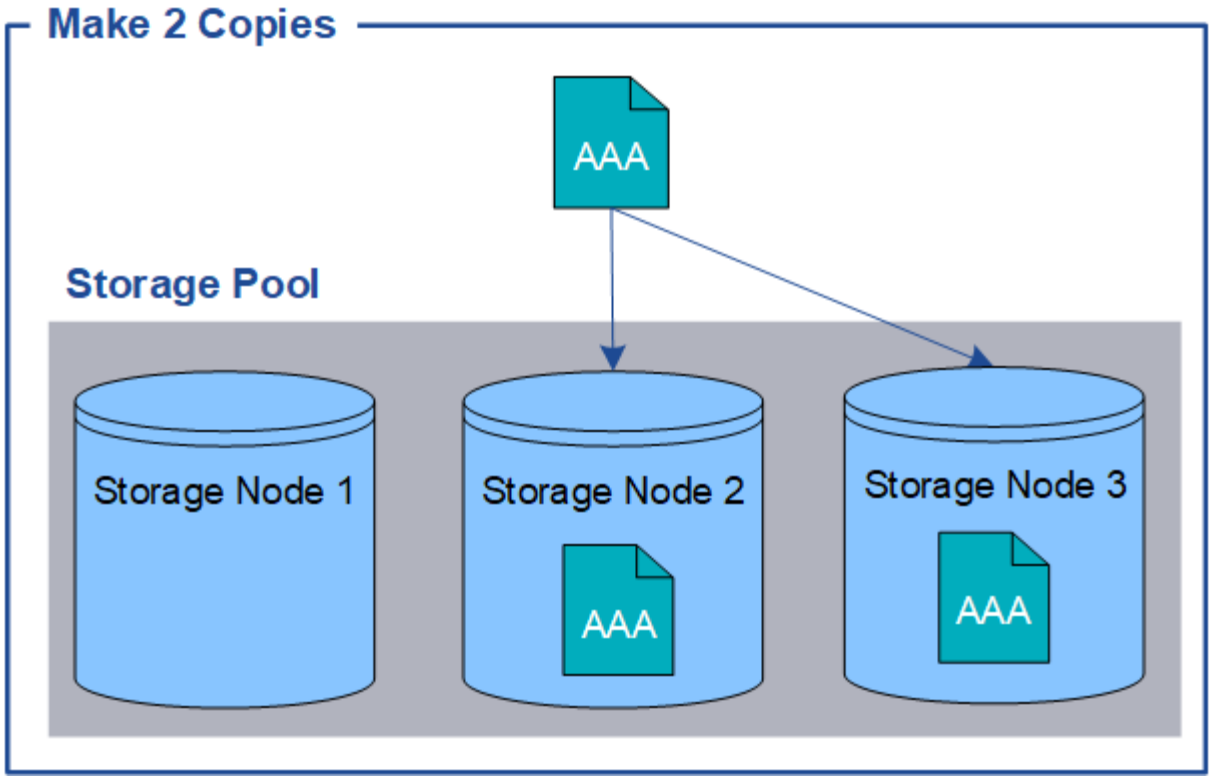
Come vengono memorizzati gli oggetti (codifica di replicazione o cancellazione)

Che cosa è la replicazione?

La replica è uno dei due metodi utilizzati da StorageGRID per archiviare 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 dell'oggetto e memorizza le copie sui nodi di archiviazione.

Quando si configura una regola ILM per creare copie replicate, si specifica quante copie devono essere create, dove devono essere posizionate e per quanto tempo devono essere conservate in ogni posizione.

Nell'esempio seguente, la regola ILM specifica che due copie replicate di ciascun oggetto devono essere posizionate in un pool di archiviazione contenente tre nodi di archiviazione.



Quando StorageGRID abbina gli oggetti a questa regola, crea due copie dell'oggetto, posizionando ciascuna copia su un diverso nodo di archiviazione nel pool di archiviazione. Le due copie possono essere posizionate su due qualsiasi dei tre nodi di archiviazione disponibili. In questo caso, la regola ha posizionato copie degli oggetti sui nodi di archiviazione 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato se uno qualsiasi dei nodi nel pool di archiviazione si guasta.

> StorageGRID può archiviare solo una copia replicata di un oggetto su un dato nodo di archiviazione. Se la griglia include tre nodi di archiviazione e si crea una regola ILM a 4 copie, verranno create solo tre copie: una copia per ciascun nodo di archiviazione. L'avviso **Posizionamento ILM non realizzabile** viene attivato per indicare che la regola ILM non può essere applicata completamente.

Informazioni correlate

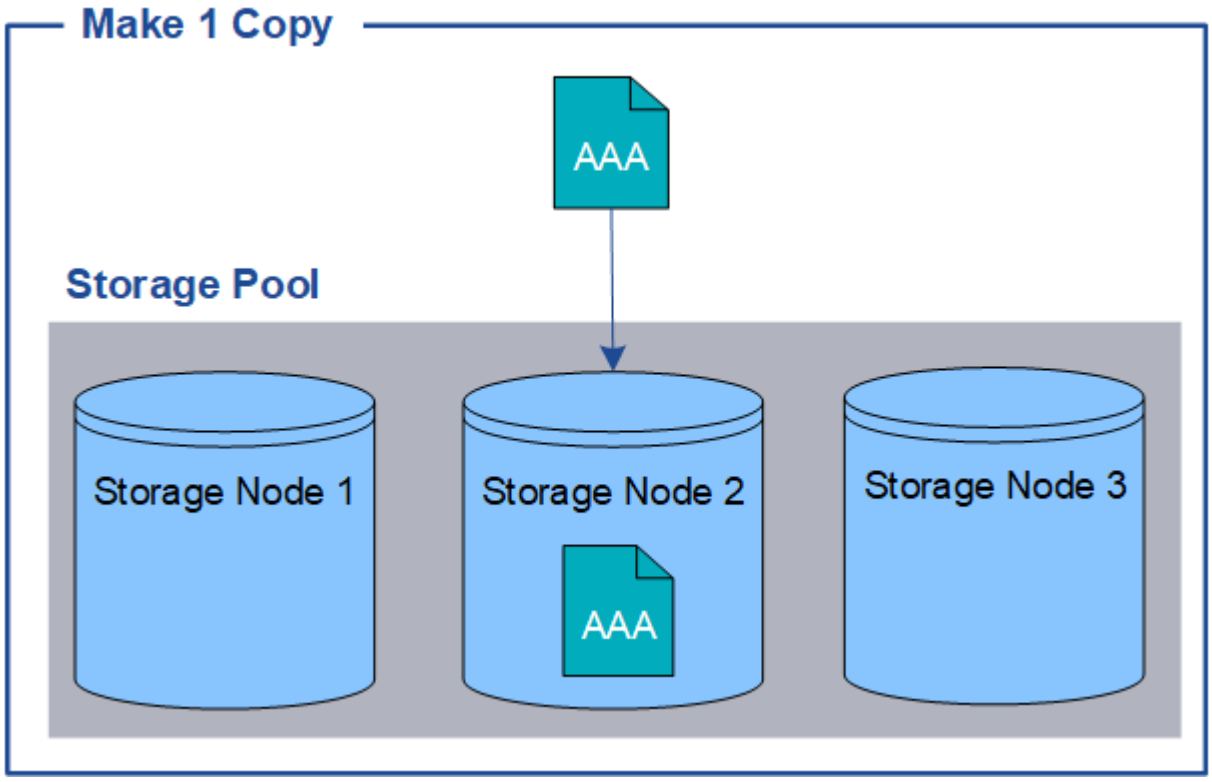
- "Che cosa è la codifica di cancellazione"
- "Che cos'è un pool di archiviazione"
- "Abilita la protezione contro la perdita del sito utilizzando la codifica di replicazione e cancellazione"

Perché non dovresti usare la replicazione a copia singola

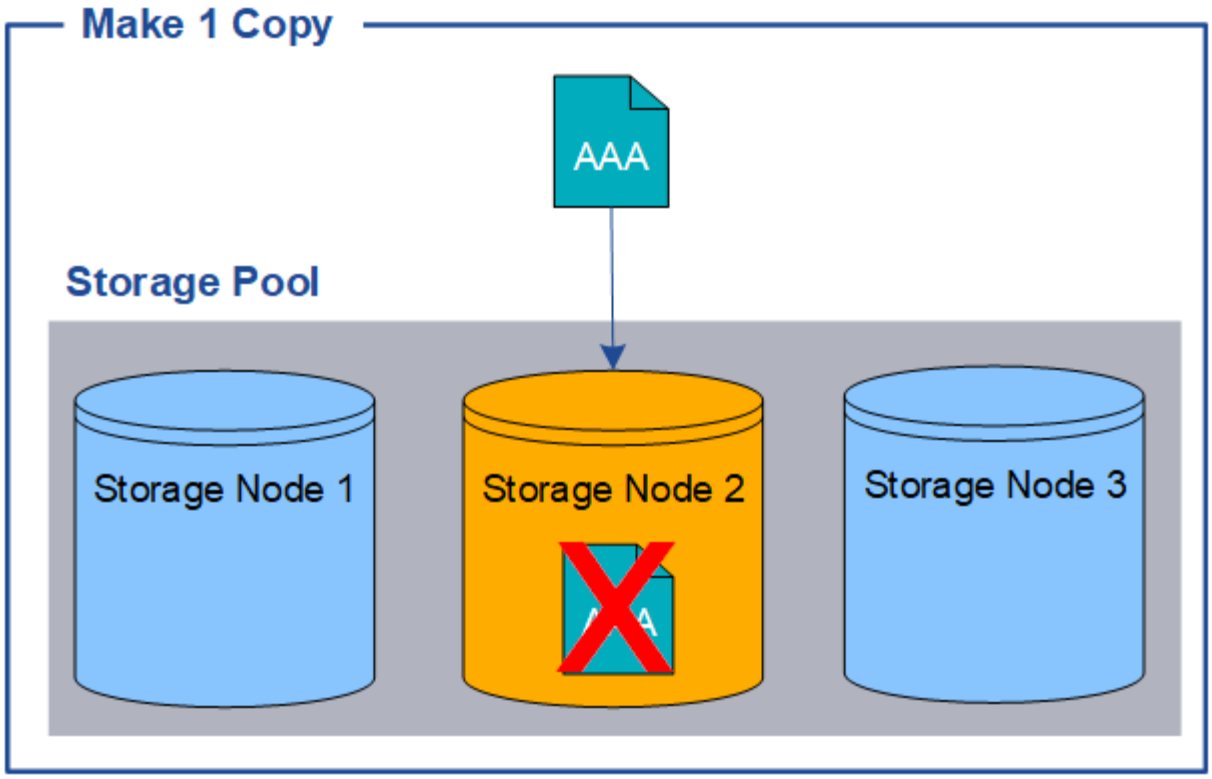
Quando si crea una regola ILM per creare copie replicate, è necessario specificare sempre almeno due copie per qualsiasi periodo di tempo nelle istruzioni di posizionamento.

> Non utilizzare una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

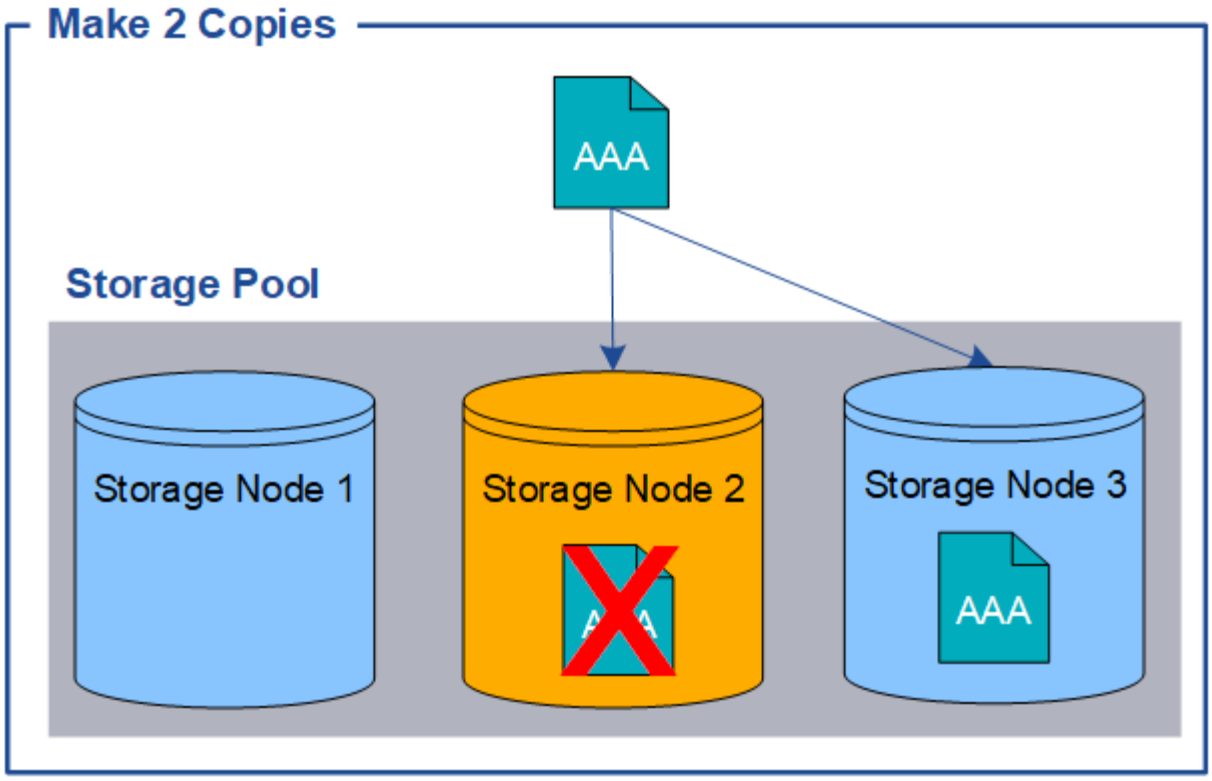
Nell'esempio seguente, la regola ILM Make 1 Copy specifica che una copia replicata di un oggetto venga inserita in un pool di archiviazione contenente tre nodi di archiviazione. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID ne posiziona una singola copia su un solo nodo di archiviazione.



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



Per evitare di perdere i dati degli oggetti, è consigliabile effettuare sempre almeno due copie di tutti gli oggetti che si desidera proteggere con la replica. Se esistono due o più copie, è comunque possibile accedere all'oggetto se un nodo di archiviazione si guasta o va offline.



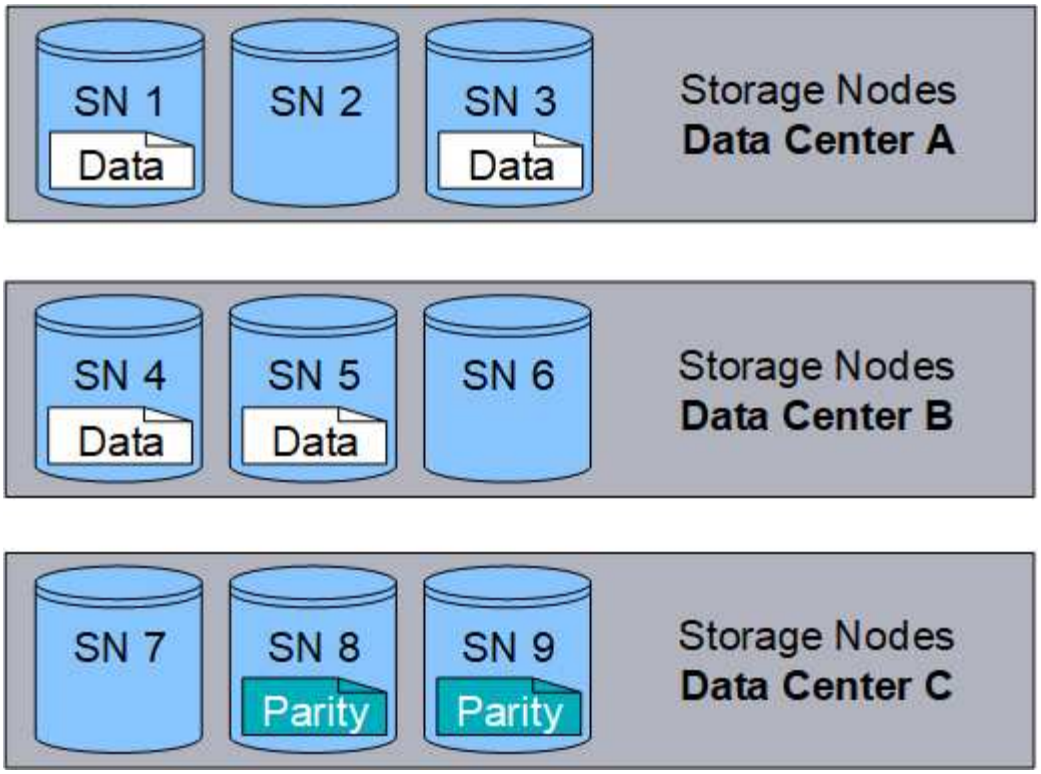
Che cos'è la codifica di cancellazione?

La codifica di cancellazione è uno dei due metodi utilizzati StorageGRID per archiviare i dati degli oggetti (l'altro metodo è la replica). Quando gli oggetti corrispondono a una regola ILM che utilizza la codifica di cancellazione, tali oggetti vengono suddivisi in frammenti di dati, vengono calcolati frammenti di parità aggiuntivi e ogni frammento viene archiviato su un diverso nodo di archiviazione.

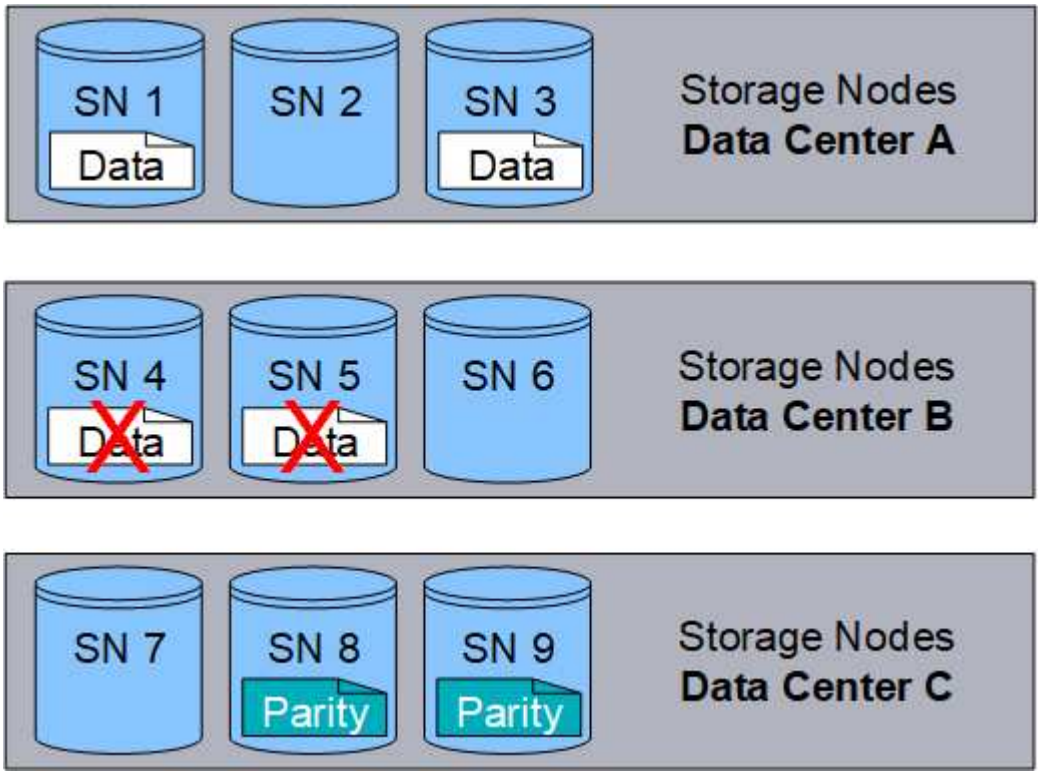
Quando si accede a un oggetto, questo viene riassemblato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità si danneggia o viene perso, l'algoritmo di codifica di cancellazione può ricreare quel frammento utilizzando un sottoinsieme dei dati e dei frammenti di parità rimanenti.

Quando si creano regole ILM, StorageGRID crea profili di codifica di cancellazione che supportano tali regole. È possibile visualizzare un elenco di profili di codifica di cancellazione,"rinominare un profilo di codifica di cancellazione" , O"disattivare un profilo di codifica di cancellazione se non è attualmente utilizzato in nessuna regola ILM" .

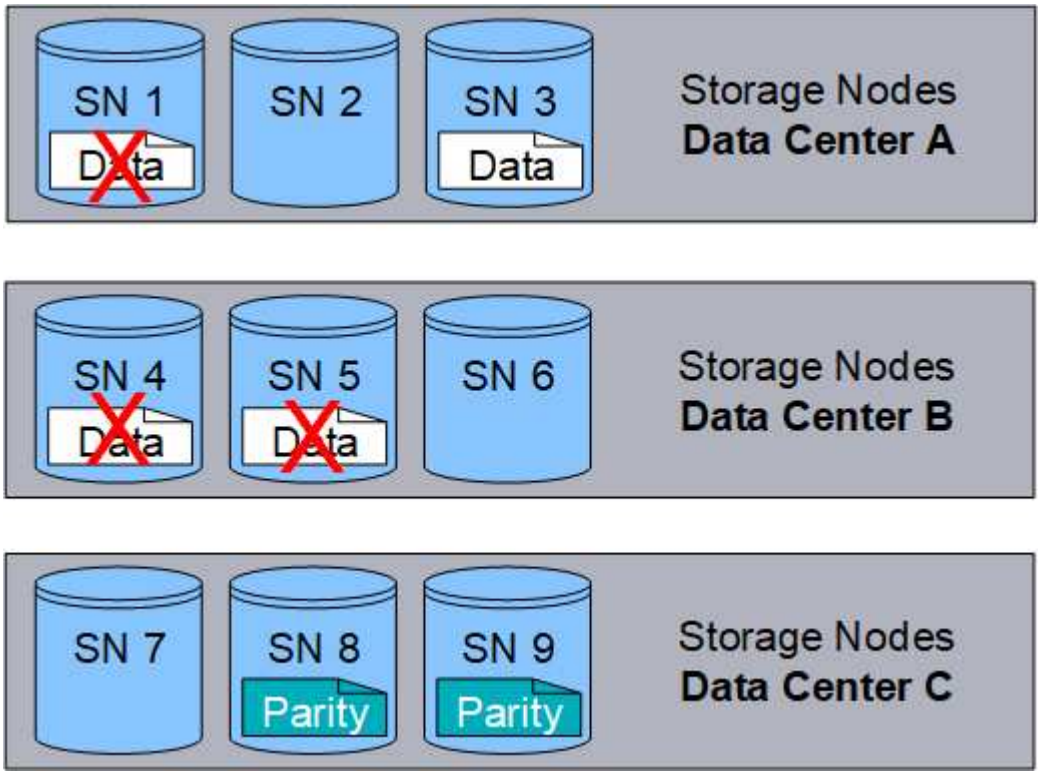
L'esempio seguente illustra l'uso di un algoritmo di codifica di cancellazione sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di codifica di cancellazione 4+2. Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e dai dati dell'oggetto vengono calcolati due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



Lo schema di codifica a cancellazione 4+2 può essere configurato in vari modi. Ad esempio, è possibile configurare un pool di archiviazione a sito singolo contenente sei nodi di archiviazione. Per"protezione contro la perdita del sito" , è possibile utilizzare un pool di archiviazione contenente tre siti con tre nodi di archiviazione in ciascun sito. Un oggetto può essere recuperato finché rimangono disponibili quattro dei sei frammenti (dati o parità). È possibile 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, a patto che tutti gli altri frammenti rimangano accessibili.



Se vengono persi più di due nodi di archiviazione, l'oggetto non sarà recuperabile.



Informazioni correlate

- "Che cosa è la replicazione"
- "Che cos'è un pool di archiviazione"
- "Cosa sono gli schemi di codifica di cancellazione"
- "Rinominare un profilo di codifica di cancellazione"
- "Disattivare un profilo di codifica di cancellazione"

Cosa sono gli schemi di codifica di cancellazione?

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

Quando si crea o si modifica una regola ILM, si seleziona uno schema di codifica di cancellazione disponibile. StorageGRID crea automaticamente schemi di codifica di cancellazione in base al numero di nodi di archiviazione e siti che compongono il pool di archiviazione che si intende utilizzare.

Protezione dei dati

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

IL `k + m = n` i frammenti sono sparsi `n` Nodi di archiviazione per garantire la protezione dei dati come segue:

- Per recuperare o riparare un oggetto, `k` sono necessari frammenti.
- Un oggetto può sostenere fino a `m` frammenti persi o corrotti. Più alto è il valore di `m` , maggiore è la tolleranza al guasto.

La migliore protezione dei dati è fornita dallo schema di codifica di cancellazione con la più alta tolleranza ai guasti del nodo o del volume all'interno di un pool di archiviazione.

Spese di archiviazione generali

Il sovraccarico di archiviazione di uno schema di codifica di cancellazione viene calcolato dividendo il numero di frammenti di parità(`m`) dal numero di frammenti di dati(`k`). È possibile utilizzare il sovraccarico di archiviazione per calcolare la quantità di spazio su disco richiesta da ciascun oggetto con codice di cancellazione:

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

Ad esempio, se si archivia un oggetto da 10 MB utilizzando lo schema 4+2 (che ha un overhead di archiviazione del 50%), l'oggetto consuma 15 MB di spazio di archiviazione della griglia. Se si memorizza lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (che ha un overhead di archiviazione del 33%), l'oggetto consuma circa 13,3 MB.

Selezionare 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 oggetto
- Hanno prestazioni migliori perché la dimensione del frammento è maggiore
- Possono richiedere che vengano aggiunti meno nodi in un"espansione quando è necessario più spazio di archiviazione"

Linee guida per i pool di stoccaggio

Quando si seleziona il pool di archiviazione da utilizzare per una regola che creerà una copia con codice di cancellazione, attenersi alle seguenti linee guida per i pool di archiviazione:

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

  > Non è possibile utilizzare la codifica di cancellazione se il pool di archiviazione include due siti.

  - Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti
  - Schemi di codifica di cancellazione per pool di archiviazione monosito
- Non utilizzare un pool di archiviazione che includa il sito Tutti i siti.
- Il pool di archiviazione dovrebbe includere almeno *`k+m`* `+1` Nodi di archiviazione in grado di archiviare dati di oggetti.

  > Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano solo metadati degli oggetti e non dati degli oggetti. Per ulteriori informazioni, consultare "Tipi di nodi di archiviazione" .

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

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

Nella tabella seguente vengono descritti gli schemi di codifica di cancellazione attualmente supportati da StorageGRID per i pool di archiviazione che includono tre o più siti. Tutti questi schemi garantiscono una protezione contro le perdite del sito. Anche se un sito può andare perso, l'oggetto sarà comunque accessibile.

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

Schema di codifica di cancellazione (*k+m*)	Numero minimo di siti distribuiti	Numero consigliato di nodi di archiviazione in ogni sito	Numero totale consigliato di nodi di archiviazione	Protezione contro le perdite del sito?	Spese di archiviazione generali
4+2	3	3	9	SÌ	50%
6+2	4	3	12	SÌ	33%
8+2	5	3	15	SÌ	25%
6+3	3	4	12	SÌ	50%
9+3	4	4	16	SÌ	33%
2+1	3	3	9	SÌ	50%
4+1	5	3	15	SÌ	25%
6+1	7	3	21	SÌ	17%
7+5	3	5	15	SÌ	71%

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

Quando si seleziona uno schema di codifica di cancellazione che garantisca la protezione del sito, è necessario valutare 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 avendo più segmenti di parità (ovvero, quando `m` ha un valore più alto.)
- **Traffico di rete**: durante il ripristino da guasti, utilizzando uno schema con più frammenti (ovvero, un totale più elevato per `k+m`) crea più traffico di rete.
- **Sovraccarico di archiviazione**: gli schemi con sovraccarico più elevato richiedono più spazio di archiviazione per oggetto.

Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3 (entrambi con un overhead di archiviazione del 50%), selezionare lo schema 6+3 se è richiesta una tolleranza agli errori aggiuntiva. Selezionare lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, seleziona 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 l'assistenza tecnica.

Schemi di codifica di cancellazione per pool di archiviazione monosito

Un pool di archiviazione 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 nodi di archiviazione.

Il numero minimo di nodi di archiviazione richiesti è `k+m` , ma un pool di archiviazione con `k+m +1` Si consiglia l'uso di Storage Nodes. Ad esempio, lo schema di codifica di cancellazione 2+1 richiede un pool di archiviazione con un minimo di tre nodi di archiviazione, ma si consigliano quattro nodi di archiviazione.

Schema di codifica di cancellazione (*k*+*m*)	Numero minimo di nodi di archiviazione	Numero consigliato di nodi di archiviazione	Spese di archiviazione generali
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 della codifica di cancellazione

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

Vantaggi della codifica di cancellazione

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

- **Affidabilità**: l'affidabilità viene misurata in termini di tolleranza ai guasti, ovvero il numero di guasti simultanei che possono essere sostenuti senza perdita di dati. Con la replicazione, più copie identiche vengono archiviate su nodi diversi e in più siti. Con la codifica di cancellazione, un oggetto viene codificato in frammenti di dati e parità e distribuito su molti nodi e siti. Questa dispersione garantisce protezione contro i guasti sia del sito che del nodo. Rispetto alla replicazione, la codifica di cancellazione garantisce una maggiore affidabilità a costi di archiviazione comparabili.
- **Disponibilità**: la disponibilità può essere definita come la capacità di recuperare oggetti se i nodi di archiviazione falliscono o diventano inaccessibili. Rispetto alla replicazione, la codifica di cancellazione garantisce una maggiore disponibilità a costi di archiviazione comparabili.
- **Efficienza di archiviazione**: per livelli simili di disponibilità e affidabilità, gli oggetti protetti tramite codifica di cancellazione consumano meno spazio su disco rispetto a quanto farebbero se protetti tramite replica. Ad esempio, un oggetto da 10 MB replicato su due siti consuma 20 MB di spazio su disco (due copie), mentre un oggetto codificato con cancellazione su tre siti con uno schema di codifica con cancellazione 6+3 consuma solo 15 MB di spazio su disco.

