# Esempio di regole e policy ILM

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-115/ilm/example-1-ilm-rules-and-policy-for-object-storage.html on October 03, 2025. Always check docs.netapp.com for the latest.

# Sommario


Esempio di regole e policy ILM . . . 1
Esempio 1: Regole ILM e policy per lo storage a oggetti . . . 1
ILM regola 1 per esempio 1: Copia dei dati degli oggetti in due data center . . . 1
ILM regola 2 per esempio 1: Erasure coding profile with bucket matching . . . 2
Policy ILM per esempio 1 . . . 3
Esempio 2: Regole ILM e policy per il filtraggio delle dimensioni degli oggetti EC . . . 4
ILM regola 1 per esempio 2: Utilizzare EC per tutti gli oggetti di dimensioni superiori a 200 KB . . . 4
ILM regola 2 per esempio 2: Due copie replicate . . . 5
Criterio ILM per esempio 2: Utilizzare EC per oggetti di dimensioni superiori a 200 KB . . . 6
Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine . . . 7
ILM regola 1 per esempio 3: Utilizzare EC per file di immagine di dimensioni superiori a 200 KB . . . 7
ILM regola 2 per esempio 3: Replica 3 copie per tutti i file immagine rimanenti . . . 9
Policy ILM per esempio 3: Migliore protezione per i file di immagine . . . 10
Esempio 4: Regole ILM e policy per gli oggetti con versione S3 . . . 10
ILM regola 1 per esempio 4: Salva tre copie per 10 anni . . . 11
ILM regola 2 per esempio 4: Salva due copie di versioni non correnti per 2 anni . . . 12
Policy ILM per esempio 4: Oggetti con versione S3 . . . 13
Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione . . . 14
ILM regola 1 per esempio 5: Ingest rigoroso per garantire il data center di Parigi . . . 15
ILM regola 2 per esempio 5: Acquisizione bilanciata per altri oggetti . . . 16
Policy ILM per esempio 5: Combinazione di comportamenti di acquisizione . . . 17
Esempio 6: Modifica di un criterio ILM . . . 18
In che modo la modifica di un criterio ILM influisce sulle performance . . . 19
Policy ILM attiva ad esempio 6: Protezione dei dati in due siti . . . 19
Policy ILM proposta per esempio 6: Protezione dei dati in tre siti . . . 20
Attivazione della policy ILM proposta, ad esempio 6 . . . 22
Esempio 7: Policy ILM conforme per il blocco oggetti S3 . . . 23
Esempio di bucket e oggetti per S3 Object Lock . . . 23
ILM regola 1 per S3 Object Lock esempio: Erasure coding profile with bucket matching . . . 24
ILM regola 2 per S3 Object Lock esempio: Regola non conforme . . . 26
ILM regola 3 per S3 Object Lock esempio: Regola predefinita . . . 27
Esempio di policy ILM conforme per S3 Object Lock . . . 28

# Esempio di regole e policy ILM

Puoi utilizzare gli esempi di questa sezione come punto di partenza per le tue regole e policy ILM.

- "Esempio 1: Regole ILM e policy per lo storage a oggetti"
- "Esempio 2: Regole ILM e policy per il filtraggio delle dimensioni degli oggetti EC"
- "Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine"
- "Esempio 4: Regole ILM e policy per gli oggetti con versione S3"
- "Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"
- "Esempio 6: Modifica di un criterio ILM"
- "Esempio 7: Policy ILM conforme per il blocco oggetti S3"

# Esempio 1: Regole ILM e policy per lo storage a oggetti

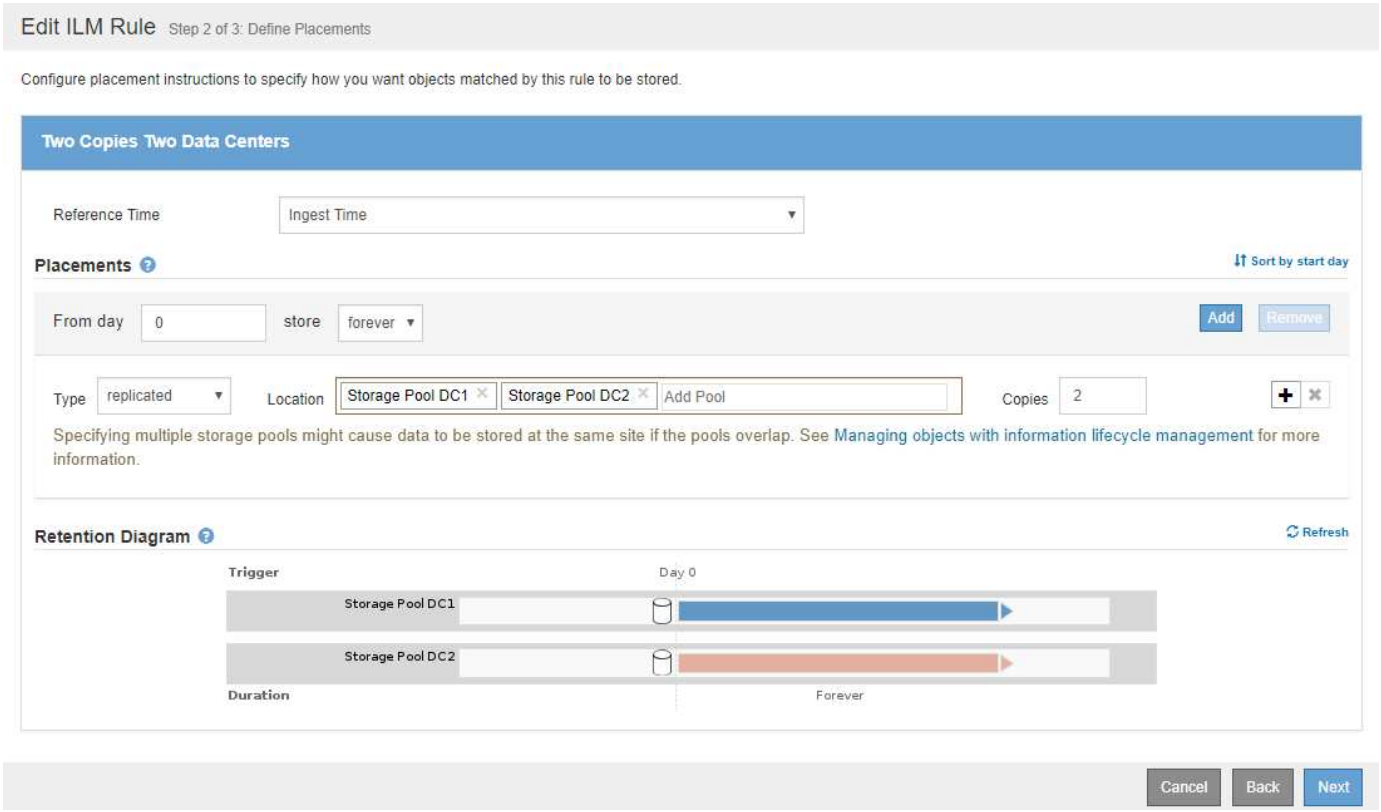
È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per la definizione di un criterio ILM in modo da soddisfare i requisiti di protezione e conservazione degli oggetti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

## ILM regola 1 per esempio 1: Copia dei dati degli oggetti in due data center

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

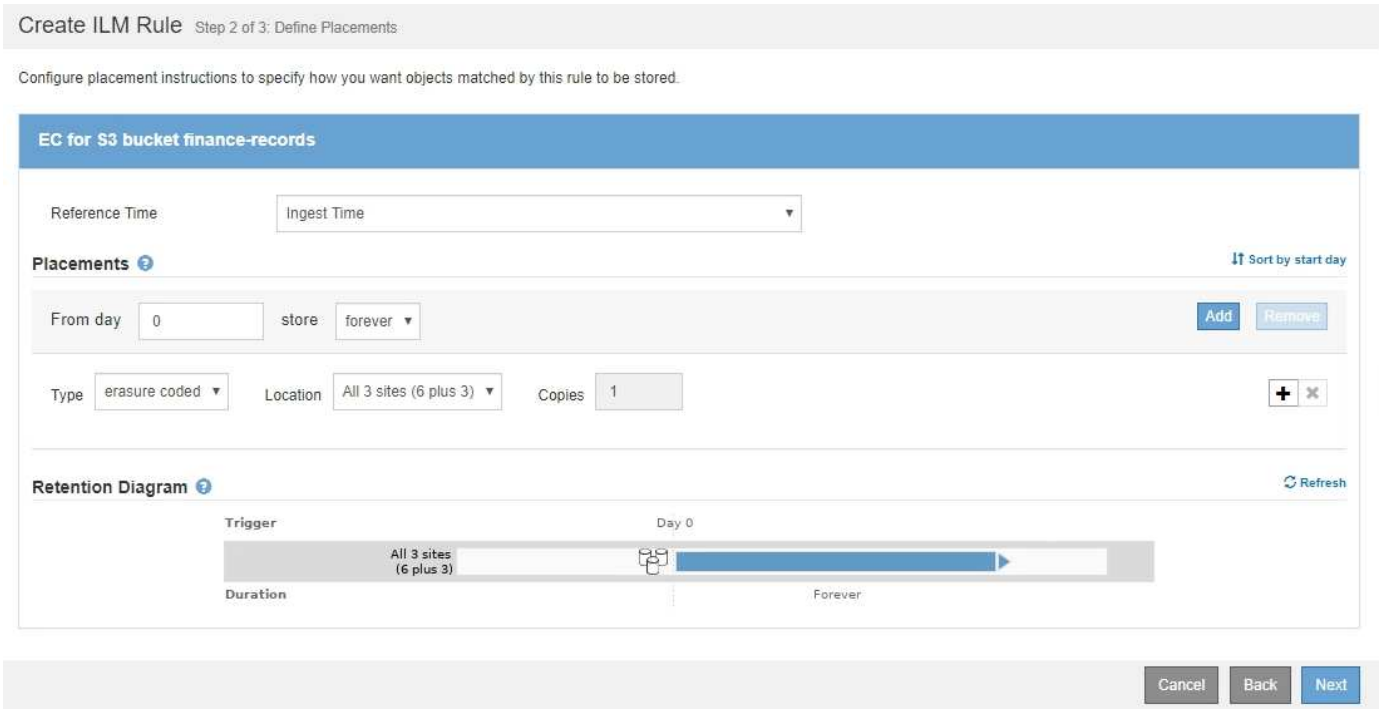
| Definizione della regola | Valore di esempio |
|---|---|
| Pool di storage | Due pool di storage, ciascuno in diversi data center, denominati Storage Pool DC1 e Storage Pool DC2. |
| Nome regola | Due copie di due data center |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamento dei contenuti | Il giorno 0, conserva due copie replicate per sempre, una nello Storage Pool DC1 e una nello Storage Pool DC2. |