> Lo spazio su disco per gli oggetti con codice di cancellazione viene calcolato sommando le dimensioni dell'oggetto al sovraccarico di archiviazione. La percentuale di sovraccarico di archiviazione è il 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:

- Si consiglia un numero maggiore di nodi e siti di archiviazione, a seconda dello schema di codifica di cancellazione. Al contrario, se si replicano i dati degli oggetti, è necessario un solo nodo di archiviazione per ogni copia. Vedere"Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti" E"Schemi di codifica di cancellazione per pool di archiviazione monosito" .
- Aumento dei costi e della complessità delle espansioni di storage. Per espandere una distribuzione che utilizza la replica, è necessario aggiungere capacità di archiviazione in ogni posizione in cui vengono eseguite le copie degli oggetti. Per espandere una distribuzione che utilizza la codifica di cancellazione, è necessario considerare sia lo schema di codifica di cancellazione in uso sia il livello di riempimento dei nodi di archiviazione esistenti. Ad esempio, se si attende che i nodi esistenti siano pieni al 100%, è necessario aggiungere almeno `k+m` Nodi di archiviazione, ma se si espande quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e continuare a massimizzare la capacità di archiviazione utilizzabile. Per ulteriori informazioni, consultare "Aggiungere capacità di archiviazione per oggetti con codice di cancellazione" .
- Quando si utilizza la codifica di cancellazione su siti distribuiti geograficamente, si verificano latenze di recupero maggiori. I frammenti di un oggetto codificato in modo da essere cancellato e distribuito su siti remoti richiedono più tempo per essere recuperati tramite connessioni WAN rispetto a un oggetto replicato e disponibile localmente (lo stesso sito a cui si connette il client).
- Quando si utilizza la codifica di cancellazione su siti distribuiti geograficamente, si verifica un utilizzo maggiore del traffico di rete WAN per recuperi e riparazioni, in particolare per oggetti recuperati frequentemente o per riparazioni di oggetti su connessioni di rete WAN.
- Quando si utilizza la codifica di cancellazione su più siti, la velocità massima di elaborazione degli oggetti diminuisce drasticamente all'aumentare della latenza di rete tra i siti. Questa diminuzione è dovuta alla corrispondente diminuzione della velocità di trasmissione della rete TCP, che influisce sulla velocità con cui il sistema StorageGRID può archiviare e recuperare frammenti di oggetti.
- Maggiore utilizzo delle risorse di elaborazione.

Quando utilizzare la codifica di cancellazione

La codifica di cancellazione è più adatta ai 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 utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

- Archiviazione a lungo termine o a freddo per contenuti recuperati raramente.
- Elevata disponibilità e affidabilità dei dati.
- Protezione contro guasti completi del sito e del nodo.
- Efficienza di archiviazione.
- Distribuzioni in un unico sito che richiedono una protezione efficiente dei dati con una sola copia con codice di cancellazione anziché più copie replicate.
- Distribuzioni multi-sito in cui la latenza tra i siti è inferiore a 100 ms.

Come viene determinata la ritenzione dell'oggetto

StorageGRID offre opzioni sia agli amministratori della griglia sia ai singoli utenti tenant per specificare per quanto tempo archiviare gli oggetti. In generale, tutte le istruzioni di conservazione fornite da un utente tenant hanno la precedenza sulle istruzioni di conservazione fornite dall'amministratore della griglia.

Come gli utenti tenant controllano la conservazione degli oggetti

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

- Se l'impostazione globale Blocco oggetti S3 è abilitata per la griglia, gli utenti del tenant S3 possono creare bucket con Blocco oggetti S3 abilitato e quindi selezionare un **Periodo di conservazione predefinito** per ciascun bucket.
- Se l'impostazione globale S3 Object Lock è abilitata per la griglia, gli utenti del tenant S3 possono creare bucket con S3 Object Lock abilitato e quindi utilizzare l'API REST S3 per specificare le impostazioni di conservazione fino alla data di scadenza e di conservazione legale per ogni versione dell'oggetto aggiunta a tale bucket.
  - Una versione di un oggetto sottoposta a conservazione legale non può essere eliminata con alcun metodo.
  - Prima che venga raggiunta la data di conservazione di una versione di un oggetto, tale versione non può essere eliminata con alcun metodo.
  - Gli oggetti nei bucket con S3 Object Lock abilitato vengono conservati da ILM "per sempre". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta del client o dalla scadenza del ciclo di vita del bucket. Vedere "Gestisci gli oggetti con S3 Object Lock" .
- Gli utenti del tenant S3 possono aggiungere ai propri bucket una configurazione del ciclo di vita che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID archivia un oggetto finché non viene raggiunta la data o il numero di giorni specificati nell'azione Scadenza, a meno che il client non elimini prima l'oggetto. Vedere "Crea la configurazione del ciclo di vita S3" .

- Un client S3 può inviare una richiesta di eliminazione di un oggetto. StorageGRID dà sempre priorità alle richieste di eliminazione del client rispetto al ciclo di vita del bucket S3 o all'ILM quando decide 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 del blocco degli oggetti S3 per ciascun tenant. Quindi, gli utenti tenant possono impostare un periodo di conservazione predefinito per ciascuno dei loro bucket. Il periodo di conservazione massimo viene applicato anche a tutti gli oggetti appena acquisiti per quel bucket (data di conservazione dell'oggetto).
- Creare istruzioni di posizionamento ILM per controllare per quanto tempo gli oggetti vengono conservati. Quando gli oggetti corrispondono a una regola ILM, StorageGRID li memorizza finché non è trascorso l'ultimo periodo di tempo nella regola ILM. Gli oggetti vengono conservati indefinitamente se nelle istruzioni di posizionamento è specificato "per sempre".
- Indipendentemente da chi controlla per quanto tempo gli oggetti vengono conservati, le impostazioni ILM controllano quali tipi di copie degli oggetti (replicate o con codice di cancellazione) vengono archiviate e dove si trovano le copie (nodi di archiviazione o pool di archiviazione cloud).

Come interagiscono il ciclo di vita del bucket S3 e ILM

Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita. Di conseguenza, un oggetto potrebbe essere mantenuto sulla griglia anche dopo che sono scadute tutte le istruzioni ILM per il posizionamento dell'oggetto.

Esempi di conservazione degli oggetti

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

Esempio 1: il ciclo di vita del bucket S3 conserva gli oggetti più a lungo di ILM

ILM

Conservare due copie per 1 anno (365 giorni)

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Risultato

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

> Se il ciclo di vita del bucket specifica che gli oggetti devono essere conservati più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento ILM quando determina il numero e il tipo di copie da archiviare. In questo esempio, due copie dell'oggetto continueranno a essere archiviate 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

Conservare due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Scadenza degli oggetti in 1 anno (365 giorni)

Risultato

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

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

ILM

Conserva due copie sui nodi di archiviazione "per sempre"

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Richiesta di eliminazione del cliente

Emesso il giorno 400

Risultato

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

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

Blocco oggetto S3

La data di conservazione per una versione dell'oggetto è il 31/03/2026. Non è in vigore alcun blocco legale.

Regola ILM conforme

Conserva due copie sui nodi di archiviazione "per sempre"

Richiesta di eliminazione del cliente

Pubblicato il 31/03/2024

Risultato

StorageGRID non eliminerà la versione dell'oggetto perché la data di conservazione è ancora lontana 2 anni.

Come vengono eliminati gli oggetti

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

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

- Eliminazione sincrona: quando StorageGRID riceve una richiesta di eliminazione da parte del client, tutte le copie degli oggetti vengono rimosse immediatamente. Dopo aver rimosso le copie, il cliente viene

informato che l'eliminazione è avvenuta con successo.

- 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 correttamente. Le copie degli oggetti vengono rimosse in seguito tramite l'elaborazione ILM in background.

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

La tabella riepiloga quando StorageGRID utilizza ciascun metodo.

Metodo di esecuzione dell'eliminazione	Quando utilizzato
Gli oggetti vengono messi in coda per l'eliminazione	Quando **una** delle seguenti condizioni è vera: • L'eliminazione automatica degli oggetti è stata attivata da uno dei seguenti eventi: ◦ È stata raggiunta la data di scadenza o il numero di giorni 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 in cui è abilitato il blocco degli oggetti S3 non possono essere eliminati se sono sottoposti a conservazione legale o se è stata specificata una data di conservazione fino a quando non è stata ancora rispettata. • Un client S3 richiede l'eliminazione e una o più di queste condizioni sono vere: ◦ Le copie non possono essere eliminate 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. Quindi passa all'esecuzione dell'eliminazione sincrona. Assicurandosi che la coda di eliminazione in background abbia oggetti da elaborare, StorageGRID può elaborare le eliminazioni in modo più efficiente, soprattutto per i client con bassa concorrenza, contribuendo al contempo a prevenire gli arretrati di eliminazione dei client.

Tempo necessario per eliminare gli oggetti

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

- Quando StorageGRID esegue l'eliminazione sincrona, potrebbero essere necessari fino a 30 secondi prima che StorageGRID restituisca un risultato al client. Ciò significa che l'eliminazione può sembrare più

lenta, anche se in realtà le copie vengono rimosse più rapidamente rispetto a quando StorageGRID mette in coda gli oggetti per l'eliminazione.

- Se si monitorano attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, si potrebbe notare che la velocità di eliminazione sembra essere lenta dopo l'eliminazione di un certo numero di oggetti. Questa modifica si verifica quando StorageGRID passa dalla messa in coda degli oggetti per l'eliminazione all'esecuzione dell'eliminazione sincrona. L'apparente riduzione del tasso 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 si eliminano un gran numero di oggetti e la priorità è liberare spazio rapidamente, si può prendere in considerazione l'utilizzo di una richiesta client per eliminare gli oggetti anziché eliminarli tramite ILM o altri metodi. In generale, lo spazio viene liberato più rapidamente quando l'eliminazione viene eseguita dai client, perché StorageGRID può utilizzare l'eliminazione sincrona.

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

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

Come vengono eliminati gli oggetti con versione S3

Quando il controllo delle versioni è abilitato per un bucket S3, StorageGRID segue il comportamento di Amazon S3 quando risponde alle richieste di eliminazione, indipendentemente dal fatto 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 sottoposti a controllo di versione, le richieste di eliminazione degli oggetti non eliminano la versione corrente dell'oggetto e non liberano spazio. Al contrario, una richiesta di eliminazione di un oggetto crea un marcatore di eliminazione di zero byte come versione corrente dell'oggetto, il che rende la versione precedente dell'oggetto "non corrente". Un marcatore di eliminazione di un oggetto diventa un marcatore di eliminazione di un oggetto scaduto quando è la versione corrente e non ci sono versioni non correnti.

Anche se l'oggetto non è stato rimosso, StorageGRID si comporta come se la versione corrente dell'oggetto non fosse più disponibile. Le richieste a 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.

Per liberare spazio durante l'eliminazione di oggetti sottoposti a controllo di versione o per rimuovere i marcatori di eliminazione, utilizzare una delle seguenti opzioni:

- **Richiesta client S3**: specificare l'ID della versione dell'oggetto nella richiesta S3 DELETE Object(`DELETE /object?versionId=ID`). Tieni presente che questa richiesta rimuove solo le copie degli oggetti per la versione specificata (le altre versioni continuano a occupare spazio).
- **Ciclo di vita del bucket**: utilizzare il `NoncurrentVersionExpiration` azione 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.

  IL `NewerNoncurrentVersions` l'azione nella configurazione del ciclo di vita del bucket specifica il numero di versioni non correnti conservate in un bucket S3 con versione. Se ci sono più versioni non correnti di `NewerNoncurrentVersions` specifica che StorageGRID rimuove le versioni precedenti

quando è trascorso il valore NoncurrentDays. IL `NewerNoncurrentVersions` la soglia sovrascrive le regole del ciclo di vita fornite da ILM, il che significa che un oggetto non corrente con una versione all'interno di `NewerNoncurrentVersions` la soglia viene mantenuta se ILM ne richiede l'eliminazione.

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

- **ILM**:"Clonare una policy attiva" e aggiungere due regole ILM alla nuova policy:
  - Prima regola: utilizzare "Tempo non corrente" come tempo di riferimento per far corrispondere le versioni non correnti dell'oggetto. In"Passaggio 1 (Immissione dei dettagli) della procedura guidata Crea una regola ILM" , seleziona **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?"
  - Seconda regola: utilizzare **Tempo di acquisizione** in modo che corrisponda alla versione corrente. La regola "Tempo non corrente" deve comparire nella policy sopra la regola **Tempo di inserimento**.

    Per rimuovere i marcatori di eliminazione degli oggetti scaduti, utilizzare una regola **Tempo di acquisizione** che corrisponda ai marcatori di eliminazione correnti. I marcatori di eliminazione vengono rimossi solo quando è trascorso un **periodo di tempo** di **giorni** e l'attuale marcatore di eliminazione è scaduto (non ci sono versioni non correnti).
- **Elimina oggetti nel bucket**: usa il gestore tenant per"elimina tutte le versioni dell'oggetto" , compresi i marcatori di eliminazione, da un bucket.

Quando un oggetto con versione viene eliminato, StorageGRID crea un marcatore di eliminazione a zero byte come versione corrente dell'oggetto. Prima di poter eliminare un bucket con versione, è necessario rimuovere tutti gli oggetti e i marcatori di eliminazione.

- 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 dagli oggetti di eliminazione nelle operazioni del bucket.
- I marcatori di eliminazione da un bucket creato in StorageGRID 11.8 o versione successiva possono essere rimossi tramite ILM, regole del ciclo di vita del bucket, operazioni di eliminazione degli oggetti nelle bucket o un'eliminazione esplicita del client S3.

Informazioni correlate

- "Utilizzare l'API REST S3"
- "Esempio 4: regole e policy ILM per oggetti con versione S3"

Creare e assegnare gradi di archiviazione

I gradi di archiviazione identificano il tipo di archiviazione utilizzato da un nodo di archiviazione. È possibile creare gradi di archiviazione se si desidera che le regole ILM posizionino determinati oggetti su determinati nodi di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Informazioni su questo compito

Quando installi StorageGRID per la prima volta, il livello di archiviazione **Predefinito** viene assegnato

automaticamente a ogni nodo di archiviazione nel tuo sistema. Se necessario, è possibile definire gradi di archiviazione personalizzati e assegnarli a diversi nodi di archiviazione.

Utilizzando gradi di archiviazione personalizzati è possibile creare pool di archiviazione ILM che contengono solo un tipo specifico di nodo di archiviazione. Ad esempio, potresti voler archiviare determinati oggetti sui nodi di archiviazione più veloci, come gli storage appliance all-flash StorageGRID .

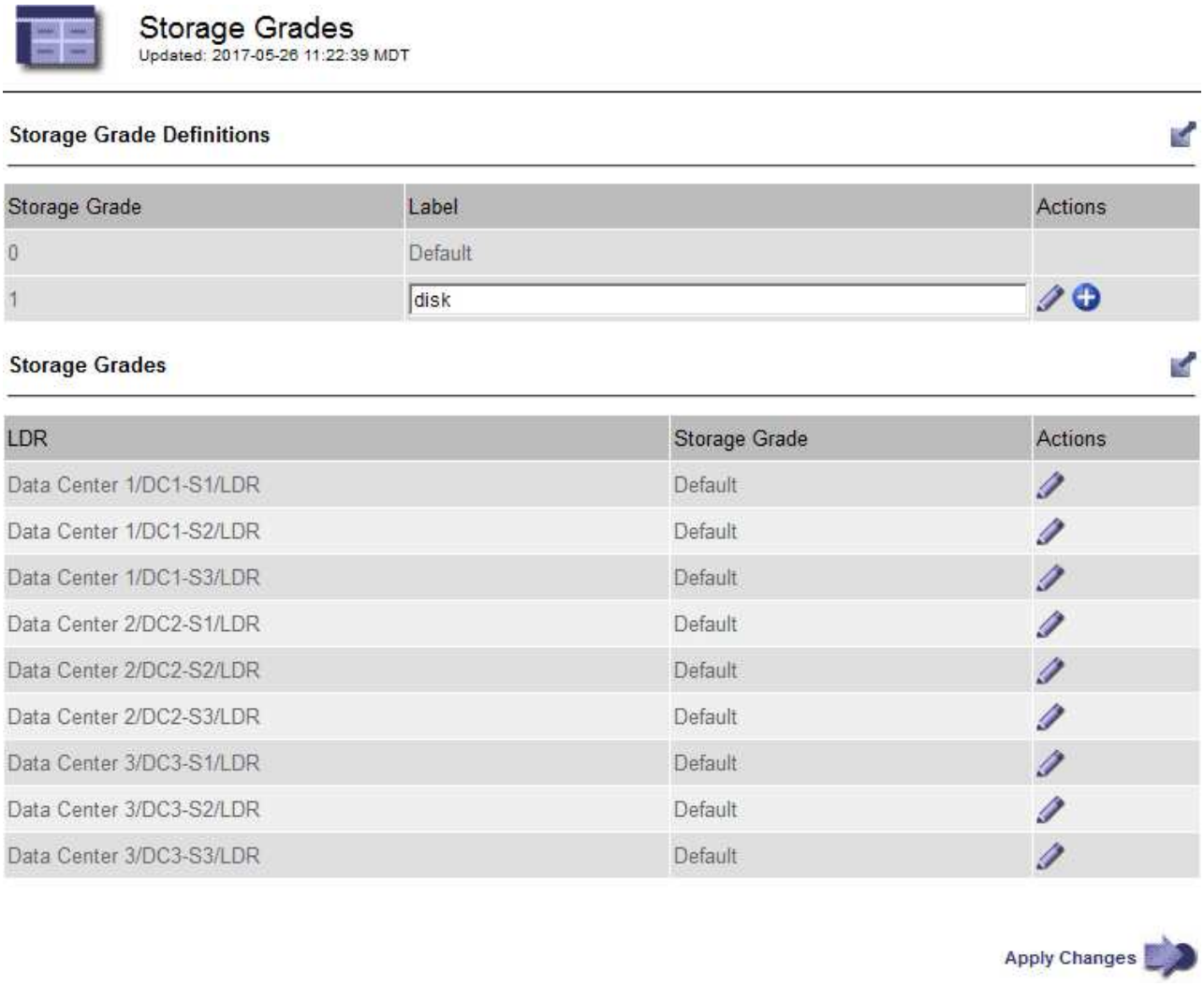
> Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano solo metadati degli oggetti e non dati degli oggetti. Ai nodi di archiviazione solo metadati non può essere assegnato un grado di archiviazione. Per ulteriori informazioni, consultare "Tipi di nodi di archiviazione" .

Se il grado di archiviazione non è un problema (ad esempio, tutti i nodi di archiviazione sono identici), è possibile saltare questa procedura e utilizzare la selezione **include tutti i gradi di archiviazione** per il grado di archiviazione quando si"creare pool di archiviazione" . Utilizzando questa selezione si garantisce che il pool di archiviazione includa tutti i nodi di archiviazione del sito, indipendentemente dal loro grado di archiviazione.

> Non creare più livelli di archiviazione del necessario. Ad esempio, non creare un grado di archiviazione per ogni nodo di archiviazione. Assegna invece ogni grado di archiviazione a due o più nodi. I gradi di archiviazione assegnati a un solo nodo possono causare arretrati ILM se il nodo in questione non è più disponibile.

Passi

1. Selezionare **ILM** > **Gradi di archiviazione**.
2. Definisci gradi di archiviazione personalizzati:
   a. Per ogni grado di archiviazione personalizzato che desideri aggiungere, seleziona *Inserisci* per aggiungere una riga.
   b. Inserisci un'etichetta descrittiva.



c. Selezionare **Applica modifiche**.

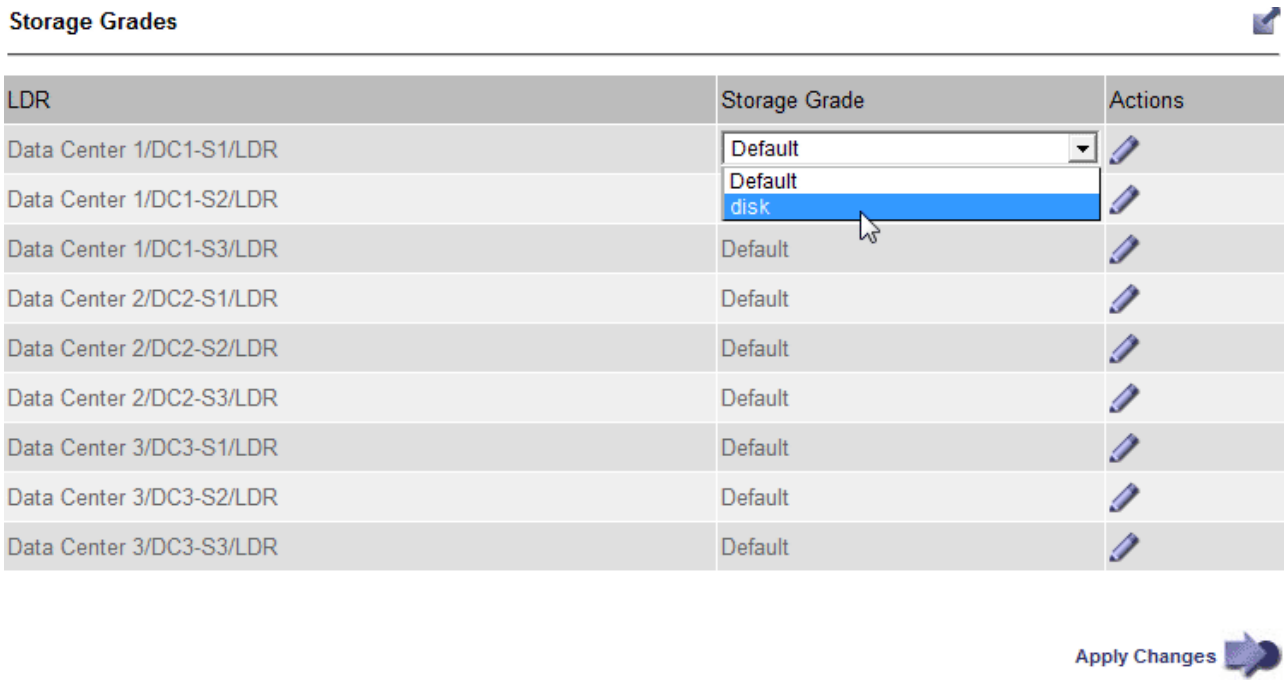
d. Facoltativamente, se devi modificare un'etichetta salvata, seleziona **Modifica*** **e seleziona *Applica modifiche**.

Non è possibile eliminare i gradi di archiviazione.

3. Assegna nuovi gradi di archiviazione ai nodi di archiviazione:

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

b. Selezionare dall'elenco il grado di conservazione appropriato.



Assegnare un grado di archiviazione a un determinato nodo di archiviazione una sola volta. Un nodo di archiviazione ripristinato dopo un errore mantiene il grado di archiviazione assegnato in precedenza. Non modificare questa assegnazione dopo l'attivazione della policy ILM. Se l'assegnazione viene modificata, i dati vengono archiviati in base al nuovo grado di archiviazione.

a. Selezionare **Applica modifiche**.

Utilizzare pool di archiviazione

Che cos'è un pool di archiviazione?

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

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

Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano dati e metadati degli oggetti oppure solo metadati degli oggetti. I nodi di archiviazione solo metadati non possono essere utilizzati nei pool di archiviazione. Per ulteriori informazioni, consultare "Tipi di nodi di archiviazione" .

I pool di archiviazione hanno due attributi:

- **Livello di archiviazione**: per i nodi di archiviazione, le prestazioni relative dell'archiviazione di supporto.
- **Sito**: Il centro dati in cui verranno archiviati gli oggetti.

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

Linee guida per la creazione di pool di archiviazione

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

Vedere "Esempi di abilitazione della protezione contro la perdita del sito mediante la codifica di replicazione e cancellazione" .

Linee guida per tutti i pool di archiviazione

- Mantenere le configurazioni dei pool di archiviazione il più semplici possibile. Non creare più pool di archiviazione del necessario.
- Creare pool di archiviazione con il maggior numero possibile di nodi. Ogni pool di archiviazione dovrebbe contenere due o più nodi. Un pool di archiviazione con nodi insufficienti può causare arretrati ILM se un nodo diventa non disponibile.
- Evitare di creare o utilizzare pool di archiviazione sovrapposti (che contengono uno o più nodi uguali). Se i pool di archiviazione si sovrappongono, è possibile che più copie dei dati degli oggetti vengano salvate sullo stesso nodo.
- In generale, non utilizzare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) o il sito All Sites. Questi elementi vengono aggiornati automaticamente per includere tutti i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato.

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

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

  Durante l'installazione StorageGRID viene creato automaticamente un pool di archiviazione per ogni sito.

  L'utilizzo di un pool di archiviazione per ogni sito garantisce che le copie degli oggetti replicati vengano posizionate esattamente dove previsto (ad esempio, una copia di ogni oggetto in ogni sito per la protezione contro la perdita del sito).

- Se si aggiunge un sito in un'espansione, creare un nuovo pool di archiviazione che contenga solo il nuovo sito. Poi,"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 archiviazione, il sistema distribuisce le copie per bilanciare l'utilizzo del disco tra i pool.
- Se i pool di archiviazione si sovrappongono (contengono gli stessi nodi di archiviazione), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. È necessario assicurarsi che i pool di archiviazione selezionati non contengano gli stessi nodi di archiviazione.

Linee guida per i pool di archiviazione utilizzati per le copie con codice di cancellazione

- Per la protezione contro la perdita del sito utilizzando"codifica di cancellazione" , creare pool di archiviazione costituiti da almeno tre siti. Se un pool di archiviazione include solo due siti, non è possibile utilizzare tale pool di archiviazione per la codifica di cancellazione. Non sono disponibili schemi di codifica di cancellazione per un pool di archiviazione con due siti.
- Il numero di nodi di archiviazione e siti contenuti nel pool di archiviazione determina quali"schemi di codifica di cancellazione" sono disponibili.

- Se possibile, un pool di archiviazione dovrebbe includere un numero di nodi di archiviazione superiore a quello minimo richiesto per lo schema di codifica di cancellazione selezionato. Ad esempio, se si utilizza uno schema di codifica di cancellazione 6+3, è necessario disporre di almeno nove nodi di archiviazione. Tuttavia, si consiglia di avere almeno un nodo di archiviazione aggiuntivo per sito.
- Distribuire i nodi di archiviazione tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di codifica di cancellazione 6+3, configurare un pool di archiviazione che includa almeno tre nodi di archiviazione in tre siti.
- Se si hanno requisiti di throughput elevati, non è consigliabile utilizzare un pool di archiviazione che includa più siti se la latenza di rete tra i siti è superiore a 100 ms. Con l'aumentare della latenza, la velocità con cui StorageGRID può creare, posizionare e recuperare frammenti di oggetti diminuisce drasticamente a causa della diminuzione della velocità di trasmissione della rete TCP.

  La riduzione della produttività influisce sulle velocità massime raggiungibili di acquisizione e recupero degli oggetti (quando come comportamento di acquisizione è selezionato Bilanciato o Rigoroso) o potrebbe causare arretrati nella coda ILM (quando come comportamento di acquisizione è selezionato Doppio commit). Vedere "Comportamento di acquisizione delle regole ILM" .

> Se la griglia include un solo sito, non è possibile utilizzare il pool di archiviazione 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 viene aggiunto un secondo sito.

Abilita la protezione contro la perdita del sito

Se la distribuzione StorageGRID include più di un sito, è possibile utilizzare la replicazione e la codifica di cancellazione con pool di archiviazione opportunamente configurati per abilitare la protezione contro la perdita del sito.

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

- Per utilizzare la replica per la protezione contro la perdita del sito, utilizzare i pool di archiviazione specifici del sito creati automaticamente durante l'installazione StorageGRID . Quindi crea regole ILM con"istruzioni per il posizionamento" che specificano più pool di archiviazione in modo che una copia di ciascun oggetto venga posizionata in ogni sito.
- Per utilizzare la codifica di cancellazione per la protezione dalla perdita del sito,"creare pool di archiviazione costituiti da più siti" . Quindi creare regole ILM che utilizzino un pool di archiviazione composto da più siti e qualsiasi schema di codifica di cancellazione disponibile.

> Quando si configura la distribuzione StorageGRID per la protezione dalle perdite del sito, è necessario tenere conto anche degli effetti di"opzioni di ingestione" E"coerenza" .

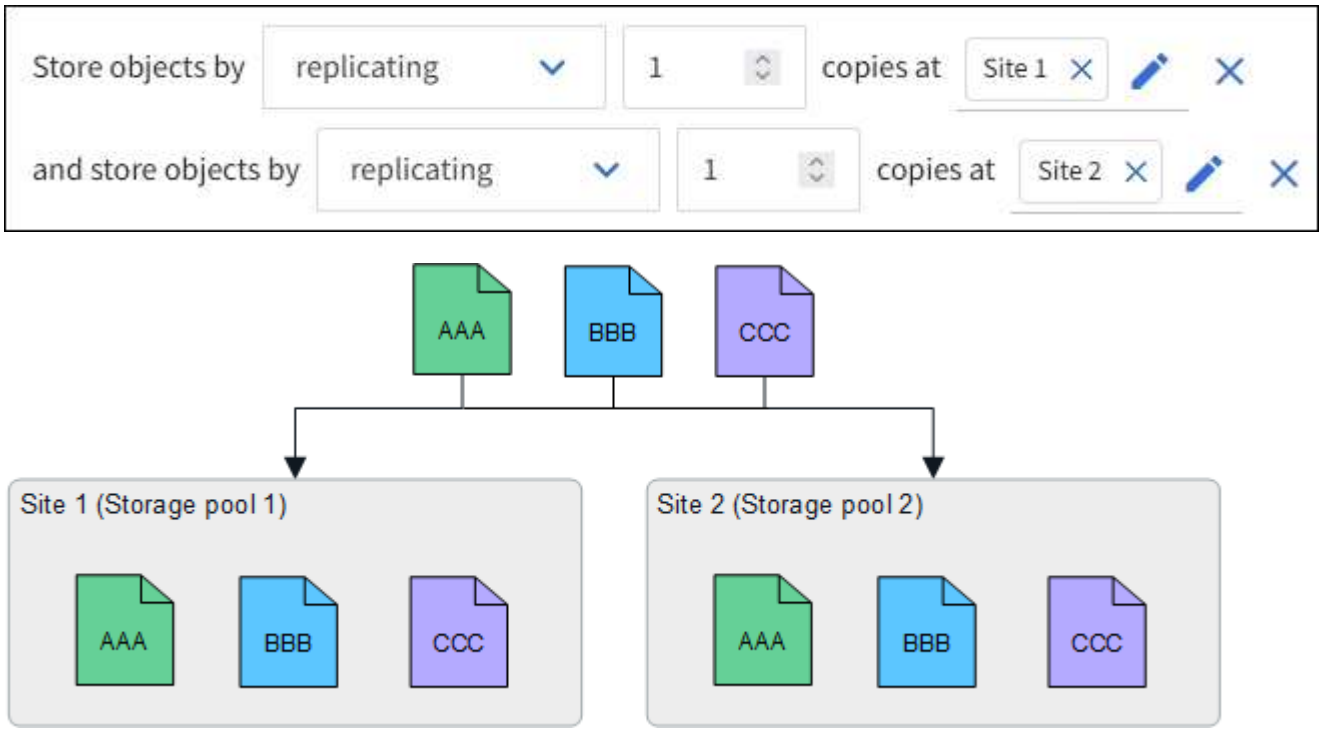
Esempio di replicazione

Per impostazione predefinita, durante l'installazione StorageGRID viene creato un pool di archiviazione per ogni sito. Disporre di pool di archiviazione costituiti da un solo sito consente di configurare regole ILM che utilizzano la replica per la protezione dalle perdite del sito. In questo esempio:

- Il pool di archiviazione 1 contiene il sito 1
- Il pool di archiviazione 2 contiene il sito 2
- La regola ILM contiene due posizionamenti:

- Memorizza gli oggetti replicandone 1 copia nel Sito 1
- Memorizza gli oggetti replicandone 1 copia nel sito 2

Posizionamenti delle regole ILM:



Se un sito viene perso, copie degli oggetti sono disponibili nell'altro sito.