## ILM regola 2 per esempio 1: Erasure coding profile with bucket matching

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

| Definizione della regola | Valore di esempio |
| --- | --- |
| Erasure Coding Profile (erasure Coding Profile | • Un pool di storage in tre data center (tutti e 3 i siti)<br>• Utilizzare uno schema di erasure coding 6+3 |
| Nome regola | EC per i record finanziari del bucket S3 |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamento dei contenuti | Per gli oggetti nel bucket S3 denominati finance-records, creare una copia con codice di cancellazione nel pool specificato dal profilo di codifica Erasure. Conserva questa copia per sempre. |

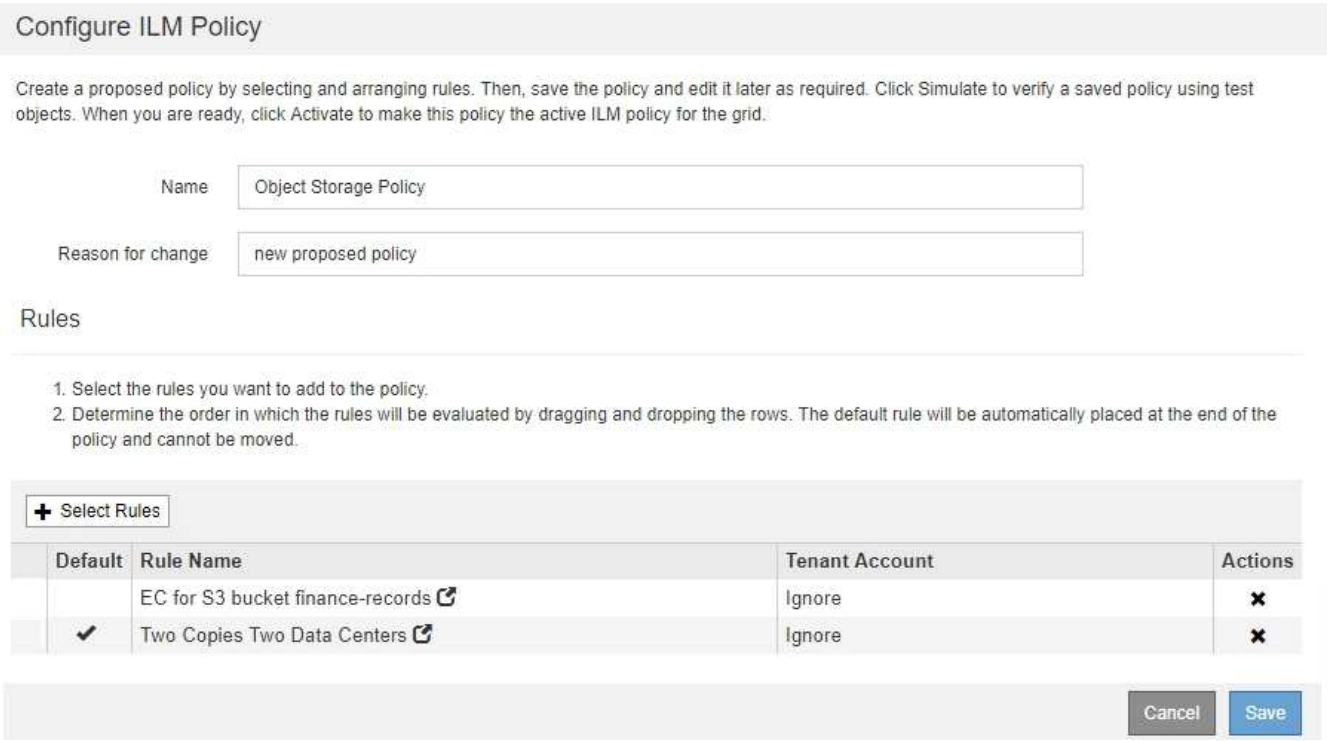



## Policy ILM per esempio 1

Il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse; tuttavia, in pratica, la maggior parte delle policy ILM è semplice.

Un tipico criterio ILM per una topologia multi-sito potrebbe includere regole ILM come le seguenti:

- Al momento dell'acquisizione, utilizzare la codifica di cancellazione 6+3 per memorizzare tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in tre data center.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita del criterio, due copie due data center, per memorizzare una copia di tale oggetto in due data center, DC1 e DC2.




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

È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire un criterio ILM che filtra in base alle dimensioni dell'oggetto per soddisfare i requisiti EC consigliati.

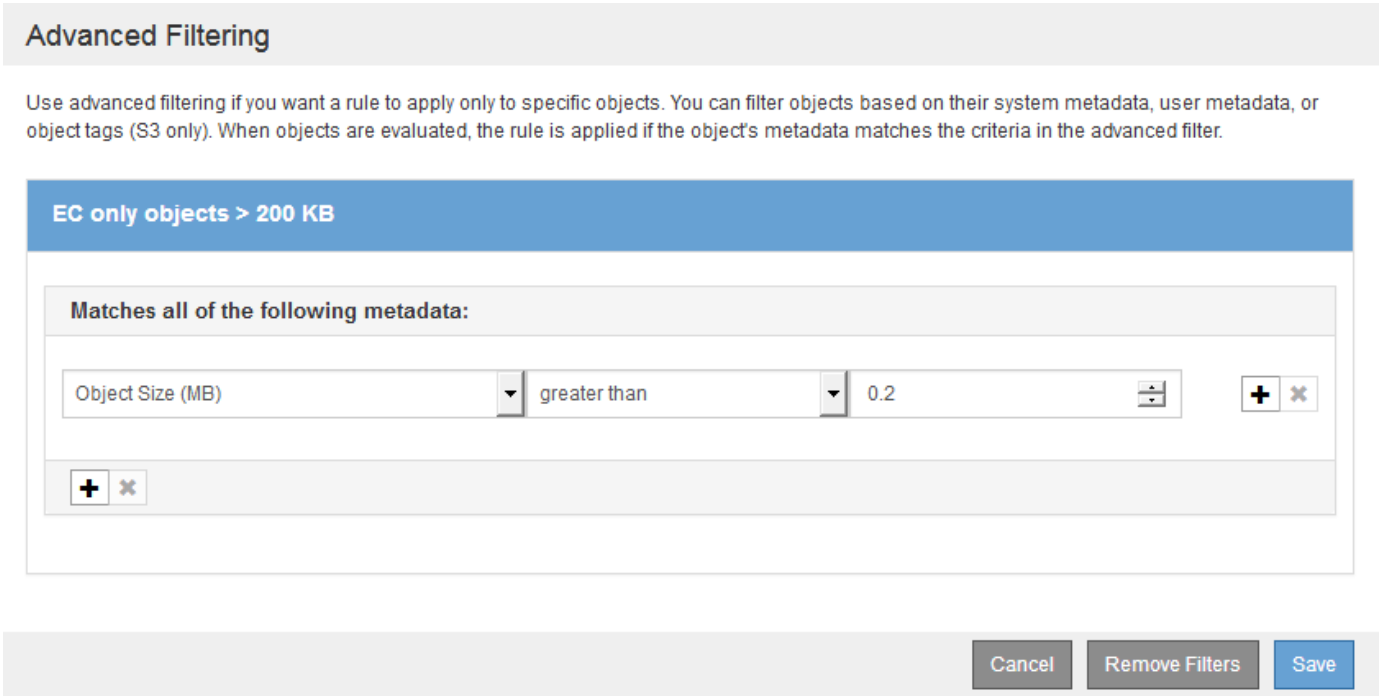
> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

## ILM regola 1 per esempio 2: Utilizzare EC per tutti gli oggetti di dimensioni superiori a 200 KB

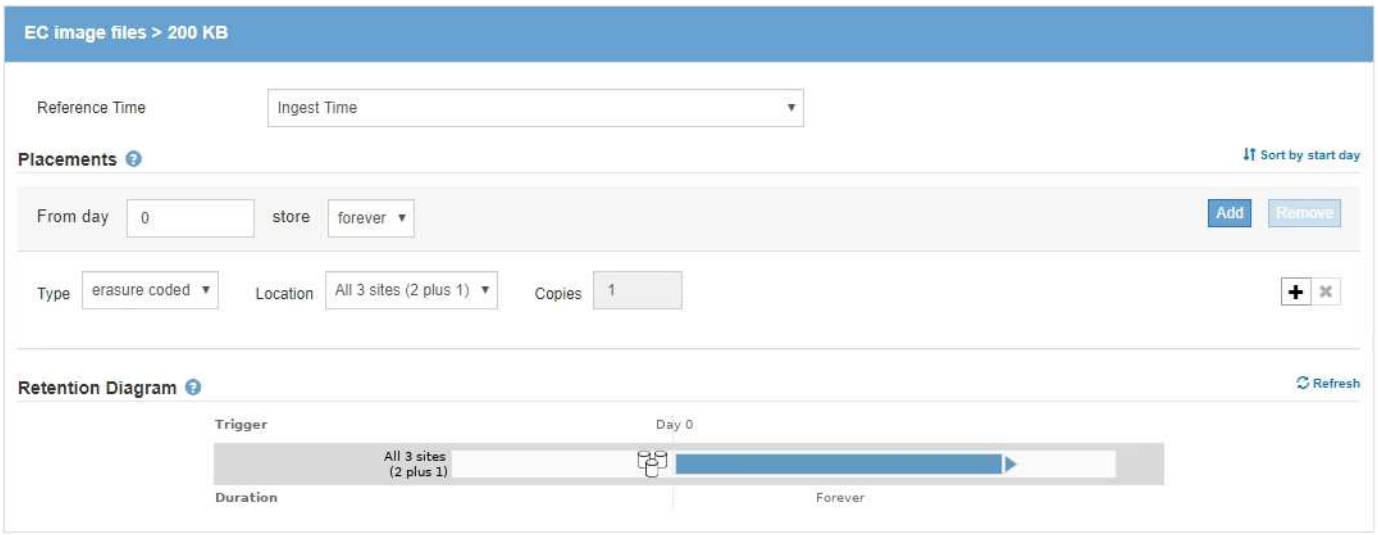
Questo esempio di cancellazione della regola ILM codifica tutti gli oggetti di dimensioni superiori a 200 KB (0.20 MB).