Esempio di codifica di cancellazione

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

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

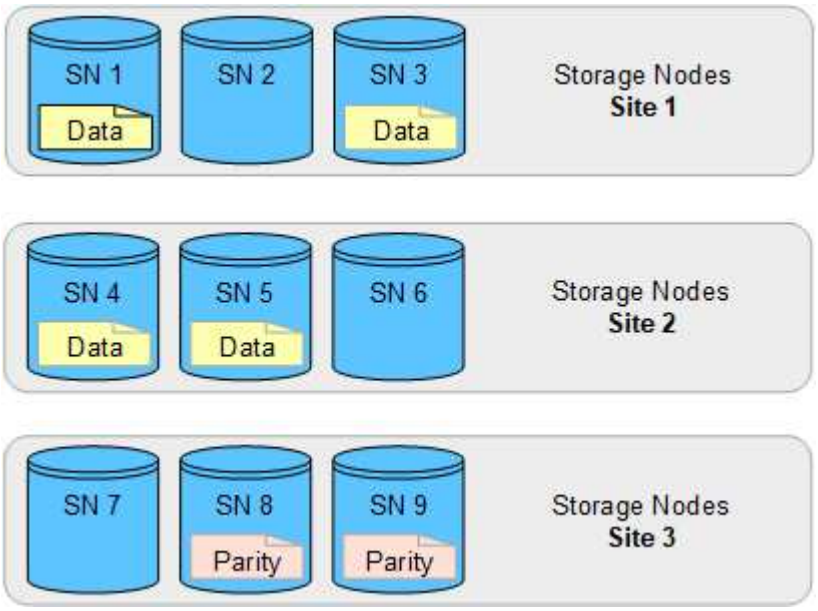
Posizionamenti delle regole ILM:

In questo esempio:

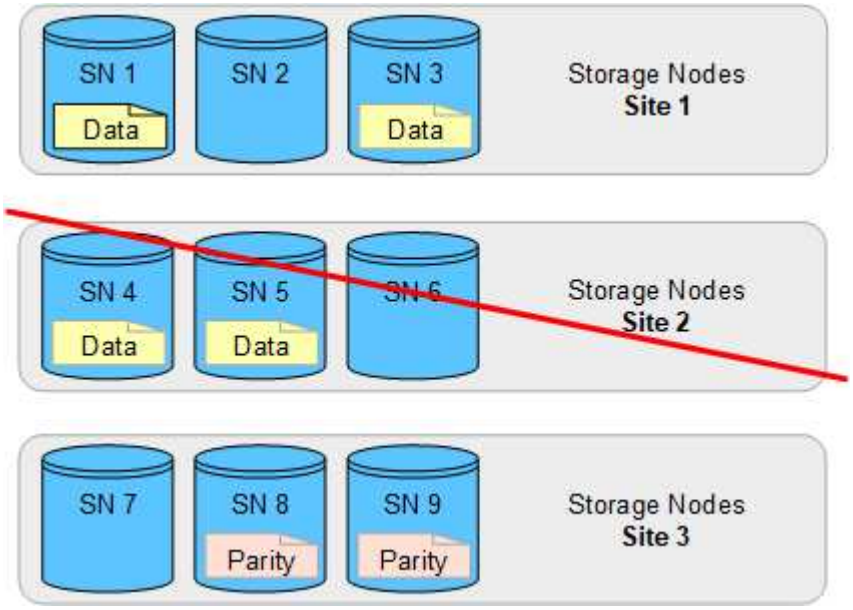
- La regola ILM utilizza uno schema di codifica a cancellazione 4+2.
- Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e dai dati dell'oggetto vengono calcolati due frammenti di parità.
- Ciascuno dei sei frammenti viene archiviato su un nodo diverso in tre siti di data center per garantire la protezione dei dati in caso di guasti dei nodi o perdite del sito.

La codifica di cancellazione è consentita nei pool di archiviazione 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:



Creare un pool di archiviazione

È possibile creare pool di archiviazione per determinare dove il sistema StorageGRID archivia i dati degli oggetti e il tipo di archiviazione utilizzato. Ogni pool di archiviazione include uno o più siti e uno o più gradi di archiviazione.

> Quando si installa StorageGRID 11.9 su una nuova griglia, vengono creati automaticamente pool di archiviazione per ciascun sito. Tuttavia, se inizialmente hai installato StorageGRID 11.6 o una versione precedente, i pool di archiviazione non vengono creati automaticamente per ogni sito.

Se si desidera creare pool di archiviazione cloud per archiviare dati di oggetti al di fuori del sistema StorageGRID , vedere"informazioni sull'utilizzo dei pool di archiviazione cloud" .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .
- Hai esaminato le linee guida per la creazione di pool di archiviazione.

Informazioni su questo compito

I pool di archiviazione determinano dove vengono archiviati i dati degli oggetti. Il numero di pool di archiviazione necessari dipende dal numero di siti nella griglia e dal tipo di copie desiderate: replicate o con codice di cancellazione.

- Per la replicazione e la codifica di cancellazione a sito singolo, creare un pool di archiviazione per ciascun sito. Ad esempio, se si desidera archiviare copie di oggetti replicati in tre siti, creare tre pool di archiviazione.
- Per la codifica di cancellazione in tre o più siti, creare un pool di archiviazione che includa una voce per ciascun sito. Ad esempio, se si desidera eliminare oggetti di codice in tre siti, creare un pool di archiviazione.

> Non includere il sito Tutti i siti in un pool di archiviazione che verrà utilizzato in un profilo di codifica di cancellazione. Aggiungere invece una voce separata al pool di archiviazione per ogni sito in cui verranno archiviati i dati con codice di cancellazione. Vederequesto passo per fare un esempio.

- Se si dispone di più di un livello di archiviazione, non creare un pool di archiviazione che includa diversi livelli di archiviazione in un singolo sito. Vedi il"Linee guida per la creazione di pool di archiviazione" .

Passi

1. Selezionare **ILM** > **Pool di archiviazione**.

   Nella scheda Pool di archiviazione sono elencati tutti i pool di archiviazione definiti.

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

2. Per creare un nuovo pool di archiviazione, selezionare **Crea**.
3. Immettere un nome univoco per il pool di archiviazione. Utilizzare un nome che sia facile da identificare quando si configurano i profili di codifica di cancellazione e le regole ILM.
4. Dall'elenco a discesa **Sito**, selezionare un sito per questo pool di archiviazione.

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

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

5. Dall'elenco a discesa **Livello di archiviazione**, selezionare il tipo di archiviazione che verrà utilizzato se una regola ILM utilizza questo pool di archiviazione.

   Il grado di archiviazione, *include tutti i gradi di archiviazione*, include tutti i nodi di archiviazione nel sito selezionato. Se hai creato gradi di archiviazione aggiuntivi per i nodi di archiviazione nella tua griglia, questi vengono elencati nel menu a discesa.

6. Se si desidera utilizzare il pool di archiviazione in un profilo di codifica di cancellazione multi-sito, selezionare **Aggiungi altri nodi** per aggiungere una voce per ciascun sito al pool di archiviazione.

   Se aggiungi più di una voce con diversi gradi di archiviazione per un sito, verrai avvisato.

   Per rimuovere una voce, seleziona l'icona Elimina .

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

   Il nuovo pool di archiviazione viene aggiunto all'elenco.

Visualizza i dettagli del pool di archiviazione

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Passi

1. Selezionare **ILM** > **Pool di archiviazione**.

   La tabella Pool di archiviazione include le seguenti informazioni per ogni pool di archiviazione che include nodi di archiviazione:

   - **Nome**: nome visualizzato univoco del pool di archiviazione.
   - **Conteggio nodi**: numero di nodi nel pool di archiviazione.
   - **Utilizzo dello spazio di archiviazione**: la percentuale dello spazio utilizzabile totale che è stata utilizzata per i dati degli oggetti su questo nodo. Questo valore non include i metadati dell'oggetto.
   - **Capacità totale**: la dimensione del pool di archiviazione, che equivale alla quantità totale di spazio utilizzabile per i dati degli oggetti per tutti i nodi nel pool di archiviazione.
   - **Utilizzo ILM**: modalità di utilizzo attuale del pool di archiviazione. Un pool di archiviazione potrebbe non essere utilizzato oppure potrebbe essere utilizzato in una o più regole ILM, profili di codifica di cancellazione o entrambi.

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

   Viene visualizzata la pagina dei dettagli del pool di archiviazione.

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

   La tabella include le seguenti informazioni per ciascun nodo:

   - Nome del nodo
   - Nome del sito
   - Grado di conservazione
   - Utilizzo dello spazio di archiviazione: percentuale dello spazio totale utilizzabile per i dati degli oggetti che è stato utilizzato per il nodo di archiviazione.

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

4. Visualizzare la scheda **Utilizzo ILM** per determinare se il pool di archiviazione è attualmente utilizzato in regole ILM o profili di codifica di cancellazione.
5. Facoltativamente, vai alla **pagina delle regole ILM** per scoprire e gestire tutte le regole che utilizzano il pool di archiviazione.

   Vedi il"istruzioni per lavorare con le regole ILM" .

Modifica pool di archiviazione

È possibile modificare un pool di archiviazione per cambiarne il nome o per aggiornare i siti e i livelli di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .
- Hai esaminato il"linee guida per la creazione di pool di archiviazione" .
- Se si prevede di modificare un pool di archiviazione utilizzato da una regola nel criterio ILM attivo, è necessario considerare in che modo le modifiche influiranno sul posizionamento dei dati degli oggetti.

Informazioni su questo compito

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

Passi

1. Selezionare **ILM** > **Pool di archiviazione**.
2. Selezionare la casella di controllo per il pool di archiviazione che si desidera modificare.

   Non è possibile modificare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti).

3. Selezionare **Modifica**.
4. Se necessario, modificare il nome del pool di archiviazione.

5. Se necessario, selezionare altri siti e gradi di stoccaggio.

   Non è possibile modificare il sito o il grado di archiviazione se il pool di archiviazione viene utilizzato in un profilo di codifica di cancellazione e la modifica renderebbe non valido lo schema di codifica di cancellazione. Ad esempio, se un pool di archiviazione utilizzato in un profilo di codifica di cancellazione include attualmente un grado di archiviazione con un solo sito, non è possibile utilizzare un grado di archiviazione con due siti perché la modifica renderebbe non valido lo schema di codifica di cancellazione.

   > L'aggiunta o la rimozione di siti da un pool di archiviazione esistente non sposterà alcun dato codificato per la cancellazione esistente. Se si desidera spostare i dati esistenti dal sito, è necessario creare un nuovo pool di archiviazione e un profilo EC per ricodificare i dati.

6. Seleziona **Salva**.

Dopo aver finito

Se hai aggiunto un nuovo sito o un nuovo livello di archiviazione a un pool di archiviazione utilizzato nel criterio ILM attivo, attiva un nuovo criterio ILM per forzare StorageGRID a utilizzare il nuovo sito o livello di archiviazione. Ad esempio, clona la tua policy ILM esistente e poi attiva il clone. Vedere "Lavorare con le regole e le politiche ILM" .

Rimuovere un pool di archiviazione

È possibile rimuovere un pool di archiviazione non utilizzato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"autorizzazioni di accesso richieste" .

Passi

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

   Non è possibile rimuovere un pool di archiviazione se è utilizzato in una regola ILM o in un profilo di codifica di cancellazione. Se necessario, selezionare ***nome pool di archiviazione*** > **Utilizzo ILM** per determinare dove viene utilizzato il pool di archiviazione.

3. Se il pool di archiviazione che si desidera rimuovere non è in uso, selezionare la casella di controllo.
4. Seleziona **Rimuovi**.
5. Selezionare **OK**.

Utilizzare i pool di archiviazione cloud

Che cos'è un Cloud Storage Pool?

Un Cloud Storage Pool consente di utilizzare ILM per spostare i dati degli oggetti all'esterno del sistema StorageGRID . Ad esempio, potresti voler spostare gli oggetti a cui si accede raramente su un archivio cloud più economico, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive nell'archivio BLOB di

Microsoft Azure. In alternativa, potresti voler mantenere un backup cloud degli oggetti StorageGRID per migliorare il ripristino in caso di emergenza.

Dal punto di vista ILM, un Cloud Storage Pool è simile a un pool di archiviazione. Per archiviare gli oggetti in una delle due posizioni, selezionare il pool durante la creazione delle istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di archiviazione sono costituiti da nodi di archiviazione all'interno del sistema StorageGRID , un pool di archiviazione cloud è costituito da un bucket esterno (S3) o da un contenitore (archiviazione BLOB di Azure).

La tabella confronta i pool di archiviazione con i pool di archiviazione cloud e mostra le principali somiglianze e differenze.

	Pool di stoccaggio	**Pool di archiviazione cloud**
Come viene creato?	Utilizzando l'opzione **ILM** > **Pool di archiviazione** in Grid Manager.	Utilizzando l'opzione **ILM** > **Pool di archiviazione** > **Pool di archiviazione cloud** in Grid Manager. È necessario configurare il bucket o il contenitore esterno prima di poter creare il Cloud Storage Pool.
Quante piscine puoi creare?	Illimitato.	Fino a 10.
Dove vengono conservati gli oggetti?	Su uno o più nodi di archiviazione all'interno StorageGRID.	In un bucket Amazon S3, in un contenitore di archiviazione BLOB di Azure o in un Google Cloud esterno al sistema StorageGRID . Se il Cloud Storage Pool è un bucket Amazon S3: • Facoltativamente, è possibile configurare un ciclo di vita del bucket per trasferire gli oggetti in un archivio a basso costo e a lungo termine, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema di archiviazione esterno deve supportare la classe di archiviazione Glacier e l'API S3 RestoreObject. • È possibile creare pool di archiviazione cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta la regione segreta AWS. Se il Cloud Storage Pool è un contenitore di archiviazione BLOB di Azure, StorageGRID trasferisce l'oggetto al livello Archivio. **Nota:** in generale, non configurare la gestione del ciclo di vita dell'archiviazione BLOB di Azure per il contenitore utilizzato per un pool di archiviazione cloud. Le operazioni di RestoreObject 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.

	Pool di stoccaggio	Pool di archiviazione cloud
Quale metodo di protezione dei dati viene utilizzato?	Codifica di replicazione o cancellazione.	Replicazione.
Quante copie di ciascun oggetto sono consentite?	Multiplo.	Una copia nel Cloud Storage Pool e, facoltativamente, una o più copie in StorageGRID. **Nota:** non è possibile archiviare un oggetto in più di un Cloud Storage Pool contemporaneamente.
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Archiviazione a basso costo. **Nota**: i dati FabricPool non possono essere suddivisi in livelli nei Cloud Storage Pool.

Ciclo di vita di un oggetto Cloud Storage Pool

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti 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 pool di archiviazione cloud S3.

> "Glacier" si riferisce sia alla classe di archiviazione Glacier sia alla classe di archiviazione Glacier Deep Archive, con un'eccezione: la classe di archiviazione Glacier Deep Archive non supporta il livello di ripristino accelerato. È supportato solo il recupero in blocco o standard.

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

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 archiviazione cloud S3**
   - Quando l'oggetto corrisponde a una regola ILM che utilizza un pool di archiviazione cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di archiviazione cloud.
   - Quando l'oggetto è stato spostato nel pool di archiviazione cloud S3, l'applicazione client può recuperarlo utilizzando una richiesta S3 GetObject da StorageGRID, a meno che l'oggetto non sia stato trasferito nello storage Glacier.
3. **Oggetto trasferito a Glacier (stato non recuperabile)**

- Facoltativamente, l'oggetto può essere trasferito nello storage Glacier. Ad esempio, il bucket S3 esterno potrebbe utilizzare la configurazione del ciclo di vita per trasferire un oggetto allo storage Glacier immediatamente o dopo un certo numero di giorni.

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

- Durante la transizione, l'applicazione client può utilizzare una richiesta S3 HeadObject per monitorare lo stato dell'oggetto.

4. **Oggetto ripristinato dal deposito Glacier**

   Se un oggetto è stato trasferito nello storage Glacier, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nello storage pool S3 Cloud. La richiesta specifica per quanti giorni la copia deve essere disponibile nel Cloud Storage Pool 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 torna automaticamente allo stato non recuperabile.

   > Se una o più copie dell'oggetto sono presenti anche sui nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier inviando una richiesta RestoreObject. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando 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 Cloud Storage Pool

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

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 archiviazione cloud di Azure**

   Quando l'oggetto corrisponde a una regola ILM che utilizza un pool di archiviazione cloud di Azure come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di archiviazione BLOB di Azure esterno specificato dal pool di archiviazione cloud.

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

   Subito dopo aver spostato l'oggetto nel pool di archiviazione cloud di Azure, StorageGRID trasferisce automaticamente l'oggetto al livello di archivio di archiviazione BLOB di Azure.

4. **Oggetto ripristinato dal livello Archivio**

   Se un oggetto è stato trasferito al livello Archivio, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel pool di archiviazione cloud di Azure.

Quando StorageGRID riceve RestoreObject, trasferisce temporaneamente l'oggetto al livello Cool di archiviazione BLOB di Azure. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID riporta l'oggetto al livello Archivio.

> Se una o più copie dell'oggetto sono presenti anche sui nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso all'archivio inviando una richiesta RestoreObject. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta GetObject.

5. **Oggetto recuperato**

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

Informazioni correlate

"Utilizzare l'API REST S3"

Quando utilizzare i pool di archiviazione cloud

Utilizzando i Cloud Storage Pool, è possibile eseguire il backup o suddividere i dati in livelli in una posizione esterna. Inoltre, è possibile eseguire il backup o suddividere i dati in più cloud.

Eseguire il backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un Cloud Storage Pool per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati degli oggetti nel Cloud Storage Pool possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario inviare una richiesta S3 RestoreObject per accedere alla copia dell'oggetto di backup 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 archiviazione o 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 recuperato.

Per implementare una soluzione di backup:

1. Crea un singolo Cloud Storage Pool.
2. Configurare una regola ILM che memorizzi simultaneamente copie di oggetti su nodi di archiviazione (come copie replicate o con codice di cancellazione) e una singola copia di oggetti nel pool di archiviazione cloud.
3. Aggiungi la regola alla tua policy ILM. Quindi, simulare e attivare la policy.

Dati di livello da StorageGRID alla posizione esterna

È possibile utilizzare un Cloud Storage Pool per archiviare oggetti al di fuori del sistema StorageGRID . Supponiamo, ad esempio, di avere un gran numero di oggetti che devi conservare, ma che prevedi di accedervi raramente, se non mai. È possibile utilizzare un Cloud Storage Pool per suddividere gli oggetti in livelli di archiviazione più economici e liberare spazio in StorageGRID.

Per implementare una soluzione a livelli:

1. Crea un singolo Cloud Storage Pool.
2. Configura una regola ILM che sposta gli oggetti raramente utilizzati dai nodi di archiviazione al pool di archiviazione cloud.
3. Aggiungi la regola alla tua policy ILM. Quindi, simulare e attivare la policy.

Gestisci più endpoint cloud

È possibile configurare più endpoint del Cloud Storage Pool se si desidera suddividere in livelli o eseguire il backup dei dati degli oggetti su più cloud. I filtri nelle regole ILM consentono di specificare quali oggetti vengono archiviati in ciascun Cloud Storage Pool. Ad esempio, potresti voler archiviare oggetti da alcuni tenant o bucket in Amazon S3 Glacier e oggetti da altri tenant o bucket nell'archiviazione BLOB di Azure. Oppure potresti voler spostare i dati tra Amazon S3 Glacier e Azure Blob Storage.

> Quando si utilizzano più endpoint Cloud Storage Pool, tenere 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 pool di archiviazione cloud.
2. Configurare le regole ILM per archiviare i dati degli oggetti appropriati al momento opportuno in ogni Cloud Storage Pool. Ad esempio, archivia gli oggetti dal bucket A nel Cloud Storage Pool A e archivia gli oggetti dal 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. Quindi, simulare e attivare la policy.

Considerazioni sui pool di archiviazione cloud

Se si prevede di utilizzare un Cloud Storage Pool per spostare oggetti fuori dal sistema StorageGRID , è necessario esaminare le considerazioni per la configurazione e l'utilizzo dei Cloud Storage Pool.

Considerazioni generali

- In generale, l'archiviazione cloud, come Amazon S3 Glacier o Azure Blob Storage, è un modo economico per archiviare dati di oggetti. Tuttavia, i costi per recuperare i dati dall'archiviazione cloud sono relativamente elevati. Per ottenere il costo complessivo più basso, è necessario considerare quando e con quale frequenza si accederà agli oggetti nel Cloud Storage Pool. Si consiglia di utilizzare un pool di archiviazione cloud solo per i contenuti a cui si prevede di accedere raramente.
- L'utilizzo di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva necessaria per recuperare un oggetto dalla destinazione di Cloud Storage Pool.
- Gli oggetti con S3 Object Lock abilitato non possono essere inseriti nei Cloud Storage Pool.
- Se il bucket S3 di destinazione per un Cloud Storage Pool ha abilitato il blocco degli oggetti S3, il tentativo di configurare la replica del bucket (PutBucketReplication) fallirà con un errore AccessDenied.
- Le seguenti combinazioni di piattaforma, autenticazione e protocollo con blocco oggetto S3 non sono supportate per i pool di archiviazione cloud:
  - **Piattaforme**: Google Cloud Platform e Azure

- **Tipi di autenticazione**: ruoli IAM ovunque e accesso anonimo
- **Protocollo**: HTTP

Considerazioni sulle porte utilizzate per i pool di archiviazione cloud

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

Per impostazione predefinita, i pool di archiviazione cloud utilizzano le seguenti porte:

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

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

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

Considerazioni sui costi

Per accedere allo storage nel cloud tramite un Cloud Storage Pool è necessaria la connettività di rete al cloud. È necessario considerare il costo dell'infrastruttura di rete che verrà utilizzata per accedere al cloud e predisporla in modo appropriato, in base alla quantità di dati che si prevede di spostare tra StorageGRID e il cloud utilizzando il Cloud Storage Pool.

Quando StorageGRID si connette all'endpoint esterno del Cloud Storage Pool, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Sebbene a queste richieste siano associati alcuni 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 è necessario spostare oggetti da un endpoint Cloud Storage Pool esterno a StorageGRID. Gli oggetti potrebbero essere spostati nuovamente su StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un Cloud Storage Pool e si decide di archiviare l'oggetto in StorageGRID . In questo caso, è necessario riconfigurare le regole e i criteri ILM. Quando si verifica 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 codice di cancellazione. Dopo che l'oggetto viene spostato nuovamente su 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 recuperato.

> Quando gli oggetti vengono spostati nuovamente su StorageGRID da un Cloud Storage Pool, StorageGRID invia più richieste all'endpoint del Cloud Storage Pool per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare l'assistenza tecnica per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

I criteri per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono concedere a StorageGRID l'autorizzazione per spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando necessario e altro ancora. Idealmente, StorageGRID dovrebbe avere accesso 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

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

Se si desidera trasferire oggetti dal Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e utilizzare una soluzione di archiviazione che implementi la classe di archiviazione Glacier e supporti l'API S3 RestoreObject.

Ad esempio, supponiamo di voler trasferire immediatamente tutti gli oggetti spostati da StorageGRID al Cloud Storage Pool allo storage Amazon S3 Glacier. Dovresti creare una configurazione del ciclo di vita sul bucket S3 esterno che specifica una singola azione (**Transizione**) come segue:

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

Questa regola trasferirà tutti gli oggetti bucket ad Amazon S3 Glacier il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al Cloud Storage Pool).

> Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai azioni **Scadenza** per definire quando scadono gli oggetti. Le azioni di scadenza determinano l'eliminazione degli oggetti scaduti da parte del sistema di archiviazione esterno. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non verrà trovato.

Se si desidera trasferire gli oggetti nel Cloud Storage Pool a S3 Glacier Deep Archive (anziché ad Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tieni presente che non puoi utilizzare il `Expedited` livello per ripristinare gli oggetti dall'archivio profondo del ghiacciaio S3.

Azure: considerazioni sul livello di accesso

Quando si configura un account di archiviazione di Azure, è possibile impostare il livello di accesso predefinito su Accesso frequente o Accesso sporadico. Quando si crea un account di archiviazione da utilizzare con un Cloud Storage Pool, è consigliabile utilizzare il livello Hot come livello predefinito. Anche se StorageGRID imposta immediatamente il livello su Archivio quando sposta gli oggetti nel Cloud Storage Pool, l'utilizzo di un'impostazione predefinita su Caldo garantisce che non verrà addebitata alcuna commissione per l'eliminazione anticipata degli oggetti rimossi dal livello Freddo prima del minimo di 30 giorni.

Azure: gestione del ciclo di vita non supportata

Non utilizzare la gestione del ciclo di vita dell'archiviazione BLOB di Azure per il contenitore utilizzato con un pool di archiviazione cloud. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

"Creare un pool di archiviazione cloud"

Confronta i pool di archiviazione cloud e la replica di CloudMirror

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

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Qual è lo scopo principale?	Funziona come destinazione di archivio. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure una copia aggiuntiva. Ciò significa che, invece di conservare due copie in loco, è possibile conservarne una copia in StorageGRID e inviarne una copia 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.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Come è impostato?	Definiti allo stesso modo dei pool di archiviazione, utilizzando Grid Manager o Grid Management API. Può essere selezionato come posizione di posizionamento in una regola ILM. Mentre un pool di archiviazione è costituito da un gruppo di nodi di archiviazione, un pool di archiviazione cloud viene definito utilizzando un endpoint S3 o Azure remoto (indirizzo IP, credenziali e così via).	Un utente tenant"configura la replica di CloudMirror" definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) tramite Tenant Manager o l'API S3. Dopo aver configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà di quell'account tenant può essere configurato in modo che punti all'endpoint CloudMirror.
Chi è responsabile della sua istituzione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Livello di archivio BLOB di Azure • Piattaforma Google Cloud (GCP)	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Piattaforma Google Cloud (GCP)
Cosa determina lo spostamento degli oggetti 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'atto di ingerire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti 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 vengono recuperati 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 in un archivio, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia speculare nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Supponiamo, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti su un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è obbligatorio utilizzare StorageGRID .
Riesci a leggere direttamente dalla destinazione?	No. Gli oggetti spostati in un Cloud Storage Pool vengono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero da Cloud Storage Pool).	Sì, perché la copia speculare è una copia indipendente.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Cosa succede se un oggetto viene eliminato dalla sorgente?	L'oggetto viene eliminato anche 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 si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID non riusciti 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 è possibile accedervi direttamente prima che i nodi StorageGRID vengano ripristinati.

Creare un pool di archiviazione cloud

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

Quando si crea un Cloud Storage Pool, si specifica il nome e la posizione del bucket o del contenitore esterno che StorageGRID utilizzerà per archiviare gli oggetti, il tipo di provider cloud (Amazon S3/GCP o Azure Blob Storage) e le informazioni necessarie a StorageGRID per accedere al bucket o al contenitore esterno.

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"autorizzazioni di accesso richieste" .
- Hai esaminato il"considerazioni per i pool di archiviazione cloud" .
- Il bucket o contenitore esterno a cui fa riferimento il Cloud Storage Pool esiste già e si dispone diinformazioni sull'endpoint del servizio .
- Per accedere al secchio o al contenitore, hai ilinformazioni sull'account per il tipo di autenticazione sceglierai tu.

Passi

1. Selezionare **ILM** > **Pool di archiviazione** > **Pool di archiviazione cloud**.
2. Seleziona **Crea**, quindi inserisci le seguenti informazioni:

Campo	Descrizione
Nome del pool di archiviazione cloud	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Utilizzare un nome che sia facile da identificare quando si configurano le regole ILM.

Campo	Descrizione
Tipo di fornitore	Quale provider cloud utilizzerai per questo Cloud Storage Pool: • **Amazon S3/GCP**: seleziona questa opzione per un provider Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o un altro provider compatibile con S3. • **Archiviazione BLOB di Azure**
Secchio o contenitore	Nome del bucket S3 esterno o del contenitore di Azure. Non è possibile modificare questo valore dopo aver salvato il Cloud Storage Pool.

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

Amazon S3/GCP

a. Per il protocollo, selezionare HTTPS o HTTP.

> Non utilizzare connessioni HTTP per dati sensibili.

b. 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 URL utilizzare, in base alle informazioni fornite. Ad esempio, se si specifica un indirizzo IP, StorageGRID utilizzerà un URL in stile percorso. Seleziona questa opzione solo se non sai quale stile specifico utilizzare.
Stile ospitato virtuale	Utilizzare un URL in stile virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del nome di dominio. Esempio: `https://bucket-name.s3.company.com/key-name`
Stile percorso	Utilizzare un URL in stile percorso per accedere al bucket. Gli URL in stile percorso includono il nome del bucket alla fine. Esempio: `https://s3.company.com/bucket-name/key-name` **Nota:** l'opzione URL in stile percorso non è consigliata e verrà deprecata in una futura versione di StorageGRID.

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

Archiviazione BLOB di Azure

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

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

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

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

4. 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 provider compatibili con S3

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

Ruoli IAM ovunque

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 AWS IAM Roles Anywhere**: seleziona la regione per il Cloud Storage Pool. Ad esempio, `us-east-1` .
b. **URN dell'ancora di trust**: immettere l'URN dell'ancora di trust che convalida le richieste di credenziali STS di breve durata. Può essere una CA radice o intermedia.
c. **URN del profilo**: immettere l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia considerato attendibile.
d. **URN del ruolo**: immettere l'URN del ruolo IAM che può essere assunto da chiunque sia considerato attendibile.
e. **Durata sessione**: immettere 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 la verifica del server IAM Roles Anywhere. Se omesso, il server non verrà verificato.
g. **Certificato dell'entità finale**: la chiave pubblica, in formato PEM, del certificato X509 firmato dal trust anchor. 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 S3 dei servizi cloud commerciali (C2S)

a. **URL delle credenziali temporanee**: immettere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati al proprio 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 PEM ed emesso da un'autorità di certificazione governativa (CA) appropriata.
c. **Certificato client**: seleziona **Sfoglia** e carica il certificato che StorageGRID utilizzerà per identificarsi sul server CAP. Il certificato client deve essere codificato PEM, rilasciato da un'autorità di certificazione governativa (CA) appropriata e deve consentire l'accesso al tuo account C2S.
d. **Chiave privata client**: selezionare **Sfoglia** e caricare la chiave privata codificata PEM per il certificato client.
e. Se la chiave privata del client è crittografata, immettere la passphrase per decrittografare la chiave privata del client. In caso contrario, lasciare vuoto il campo **Passphrase della chiave privata del client**.