| Definizione della regola | Valore di esempio |
|---|---|
| Nome regola | Solo oggetti EC > 200 KB |
| Tempo di riferimento | Tempo di acquisizione |
| Filtro avanzato per le dimensioni dell'oggetto | Dimensione oggetto (MB) maggiore di 0.20 |

| Definizione della regola | Valore di esempio |
| --- | --- |
| Posizionamento dei contenuti | Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti |



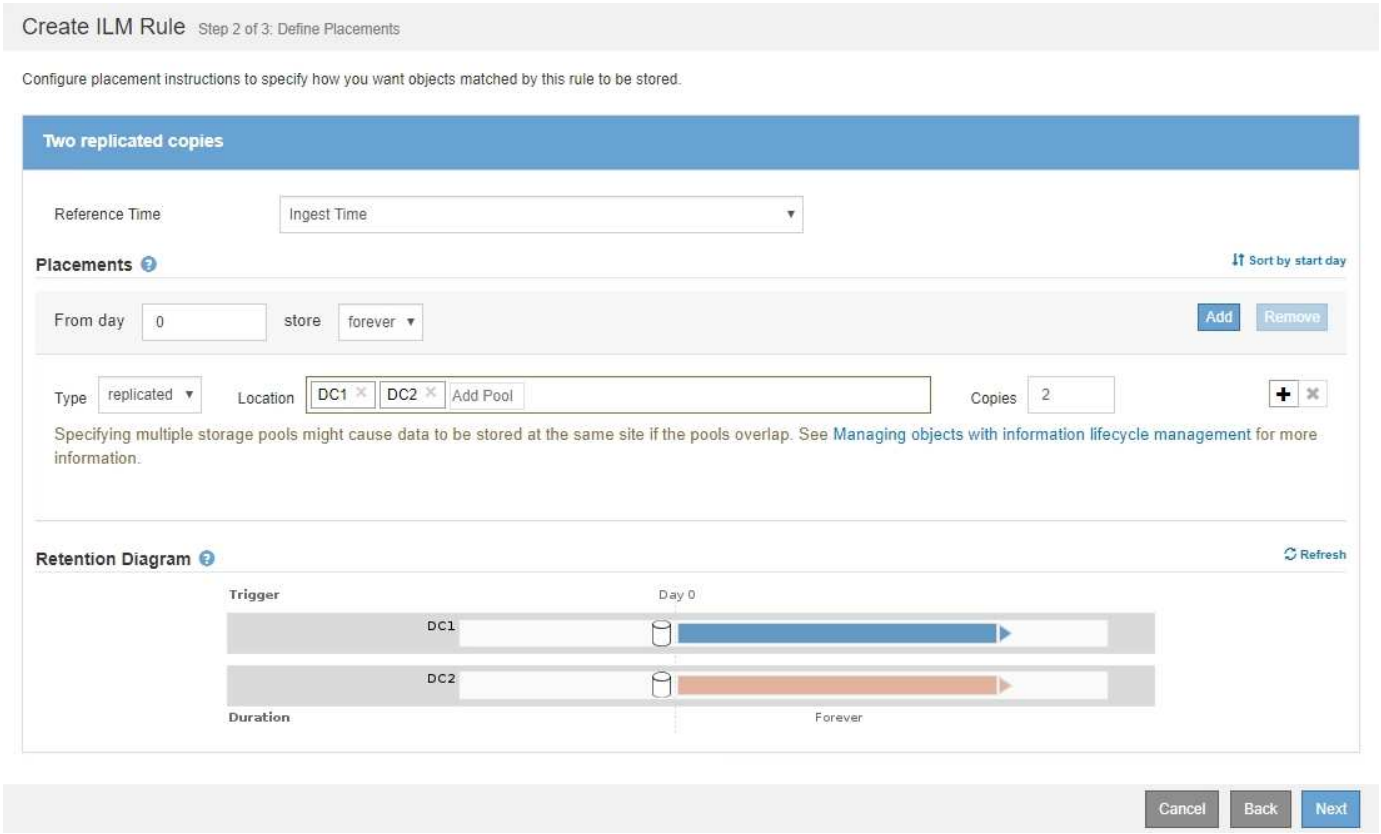

Le istruzioni di posizionamento specificano che una copia 2+1 con codice di cancellazione deve essere creata utilizzando tutti e tre i siti.




## ILM regola 2 per esempio 2: Due copie replicate

Questa regola ILM di esempio crea due copie replicate e non filtra in base alle dimensioni dell'oggetto. Questa è la seconda regola del criterio. Poiché la regola ILM 1, ad esempio 2, filtra tutti gli oggetti di dimensioni superiori a 200 KB, la regola ILM 2, ad esempio 2, si applica solo agli oggetti di dimensioni inferiori o pari a 200 KB.

| Definizione della regola | Valore di esempio |
| --- | --- |
| Nome regola | Due copie replicate |
| Tempo di riferimento | Tempo di acquisizione |
| Filtro avanzato per le dimensioni dell'oggetto | Nessuno |
| Posizionamento dei contenuti | Creare due copie replicate e salvarle in due data center, DC1 e DC2 |

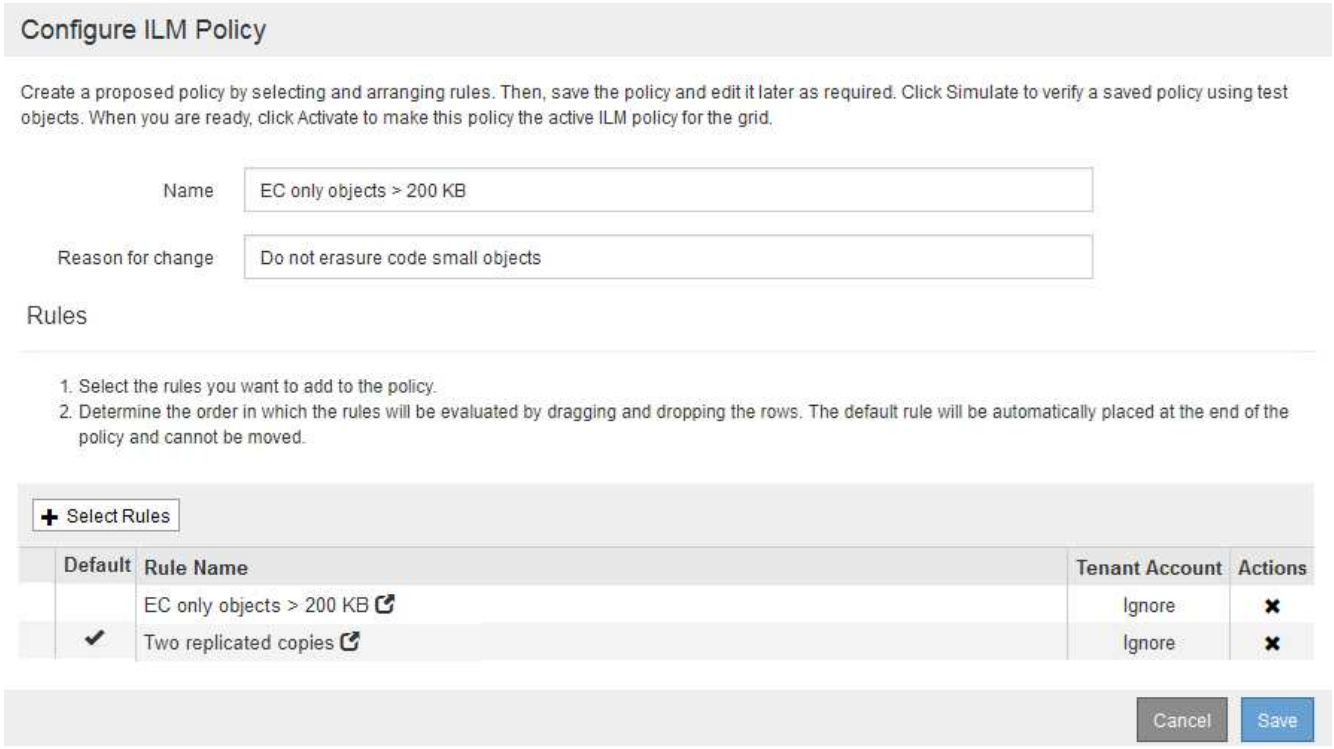



## Criterio ILM per esempio 2: Utilizzare EC per oggetti di dimensioni superiori a 200 KB

In questo esempio di policy, gli oggetti di dimensioni superiori a 200 KB vengono sottoposti a erasure coding. Vengono create due copie replicate di tutti gli altri oggetti.

Questo esempio di policy ILM include le seguenti regole ILM:

- Erasure coding di tutti gli oggetti di dimensioni superiori a 200 KB.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita per creare due copie replicate di tale oggetto. Poiché gli oggetti di dimensioni superiori a 200 KB sono stati filtrati dalla regola 1, la regola 2 si applica solo agli oggetti di dimensioni inferiori o pari a 200 KB.




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

È possibile utilizzare le seguenti regole e policy di esempio per garantire che le immagini di dimensioni superiori a 200 KB vengano erasure coded e che vengano eseguite tre copie di immagini più piccole.