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

Archiviazione BLOB di Azure

Per Azure Blob Storage, solo chiave condivisa

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

È possibile utilizzare il portale di Azure per trovare questi valori.

Anonimo

Non sono richieste ulteriori informazioni.

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

Opzione	Descrizione
Utilizzare i certificati CA radice nel sistema operativo Storage Node	Utilizzare i certificati Grid CA installati sul sistema operativo per proteggere le connessioni.
Utilizza un certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Selezionare **Sfoglia** e caricare il certificato codificato PEM.
Non verificare il certificato	Selezionando questa opzione le connessioni TLS al Cloud Storage Pool non saranno sicure.

6. Seleziona **Salva**.

   Quando si salva un Cloud Storage Pool, StorageGRID esegue le seguenti operazioni:

   - Verifica che il bucket o il contenitore e l'endpoint del servizio esistano e che possano essere raggiunti utilizzando le credenziali specificate.
   - Scrive un file marcatore nel bucket o nel contenitore per identificarlo come Cloud Storage Pool. Non rimuovere mai questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

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

7. Se si verifica un errore, vedere il"istruzioni per la risoluzione dei problemi dei pool di archiviazione cloud" , risolvere eventuali problemi e quindi provare a salvare nuovamente il Cloud Storage Pool.

Visualizza i dettagli del Cloud Storage Pool

È possibile visualizzare i dettagli di un Cloud Storage Pool per determinare dove viene utilizzato e vedere quali nodi e livelli di archiviazione sono inclusi.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Passi

1. Selezionare **ILM** > **Pool di archiviazione** > **Pool di archiviazione cloud**.

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

   - **Nome**: il nome visualizzato univoco del pool.
   - **URI**: Uniform Resource Identifier del Cloud Storage Pool.
   - **Tipo di provider**: quale provider cloud viene utilizzato per questo Cloud Storage Pool.
   - **Contenitore**: 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 utilizzato in una o più regole ILM, profili di codifica di cancellazione o entrambi.
   - **Ultimo errore**: l'ultimo errore rilevato durante un controllo dello stato di questo Cloud Storage Pool.

2. Per visualizzare i dettagli di uno specifico Cloud Storage Pool, selezionarne il nome.

   Viene visualizzata la pagina dei dettagli del pool.

3. Visualizza la scheda **Autenticazione** per informazioni sul tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Visualizza la scheda **Verifica del server** per conoscere i dettagli della verifica, modificare la verifica, scaricare un nuovo certificato o copiare il certificato PEM.
5. Visualizzare la scheda **Utilizzo ILM** per determinare se il Cloud Storage Pool è attualmente utilizzato in regole ILM o profili di codifica di cancellazione.
6. Facoltativamente, vai alla **pagina delle regole ILM** per"conoscere e gestire tutte le regole" che utilizzano il Cloud Storage Pool.

Modifica un pool di archiviazione cloud

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .
- Hai esaminato il"considerazioni per i pool di archiviazione cloud" .

Passi

1. Selezionare **ILM** > **Pool di archiviazione** > **Pool di archiviazione cloud**.

   Nella tabella Cloud Storage Pools sono elencati i Cloud Storage Pool esistenti.

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

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

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

   > Non è possibile modificare il tipo di provider, il bucket S3 o il contenitore di Azure per un pool di archiviazione cloud.

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

4. Seleziona **Salva**.

   Quando si salva un Cloud Storage Pool, StorageGRID verifica che il bucket o il contenitore e l'endpoint del servizio esistano e che possano essere raggiunti utilizzando le credenziali specificate.

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

   Vedi le istruzioni per"risoluzione dei problemi dei pool di archiviazione cloud" , risolvere il problema e quindi provare a salvare nuovamente il Cloud Storage Pool.

Rimuovere un pool di archiviazione cloud

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"autorizzazioni di accesso richieste" .

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

Se il Cloud Storage Pool che si desidera rimuovere contiene dati di oggetti, è necessario utilizzare ILM per spostare i dati in una posizione diversa. Ad esempio, puoi spostare i dati sui nodi di archiviazione nella tua griglia o su un pool di archiviazione cloud diverso.

Passi

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

   Non è possibile rimuovere un Cloud Storage Pool se è utilizzato in una regola ILM o in un profilo di codifica di cancellazione.

3. Se si utilizza il Cloud Storage Pool, selezionare ***nome del cloud storage pool*** > **Utilizzo ILM**.
4. "Clona ogni regola ILM"che attualmente posiziona gli oggetti nel Cloud Storage Pool che desideri rimuovere.
5. Determina dove vuoi spostare gli oggetti esistenti gestiti da ciascuna regola clonata.

   È possibile utilizzare uno o più pool di archiviazione oppure un diverso Cloud Storage Pool.

6. Modifica ciascuna delle regole che hai clonato.

   Per il passaggio 2 della procedura guidata Crea regola ILM, selezionare la nuova posizione dal campo **copie in**.

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

Elimina pool di archiviazione cloud

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

Prima di iniziare

- Sono state rimosse tutte le regole ILM che potrebbero aver utilizzato il pool.
- Hai confermato che il bucket S3 o il contenitore di Azure non contiene alcun oggetto.

  Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool che contiene oggetti. Vedere "Risoluzione dei problemi dei pool di archiviazione cloud" .

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

Passi

1. Selezionare **ILM** > **Pool di archiviazione** > **Pool di archiviazione cloud**.
2. Se la colonna Utilizzo ILM indica che Cloud Storage Pool non è in uso, selezionare la casella di controllo.
3. Selezionare **Azioni** > **Rimuovi**.
4. Selezionare **OK**.

Risoluzione dei problemi dei pool di archiviazione cloud

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

Determina se si è verificato un errore

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

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

Inoltre, viene attivato un avviso di **Errore di connettività del Cloud Storage Pool** se il controllo dello stato rileva che si sono verificati uno o più nuovi errori del Cloud Storage Pool negli ultimi 5 minuti. Se ricevi una notifica via e-mail per questo avviso, vai alla pagina Pool di archiviazione (seleziona **ILM** > **Pool di**

archiviazione), esamina i messaggi di errore nella colonna Ultimo errore e fai riferimento alle linee guida per la risoluzione dei problemi riportate di seguito.

Controlla se un errore è stato risolto

Dopo aver risolto eventuali problemi di fondo, è possibile determinare 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 eliminato 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 dello stato 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 utilizzare questo bucket 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 correggere questo problema, seguire i passaggi in"Modifica un pool di archiviazione cloud" senza apportare alcuna modifica. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag S3 Object Lock su una configurazione dell'endpoint del Cloud Storage Pool.

Errore: questo pool di archiviazione cloud contiene contenuti inaspettati

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

In genere, questo errore viene visualizzato solo se si sta 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 correggere il problema:

- Se si sta configurando un nuovo Cloud Storage Pool e il bucket contiene `x-ntap-sgws-cloud-pool-uuid` file e chiavi di oggetti aggiuntivi simili all'esempio seguente, crea un nuovo bucket e usalo al suo posto.

  Esempio di una 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 scenario, contatta l'assistenza.

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

Questo errore potrebbe verificarsi nelle seguenti circostanze:

- Quando si tenta di creare o modificare un Cloud Storage Pool.
- Quando si seleziona una combinazione di piattaforma, autenticazione o protocollo non supportata con S3

Object Lock durante la configurazione di un nuovo Cloud Storage Pool. Vedere "Considerazioni sui pool di archiviazione cloud" .

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

Per correggere il problema, rivedere il messaggio di errore dall'endpoint.

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

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

Errore: non è stato trovato un pool di archiviazione cloud con questo ID

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

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

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

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

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

Potresti riscontrare questo errore quando provi a 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 Cloud Storage Pool.

Per correggere il problema, rivedere il messaggio di errore dall'endpoint.

Errore: gli oggetti sono già stati inseriti in questo bucket

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati lì da ILM, dati presenti nel bucket prima della configurazione del Cloud Storage Pool o dati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

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

- Seguire le istruzioni per spostare nuovamente gli oggetti su 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, eliminali manualmente dal bucket.

> Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbero essere stati inseriti lì da ILM. Se in seguito si tenta di 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

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

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

- Controllare le impostazioni per il Cloud Storage Pool (**ILM** > **Storage pool**).
- Controllare la configurazione di rete del server proxy di archiviazione.

Errore: il certificato X.509 è scaduto nel 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 venga convalidato il corretto Cloud Storage Pool esterno e che il pool esterno sia vuoto prima che la configurazione del Cloud Storage Pool venga eliminata.

Per risolvere il problema, prova a seguire questi passaggi:

- Aggiornare il certificato configurato per l'autenticazione nel Cloud Storage Pool.
- Assicurarsi che tutti gli avvisi di scadenza dei certificati su questo Cloud Storage Pool siano stati risolti.

Informazioni correlate

"Ciclo di vita di un oggetto Cloud Storage Pool"

Gestisci i profili di codifica di cancellazione

È possibile visualizzare i dettagli di un profilo di codifica di cancellazione e, se necessario, rinominare un profilo. È possibile disattivare un profilo di codifica di

cancellazione se non è attualmente utilizzato in alcuna regola ILM.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"autorizzazioni di accesso richieste" .

Visualizza i dettagli del profilo di codifica di cancellazione

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

Passi

1. Selezionare **CONFIGURAZIONE** > **Sistema** > **Codifica di cancellazione**.
2. Seleziona il profilo. Viene visualizzata la pagina dei dettagli del profilo.
3. Facoltativamente, visualizza la scheda Regole ILM per un elenco delle regole ILM che utilizzano il profilo e i criteri ILM che utilizzano tali regole.
4. Facoltativamente, visualizza la scheda Nodi di archiviazione per i dettagli su ciascun nodo di archiviazione nel pool di archiviazione del profilo, ad esempio il sito in cui si trova e l'utilizzo dello spazio di archiviazione.

Rinominare un profilo di codifica di cancellazione

Potresti voler rinominare un profilo di codifica di cancellazione per rendere più evidente la sua funzione.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sistema** > **Codifica di cancellazione**.
2. Seleziona il profilo che vuoi rinominare.
3. Selezionare **Rinomina**.
4. Immettere un nome univoco per il profilo di codifica di cancellazione.

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

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

5. Seleziona **Salva**.

Disattivare un profilo di codifica di cancellazione

È possibile disattivare un profilo di codifica di cancellazione se non si prevede più di utilizzarlo e se il profilo non è attualmente utilizzato in alcuna regola ILM.

> Verificare che non siano in corso operazioni di riparazione di dati codificati tramite cancellazione o procedure di disattivazione. Se si tenta di disattivare un profilo di codifica di cancellazione mentre è in corso una di queste operazioni, viene visualizzato un messaggio di errore.

Informazioni su questo compito

StorageGRID impedisce la disattivazione di un profilo di codifica di cancellazione se si verifica una delle

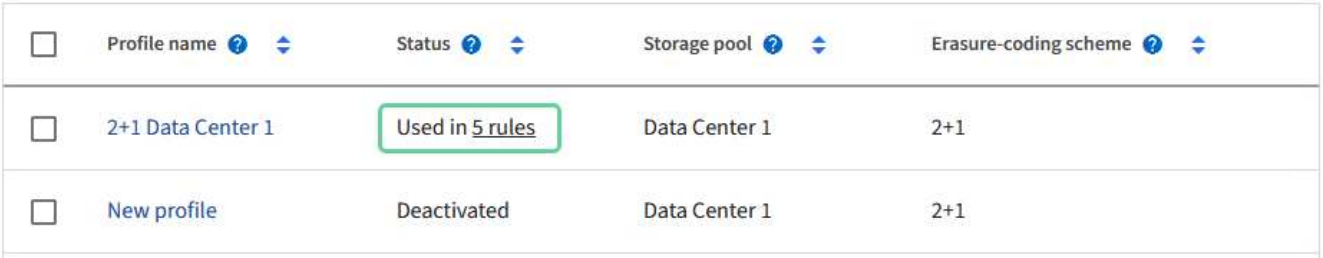
seguenti condizioni:

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

Passi

1. Selezionare **CONFIGURAZIONE** > **Sistema** > **Codifica di cancellazione**.
2. Nella scheda Attivo, rivedere la colonna **Stato** per confermare che il profilo di codifica di cancellazione che si desidera disattivare non sia utilizzato in alcuna regola ILM.

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



3. Se il profilo viene utilizzato in una regola ILM, attenersi alla seguente procedura:
   a. Selezionare **ILM** > **Regole**.
   b. Selezionare ciascuna regola e rivedere il diagramma di conservazione per determinare se la regola utilizza il profilo di codifica di cancellazione che si desidera disattivare.
   c. Se la regola ILM utilizza il profilo di codifica di cancellazione che si desidera disattivare, determinare se la regola viene utilizzata in un criterio ILM.
   d. Completare i passaggi aggiuntivi nella tabella, in base al punto in cui viene utilizzato il profilo di codifica di cancellazione.

Dove è stato utilizzato il profilo?	**Ulteriori passaggi da eseguire prima di disattivare il profilo**	**Fare riferimento a queste istruzioni aggiuntive**
Mai utilizzato in nessuna regola ILM	Non sono richiesti passaggi aggiuntivi. Continuare con questa procedura.	*Nessuno*
In una regola ILM che non è mai stata utilizzata in nessuna politica ILM	i. Modifica o elimina tutte le regole ILM interessate. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. ii. Continuare con questa procedura.	"Lavorare con le regole e le politiche ILM"

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
In una regola ILM che è attualmente in una policy ILM attiva	i. Clonare la policy. ii. Rimuovere la regola ILM che utilizza il profilo di codifica di cancellazione. iii. Aggiungere una o più nuove regole ILM per garantire la protezione degli oggetti. iv. Salva, simula e attiva la nuova policy. v. Attendi che la nuova policy venga applicata e che gli oggetti esistenti vengano spostati in nuove posizioni in base alle nuove regole aggiunte. **Nota:** a seconda del numero di oggetti e delle dimensioni del sistema StorageGRID , potrebbero essere necessarie settimane o addirittura mesi prima che le operazioni ILM spostino gli oggetti in nuove posizioni, in base alle nuove regole ILM. Sebbene sia possibile tentare in tutta sicurezza di disattivare un profilo di codifica di cancellazione mentre 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 rimossa dal criterio. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. vii. Continuare con questa procedura.	"Creare una policy ILM" "Lavorare con le regole e le politiche ILM"
In una regola ILM che è attualmente in una politica ILM	i. Modifica la politica. ii. Rimuovere la regola ILM che utilizza il profilo di codifica di cancellazione. iii. Aggiungere una o più nuove regole ILM per garantire che tutti gli oggetti siano protetti. iv. Salva la polizza. v. Modifica o elimina la regola rimossa dal criterio. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. vi. Continuare con questa procedura.	"Creare una policy ILM" "Lavorare con le regole e le politiche ILM"

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

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

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

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

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

Risultati

- Se StorageGRID è in grado di disattivare il profilo di codifica di cancellazione, il suo stato è Disattivato. Non è più possibile selezionare questo profilo per nessuna regola ILM. Non è possibile 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 dell'oggetto sono ancora associati a questo profilo. Potrebbe essere necessario attendere diverse settimane prima di provare nuovamente la procedura di disattivazione.

Configurare le regioni (facoltativo e solo S3)

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

Se si desidera utilizzare una regione bucket S3 come filtro in una regola, è necessario prima creare le regioni che possono essere utilizzate dai bucket nel sistema.

Non è possibile modificare la regione di un bucket dopo averlo creato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Informazioni su questo compito

Quando si crea un bucket S3, è possibile specificare che il bucket venga creato in una regione specifica. Specificando una regione, il bucket può essere geograficamente vicino ai suoi utenti, il che può aiutare a ottimizzare la latenza, ridurre al minimo i costi e soddisfare i requisiti normativi.

Quando si crea una regola ILM, potrebbe essere opportuno utilizzare la regione associata a un bucket S3 come filtro avanzato. Ad esempio, è possibile progettare una regola che si applica solo agli oggetti nei bucket S3 creati in `us-west-2` regione. È quindi possibile specificare che copie di tali oggetti vengano posizionate su nodi di archiviazione in un sito di data center all'interno di quella regione per ottimizzare la latenza.

Quando si configurano le regioni, seguire queste linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati appartenenti a `us-east-1` regione.
- È necessario creare le regioni utilizzando Grid Manager prima di poter specificare una regione non predefinita quando si creano bucket utilizzando Tenant Manager o Tenant Management API oppure con l'elemento di richiesta LocationConstraint per le richieste S3 PUT Bucket API. Si verifica un errore se una richiesta PUT Bucket utilizza una regione non definita in StorageGRID.
- Quando si crea il bucket S3, è necessario utilizzare il nome esatto della regione. I nomi delle regioni sono sensibili alle maiuscole e alle minuscole. I caratteri validi sono numeri, lettere e trattini.

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

- Non è possibile eliminare o modificare una regione se è utilizzata in una regola assegnata a un criterio (attivo o inattivo).
- Se si utilizza una regione non valida come filtro avanzato in una regola ILM, non è possibile aggiungere tale regola a un criterio.

  Una regione non valida può verificarsi se si utilizza una regione come filtro avanzato in una regola ILM ma in seguito si elimina tale regione oppure se si utilizza l'API di gestione della griglia per creare una regola e si specifica una regione che non è stata definita.

- Se elimini una regione dopo averla utilizzata per creare un bucket S3, dovrai aggiungere nuovamente la regione se desideri utilizzare il filtro avanzato Vincolo di posizione per trovare oggetti in quel bucket.

Passi

1. Selezionare **ILM** > **Regioni**.

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

2. Per aggiungere una regione:
   a. Seleziona **Aggiungi un'altra regione**.
   b. Inserisci il nome della regione che desideri utilizzare durante la creazione dei bucket S3.

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

3. Per rimuovere una regione non utilizzata, seleziona l'icona Elimina ✕ .

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

4. Una volta completate le modifiche, seleziona **Salva**.

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

Crea regola ILM

Utilizzare le regole ILM per gestire gli oggetti

Per gestire gli oggetti, è necessario creare un set di regole di gestione del ciclo di vita delle informazioni (ILM) e organizzarle in una policy ILM.

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

I metadati degli oggetti non sono gestiti dalle regole ILM. I metadati degli oggetti vengono invece archiviati in un database Cassandra, in quello che è noto come archivio di metadati. In ogni sito vengono conservate automaticamente tre copie dei metadati degli oggetti per proteggere i dati da eventuali perdite.

Elementi di una regola ILM

Una regola ILM è composta da 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 dell'oggetto. Ogni regola può includere una sequenza di istruzioni di posizionamento per modificare nel tempo il numero, il tipo e la posizione delle copie dell'oggetto. Quando scade il periodo di tempo per un tirocinio, le istruzioni del tirocinio successivo vengono applicate automaticamente dalla successiva valutazione ILM.
- **Comportamento di acquisizione**: il comportamento di acquisizione di una regola consente di scegliere in che modo gli oggetti filtrati dalla regola vengono protetti durante l'acquisizione (quando un client S3 salva un oggetto nella griglia).

Filtraggio delle regole ILM

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

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

- I filtri di base consentono di applicare regole diverse a gruppi di oggetti ampi e distinti. Questi filtri consentono di applicare una regola a specifici account 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, potrebbe essere necessario archiviare i registri finanziari della tua azienda 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 suddiviso i dati dei diversi reparti in bucket S3 separati, è possibile creare facilmente una regola che si applica a tutti i record finanziari e una seconda regola che si applica a tutti i dati di marketing.

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

È possibile 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. È possibile creare filtri che identificano ogni tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag dell'oggetto S3 o a qualsiasi altro criterio rilevante, quindi creare regole separate per archiviare in modo appropriato ogni set di oggetti.

È possibile combinare i filtri in base alle proprie esigenze in un'unica regola. Ad esempio, il reparto marketing potrebbe voler archiviare file di immagini di grandi dimensioni in modo diverso rispetto ai record dei fornitori, mentre il reparto delle risorse umane potrebbe dover archiviare i record del personale in una specifica area geografica e le informazioni sulle politiche in modo centralizzato. In questo caso è possibile creare regole che filtrano in base all'account del tenant per separare i record da ciascun reparto, utilizzando al contempo filtri in ogni regola per identificare il tipo specifico di oggetti a cui si applica la regola.

Istruzioni per il posizionamento delle regole ILM

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

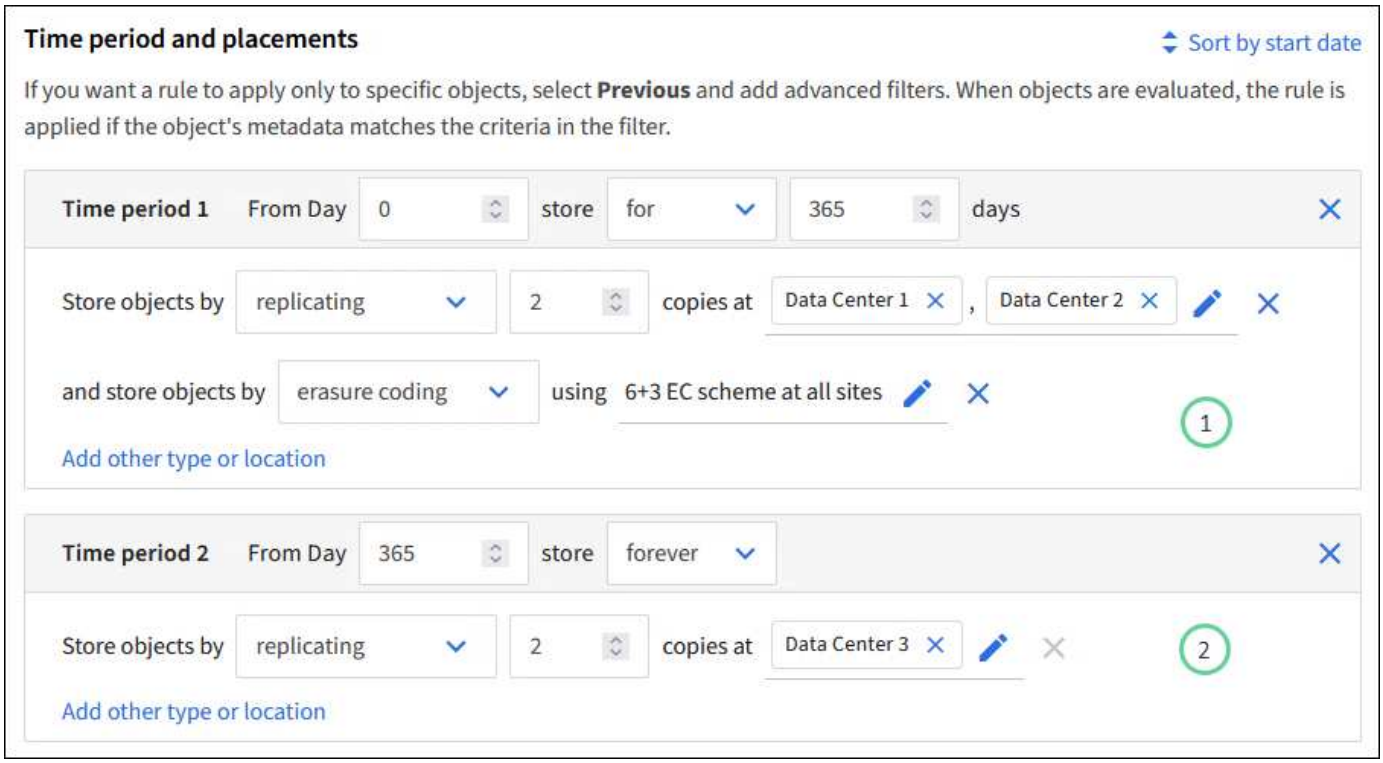
Quando si creano istruzioni di posizionamento:

- Si inizia specificando l'ora di riferimento, che determina quando iniziano le istruzioni di posizionamento. Il momento di riferimento potrebbe essere il momento in cui un oggetto viene acquisito, quando si accede a un oggetto, quando un oggetto con versione diventa non corrente o un momento definito dall'utente.
- Successivamente, si specifica quando verrà applicato il posizionamento, in relazione all'orario di riferimento. Ad esempio, un posizionamento potrebbe iniziare il giorno 0 e continuare per 365 giorni, in relazione al momento in cui l'oggetto è stato acquisito.
- Infine, si specifica il tipo di copie (codifica di replicazione o di cancellazione) e la posizione in cui vengono archiviate le copie. Ad esempio, potresti voler archiviare due copie replicate in due siti diversi.

Ogni 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 oggetti in posizioni diverse in periodi di tempo diversi, seleziona **Aggiungi un altro periodo di tempo** per aggiungere il periodo di tempo successivo. Quindi, specificare 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.



Le prime istruzioni di posizionamento (1) ha due linee 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 codice di cancellazione 6+3 utilizzando tutti i siti del data center.

La seconda istruzione di posizionamento (2) ne crea due copie dopo un anno e le conserva per sempre.

Quando si definisce il set di istruzioni di posizionamento per una regola, è necessario assicurarsi che almeno un'istruzione di posizionamento inizi al giorno 0, che non vi siano intervalli tra i periodi di tempo definiti e che l'istruzione di posizionamento finale continui per sempre o finché non saranno più necessarie copie dell'oggetto.

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

Comportamento di acquisizione delle regole ILM

Il comportamento di acquisizione controlla se le copie degli oggetti vengono posizionate immediatamente in base alle istruzioni della regola 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 effettuare tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono effettuate copie provvisorie e il client riceve un messaggio di conferma dell'operazione riuscita. Quando possibile, vengono effettuate le copie specificate nella norma ILM.
- **Rigoroso**: tutte le copie specificate nella regola ILM devono essere eseguite prima che il risultato positivo venga restituito al client.

- **Doppio commit**: StorageGRID crea immediatamente copie provvisorie dell'oggetto e restituisce il risultato positivo al client. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

Informazioni correlate

- "Opzioni di acquisizione"
- "Vantaggi, svantaggi e limitazioni delle opzioni di ingestione"
- "Come la coerenza e le regole ILM interagiscono per influenzare la protezione dei dati"

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applica solo agli oggetti appartenenti all'inquilino A.
- Realizza due copie replicate di quegli oggetti e conserva ciascuna copia in un luogo diverso.
- Conservare le due copie "per sempre", il che significa che StorageGRID non le eliminerà automaticamente. StorageGRID conserverà invece questi oggetti finché non verranno eliminati da una richiesta di eliminazione del client o dalla scadenza del ciclo di vita di un bucket.
- Utilizzare l'opzione Bilanciato 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 effettuare immediatamente entrambe le copie richieste.

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

Informazioni correlate

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

Accedi alla procedura guidata Crea una regola ILM

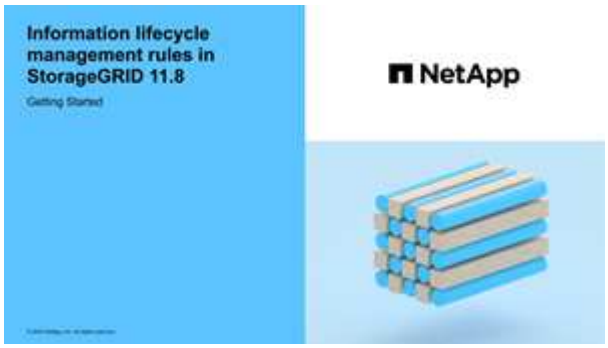
Le regole ILM consentono di gestire il posizionamento dei dati degli oggetti nel tempo. Per creare una regola ILM, utilizzare la procedura guidata Crea una regola ILM.

> Se si desidera creare la regola ILM predefinita per una policy, seguire la procedura"istruzioni per la creazione di una regola ILM predefinita" Invece.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .
- Se si desidera specificare a quali account tenant si applica questa regola, è necessario"Autorizzazione degli account degli inquilini" oppure conosci l'ID account per ogni account.
- Se si desidera che la regola filtri gli oggetti in base ai metadati dell'ora dell'ultimo accesso, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati dal bucket S3.
- Hai configurato tutti i Cloud Storage Pool che intendi utilizzare. Vedere "Crea un pool di archiviazione cloud" .
- Hai familiarità con il"opzioni di ingestione" .

- Se è necessario creare una regola conforme da utilizzare con S3 Object Lock, è necessario avere familiarità con"requisiti per S3 Object Lock" .
- Facoltativamente, hai guardato il video: "Video: panoramica delle regole ILM" .



Informazioni su questo compito

Durante la creazione delle regole ILM:

- Prendiamo in considerazione la topologia e le configurazioni di archiviazione del sistema StorageGRID .
- Considera quali tipi di copie di oggetti vuoi realizzare (replicate o con codice di cancellazione) e il numero di copie necessarie per ciascun oggetto.
- Determinare 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.
- Considera dove vuoi che vengano posizionate le copie degli oggetti nel tempo.
- Decidi quale opzione di ingestione utilizzare (Bilanciata, Rigorosa o Doppio commit).

Passi

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

Passaggio 1 di 3: Inserisci i dettagli

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

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

Informazioni su questo compito

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

Passi

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

   Dovresti descrivere lo scopo o la funzione della regola in modo da poterla riconoscere in seguito.

3. Facoltativamente, seleziona uno o più account tenant S3 a cui si applica questa regola. Se questa regola si applica a tutti gli inquilini, lasciare vuoto questo campo.

   Se non si dispone né dell'autorizzazione di accesso Root né dell'autorizzazione Account tenant, non è possibile selezionare i tenant dall'elenco. In alternativa, immettere l'ID tenant oppure più ID come stringa delimitata da virgole.

4. Facoltativamente, specificare 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, selezionare facoltativamente **Sì** per applicare la regola solo alle versioni precedenti degli oggetti nei bucket S3 in cui è abilitato il controllo delle versioni.

   Se selezioni **Sì**, "Tempo non corrente" verrà automaticamente selezionato per il 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 abilitati al controllo delle versioni. Vedere"Operazioni sui bucket, PutBucketVersioning" E"Gestisci gli oggetti con S3 Object Lock" .

   È possibile utilizzare questa opzione per ridurre l'impatto sull'archiviazione degli oggetti sottoposti a controllo delle versioni, filtrando le versioni degli oggetti non correnti. Vedere "Esempio 4: regole e policy ILM per oggetti con versione S3" .

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

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

7. Selezionare **Continua**. "Fase 2 (Definire i posizionamenti)"viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare filtri avanzati nelle regole ILM

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

Nella tabella sono indicati i tipi di metadati che è possibile specificare nei filtri avanzati, gli operatori che è possibile utilizzare 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 acceso o prima • è dopo • è acceso o dopo	Ora e data in cui l'oggetto è stato ingerito. **Nota:** per evitare problemi di risorse durante l'attivazione di un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Tempo di acquisizione in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore, per garantire che gli oggetti esistenti non vengano spostati inutilmente.
Chiave	• è uguale • non è uguale • contiene • non contiene • inizia con • non inizia con • finisce con • non finisce con	Tutta o parte di una chiave univoca dell'oggetto S3. Ad esempio, potresti voler abbinare oggetti che terminano con `.txt` o inizia con `test-object/` .
Ultimo orario di accesso	• È • non è • è prima • è acceso o prima • è dopo • è acceso o dopo	Ora e data dell'ultimo recupero (lettura o visualizzazione) dell'oggetto. **Nota:** se hai intenzione di"usa l'ultimo orario di accesso" come filtro avanzato, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati per il bucket S3.
Vincolo di posizione (solo S3)	• è uguale • non è uguale	La regione in cui è stato creato un bucket S3. Utilizzare **ILM** > **Regioni** per definire le regioni visualizzate. **Nota:** il valore us-east-1 corrisponderà agli oggetti nei bucket creati nella regione us-east-1 e agli oggetti nei bucket per i quali non è specificata alcuna regione. Vedere "Configurare le regioni (facoltativo e solo S3)" .