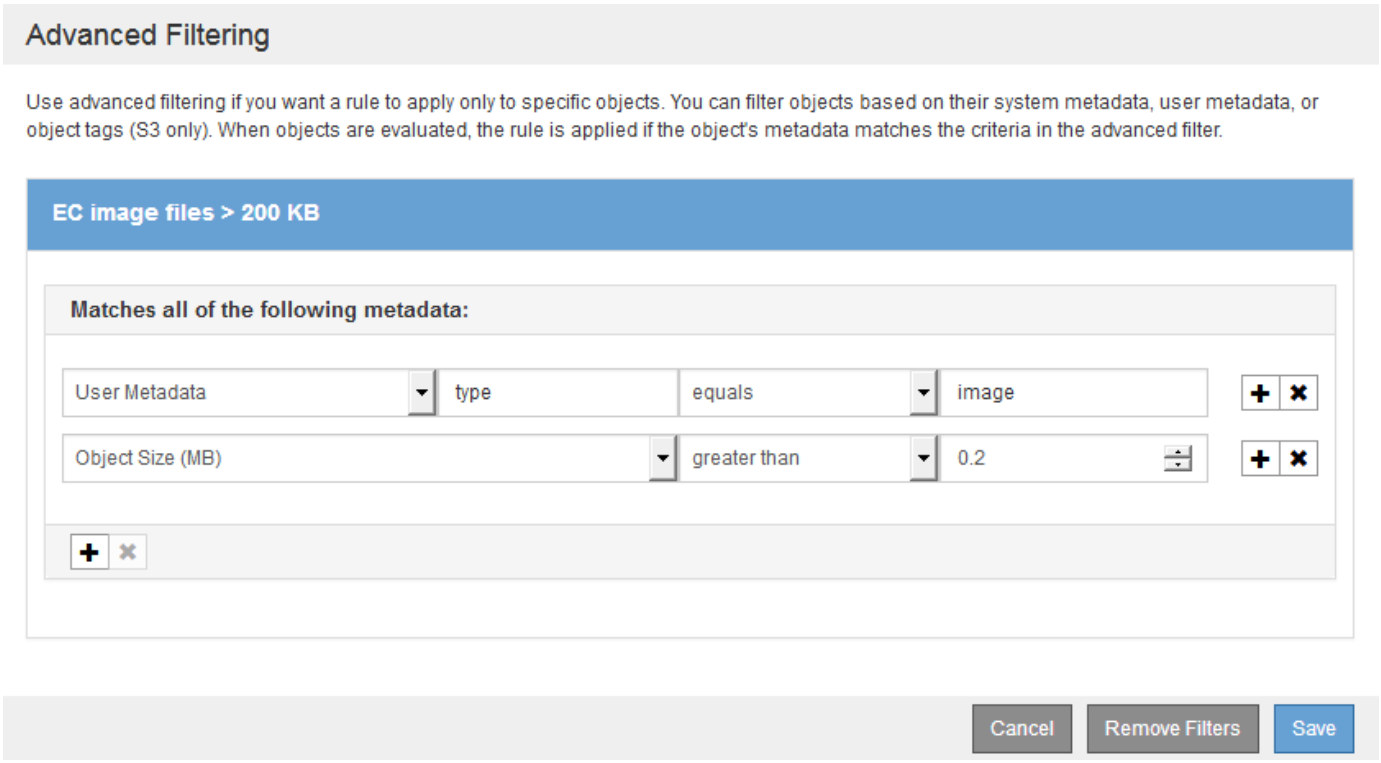
> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

## ILM regola 1 per esempio 3: Utilizzare EC per file di immagine di dimensioni superiori a 200 KB

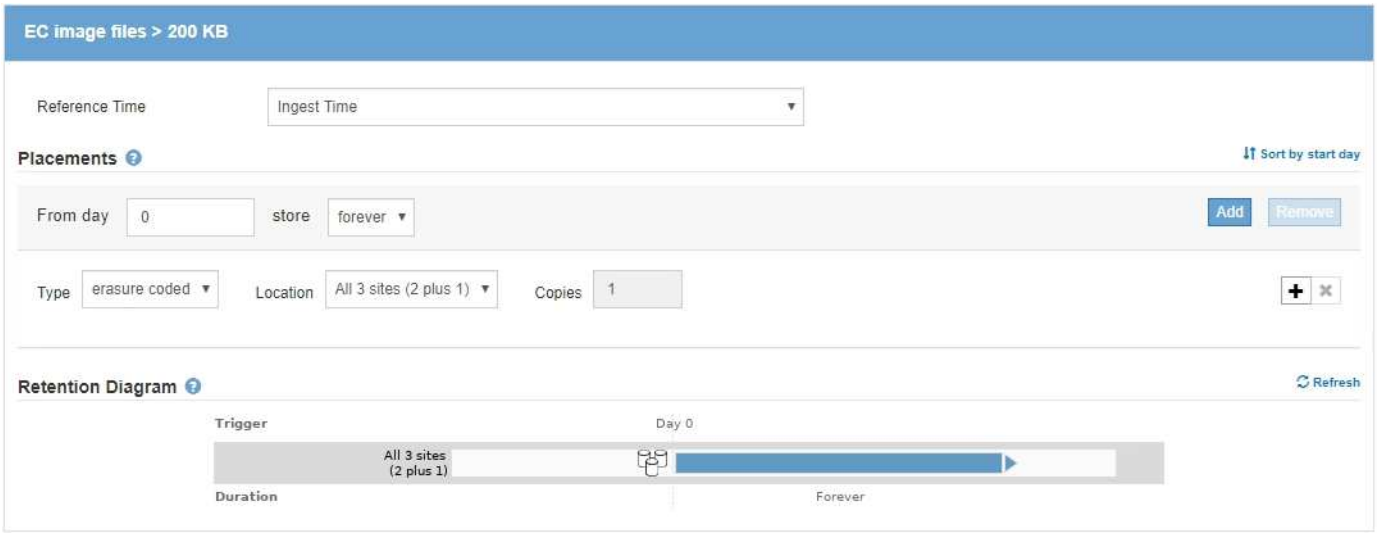
Questa regola ILM di esempio utilizza un filtro avanzato per eseguire la cancellazione di tutti i file di immagine di dimensioni superiori a 200 KB.