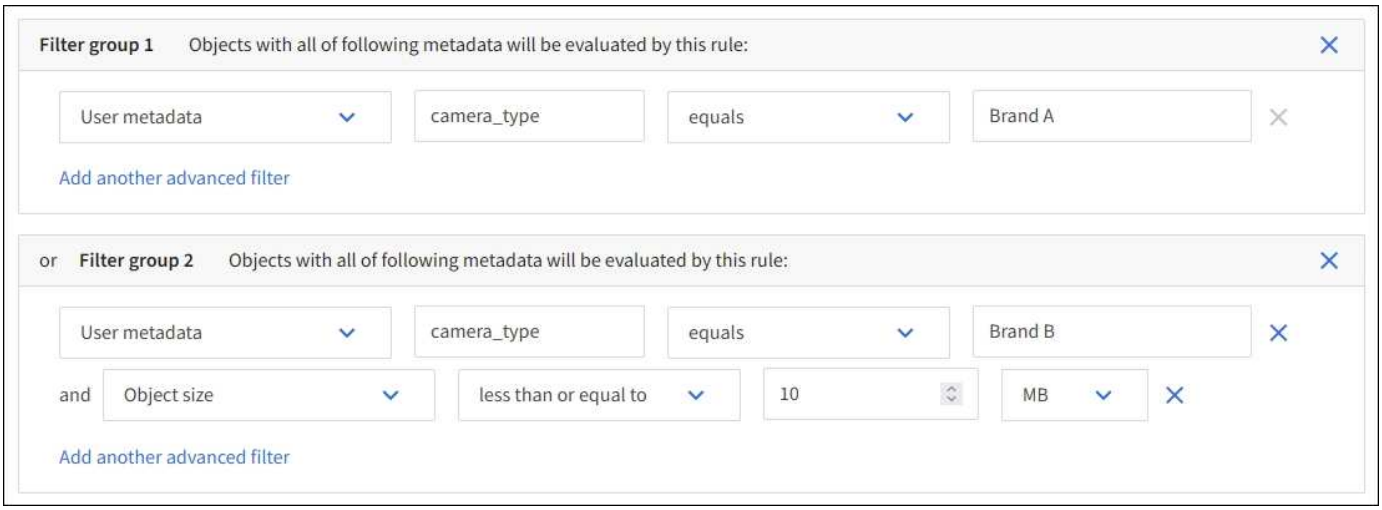
Tipo di metadati	Operatori supportati	Valore dei metadati
Dimensione dell'oggetto	• è uguale • non è uguale • meno di • minore o uguale a • maggiore di • maggiore o uguale a	Le dimensioni dell'oggetto. La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.
Metadati utente	• contiene • finisce con • è uguale • esiste • inizia con • non contiene • non finisce con • non è uguale • non esiste • non inizia con	Coppia chiave-valore, dove **Nome metadati utente** è la chiave e **Valore metadati** è il valore. Ad esempio, per filtrare gli oggetti che hanno metadati utente di `color=blue` , specificare `color` per **Nome metadati utente**, `equals` per l'operatore, e `blue` per **Valore metadati**. **Nota:** i nomi dei metadati utente non sono sensibili alle maiuscole e alle minuscole; lo sono invece i valori dei metadati utente.
Tag oggetto (solo S3)	• contiene • finisce con • è uguale • esiste • inizia con • non contiene • non finisce con • non è uguale • non esiste • non inizia con	Coppia chiave-valore, dove **Nome tag oggetto** è la chiave e **Valore tag oggetto** è il valore. Ad esempio, per filtrare gli oggetti che hanno un tag oggetto di `Image=True` , specificare `Image` per **nome tag oggetto**, `equals` per l'operatore, e `True` per **valore tag oggetto**. **Nota:** i nomi e i valori dei tag degli oggetti sono sensibili alle maiuscole e alle minuscole. È necessario immettere questi elementi esattamente come sono stati definiti per l'oggetto.

Specificare più tipi e valori di metadati

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

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

Utilizzando più voci è possibile avere un controllo preciso sugli oggetti da abbinare. Nell'esempio seguente, la regola si applica agli oggetti che hanno Brand A o Brand B come valore dei metadati utente camera_type. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.



Fase 2 di 3: definire i posizionamenti

Il passaggio **Definisci posizionamenti** della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano per quanto tempo gli oggetti vengono archiviati, il tipo di copie (replicate o con codice di cancellazione), la posizione di archiviazione e il numero di copie.

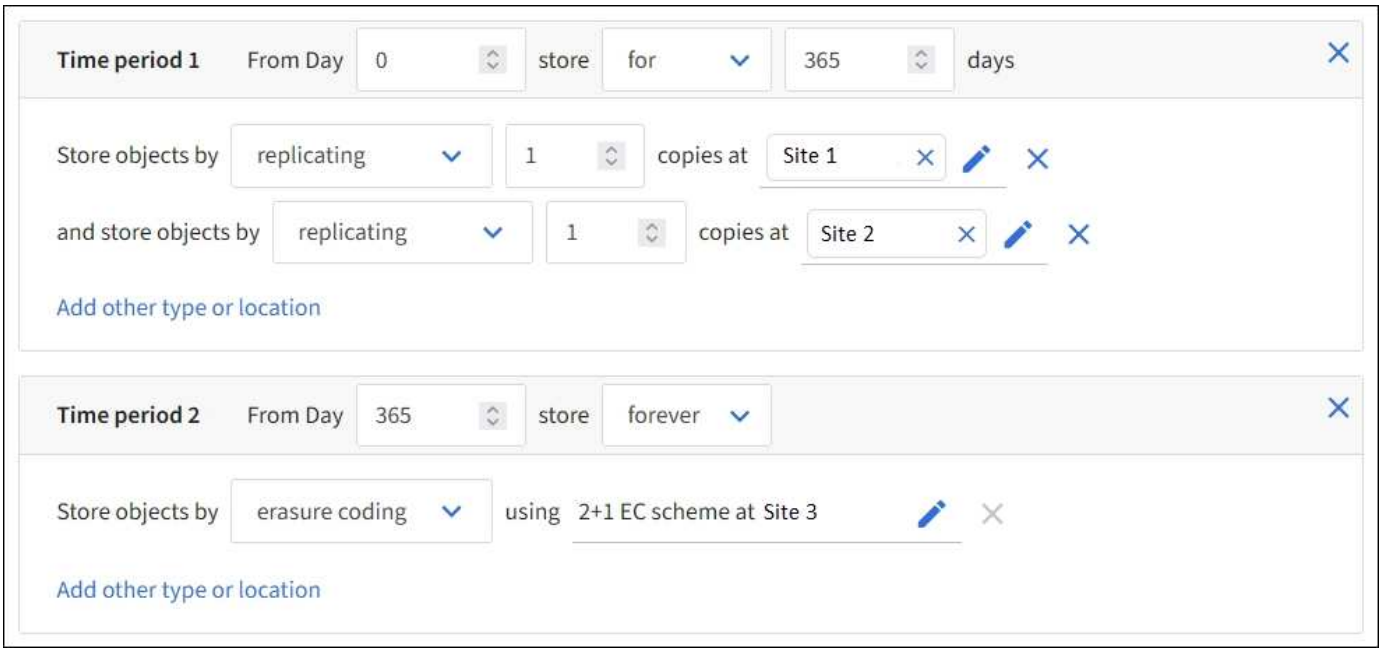
Gli screenshot mostrati sono esempi. I risultati potrebbero variare a seconda della versione StorageGRID .

Informazioni su questo compito

Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo. Quando si utilizzano più istruzioni, i periodi di tempo devono essere contigui e almeno un'istruzione deve iniziare il giorno 0. Le istruzioni possono continuare all'infinito oppure finché non avrai più bisogno di copie dell'oggetto.

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

In questo esempio, la regola ILM memorizza una copia replicata nel Sito 1 e una copia replicata nel Sito 2 per il primo anno. Dopo un anno, viene realizzata una copia con codice di cancellazione 2+1 e salvata in un solo sito.



Passi

1. Per **Tempo di riferimento**, seleziona il tipo di tempo da utilizzare per calcolare l'ora di inizio di un'istruzione di tirocinio.

Opzione	Descrizione
Tempo di ingestione	Il momento in cui l'oggetto è stato ingerito.
Ultimo orario di accesso	Ora dell'ultima volta in cui l'oggetto è stato recuperato (letto o visualizzato). Per utilizzare questa opzione, è necessario abilitare gli aggiornamenti all'ora dell'ultimo accesso per il bucket S3. Fare riferimento a "Utilizzare l'orario 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** per la domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?" in"Passaggio 1 della procedura guidata Crea una regola ILM" .

   Se vuoi creare una regola *conforme*, devi selezionare **Ora di inserimento**. Fare riferimento a "Gestisci gli oggetti con S3 Object Lock" .

2. Nella sezione **Periodo di tempo e posizionamenti**, 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 (*Dal giorno 0 archivia per 365 giorni*). Almeno un'istruzione deve iniziare al giorno 0.

3. Se si desidera creare copie replicate:
   a. Dall'elenco a discesa **Memorizza oggetti per**, seleziona **replica**.
   b. Seleziona il numero di copie che desideri effettuare.

      Se si modifica il numero di copie in 1, viene visualizzato un avviso. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Fare riferimento a "Perché non dovresti usare la replicazione a copia singola" .

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

      - Aumentare il numero di copie per il periodo di tempo.
      - Aggiungere copie ad altri pool di archiviazione o a un pool di archiviazione cloud.
      - Selezionare **codifica di cancellazione** invece di **replicazione**.

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

   c. Nel campo **copie in**, seleziona i pool di archiviazione che desideri aggiungere.

      Se si specifica un solo pool di archiviazione, tenere presente che StorageGRID può archiviare solo una copia replicata di un oggetto su un dato nodo di archiviazione. Se la griglia include tre nodi di archiviazione e si seleziona 4 come numero di copie, verranno effettuate solo tre copie, una copia per ciascun nodo di archiviazione.

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

      Se si specifica più di un pool di archiviazione, tenere a mente queste regole:

      - Il numero di copie non può essere maggiore del numero di pool di archiviazione.
      - Se il numero di copie è uguale al numero di pool di archiviazione, una copia dell'oggetto viene archiviata in ciascun pool di archiviazione.
      - Se il numero di copie è inferiore al numero di pool di archiviazione, una copia viene archiviata nel sito di acquisizione, quindi il sistema distribuisce le copie rimanenti per mantenere bilanciato l'utilizzo del disco tra i pool, garantendo al contempo che nessun sito riceva più di una copia di un oggetto.
      - Se i pool di archiviazione si sovrappongono (contengono gli stessi nodi di archiviazione), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) e un altro pool di archiviazione.

4. Se vuoi creare una copia con codice di cancellazione:
   a. Dall'elenco a discesa **Memorizza oggetti per**, seleziona **codifica di cancellazione**.

      > La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

   b. Se non hai aggiunto un filtro Dimensione oggetto per un valore superiore a 200 KB, seleziona **Precedente** per tornare al passaggio 1. Quindi, seleziona **Aggiungi un filtro avanzato** e imposta un

filtro **Dimensione oggetto** su un valore maggiore di 200 KB.

c. Selezionare il pool di archiviazione che si desidera aggiungere e lo schema di codifica di cancellazione che si desidera utilizzare.

La posizione di archiviazione per una copia con codice di cancellazione include il nome dello schema di codifica di cancellazione, seguito dal nome del pool di archiviazione.

Gli schemi di codifica di cancellazione disponibili sono limitati dal numero di nodi di archiviazione nel pool di archiviazione selezionato. UN `Recommended` Il badge appare accanto agli schemi che forniscono entrambi i"migliore protezione o il minimo sovraccarico di archiviazione" .

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 alla fine del periodo di tempo finale, a meno che un altro periodo di tempo non termini con **per sempre**.
> - A seconda di"impostazioni del periodo di conservazione del bucket e del tenant" , gli oggetti potrebbero non essere eliminati anche se termina il periodo di conservazione ILM.

6. Se si desidera archiviare oggetti in un Cloud Storage Pool:
   a. Nell'elenco a discesa **Archivia oggetti per**, seleziona **replica**.
   b. Selezionare il campo **copie in**, quindi selezionare un Cloud Storage Pool.

Quando si utilizzano i Cloud Storage Pool, tenere a mente queste regole:

- Non è possibile selezionare più di un Cloud Storage Pool in una singola istruzione di posizionamento. Allo stesso modo, non è possibile selezionare un Cloud Storage Pool e un pool di archiviazione nella stessa istruzione di posizionamento.
- È possibile archiviare solo una copia di un oggetto in un determinato Cloud Storage Pool. Se si imposta **Copie** su 2 o più, viene visualizzato un messaggio di errore.
- Non è possibile archiviare più di una copia dell'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.
- È possibile archiviare un oggetto in un Cloud Storage Pool nello stesso momento in cui l'oggetto viene archiviato come copie replicate o con codice di cancellazione in StorageGRID. Tuttavia, è necessario includere più di una riga nelle istruzioni di posizionamento per il periodo di tempo, in modo da poter specificare il numero e il tipo di copie per ogni posizione.

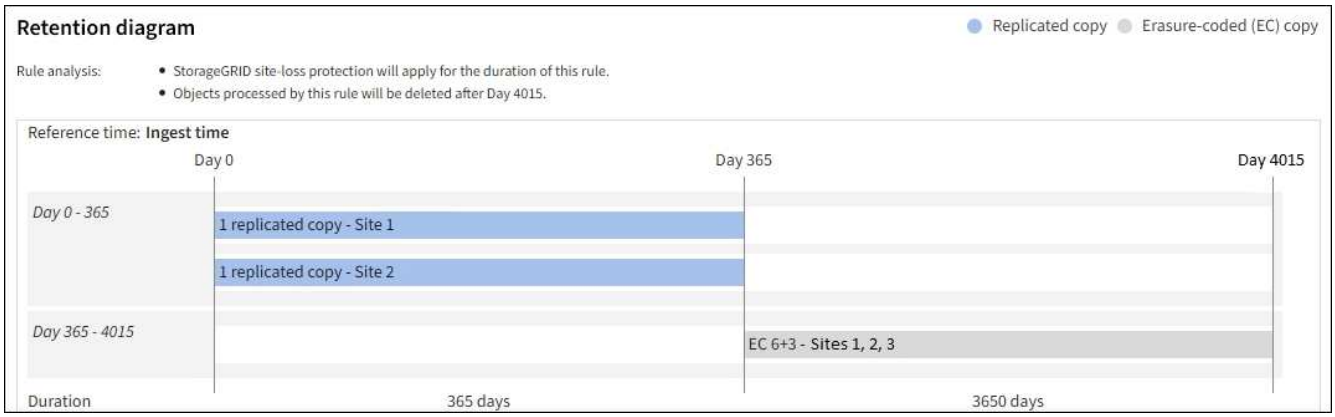
7. Nel diagramma di ritenzione, conferma le istruzioni di posizionamento.

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 altri 10 anni, una copia con codice di cancellazione 6+3 verrà salvata in tre siti. Dopo 11 anni totali, gli oggetti verranno eliminati da StorageGRID.

La sezione Analisi delle regole del diagramma di conservazione afferma:

- La protezione contro le perdite del sito StorageGRID sarà valida per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola verranno eliminati dopo il giorno 4015.

  Fare riferimento a "Abilita la protezione contro la perdita del sito."



8. Selezionare **Continua**. "Passaggio 3 (selezionare il comportamento di acquisizione)"viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare l'orario dell'ultimo accesso nelle regole ILM

È possibile utilizzare l'orario dell'ultimo accesso come orario di riferimento in una regola ILM. Ad esempio, potresti voler lasciare gli oggetti visualizzati negli ultimi tre mesi sui nodi di archiviazione locali, spostando invece gli oggetti non visualizzati di recente in una posizione esterna. È anche possibile utilizzare l'ora dell'ultimo accesso come filtro avanzato se si desidera che una regola ILM venga applicata solo agli oggetti a cui si è effettuato l'ultimo accesso in una data specifica.

Informazioni su questo compito

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

- Quando si utilizza l'orario dell'ultimo accesso come orario di riferimento, tenere presente che la modifica dell'orario dell'ultimo accesso per un oggetto non attiva una valutazione ILM immediata. Al contrario, vengono valutati i posizionamenti dell'oggetto e l'oggetto viene spostato secondo necessità quando l'ILM in background valuta l'oggetto. Potrebbero volerci due settimane o più dopo l'accesso all'oggetto.

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

- Quando si utilizza l'orario dell'ultimo accesso come filtro avanzato o come orario di riferimento, è necessario abilitare gli aggiornamenti dell'orario dell'ultimo accesso per i bucket S3. Puoi usare il"Responsabile degli inquilini" o il"API di gestione degli inquilini" .

  Per impostazione predefinita, gli aggiornamenti dell'orario dell'ultimo accesso sono disabilitati per i bucket S3.

  Tieni presente che l'abilitazione 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 vengono recuperati.

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

Tipo di richiesta	Se l'orario dell'ultimo accesso viene aggiornato quando gli aggiornamenti dell'orario dell'ultimo accesso sono disabilitati	Se l'orario dell'ultimo accesso viene aggiornato quando sono abilitati gli aggiornamenti dell'orario dell'ultimo accesso
Richiesta di recupero di un oggetto, del suo elenco di controllo di accesso o dei suoi metadati	NO	SÌ
Richiesta di aggiornamento dei metadati di un oggetto	SÌ	SÌ
Richiesta di copiare un oggetto da un bucket all'altro	• No, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia sorgente • Sì, per la copia di destinazione
Richiesta di completamento di un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Passaggio 3 di 3: seleziona il comportamento di acquisizione

Il passaggio **Seleziona comportamento di acquisizione** della procedura guidata Crea regola ILM consente di scegliere in che modo gli oggetti filtrati da questa regola vengono protetti durante l'acquisizione.

Informazioni su questo compito

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.

Passi

1. Seleziona il"comportamento di ingestione" da usare.

   Per ulteriori informazioni, consultare "Vantaggi, svantaggi e limitazioni delle opzioni di ingestione" .

   > Non è possibile utilizzare l'opzione Bilanciato o Rigoroso se la regola utilizza uno di questi posizionamenti:
   >
   > - Un pool di archiviazione cloud al giorno 0
   > - Un pool di archiviazione cloud quando la regola utilizza un orario di creazione definito dall'utente come orario di riferimento
   >
   > Vedere "Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso" .

2. Seleziona **Crea**.

   Viene creata la regola ILM. La regola non diventa attiva finché non viene aggiunta a un"Politica ILM" e tale politica viene attivata.

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

Crea una regola ILM predefinita

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Informazioni su questo compito

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

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 account tenant.

Quando crei la regola predefinita, tieni a mente questi requisiti:

- La regola predefinita verrà automaticamente posizionata come ultima regola quando la aggiungi a un criterio.
- 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 utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per una policy. Le regole di codifica di cancellazione dovrebbero utilizzare un filtro avanzato per impedire che gli oggetti più piccoli vengano codificati in modo errato.

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

Passi

1. Selezionare **ILM** > **Regole**.
2. Seleziona **Crea**.

   Viene visualizzato il passaggio 1 (Immissione dei dettagli) della procedura guidata Crea regola ILM.

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

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

6. Lasciare la selezione a discesa Nome bucket come **applicabile a tutti i bucket**.

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

7. Mantenere la risposta predefinita, **No**, per la domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?"
8. Non aggiungere filtri avanzati.

   La regola predefinita non può specificare alcun filtro.

9. Selezionare **Avanti**.

   Viene visualizzato il passaggio 2 (Definizione dei posizionamenti).

10. Per Tempo di riferimento, selezionare un'opzione qualsiasi.

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

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

> Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per una policy. Le regole di codifica di cancellazione dovrebbero includere il filtro avanzato **Dimensione oggetto (MB) maggiore di 200 KB** per impedire che oggetti più piccoli vengano codificati in modo da essere cancellati.

- Se si utilizza (o si prevede di abilitare) l'impostazione globale S3 Object Lock, la regola predefinita deve essere conforme:
  - Deve creare almeno due copie replicate dell'oggetto o una copia con codice di cancellazione.
  - Queste copie devono essere presenti sui nodi di archiviazione per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
  - Le copie degli oggetti non possono essere salvate in un Cloud Storage Pool.
  - Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando l'ora di acquisizione come ora di riferimento.
  - Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

12. Consultare il diagramma di ritenzione per confermare le istruzioni di posizionamento.
13. Selezionare **Continua**.

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

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

Gestire le policy ILM

Utilizzare le policy ILM

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

> Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Criterio ILM predefinito

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

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

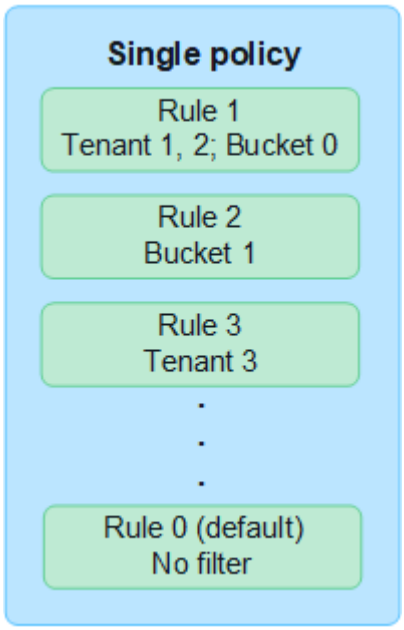
Se la policy predefinita non soddisfa i requisiti di archiviazione, è possibile creare regole e policy personalizzate. Vedere"Crea una regola ILM" E"Creare una policy ILM" .

Una o più polizze ILM attive?

È possibile avere una o più polizze ILM attive contemporaneamente.

Una politica

Se la griglia utilizzerà uno schema di protezione dei dati semplice con poche regole specifiche per tenant e bucket, utilizzare un singolo criterio ILM attivo. Le regole ILM possono contenere filtri per gestire diversi bucket o tenant.



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

Politiche multiple

Per offrire agli inquilini diverse opzioni di qualità del servizio, è possibile avere più di una polizza attiva contemporaneamente. Ogni policy può gestire tenant, bucket S3 e oggetti specifici. Quando si applica o si modifica una policy per un set specifico di tenant o oggetti, le policy applicate ad altri tenant e oggetti non vengono modificate.

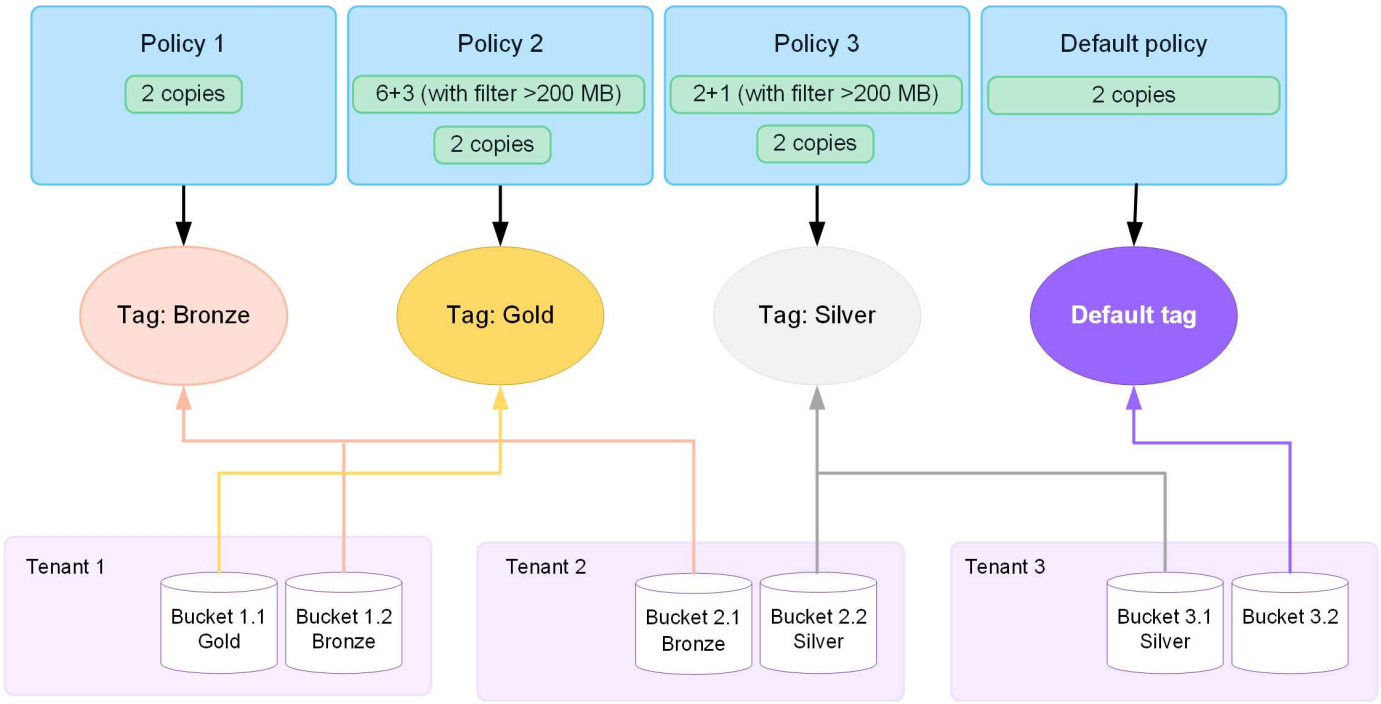
Tag di policy ILM

Se si desidera consentire ai tenant di passare facilmente da una policy di protezione dei dati all'altra per ogni bucket, utilizzare più policy ILM con *tag policy ILM*. Si assegna ogni policy ILM a un tag, quindi i tenant taggano un bucket per applicare la policy a quel bucket. È possibile impostare i tag dei criteri ILM solo sui bucket S3.

Ad esempio, potresti avere tre tag denominati Oro, Argento e Bronzo. È possibile assegnare un criterio ILM a ciascun tag, in base alla durata e alla posizione in cui tale criterio archivia gli oggetti. Gli inquilini possono scegliere quale policy utilizzare etichettando i propri bucket. Un bucket contrassegnato come Gold è gestito dalla policy Gold e riceve il livello Gold di protezione dei dati e prestazioni.

Tag di policy ILM predefinito

Un tag di policy ILM predefinito viene creato automaticamente quando si installa StorageGRID. Ogni griglia deve avere una policy attiva assegnata al tag Default. Il criterio predefinito si applica a tutti i bucket S3 non taggati.



In che modo una policy ILM valuta gli oggetti?

Una policy 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 in base al set ordinato di regole ILM nella policy, come segue:

1. Se i filtri per la prima regola nel criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di quella regola e archiviato in base alle istruzioni di posizionamento di quella regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato rispetto a ogni regola successiva nel criterio finché non viene trovata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di posizionamento e comportamento di acquisizione per la regola predefinita nel criterio. La regola predefinita è l'ultima regola di 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.

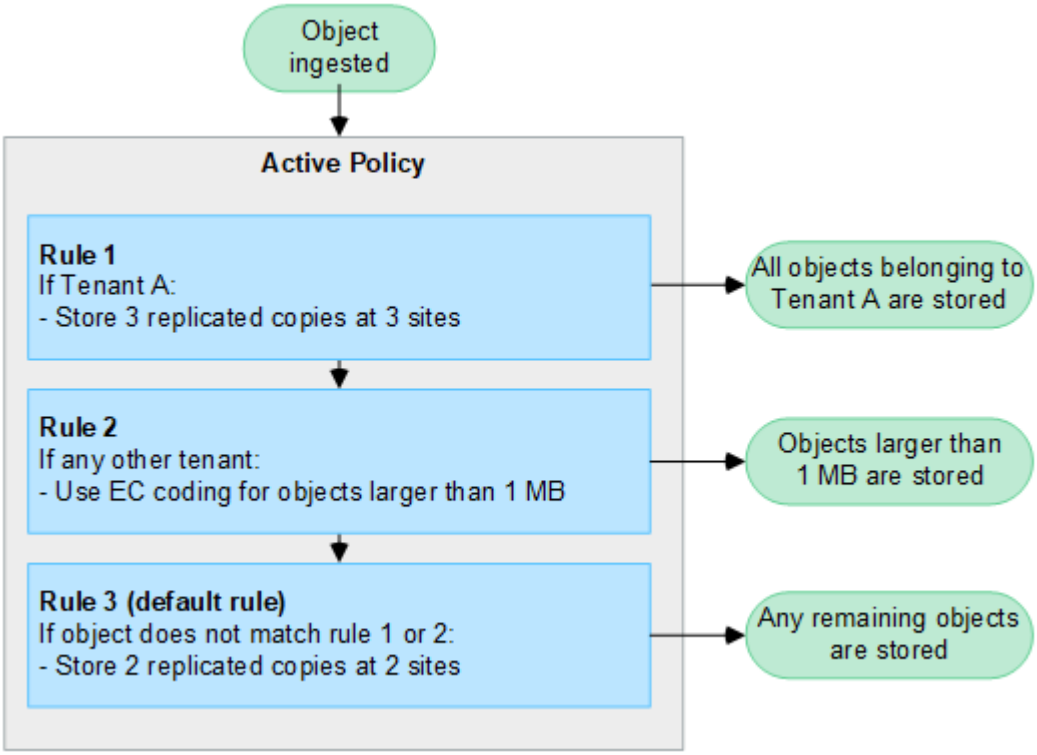
Esempio di politica ILM

Ad esempio, una policy ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per l'inquilino A**
  - Abbina tutti gli oggetti appartenenti all'inquilino A.
  - Conservare questi oggetti in tre copie replicate in tre siti.
  - Gli oggetti appartenenti ad altri tenant non sono soggetti alla Regola 1, pertanto vengono valutati in base alla Regola 2.
- **Regola 2: Codifica di cancellazione per oggetti di dimensioni superiori a 1 MB**
  - Corrisponde a tutti gli oggetti degli altri tenant, ma solo se sono maggiori di 1 MB. Questi oggetti di grandi dimensioni vengono memorizzati utilizzando la codifica di cancellazione 6+3 in tre siti.

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

- **Regola 3: 2 copie 2 data center** (predefinita)
  - È l'ultima regola predefinita della policy. Non utilizza filtri.
  - Eseguire due copie replicate di tutti gli oggetti non corrispondenti alla Regola 1 o alla Regola 2 (oggetti non appartenenti al Tenant A di dimensioni pari o inferiori a 1 MB).



Cosa sono le politiche attive e inattive?

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

Quando si crea per la prima volta un criterio ILM, si selezionano una o più regole ILM e le si dispone in un ordine specifico. Dopo aver simulato la policy per confermarne il comportamento, attivarla.

Quando si attiva un criterio ILM, StorageGRID utilizza tale criterio per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando verranno implementate le regole ILM nella nuova policy.

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

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

Considerazioni per la creazione di una politica ILM

- Nei sistemi di test utilizzare solo la policy fornita dal sistema, ovvero la policy delle copie Baseline 2. Per StorageGRID 11.6 e versioni precedenti, la regola Crea 2 copie in questo criterio utilizza il pool di archiviazione Tutti i nodi di archiviazione, che contiene tutti i siti. Se il sistema StorageGRID ha più di un

sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.

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

- Quando si progetta una nuova policy, bisogna considerare tutti i diversi tipi di oggetti che potrebbero essere inseriti nella griglia. Assicurarsi che la policy includa regole per abbinare e posizionare questi oggetti come richiesto.
- Mantenere la politica ILM il più semplice possibile. In questo modo si evitano situazioni potenzialmente pericolose in cui i dati degli oggetti non sono protetti come previsto quando nel tempo vengono apportate modifiche al sistema StorageGRID .
- Assicuratevi che le regole della policy siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'alto. Ad esempio, se la prima regola di un criterio corrisponde a un oggetto, tale 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 a un'altra regola, la regola predefinita controlla dove viene posizionato l'oggetto e per quanto tempo viene conservato.
- Prima di attivare una nuova policy, esaminare tutte le modifiche apportate dalla policy al posizionamento degli oggetti esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Creare policy ILM

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

Avere un criterio ILM attivo consente di applicare le stesse regole ILM a tutti i tenant e bucket.

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

Creare una policy ILM

Informazioni su questo compito

Prima di creare la tua politica, verifica che"politica ILM predefinita" non soddisfa i tuoi requisiti di archiviazione.

> Nei sistemi di test, utilizzare solo le policy fornite dal sistema, ovvero 2 copie della policy (per griglie a un sito) o 1 copia per sito (per griglie a più siti). Per StorageGRID 11.6 e versioni precedenti, la regola predefinita in questo criterio utilizza il pool di archiviazione All Storage Nodes, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.

> Se il"l'impostazione globale S3 Object Lock è stata abilitata" , è necessario assicurarsi che la policy ILM sia conforme ai requisiti dei bucket in cui è abilitato S3 Object Lock. In questa sezione, seguire le istruzioni che indicano di aver abilitato S3 Object Lock.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .

- Tu hai il"autorizzazioni di accesso richieste" .
- Hai"regole ILM create" in base all'abilitazione o meno del blocco oggetti S3.

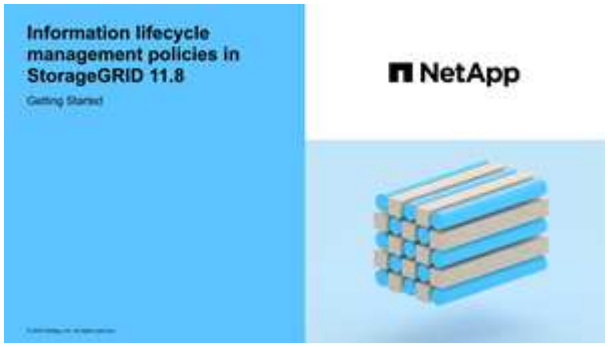
  Blocco oggetto S3 non abilitato

  - Hai"ha creato le regole ILM" che vuoi aggiungere alla polizza. Se necessario, è possibile salvare una policy, creare regole aggiuntive e quindi modificare la policy per aggiungere le nuove regole.
  - Hai"ha 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"ha creato le regole ILM conformi e non conformi" che vuoi aggiungere alla polizza. Se necessario, è possibile salvare una policy, creare regole aggiuntive e quindi modificare la policy per aggiungere le nuove regole.
  - Hai"ha creato una regola ILM predefinita" per la politica conforme.

- Facoltativamente, hai guardato il video: "Video: Panoramica delle politiche ILM"



Vedere anche "Utilizzare le policy ILM" .

Passi

1. Selezionare **ILM** > **Criteri**.

   Se l'impostazione globale Blocco oggetti S3 è abilitata, la pagina Criteri ILM indica quali regole ILM sono conformi.

2. Determina come desideri creare la policy ILM.

   Crea una nuova politica

   a. Selezionare **Crea policy**.

   Clona la politica esistente

   a. Seleziona la casella di controllo relativa al criterio da cui vuoi iniziare, quindi seleziona **Clona**.

   Modifica la policy esistente

   a. Se una policy è inattiva, puoi modificarla. Seleziona la casella di controllo per il criterio inattivo da cui vuoi iniziare, quindi seleziona **Modifica**.

3. Nel campo **Nome policy**, immettere 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 al criterio, selezionare **Seleziona regole**. Selezionare il nome di una regola per visualizzarne le impostazioni.

   Se stai clonando una policy:

   - Vengono selezionate le regole utilizzate dalla policy che stai clonando.
   - Se il criterio che stai clonando utilizzava regole senza filtri che non erano la regola predefinita, ti verrà chiesto di rimuovere tutte le regole tranne una.
   - Se la regola predefinita utilizza un filtro, ti verrà chiesto di selezionare una nuova regola predefinita.
   - Se la regola predefinita non era l'ultima regola, è possibile spostarla alla fine del nuovo criterio.

Blocco oggetto S3 non abilitato

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

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

   > Non utilizzare la regola Crea 2 copie come regola predefinita per una policy. La regola Crea 2 copie utilizza un singolo pool di archiviazione, Tutti i nodi di archiviazione, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.

Blocco oggetto S3 abilitato

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

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

   > Non utilizzare la regola Crea 2 copie come regola predefinita per una policy. La regola Crea 2 copie utilizza un singolo pool di archiviazione, Tutti i nodi di archiviazione, che contiene tutti i siti. Se si utilizza questa regola, è possibile che più copie di un oggetto vengano posizionate nello stesso sito.

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

   Ad esempio, potresti voler utilizzare un Cloud Storage Pool per archiviare oggetti in bucket in cui non è abilitato il blocco degli oggetti S3.

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

Vedere anche "Esempio 7: Politica ILM conforme per S3 Object Lock" .

6. Dopo aver selezionato la regola predefinita, seleziona **Continua**.
7. Per il passaggio Altre regole, seleziona tutte le altre regole che desideri aggiungere al criterio. Queste regole utilizzano almeno un filtro (account tenant, nome bucket, filtro avanzato o ora di riferimento non corrente). Quindi seleziona **Seleziona**.

   Nella finestra Crea un criterio sono ora elencate le regole selezionate. La regola predefinita è alla fine, mentre le altre regole sono sopra.

   Se è abilitato il blocco degli oggetti S3 e si è selezionata anche una regola "predefinita" non conforme, tale regola viene aggiunta come penultima regola nel criterio.

   > Se una regola non conserva gli oggetti per sempre, viene visualizzato un avviso. Quando si attiva questo criterio, è necessario confermare che si desidera che StorageGRID elimini gli oggetti quando scadono le istruzioni di posizionamento per la regola predefinita (a meno che un ciclo di vita del bucket non conservi gli oggetti per un periodo di tempo più lungo).

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

   Non è possibile spostare la regola predefinita. Se è abilitato il Blocco oggetto S3, non è possibile spostare la regola "predefinita" non conforme, se ne è stata selezionata una.

   > È necessario 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, iniziando dall'alto.

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

Simulare una politica

Simulare una policy sugli oggetti di prova prima di attivarla e applicarla ai dati di produzione.

Prima di iniziare

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

Passi

1. Utilizzando un client S3 o"Consolle S3" , ingerire gli oggetti necessari per testare ciascuna regola.
2. Nella pagina Criteri ILM, seleziona la casella di controllo per il criterio, quindi seleziona **Simula**.
3. Nel campo **Oggetto**, immettere S3 `bucket/object-key` per un oggetto di prova. Ad esempio, `bucket-01/filename.png` .
4. Se è abilitato il controllo delle versioni S3, è possibile immettere facoltativamente un ID versione per l'oggetto nel campo **ID versione**.
5. Selezionare **Simula**.
6. Nella sezione Risultati della simulazione, verificare che a ciascun oggetto sia stata applicata la regola corretta.

7. Per determinare quale pool di archiviazione o profilo di codifica di cancellazione è attivo, selezionare il nome della regola corrispondente per accedere alla pagina dei dettagli della regola.

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

Risultati

Eventuali modifiche alle regole della policy verranno riflesse nei risultati della simulazione e mostreranno la nuova corrispondenza e quella precedente. La finestra Criterio di simulazione conserva gli oggetti testati finché non selezioni **Cancella tutto** o l'icona di rimozione per ogni oggetto nell'elenco dei risultati della simulazione.

Informazioni correlate

"Esempio di simulazioni di policy ILM"

Attiva una politica

Quando si attiva una nuova policy ILM, gli oggetti esistenti e quelli appena acquisiti vengono gestiti da tale policy. Quando si attivano più policy, i tag delle policy ILM assegnati ai bucket determinano gli oggetti da gestire.

Prima di attivare una nuova polizza:

1. Simula la policy per verificare che si comporti come previsto.
2. Esaminare eventuali modifiche al posizionamento degli oggetti replicati e codificati con cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

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

Informazioni su questo compito

Quando si attiva una policy ILM, il sistema distribuisce la nuova policy a tutti i nodi. Tuttavia, la nuova policy attiva potrebbe non avere effetto finché tutti i nodi della griglia non saranno disponibili a riceverla. In alcuni casi, il sistema attende di implementare una nuova policy attiva per garantire che gli oggetti della griglia non vengano rimossi accidentalmente. Nello specifico:

- Se si apportano modifiche ai criteri che **aumentano la ridondanza o la durabilità dei dati**, tali modifiche vengono implementate immediatamente. Ad esempio, se si attiva una nuova policy che include una regola a tre copie anziché a due copie, tale policy verrà implementata immediatamente perché aumenta la ridondanza dei dati.
- Se si apportano modifiche ai criteri che **potrebbero ridurre la ridondanza o la durabilità dei dati**, tali modifiche non verranno implementate finché tutti i nodi della griglia non saranno disponibili. Ad esempio, se si attiva una nuova policy che utilizza una regola a due copie anziché una regola a tre copie, la nuova policy verrà visualizzata nella scheda Policy attiva, ma non avrà effetto finché tutti i nodi non saranno online e disponibili.

Passi

Seguire i passaggi per attivare una o più policy:

Attiva una politica

Se si desidera avere una sola polizza attiva, seguire questi passaggi. Se hai già una o più policy attive e stai attivando policy aggiuntive, segui i passaggi per l'attivazione di più policy.

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

   In alternativa, è possibile attivare una singola policy dalla pagina **ILM** > **Tag policy**.

2. Nella scheda Criteri, seleziona la casella di controllo per il criterio che desideri attivare, quindi seleziona **Attiva**.
3. Seguire il passaggio appropriato:
   - Se un messaggio di avviso richiede di confermare l'attivazione del criterio, selezionare **OK**.
   - Se viene visualizzato un messaggio di avviso contenente dettagli sulla policy:
     i. Esaminare i dettagli per assicurarsi che la policy gestisca i dati come previsto.
     ii. Se la regola predefinita memorizza gli oggetti per un numero limitato di giorni, rivedere il diagramma di conservazione e digitare tale numero di giorni nella casella di testo.
     iii. Se la regola predefinita memorizza gli oggetti per sempre, ma una o più altre regole hanno una conservazione limitata, digitare **sì** nella casella di testo.
     iv. Seleziona **Attiva policy**.

Attiva più policy

Per attivare più policy, è necessario creare dei tag e assegnare una policy a ciascun tag.

> Quando vengono utilizzati più tag, se i tenant riassegnano frequentemente i tag dei criteri ai bucket, le prestazioni della griglia potrebbero risentirne. Se hai tenant non attendibili, valuta la possibilità di utilizzare solo il tag Default.

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

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

4. Seleziona **Crea tag**.
5. Nella tabella dei tag dei criteri ILM, utilizzare il menu a discesa per selezionare un criterio da assegnare al tag.
6. Se nella colonna Limitazioni della policy vengono visualizzati degli avvisi, selezionare **Visualizza dettagli policy** per rivedere la policy.
7. Assicurarsi che ogni policy gestisca i dati come previsto.
8. Selezionare **Attiva policy assegnate**. Oppure seleziona **Cancella modifiche** per rimuovere l'assegnazione del criterio.

9. Nella finestra di dialogo Attiva criteri con nuovi tag, rivedere le descrizioni di come ciascun tag, criterio e regola gestirà gli oggetti. Apportare le modifiche necessarie per garantire che i criteri gestiscano gli oggetti come previsto.
10. Quando sei sicuro di voler attivare i criteri, digita **sì** nella casella di testo, quindi seleziona **Attiva criteri**.

Informazioni correlate

"Esempio 6: Modifica di una policy ILM"

Esempio di simulazioni di policy ILM

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

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

Questo esempio descrive come verificare le regole durante la simulazione di una policy.

In questo esempio, la **politica ILM di esempio** viene simulata sugli oggetti acquisiti in due bucket. La politica comprende tre regole, come segue:

- La prima regola, **Due copie, due anni per il bucket-a**, si applica solo agli oggetti nel bucket-a.
- La seconda regola, **Oggetti EC > 1 MB**, si applica a tutti i bucket ma filtra gli oggetti di dimensioni superiori a 1 MB.
- La terza regola, **Due copie, due data center**, è la regola predefinita. Non include alcun filtro e non utilizza il tempo di riferimento non corrente.

Dopo aver simulato la policy, verificare che a ciascun oggetto corrisponda la regola corretta.

In questo esempio:

- `bucket-a/bucket-a object.pdf`ha abbinato correttamente la prima regola, che filtra gli oggetti in `bucket-a .
- `bucket-b/test object greater than 1 MB.pdf`è dentro `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 corrisponde ai filtri nelle prime due regole, quindi verrà inserito dalla regola predefinita, che non include filtri.

Esempio 2: riordinare le regole durante la simulazione di una policy ILM

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

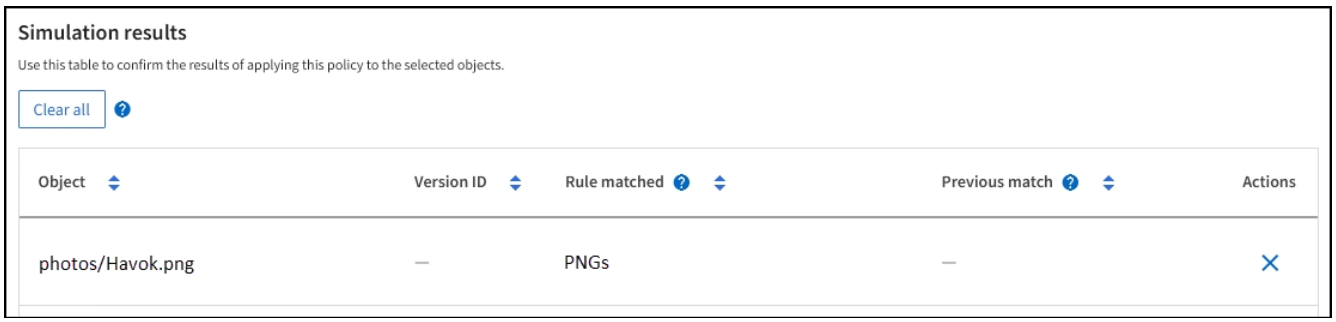
In questo esempio viene simulata la policy **Demo**. Questa politica, che ha lo scopo di trovare oggetti che hanno metadati utente series=x-men, include tre regole, come segue:

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

Passi

1. Dopo aver aggiunto le regole e salvato il criterio, seleziona **Simula**.
2. Nel campo **Oggetto**, immettere il bucket S3/chiave oggetto per un oggetto di prova e selezionare **Simula**.

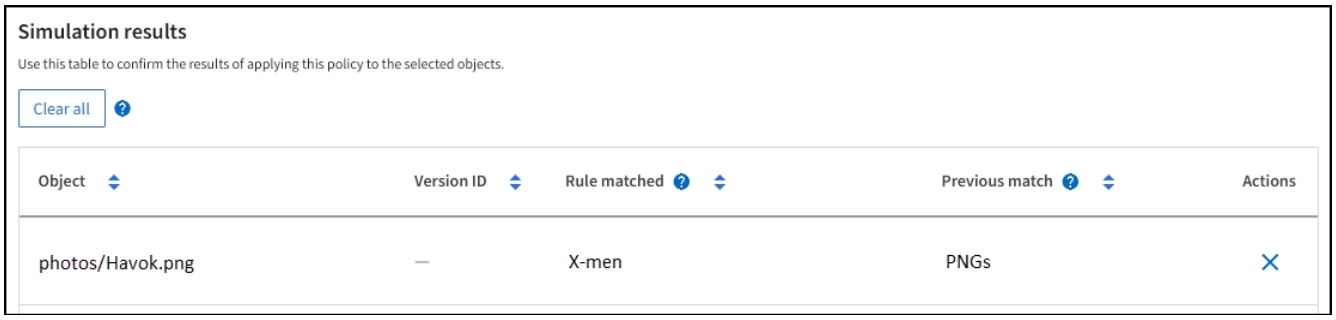
   Vengono visualizzati i risultati della simulazione, che mostrano che `Havok.png` l'oggetto è stato abbinato dalla regola **PNG**.



   Tuttavia, `Havok.png` aveva lo scopo di testare la regola degli **X-men**.

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

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



Esempio 3: correggere 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 viene simulata la policy **Demo**. Questa politica ha lo scopo di trovare oggetti che hanno `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati inaspettati quando si è simulata questa politica contro il `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati degli X-Men, l'oggetto corrispondeva alla regola predefinita: due copie di due data center.

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

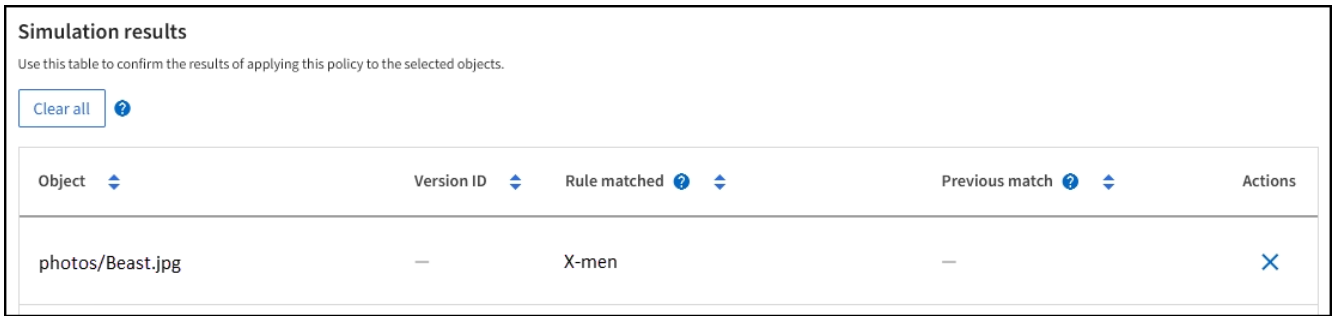
Passi

1. Selezionare **Fine** per chiudere la finestra di dialogo Simula criterio. Nella pagina dei dettagli della policy, seleziona **Diagramma di conservazione**. Quindi seleziona **Espandi tutto** o **Visualizza dettagli** per ogni regola, a seconda delle necessità.
2. Esaminare l'account tenant della regola, l'ora di riferimento e i criteri di filtraggio.

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

3. Per risolvere l'errore, correggere la regola come segue:
   - Se la regola fa parte della policy, puoi clonarla o rimuoverla dalla policy e poi modificarla.
   - Se la regola fa parte della policy attiva, è necessario clonarla. Non è possibile modificare o rimuovere una regola dal criterio attivo.
4. Eseguire nuovamente la simulazione.

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



Gestisci i tag dei criteri ILM

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"autorizzazioni di accesso richieste" .

Visualizza i dettagli del tag della policy ILM

Per visualizzare i dettagli di un tag:

1. Selezionare **ILM** > **Tag policy**.
2. Selezionare 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 tag policy ILM

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

Per modificare la descrizione di un tag esistente:

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

   In alternativa, seleziona il nome del tag. Viene visualizzata la pagina dei dettagli del tag, in cui puoi selezionare **Modifica**.

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

Rimuovi il tag della policy ILM

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

Per rimuovere un tag:

1. Selezionare **ILM** > **Tag policy**.
2. Seleziona la casella di controllo per il 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, in cui puoi selezionare **Rimuovi**.

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

Verifica una policy ILM con la ricerca dei metadati degli oggetti

Dopo aver attivato un criterio ILM, importare oggetti di prova rappresentativi nel sistema StorageGRID , quindi eseguire una ricerca dei metadati degli oggetti per confermare che le copie vengano eseguite come previsto e posizionate nelle posizioni corrette.

Prima di iniziare

Hai un identificatore di oggetto, che può essere uno dei seguenti: * **UUID**: l'identificatore univoco universale dell'oggetto. * **CBID**: Identificatore univoco dell'oggetto all'interno StorageGRID. È possibile ottenere il CBID di un oggetto dal registro di controllo. Inserire il CBID in maiuscolo. * **Chiave oggetto e bucket S3**: quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di chiave oggetto e bucket per archiviare e identificare l'oggetto. Se il bucket S3 è sottoposto a controllo di versione e si desidera cercare una versione specifica di un oggetto S3 utilizzando il bucket e la chiave dell'oggetto, si ottiene l'**ID versione**.

Passi

1. Ingerire l'oggetto.
2. Selezionare **ILM** > **Ricerca metadati oggetto**.
3. Digitare l'identificatore dell'oggetto nel campo **Identificatore**. È possibile immettere un UUID, un CBID o un bucket/chiave oggetto S3.
4. Facoltativamente, immettere un ID versione per l'oggetto (solo S3).
5. Seleziona **Cerca**.

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

   - Metadati di sistema, come ID oggetto (UUID), tipo di risultato (oggetto, marcatore di eliminazione, bucket S3) e dimensione logica dell'oggetto. Per maggiori dettagli, fare riferimento allo screenshot di esempio riportato di seguito.
   - Qualsiasi coppia chiave-valore di metadati utente personalizzati associata all'oggetto.
   - Per gli oggetti S3, qualsiasi coppia chiave-valore del tag oggetto associata all'oggetto.
   - Per le copie di oggetti replicati, la posizione di archiviazione corrente di ciascuna copia.
   - Per le copie di oggetti con codice 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'identificatore univoco dell'oggetto.
   - Per oggetti segmentati e oggetti multiparte, un elenco di segmenti di oggetti, inclusi gli identificatori di

segmento 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 archiviazione interna non elaborato. Questi metadati grezzi includono metadati di sistema interni la cui persistenza da una versione all'altra non è garantita.

6. Verificare che l'oggetto sia archiviato nella posizione o nelle posizioni corrette e che si tratti del tipo di copia corretto.

   Se l'opzione Audit è abilitata, è anche possibile monitorare il registro di audit per il messaggio ORLM Object Rules Met. Il messaggio di controllo ORLM può fornire maggiori informazioni sullo stato del processo di valutazione ILM, ma non può fornire informazioni sulla correttezza del posizionamento dei dati dell'oggetto o sulla completezza della policy ILM. Devi valutarlo tu stesso. Per maggiori dettagli, vedere "Esaminare i registri di controllo" .

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

> La seguente schermata è un esempio. I risultati varieranno a seconda della versione 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

"Utilizzare l'API REST S3"

Lavorare con le policy e le regole ILM

Man mano che cambiano i requisiti di archiviazione, potrebbe essere necessario implementare policy aggiuntive o modificare le regole ILM associate a una policy. È possibile visualizzare le metriche ILM per determinare le prestazioni del sistema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Visualizza le policy ILM

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

1. Selezionare **ILM** > **Criteri**.
2. Selezionare **Criteri** per visualizzare un elenco dei criteri attivi e inattivi. Nella tabella sono elencati il nome di ciascun criterio, i tag a cui è assegnato e se il criterio è attivo o inattivo.
3. Selezionare **Cronologia attivazioni** per visualizzare un elenco delle date di inizio e fine dell'attivazione delle polizze.
4. Selezionare il nome di una policy per visualizzarne i dettagli.

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

Modifica una policy ILM

È possibile modificare solo una policy inattiva. Se si desidera modificare una policy attiva, è possibile disattivarla oppure creare un clone e modificarlo.

Per modificare una policy:

1. Selezionare **ILM** > **Criteri**.
2. Seleziona la casella di controllo relativa alla policy che desideri modificare, quindi seleziona **Modifica**.
3. Modifica la policy seguendo le istruzioni in"Creare policy ILM" .
4. Simulare la policy prima di riattivarla.

> Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Clonare una policy ILM

Per clonare una policy ILM:

1. Selezionare **ILM** > **Criteri**.
2. Seleziona la casella di controllo relativa alla policy che desideri clonare, quindi seleziona **Clona**.
3. Crea una nuova policy partendo dalla policy che hai clonato seguendo le istruzioni in"Creare policy ILM" .

> Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Rimuovere una policy ILM

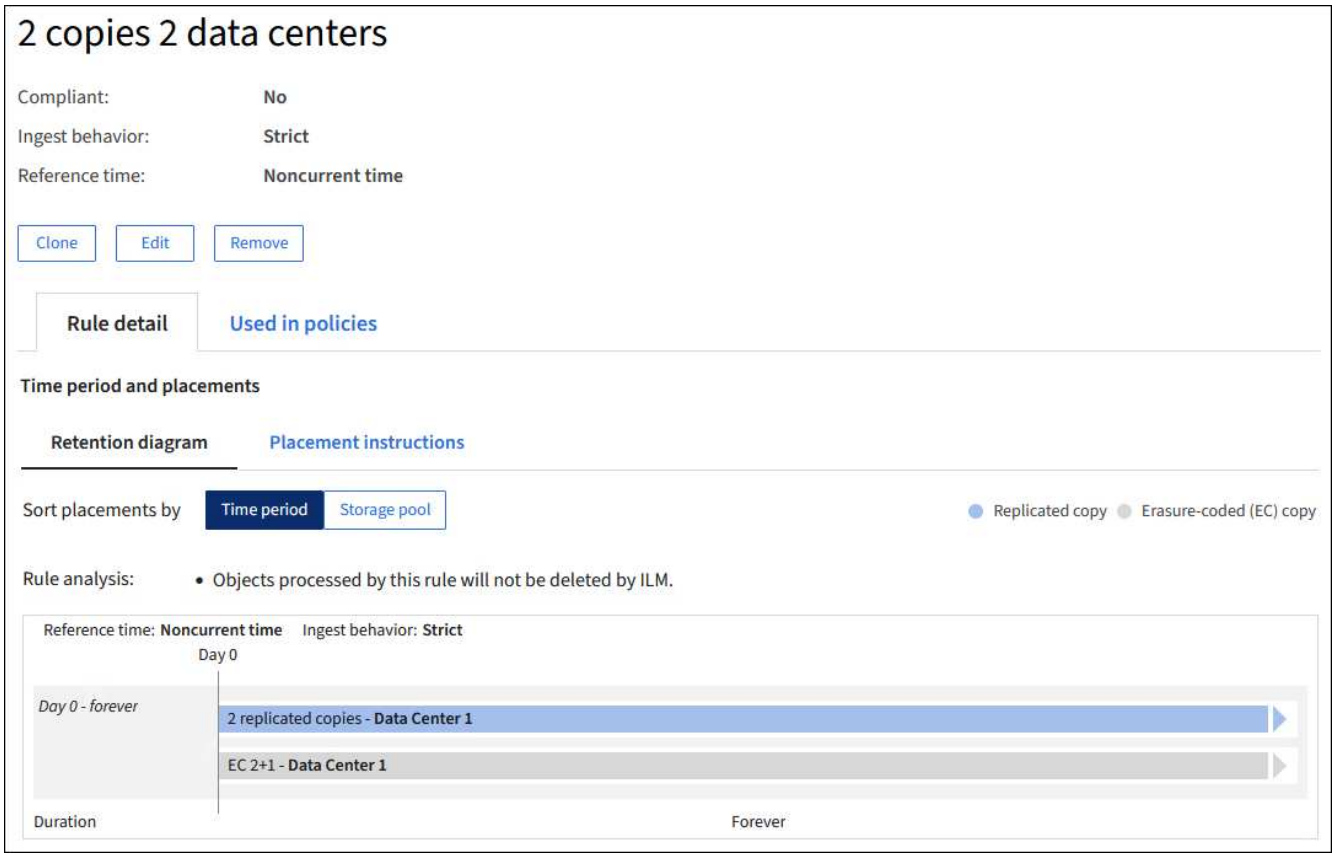
È possibile rimuovere un criterio ILM solo se è inattivo. Per rimuovere una policy:

1. Selezionare **ILM** > **Criteri**.
2. Seleziona la casella di controllo relativa al criterio inattivo che desideri 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 di posizionamento per la regola:

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



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

Clona una regola ILM

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

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

Passi

1. Selezionare **ILM** > **Regole**.
2. Seleziona la casella di controllo relativa 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 permodifica di una regola ILM E"utilizzo di filtri avanzati

nelle regole ILM" .

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

Modifica una regola ILM

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

Non è possibile modificare una regola se è utilizzata in una policy ILM. Invece, puoiclonare la regola e apportare tutte le modifiche necessarie alla copia clonata.

> ⚠ Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Passi

1. Selezionare **ILM** > **Regole**.
2. Verificare che la regola che si desidera modificare non sia utilizzata in alcuna policy ILM.
3. Se la regola che vuoi modificare non è in uso, seleziona la casella di controllo per la regola e seleziona **Azioni** > **Modifica**. In alternativa, seleziona il nome della regola, quindi seleziona **Modifica** nella pagina dei dettagli della regola.
4. Completare i passaggi della procedura guidata Modifica regola ILM. Se necessario, seguire i passaggi per"creazione di una regola ILM" E"utilizzo di filtri avanzati nelle regole ILM" .

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

Rimuovere una regola ILM

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

Passi

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

1. Clonare la policy.
2. Rimuovere la regola ILM dal clone della policy.
3. Salvare, simulare e attivare la nuova policy per assicurarsi che gli oggetti siano protetti come previsto.
4. Vai ai passaggi per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo.

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

1. Selezionare la policy inattiva.
2. Rimuovere la regola ILM dalla policy orimuovere la politica .
3. Vai ai passaggi per rimuovere una regola ILM attualmente non utilizzata.

Per rimuovere una regola ILM attualmente non utilizzata:

1. Selezionare **ILM** > **Regole**.

2. Verificare che la regola che si desidera rimuovere non sia utilizzata in alcun criterio.
3. Se la regola che vuoi rimuovere non è in uso, selezionala e seleziona **Azioni** > **Rimuovi**. È possibile selezionare più regole e rimuoverle tutte contemporaneamente.
4. Selezionare **Sì** per confermare che si desidera rimuovere la regola ILM.

Visualizza le metriche ILM

È possibile visualizzare le metriche per ILM, come il numero di oggetti nella coda e la frequenza di valutazione. È possibile monitorare queste metriche per determinare le prestazioni del sistema. Una coda o una frequenza di valutazione elevate potrebbero indicare che il sistema non è in grado di tenere il passo con la frequenza di acquisizione, che il carico delle applicazioni client è eccessivo o che si è verificata una condizione anomala.

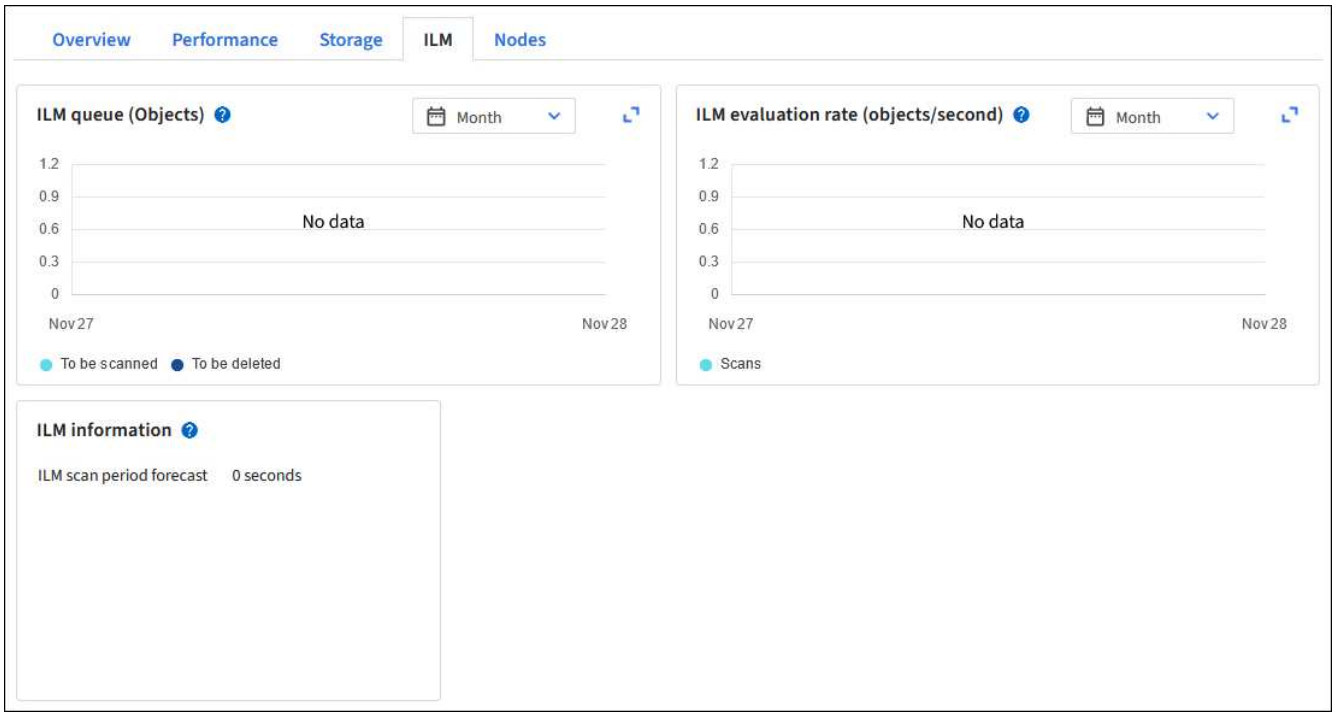
Passi

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

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

2. Monitorare le metriche nella scheda ILM.

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



Utilizzare il blocco oggetto S3

Gestisci gli oggetti con S3 Object Lock

In qualità di amministratore della griglia, puoi abilitare S3 Object Lock per il tuo sistema StorageGRID e implementare una policy ILM conforme per garantire che gli oggetti in bucket S3 specifici 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 account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se in un bucket è abilitato S3 Object Lock, è necessario il controllo delle versioni del bucket, che 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 e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con S3 Object Lock e conservazione predefinita configurata può contenere 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.

Di fatto, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurata la conservazione predefinita. Gli oggetti esistenti senza impostazioni di conservazione degli oggetti rimangono inalterati.

Modalità di conservazione

La funzionalità StorageGRID S3 Object Lock 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 finché non viene raggiunta la data di conservazione.
  - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità di 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.
  - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

Impostazioni di conservazione per le versioni degli oggetti

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

- **Modalità di conservazione**: conformità o governance.
- **Retain-until-date**: se la retain-until-date di una versione di un oggetto è futura, l'oggetto può essere recuperato, ma non eliminato.
- **Sospensione legale**: l'applicazione di una sospensione legale a una versione di un oggetto blocca

immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di scadenza, ma rimane in vigore finché non viene rimossa esplicitamente. Le sospensioni legali sono indipendenti dalla data di conservazione fino alla data di scadenza.

> Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

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

Impostazione di conservazione predefinita per i bucket

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

- **Modalità di conservazione predefinita**: conformità o governance.
- **Periodo di conservazione predefinito**: per quanto tempo devono essere conservate le nuove versioni degli oggetti aggiunte a questo bucket, a partire dal giorno in cui vengono aggiunte.

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

Vedere"Crea un bucket S3" E"Aggiorna la conservazione predefinita del blocco degli oggetti S3" .

Confronto tra S3 Object Lock e la conformità legacy

S3 Object Lock sostituisce la funzionalità Compliance disponibile nelle versioni precedenti StorageGRID . Poiché la funzionalità S3 Object Lock è conforme ai requisiti di Amazon S3, essa rende obsoleta la funzionalità proprietaria StorageGRID Compliance, ora denominata "legacy Compliance".

> L'impostazione Conformità globale è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione Blocco oggetto S3 viene abilitata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per i dettagli, vedere "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5" .

Se hai utilizzato la funzionalità Conformità legacy in una versione precedente di StorageGRID, fai riferimento alla tabella seguente per scoprire come si confronta con la funzionalità Blocco oggetti S3 in StorageGRID.

	Blocco oggetto S3	**Conformità (legacy)**
Come viene abilitata la funzionalità a livello globale?	Da Grid Manager, seleziona **CONFIGURAZIONE** > **Sistema** > **Blocco oggetto S3**.	Non più supportato.

	Blocco oggetto S3	Conformità (legacy)
Come si abilita la funzionalità per un bucket?	Gli utenti devono abilitare S3 Object Lock quando creano un nuovo bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API.	Non più supportato.
È supportato il controllo delle versioni dei bucket?	Sì. Il controllo delle versioni del bucket è obbligatorio e viene abilitato automaticamente quando S3 Object Lock è abilitato per il bucket.	NO.
Come viene impostata 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.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
È possibile modificare il periodo di conservazione?	• In modalità di conformità, la data di conservazione per una versione di un oggetto può essere aumentata ma mai diminuita. • In modalità di governance, gli utenti con autorizzazioni speciali possono ridurre o addirittura rimuovere le impostazioni di conservazione di un oggetto.	Il periodo di conservazione di un bucket può essere aumentato, ma mai diminuito.
Dove viene controllata la conservazione legale?	Gli utenti possono applicare o rimuovere una sospensione legale per qualsiasi versione dell'oggetto nel bucket.	Viene applicata una sospensione legale al bucket che interessa tutti gli oggetti al suo interno.

	Blocco oggetto S3	Conformità (legacy)
Quando è possibile eliminare gli oggetti?	• In modalità di conformità, una versione dell'oggetto può essere eliminata dopo aver raggiunto la data di conservazione, a condizione che l'oggetto non sia soggetto a conservazione legale. • In modalità di governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la data di conservazione, a condizione che l'oggetto non sia soggetto a conservazione legale.	Un oggetto può essere eliminato dopo la scadenza del periodo di conservazione, a condizione che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere eliminati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	SÌ	NO

Attività di blocco degli oggetti S3

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

> L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

Gli elenchi seguenti per gli amministratori della griglia e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzionalità S3 Object Lock.

Amministratore di rete

- Abilita l'impostazione globale di blocco degli oggetti S3 per l'intero sistema StorageGRID .
- Garantire che le politiche di gestione del ciclo di vita delle informazioni (ILM) siano *conformi*; ovvero, che soddisfino i"requisiti dei bucket con S3 Object Lock abilitato" .
- Se necessario, consentire a un tenant di utilizzare Conformità come modalità di conservazione. In caso contrario, è consentita solo la modalità Governance.
- Se necessario, impostare un periodo massimo di conservazione per un tenant.

Utente inquilino

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

    - Modalità di conservazione predefinita: Governance o Conformità, se consentita dall'amministratore della rete.
    - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica dell'oggetto:
    - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore della rete.
    - Conserva fino alla data: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per S3 Object Lock

È necessario esaminare i requisiti per abilitare l'impostazione globale S3 Object Lock, i requisiti per creare regole ILM 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

- È necessario abilitare l'impostazione globale S3 Object Lock tramite Grid Manager o Grid Management API prima che un tenant S3 possa creare un bucket con S3 Object Lock abilitato.
- Abilitando l'impostazione globale S3 Object Lock, tutti gli account tenant S3 potranno creare bucket con S3 Object Lock abilitato.
- Dopo aver abilitato l'impostazione globale Blocco oggetti S3, non è possibile disabilitarla.
- Non è possibile abilitare il blocco oggetti S3 globale a meno che la regola predefinita in tutti i criteri ILM attivi non sia *conforme* (ovvero, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetti S3 abilitato).
- Quando l'impostazione globale Blocco oggetti S3 è abilitata, non è possibile creare un nuovo criterio ILM o attivarne uno esistente, a meno che la regola predefinita nel criterio non sia conforme. Dopo aver abilitato l'impostazione globale S3 Object Lock, le pagine Regole ILM e Criteri ILM indicano quali regole ILM sono conformi.

Requisiti per le regole ILM conformi

Se si desidera abilitare l'impostazione globale S3 Object Lock, è necessario assicurarsi che la regola predefinita in tutti i criteri ILM attivi sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con S3 Object Lock abilitato e di tutti i bucket esistenti con la conformità legacy abilitata:

- Deve creare almeno due copie replicate dell'oggetto o una copia con codice di cancellazione.
- Queste copie devono essere presenti sui nodi di archiviazione per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
- Le copie degli oggetti non possono essere salvate 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 di posizionamento deve essere "per sempre".

Requisiti per le politiche ILM

Quando l'impostazione globale Blocco oggetti S3 è abilitata, i criteri ILM attivi e inattivi possono includere sia regole conformi che non conformi.

- La regola predefinita in una policy ILM attiva o inattiva deve essere conforme.
- Le regole non conformi si applicano solo agli oggetti nei bucket in cui non è abilitato S3 Object Lock o in cui non è abilitata la funzionalità legacy Compliance.
- Le regole conformi possono essere applicate agli oggetti in qualsiasi bucket; non è necessario abilitare S3 Object Lock o la conformità legacy 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 , è possibile utilizzare Tenant Manager, Tenant Management API o S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se si prevede di utilizzare S3 Object Lock, è necessario abilitarlo quando si crea il bucket. Non è possibile abilitare S3 Object Lock per un bucket esistente.
- Quando S3 Object Lock è abilitato per un bucket, StorageGRID abilita automaticamente il controllo delle versioni per quel bucket. Non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione predefinita e un periodo di conservazione per ciascun bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di impostazioni di conservazione proprie. È possibile ignorare queste impostazioni predefinite specificando una modalità di conservazione e una data di conservazione per ogni versione dell'oggetto quando viene caricata.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con S3 Object Lock abilitato.
- La replica CloudMirror 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 dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure specificare le impostazioni di conservazione per ciascuna versione dell'oggetto. Le impostazioni di conservazione a livello di oggetto possono essere specificate tramite l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia un'impostazione di conservazione fino alla data di scadenza che un'impostazione di conservazione legale, una ma non l'altra, oppure nessuna delle due. Specificando un'impostazione di conservazione fino a data o di conservazione legale per un oggetto, si protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

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

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

1. **Ingestione di oggetti**

   Quando una versione di un oggetto viene aggiunta a un bucket in cui è abilitato il blocco degli oggetti S3,

le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte 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 presenti.
- 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, vengono protetti sia l'oggetto sia tutti i metadati S3 definiti dall'utente.

2. **Conservazione ed eliminazione degli oggetti**

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

   - Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Informazioni correlate

- "Crea un bucket S3"
- "Aggiorna la conservazione predefinita del blocco degli oggetti S3"
- "Utilizzare l'API REST S3 per configurare S3 Object Lock"
- "Esempio 7: Politica ILM conforme per S3 Object Lock"

Abilita il blocco oggetti S3 a livello globale

Se un account tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, è necessario 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

- Tu hai il"Permesso di accesso root" .
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai esaminato il flusso di lavoro di S3 Object Lock e ne hai compreso le considerazioni.
- Hai confermato che la regola predefinita nel criterio ILM attivo è conforme. Vedere"Crea una regola ILM predefinita" per i dettagli.

Informazioni su questo compito

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

Dopo aver abilitato l'impostazione globale Blocco oggetti S3, rivedere le impostazioni di conformità dei tenant esistenti. Quando si abilita questa impostazione, le impostazioni di S3 Object Lock per tenant dipendono dalla versione StorageGRID al momento della creazione del tenant.

L'impostazione Conformità globale è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione Blocco oggetto S3 viene abilitata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per i dettagli, vedere "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5" .

Passi

1. Selezionare **CONFIGURAZIONE** > **Sistema** > **Blocco oggetto S3**.

   Viene visualizzata la pagina Impostazioni blocco oggetti S3.

2. Selezionare **Abilita blocco oggetto S3**.
3. Selezionare **Applica**.

   Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare S3 Object Lock dopo averlo attivato.

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 nel criterio ILM attivo 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. È necessario creare e attivare una nuova policy ILM che includa una regola conforme come regola predefinita. Selezionare **OK**. Quindi, crea una nuova policy, simulala e attivala. Vedere"Crea policy ILM" per istruzioni.

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

Se un sito del data center o più nodi di archiviazione in un sito diventano non disponibili, potrebbe essere necessario aiutare gli utenti del tenant S3 ad applicare le modifiche al blocco degli oggetti S3 o alla configurazione di conformità legacy.

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

Quando un utente tenant aggiorna le impostazioni per un bucket S3 o una versione di oggetto, StorageGRID tenta di aggiornare immediatamente i metadati del bucket o dell'oggetto in tutta la griglia. Se il sistema non riesce ad aggiornare i metadati perché un sito del data center o più nodi di archiviazione 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. Tentare di rendere nuovamente disponibili tutti i nodi o siti di archiviazione il prima possibile.
2. Se non riesci a rendere disponibili sufficienti nodi di archiviazione in ogni sito, contatta l'assistenza tecnica, che può aiutarti a ripristinare i nodi e a garantire che le modifiche vengano applicate in modo coerente in tutta la griglia.
3. Una volta risolto il problema di fondo, ricorda all'utente tenant di riprovare ad apportare le modifiche alla configurazione.

Informazioni correlate

- "Utilizzare un account tenant"
- "Utilizzare l'API REST S3"
- "Recuperare e mantenere"

Esempio di regole e policy ILM

Esempio 1: regole e policy ILM per l'archiviazione degli oggetti

È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per definire una policy ILM che soddisfi i 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 verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

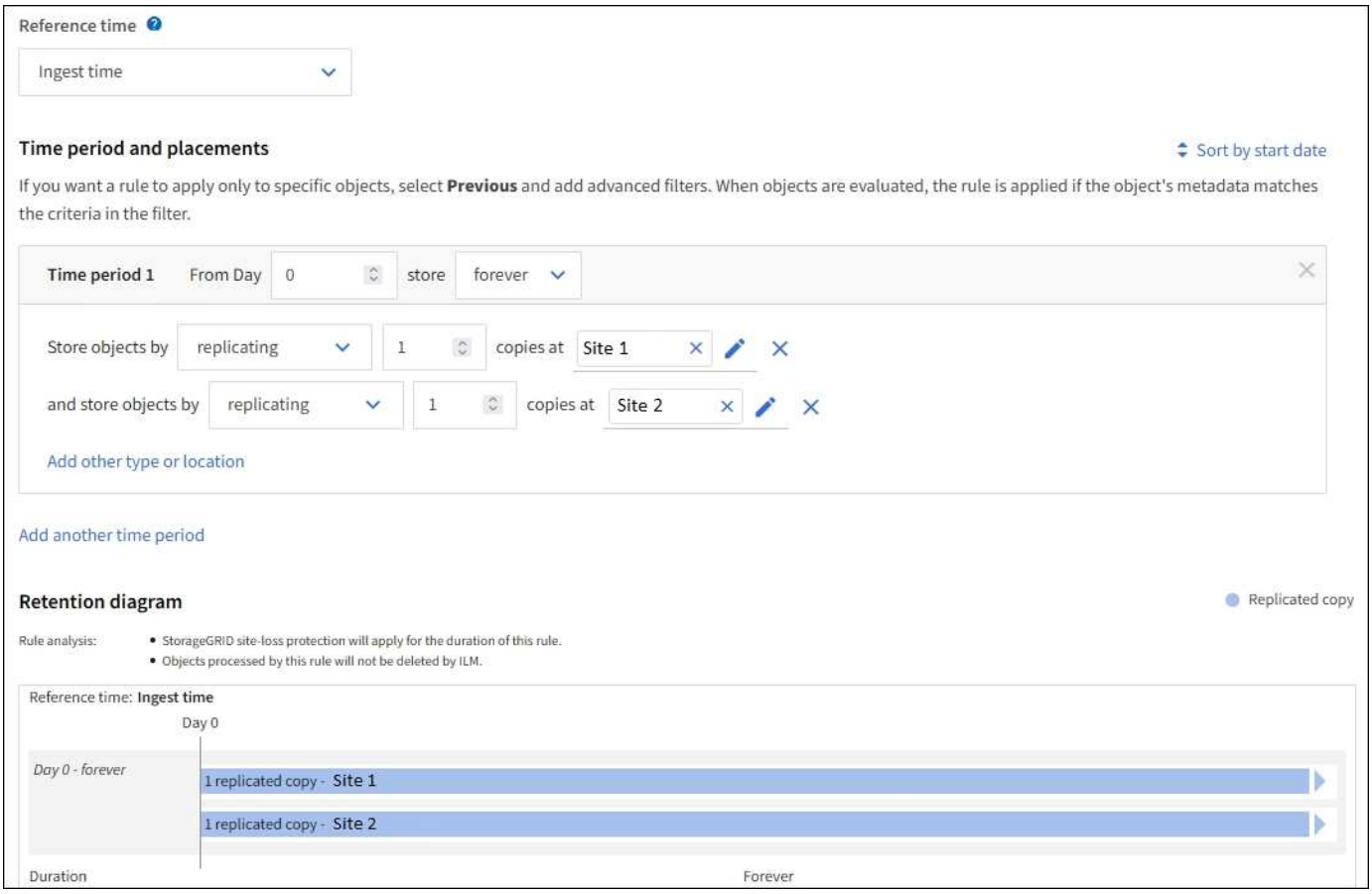
Regola ILM 1 per l'esempio 1: Copia i dati dell'oggetto in due siti

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

Definizione della regola	Valore di esempio
Pool di archiviazione monosito	Due pool di archiviazione, ciascuno contenente siti diversi, denominati Sito 1 e Sito 2.
Nome della regola	Due copie due siti
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 all'infinito, conserva una copia replicata nel sito 1 e una copia replicata nel sito 2.

La sezione Analisi delle regole del diagramma di conservazione afferma:

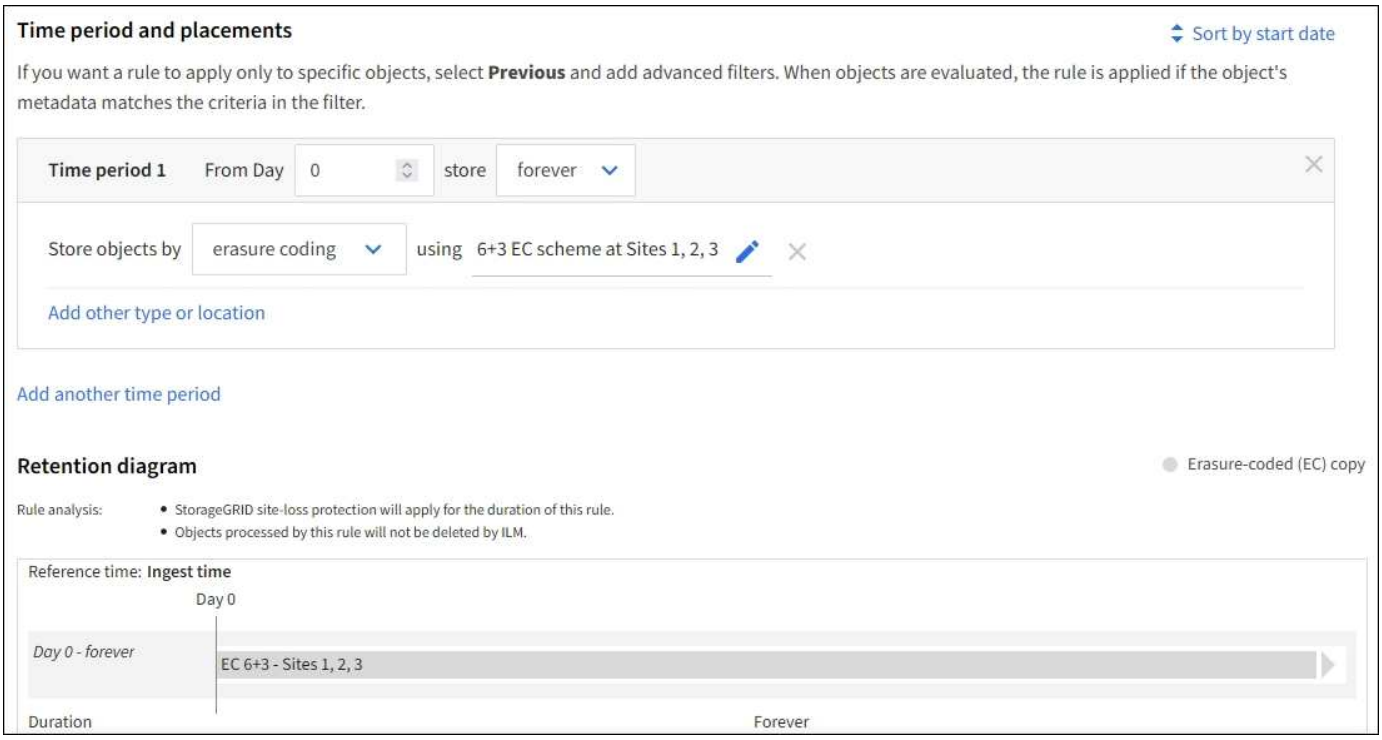
- La protezione contro le perdite del sito StorageGRID sarà valida per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola non verranno eliminati da ILM.



Regola ILM 2 per l'esempio 1: profilo di codifica di cancellazione con corrispondenza del bucket

Questa regola ILM di esempio utilizza un profilo di codifica di cancellazione e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene archiviato.

Definizione della regola	Valore di esempio
Pool di archiviazione con più siti	• Un pool di archiviazione su tre siti (siti 1, 2, 3) • Utilizzare lo schema di codifica di cancellazione 6+3
Nome della regola	S3 Bucket finance-records
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Per gli oggetti nel bucket S3 denominato finance-records, creare una copia con codice di cancellazione nel pool specificato dal profilo di codifica di cancellazione. Conserva questa copia per sempre.

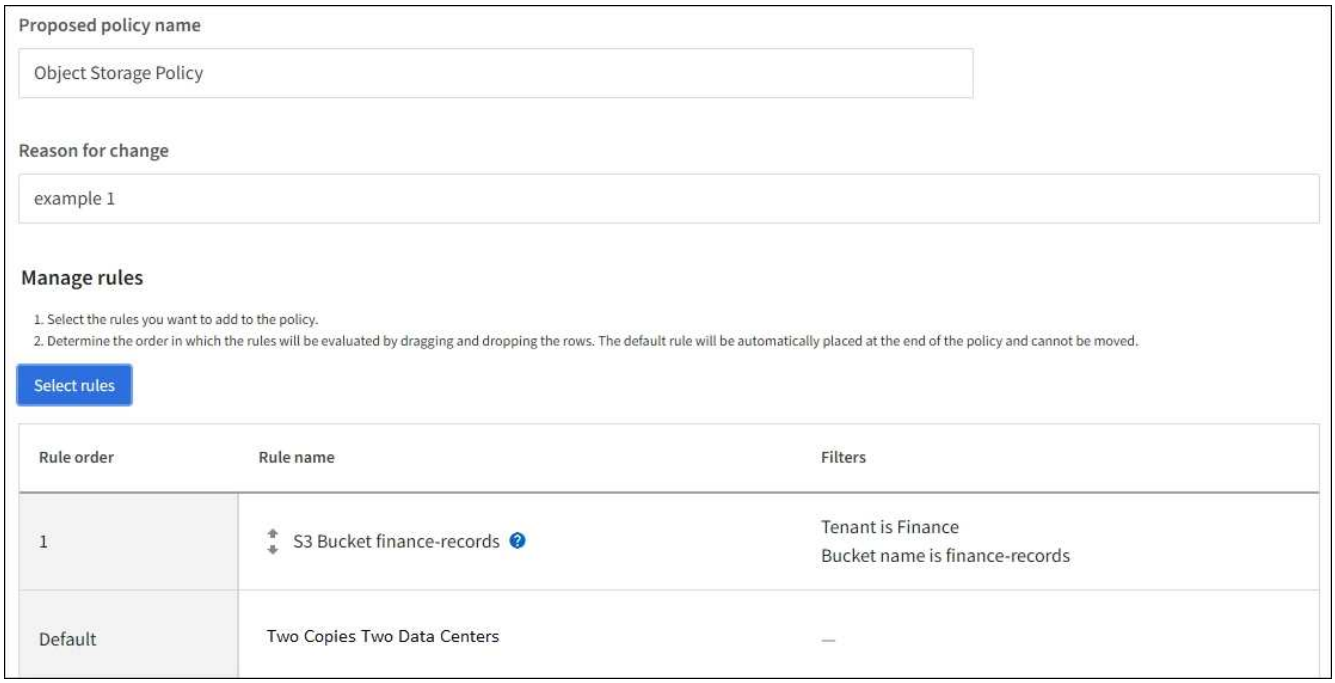


Politica ILM per esempio 1

Nella 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 griglia multi-sito potrebbe includere regole ILM come le seguenti:

- Durante l'acquisizione, archivia tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in un pool di archiviazione che contiene tre siti. Utilizzare la codifica di cancellazione 6+3.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita del criterio, Due copie due data center, per archiviare una copia di tale oggetto nel Sito 1 e una copia nel Sito 2.



Informazioni correlate

- "Utilizzare le policy ILM"
- "Creare policy ILM"

Esempio 2: regole e policy ILM per il filtraggio delle dimensioni degli oggetti EC

È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire una policy ILM che filtri in base alle dimensioni dell'oggetto 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 verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per l'esempio 2: utilizzare EC per oggetti maggiori di 1 MB

Questa regola ILM di esempio codifica gli oggetti di dimensioni superiori a 1 MB.

> La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	Solo oggetti EC > 1 MB
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto maggiore di 1 MB
Posizionamenti	Crea una copia con codice di cancellazione 2+1 utilizzando tre siti

Regola ILM 2 per esempio 2: Due copie replicate

Questa regola ILM di esempio crea due copie replicate e non filtra in base alle dimensioni dell'oggetto. Questa regola è la regola predefinita per 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	Valore di esempio
Nome della regola	Due copie replicate

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Nessuno
Posizionamenti	Dal giorno 0 all'infinito, conserva una copia replicata nel sito 1 e una copia replicata nel sito 2.

Criterio ILM per esempio 2: utilizzare EC per oggetti maggiori di 1 MB

Questo esempio di policy ILM include due regole ILM:

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

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

È possibile utilizzare le seguenti regole e policy di esempio per garantire che le immagini di dimensioni superiori a 1 MB vengano codificate con cancellazione e che vengano realizzate 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 verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

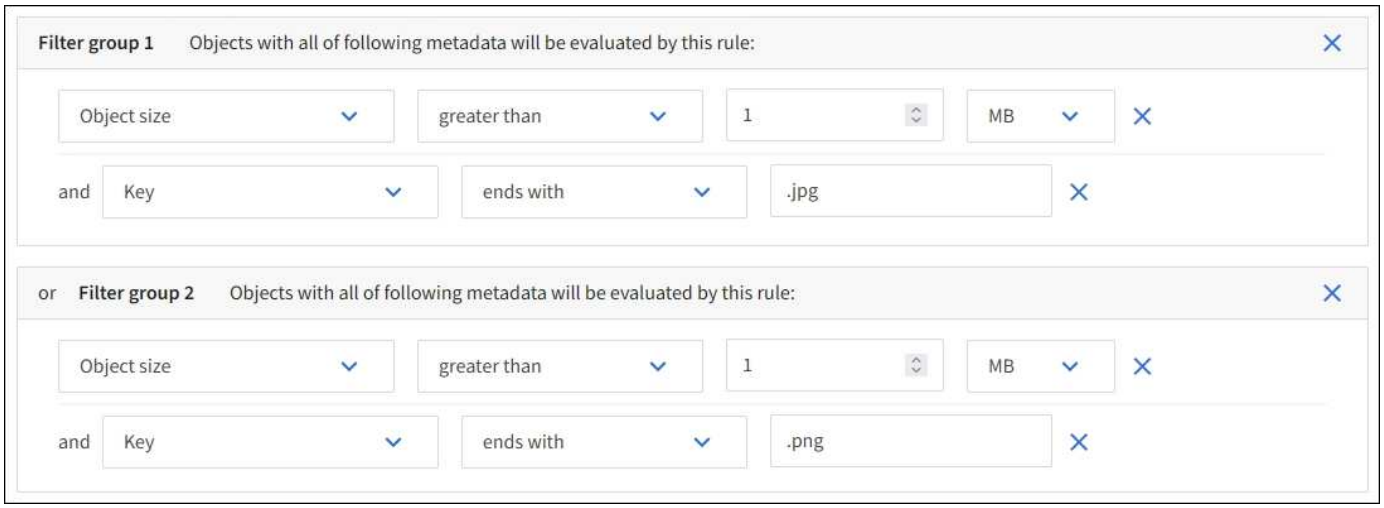
Regola ILM 1 per esempio 3: utilizzare EC per file immagine superiori a 1 MB

Questa regola ILM di esempio utilizza un filtro avanzato per cancellare il codice di 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 utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	File immagine EC > 1 MB
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto maggiore di 1 MB

Definizione della regola	Valore di esempio
Filtri avanzati per la chiave	• Termina con .jpg • Termina con .png
Posizionamenti	Crea una copia con codice di cancellazione 2+1 utilizzando tre siti



Poiché questa regola è configurata come la prima regola del criterio, 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 l'esempio 3: creare 2 copie replicate per tutti i file immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file immagine più piccoli devono essere replicati. Poiché la prima regola del criterio ha già trovato corrispondenze con 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	Valore di esempio
Nome della regola	2 copie per i file immagine
Tempo di riferimento	Tempo di ingestione
Filtri avanzati per la chiave	• Termina con .jpg • Termina con .png
Posizionamenti	Crea 2 copie replicate in due pool di archiviazione

Politica ILM per esempio 3: migliore protezione per i file immagine

Questo esempio di policy ILM include tre regole:

- La prima regola codifica tutti i file immagine di dimensioni superiori a 1 MB.
- La seconda regola crea due copie di tutti i file immagine rimanenti (ovvero immagini di dimensioni pari o inferiori a 1 MB).

- La regola predefinita si applica a tutti gli oggetti rimanenti (ovvero tutti i file non immagine).

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

Esempio 4: regole e policy ILM per oggetti con versione S3

Se disponi di un bucket S3 con il controllo delle versioni abilitato, puoi gestire le versioni degli oggetti non correnti includendo regole nella policy ILM che utilizzano "Tempo non corrente" come tempo di riferimento.

> Se si specifica un periodo di conservazione limitato per gli oggetti, tali oggetti verranno eliminati definitivamente una volta raggiunto il periodo di tempo specificato. Assicuratevi di aver capito per quanto tempo gli oggetti verranno conservati.

Come mostra questo esempio, è possibile controllare la quantità di spazio di archiviazione utilizzato dagli oggetti sottoposti a controllo di versione utilizzando diverse istruzioni di posizionamento per le versioni non correnti 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 verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

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

Informazioni correlate

"Come vengono eliminati gli oggetti"

Regola ILM 1 per esempio 4: Conservare 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 sottoposti a controllo di versione o meno.

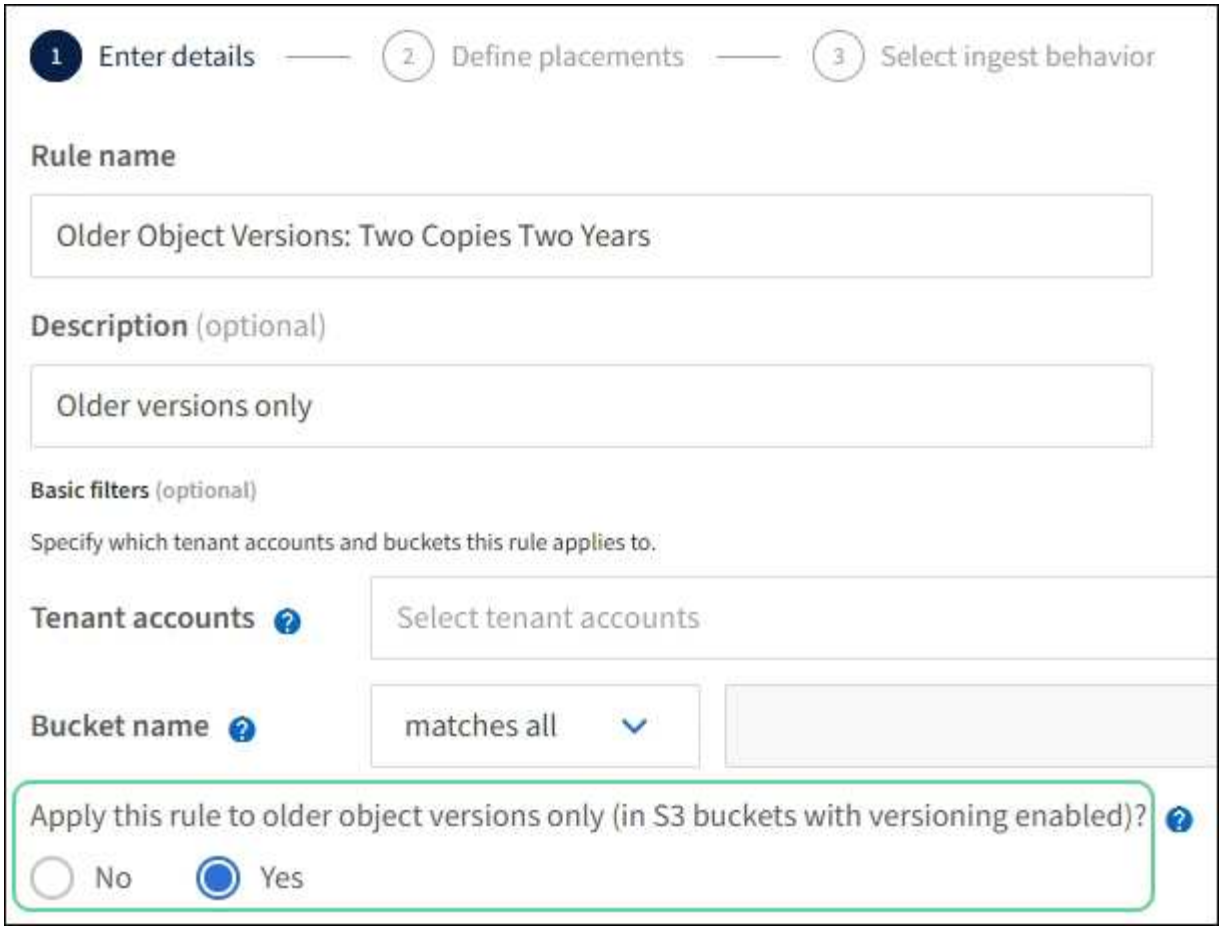
Definizione della regola	Valore di esempio
Pool di stoccaggio	Tre pool di archiviazione, ciascuno composto da data center diversi, denominati Sito 1, Sito 2 e Sito 3.
Nome della regola	Tre copie dieci anni
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conservare tre copie replicate per 10 anni (3.652 giorni), una nel sito 1, una nel sito 2 e una nel sito 3. Dopo 10 anni, eliminare tutte le copie dell'oggetto.

Regola ILM 2 per esempio 4: Salvare due copie delle versioni non correnti per 2 anni

Questa regola ILM di esempio memorizza due copie delle versioni non correnti di un oggetto con versione S3 per 2 anni.

Poiché la regola ILM 1 si applica a tutte le versioni dell'oggetto, è necessario creare un'altra regola per filtrare tutte le versioni non correnti.

Per creare una regola che utilizzi "Tempo non corrente" come orario di riferimento, seleziona **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (in bucket S3 con controllo delle versioni abilitato)?" nel passaggio 1 (Immetti dettagli) della procedura guidata Crea una regola ILM. Selezionando **Sì**, *Tempo non corrente* viene automaticamente selezionato come orario di riferimento e non è possibile selezionare un orario di riferimento diverso.



In questo esempio, vengono archiviate solo due copie delle versioni non correnti, che verranno conservate per due anni.

Definizione della regola	Valore di esempio
Pool di archiviazione	Due pool di archiviazione, ciascuno in data center diversi, Sito 1 e Sito 2.
Nome della regola	Versioni non correnti: due copie due anni
Tempo di riferimento	Tempo non corrente Selezionato automaticamente quando si seleziona **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (in bucket S3 con controllo delle versioni abilitato)?" nella procedura guidata Crea una regola ILM.
Posizionamenti	Il giorno 0 relativo al tempo non corrente (ovvero a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), conservare due copie replicate delle versioni dell'oggetto non corrente per 2 anni (730 giorni), una nel sito 1 e una nel sito 2. Dopo 2 anni, eliminare le versioni non correnti.

Criterio ILM per esempio 4: oggetti con versione S3

Se si desidera gestire le versioni precedenti di un oggetto in modo diverso rispetto alla versione corrente, le regole che utilizzano "Tempo non corrente" come orario di riferimento devono comparire nel criterio ILM prima delle regole che si applicano alla versione corrente dell'oggetto.

Una policy ILM per oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

- Conservare tutte le versioni precedenti (non aggiornate) di ciascun oggetto per 2 anni, a partire dal giorno in cui la versione è diventata non aggiornata.

> Le regole "Tempo non corrente" devono comparire nel criterio prima delle regole che si applicano alla versione corrente dell'oggetto. In caso contrario, le versioni degli oggetti non correnti non verranno mai abbinate dalla regola "Tempo non corrente".

- Al momento dell'ingestione, creare tre copie replicate e conservarne una copia in ciascuno dei tre siti. Conservare copie della versione corrente dell'oggetto per 10 anni.

Quando si simula la policy di esempio, ci si aspetterebbe che gli oggetti di prova vengano valutati come segue:

- Tutte le versioni non correnti degli oggetti verrebbero confrontate con la prima regola. Se una versione non corrente di un oggetto è più vecchia di 2 anni, ILM la elimina definitivamente (tutte le copie della versione non corrente vengono rimosse dalla griglia).
- La versione corrente dell'oggetto verrebbe abbinata alla seconda regola. Quando la versione corrente dell'oggetto è stata archiviata per 10 anni, il processo ILM aggiunge un marcatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente dell'oggetto "non corrente". La prossima volta che si verifica la valutazione ILM, questa versione non corrente viene abbinata alla prima regola. Di conseguenza, la copia nel Sito 3 viene eliminata e le due copie nel Sito 1 e nel Sito 2 vengono conservate per altri 2 anni.

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

È possibile utilizzare un filtro di posizione e il comportamento di acquisizione Rigoroso in una regola per impedire che gli oggetti vengano salvati in una posizione specifica del data center.

In questo esempio, un inquilino con sede a Parigi non vuole immagazzinare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, compresi tutti gli oggetti provenienti da altri account tenant, possono essere archiviati nel data center di Parigi o in quello degli Stati Uniti.

> 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 verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

- "Opzioni di acquisizione"
- "Crea regola ILM: seleziona il comportamento di acquisizione"

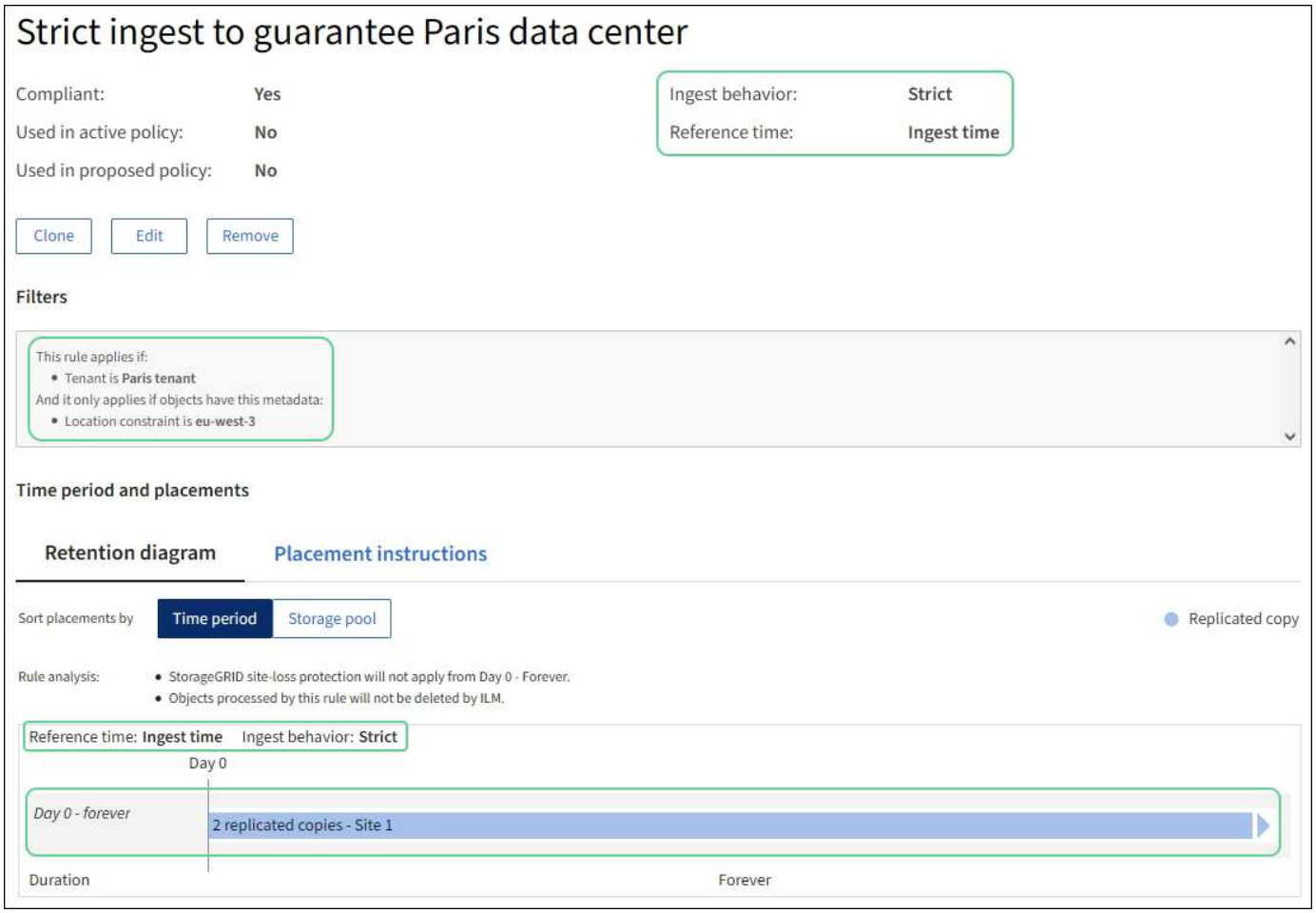
Regola ILM 1 per esempio 5: Ingestione rigorosa per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento di ingestione Strict per garantire che gli oggetti salvati da un tenant con sede a Parigi nei bucket S3 con la regione impostata su eu-west-3 (Parigi) non vengano mai

archiviati nel data center statunitense.

Questa regola si applica agli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-west-3 (Parigi).

Definizione della regola	Valore di esempio
Conto inquilino	inquilino di Parigi
Filtro avanzato	Il vincolo di posizione è uguale a eu-west-3
Pool di stoccaggio	Sito 1 (Parigi)
Nome della regola	Rigoroso inserimento per garantire il data center di Parigi
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre nel sito 1 (Parigi)
Comportamento di ingestione	Rigoroso. Utilizzare sempre i posizionamenti di questa regola durante l'acquisizione. L'acquisizione fallisce se non è possibile archiviare due copie dell'oggetto nel data center di Parigi.



Regola ILM 2 per esempio 5: Ingestione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciato per garantire un'efficienza ILM ottimale per tutti gli oggetti non corrispondenti alla prima regola. Verranno conservate due copie di tutti gli oggetti che soddisfano questa regola: una nel centro dati degli Stati Uniti e una nel centro dati di Parigi. Se la regola non può essere soddisfatta immediatamente, vengono conservate copie provvisorie in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi regione.

Definizione della regola	Valore di esempio
Conto inquilino	Ignorare
Filtro avanzato	*Non specificato*
Pool di stoccaggio	Sito 1 (Parigi) e Sito 2 (Stati Uniti)
Nome della regola	2 copie 2 data center
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre in due data center
Comportamento di ingestione	Equilibrato. Se possibile, gli oggetti che corrispondono a questa regola vengono posizionati secondo le istruzioni di posizionamento della regola. In caso contrario, vengono effettuate copie provvisorie in qualsiasi luogo disponibile.

Politica ILM per l'esempio 5: combinazione di comportamenti di acquisizione

L'esempio di policy ILM include due regole con comportamenti di acquisizione diversi.

Una policy ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Archiviare gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-west-3 (Parigi) solo nel data center di Parigi. L'acquisizione non riesce se il data center di Parigi non è disponibile.
- Archiviare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) sia nel data center statunitense che in quello di Parigi. Se non è possibile soddisfare le istruzioni di posizionamento, effettuare copie provvisorie in qualsiasi luogo disponibile.

Quando si simula la policy di esempio, ci si aspetta che gli oggetti di prova vengano valutati come segue:

- Tutti gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-west-3 vengono abbinati alla prima regola e vengono archiviati nel data center di Parigi. Poiché la prima regola utilizza l'acquisizione rigorosa, questi oggetti non vengono mai archiviati nel data center statunitense. Se i nodi di archiviazione nel data center di Parigi non sono disponibili, l'acquisizione fallisce.
- Tutti gli altri oggetti vengono abbinati dalla seconda regola, compresi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-west-3. In ogni data center viene

salvata una copia di ogni oggetto. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie provvisorie in qualsiasi posizione disponibile.

Esempio 6: Modificare una policy ILM

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

Prima di modificare una policy, è necessario comprendere in che modo le modifiche ai posizionamenti 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 politica attiva, prima"creare una politica" . Dopodiché, devi"simulare" poi"attivare" la nuova politica.

> 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 verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Come la modifica di una policy ILM influisce sulle prestazioni

Quando si attiva una nuova policy ILM, le prestazioni del sistema StorageGRID potrebbero essere temporaneamente compromesse, soprattutto se le istruzioni di posizionamento nella nuova policy richiedono lo spostamento di molti oggetti esistenti in nuove posizioni.

Quando si attiva una nuova policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, rivedere tutte le modifiche apportate al posizionamento degli oggetti replicati e con codice di cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Per garantire che una nuova policy ILM non influisca sul posizionamento degli oggetti replicati e codificati per la cancellazione esistenti, è possibile"creare una regola ILM con un filtro temporale di acquisizione" . Ad esempio, **L'ora di ingestione *è uguale o successiva <data e ora>***, in modo che la nuova regola si applichi solo agli oggetti ingeriti nella data e ora specificate o successivamente.

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

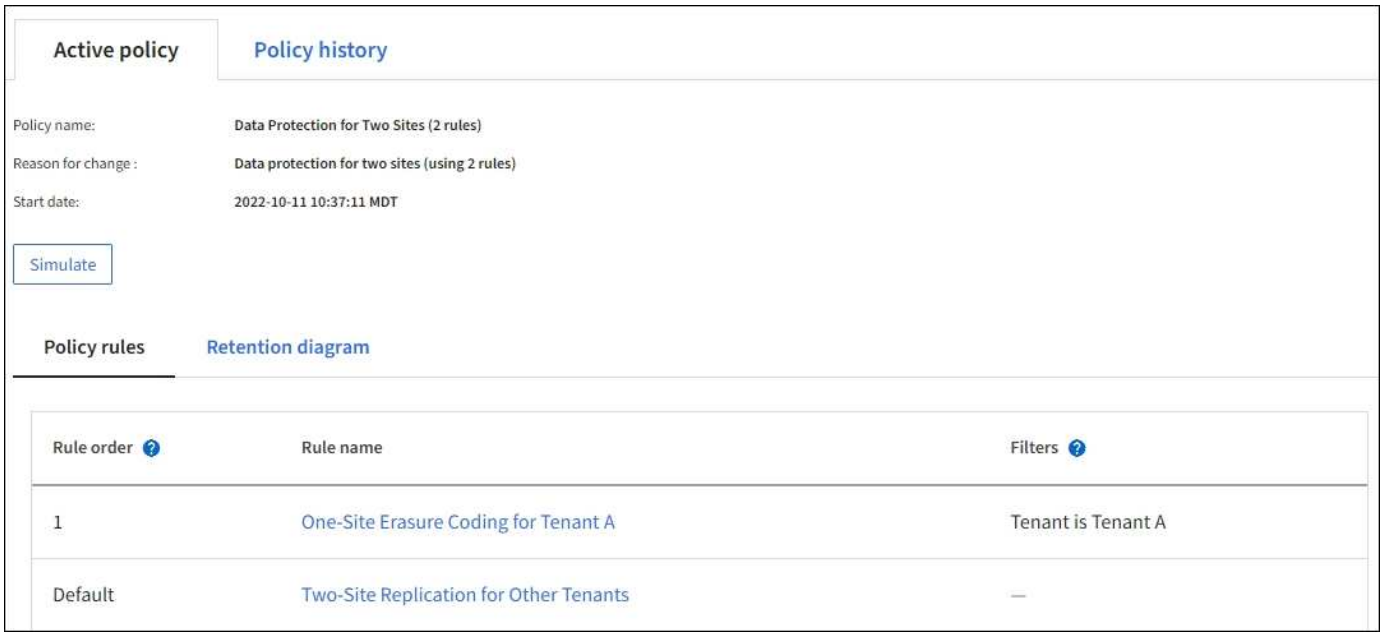
- Applicazione di un profilo di codifica di cancellazione diverso agli oggetti con codifica di cancellazione esistenti.

  > StorageGRID considera ogni profilo di codifica di cancellazione come univoco e non riutilizza i frammenti di codifica di cancellazione quando viene utilizzato un nuovo profilo.

- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, convertendo una grande percentuale di oggetti replicati in oggetti con codice di cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un gran numero di oggetti da o verso un pool di archiviazione cloud o da o verso un sito remoto.

Criterio ILM attivo 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 tramite replica a 2 copie.

Regola 1: Codifica di cancellazione in un unico sito per l'inquilino A

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione in un unico sito per l'inquilino A
Conto inquilino	Inquilino A
Pool di archiviazione	Sito 1
Posizionamenti	Codifica di cancellazione 2+1 nel sito 1 dal giorno 0 all'infinito

Regola 2: Replicazione a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a due siti per altri tenant
Conto inquilino	Ignorare
Pool di archiviazione	Sito 1 e Sito 2

Definizione della regola	Valore di esempio
Posizionamenti	Due copie replicate dal giorno 0 all'infinito: una copia nel Sito 1 e una copia nel Sito 2.

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

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

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore della griglia ha creato due nuovi pool di archiviazione: un pool di archiviazione per il sito 3 e un pool di archiviazione contenente tutti e tre i siti (diverso dal pool di archiviazione predefinito Tutti i nodi di archiviazione). Quindi, l'amministratore ha creato due nuove regole ILM e una nuova policy ILM, studiate per proteggere i dati in tutti e tre i siti.

Quando questa nuova policy ILM verrà attivata, gli oggetti appartenenti al Tenant A saranno protetti tramite codifica di cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e oggetti più piccoli appartenenti al Tenant A) saranno protetti in tre siti tramite replica a 3 copie.

Regola 1: Codifica di cancellazione a tre siti per l'inquilino A

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione a tre siti per l'inquilino A
Conto inquilino	Inquilino A
Pool di archiviazione	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 all'infinito

Regola 2: Replicazione a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a tre siti per altri tenant
Conto inquilino	Ignorare
Pool di archiviazione	Sito 1, Sito 2 e Sito 3
Posizionamenti	Tre copie replicate dal giorno 0 all'infinito: una copia nel Sito 1, una copia nel Sito 2 e una copia nel Sito 3.

Attivazione della politica ILM ad esempio 6

Quando si attiva 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 in eventuali regole nuove o aggiornate.

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

Quando si attiva una nuova policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, rivedere tutte le modifiche apportate al posizionamento degli oggetti replicati e con codice di cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

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 mediante la codifica di cancellazione 2+1 nel Sito 1. Nella nuova politica ILM, gli oggetti appartenenti al Tenant A saranno protetti mediante la codifica di cancellazione 2+1 nei 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. Quindi, ciascuno dei tre frammenti viene conservato 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 codifica di cancellazione, vengono creati e distribuiti ai tre siti frammenti completamente nuovi con codifica di cancellazione.

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

Cosa succede quando cambiano le istruzioni di replicazione

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti ad altri tenant vengono protetti mediante due copie replicate nei pool di archiviazione nei siti 1 e 2. Nella nuova policy ILM, gli oggetti appartenenti ad altri tenant saranno protetti mediante tre copie replicate in pool di archiviazione nei siti 1, 2 e 3.

Quando viene attivata la nuova policy ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID ne crea tre copie e ne salva una in ogni sito.
- Gli oggetti esistenti appartenenti a questi altri inquilini vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie degli oggetti esistenti nel Sito 1 e nel Sito 2 continuano a soddisfare i requisiti di replicazione della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il Sito 3.

Impatto sulle prestazioni dell'attivazione di questa policy

Quando viene attivata la policy ILM in questo esempio, le prestazioni complessive del sistema StorageGRID saranno temporaneamente compromesse. Saranno necessari livelli di risorse di rete superiori al normale per creare nuovi frammenti con codice 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 al normale. Le latenze torneranno ai livelli normali dopo che le

istruzioni di posizionamento saranno state completamente implementate nella griglia.

Per evitare problemi di risorse durante l'attivazione di un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Tempo di acquisizione in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore, per garantire che gli oggetti esistenti non vengano spostati inutilmente.

Contattare l'assistenza tecnica se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

Esempio 7: Politica ILM conforme per S3 Object Lock

È possibile utilizzare il bucket S3, le regole ILM e la policy ILM in questo esempio come punto di partenza quando si definisce una policy ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con S3 Object Lock abilitato.

Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti StorageGRID , puoi utilizzare questo esempio anche per gestire eventuali bucket esistenti in cui è abilitata la funzionalità di conformità legacy.

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 verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

- "Gestisci gli oggetti con S3 Object Lock"
- "Creare una policy ILM"

Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato Tenant Manager per creare un bucket con S3 Object Lock abilitato per archiviare i record bancari critici.

Definizione di bucket	Valore di esempio
Nome dell'account dell'inquilino	Banca ABC
Nome del bucket	registri bancari
Regione del bucket	us-east-1 (predefinito)

Ogni oggetto e versione dell'oggetto che viene aggiunto al bucket dei record bancari utilizzerà i seguenti valori per `retain-until-date` E `legal hold` impostazioni.

Impostazione per ogni oggetto	Valore di esempio
`retain-until-date`	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione dell'oggetto ha la sua `retain-until-date` collocamento. Questa impostazione può essere aumentata, ma non diminuita.
`legal hold`	"OFF" (Non in vigore) È possibile applicare o rimuovere un blocco legale su qualsiasi versione dell'oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è sottoposto a una sospensione legale, l'oggetto non può essere eliminato anche se `retain-until-date` è stato raggiunto.

Regola ILM 1 per esempio di blocco oggetto S3: profilo di codifica di cancellazione con corrispondenza bucket

Questa regola ILM di esempio si applica solo al conto tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto nel `bank-records` bucket e quindi utilizza la codifica di cancellazione per archiviare l'oggetto sui nodi di archiviazione 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 nodi di archiviazione dal giorno 0 all'infinito, utilizzando l'ora di ingestione come ora di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola conforme: Oggetti EC nel bucket dei registri bancari - Bank of ABC
Conto inquilino	Banca ABC
Nome del 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	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 conservalo per sempre
Profilo di codifica di cancellazione	• Creare una copia con codice di cancellazione sui nodi di archiviazione in tre siti di data center • Utilizza lo schema di codifica di cancellazione 6+3

Esempio di regola ILM 2 per blocco oggetto S3: regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie replicate dell'oggetto sui nodi di archiviazione. Dopo un anno, ne memorizza una copia per sempre su un Cloud Storage Pool. 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	Valore di esempio
Nome della regola	Regola non conforme: utilizzare Cloud Storage Pool
Conti degli inquilini	Non specificato
Nome del bucket	Non specificato, ma si applicherà solo ai bucket in cui non è abilitato S3 Object Lock (o la funzionalità legacy Compliance).
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Posizionamenti	• Il giorno 0, conserva due copie replicate sui nodi di archiviazione 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 esempio di blocco oggetto S3: regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti nei pool di archiviazione in due data center. Questa regola conforme è concepita per essere la regola predefinita nella policy ILM. Non include alcun filtro, non utilizza il tempo di riferimento non corrente e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: due copie dell'oggetto vengono conservate sui nodi di archiviazione dal giorno 0 all'infinito, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola di conformità predefinita: due copie, due data center
Conto inquilino	Non specificato
Nome del bucket	Non specificato
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione

Definizione della regola	Valore di esempio
Posizionamenti	Dal giorno 0 all'infinito, conserva due copie replicate: una sui nodi di archiviazione nel Data Center 1 e una sui nodi di archiviazione 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 sistema, compresi quelli nei bucket con S3 Object Lock abilitato, è necessario selezionare le regole ILM che soddisfano i requisiti di archiviazione per tutti gli oggetti. Quindi, è necessario simulare e attivare la policy.

Aggiungere 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 gli oggetti di dimensioni superiori a 1 MB in un bucket specifico con S3 Object Lock abilitato. Gli oggetti vengono archiviati sui nodi di archiviazione dal giorno 0 all'infinito.
2. Una regola non conforme che crea due copie replicate dell'oggetto sui nodi di archiviazione per un anno e poi sposta una copia dell'oggetto in un pool di archiviazione cloud per sempre. Questa regola non si applica ai bucket con S3 Object Lock abilitato perché utilizza un Cloud Storage Pool.
3. La regola di conformità predefinita che crea due copie replicate degli oggetti sui nodi di archiviazione dal giorno 0 all'infinito.

Simulare la politica

Dopo aver aggiunto regole alla policy, scelto una regola conforme predefinita e organizzato le altre regole, dovresti simulare la policy testando gli oggetti dal bucket con S3 Object Lock abilitato e da altri bucket. Ad esempio, quando si simula la policy di esempio, ci si aspetterebbe che gli oggetti di prova vengano valutati come segue:

- La prima regola corrisponderà solo agli oggetti di prova che sono maggiori di 1 MB 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 account tenant.
- La regola predefinita corrisponderà 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 in cui è abilitato il blocco oggetti S3 per tutti gli altri account tenant.

Attiva la politica

Quando sei completamente soddisfatto che la nuova policy protegga i dati degli oggetti come previsto, puoi attivarla.

Esempio 8: Priorità per il ciclo di vita del bucket S3 e policy ILM

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

Esempio di ciclo di vita del bucket che ha la priorità sulla policy ILM

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il 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 del prefisso "docs/".
  - Dopo 100 giorni viene creato un marcatore di eliminazione e "docs/text" diventa non corrente.
  - Dopo 5 giorni, per un totale di 105 giorni dall'acquisizione, "docs/text" viene eliminato.
  - Dopo 95 giorni, per un totale di 200 giorni dall'inserimento e 100 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.
- Viene acquisito un oggetto denominato "video/film". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
  - Dopo 50 giorni viene creato un marcatore di eliminazione e "video/film" diventa non corrente.
  - Dopo 20 giorni, ovvero 70 giorni in totale dall'acquisizione, "video/film" viene eliminato.
  - Dopo 30 giorni, per un totale di 100 giorni dall'inserimento e 50 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.

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

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il 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 del prefisso "docs/".

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

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

- Viene acquisito un oggetto denominato "video/film". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
  - Dopo 50 giorni viene creato un marcatore di eliminazione e "video/film" diventa non corrente.

- Dopo 20 giorni, ovvero 70 giorni in totale dall'acquisizione, "video/film" viene eliminato.
- Dopo 30 giorni, per un totale di 100 giorni dall'inserimento 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

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il 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 e ripulire le versioni non correnti dopo 20 giorni. Di conseguenza, la regola ingest-time manterrà per sempre i marcatori di eliminazione scaduti.
  - Il ciclo di vita del bucket duplica il comportamento della policy ILM durante l'aggiunta `"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 sostituisce le impostazioni di conservazione ILM.
  - Quando un tenant invia una richiesta di eliminazione di un oggetto, viene creato un marcatore di eliminazione e l'oggetto diventa non corrente.
  - Dopo 20 giorni, l'oggetto non corrente viene eliminato e il marcatore di eliminazione scade.
  - Poco dopo, il marcatore di eliminazione scaduto viene eliminato.

Informazioni sul copyright

Informazioni sul marchio commerciale