| Definizione della regola | Valore di esempio |
|---|---|
| Nome regola | File immagine EC > 200 KB |
| Tempo di riferimento | Tempo di acquisizione |
| Filtro avanzato per i metadati utente | Il tipo di metadati utente equivale ai file di immagine |

| Definizione della regola | Valore di esempio |
| --- | --- |
| Filtro avanzato per le dimensioni dell'oggetto | Dimensione oggetto (MB) maggiore di 0.2 |
| Posizionamento dei contenuti | Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti |



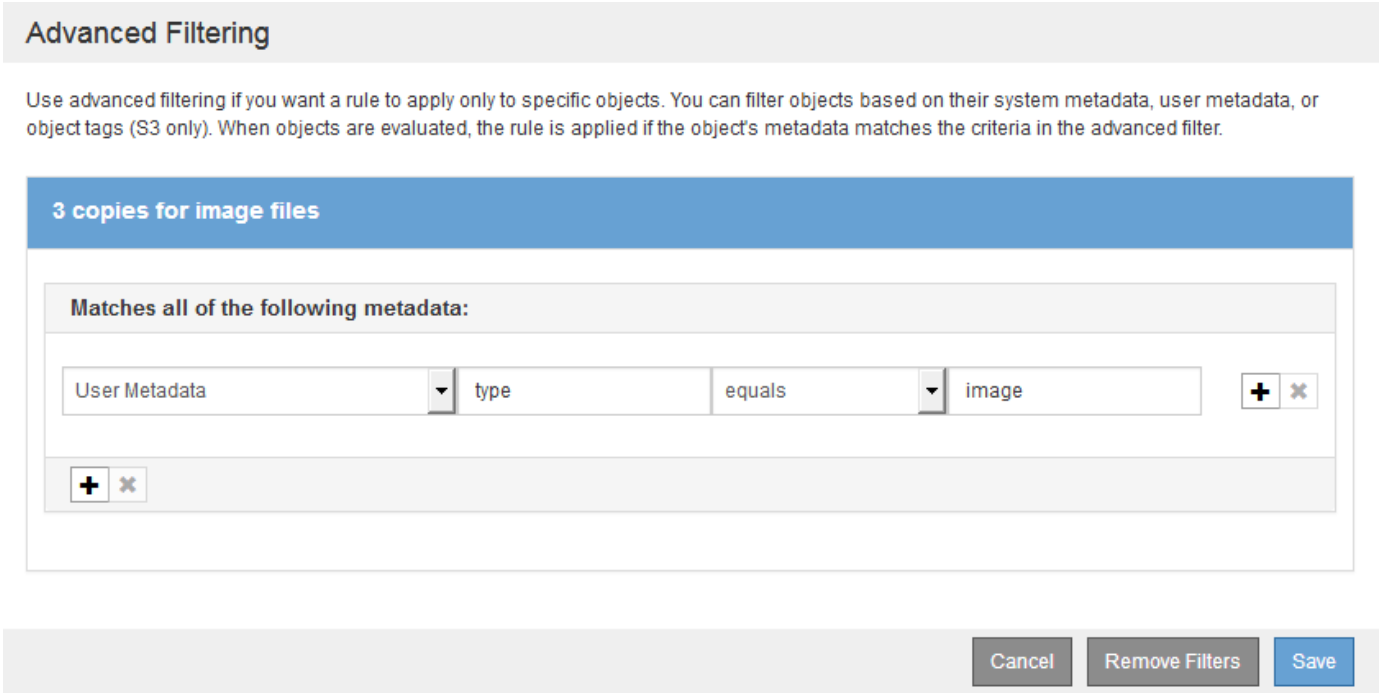

Poiché questa regola è configurata come prima regola del criterio, l'istruzione di posizionamento della codifica di cancellazione si applica solo alle immagini di dimensioni superiori a 200 KB.



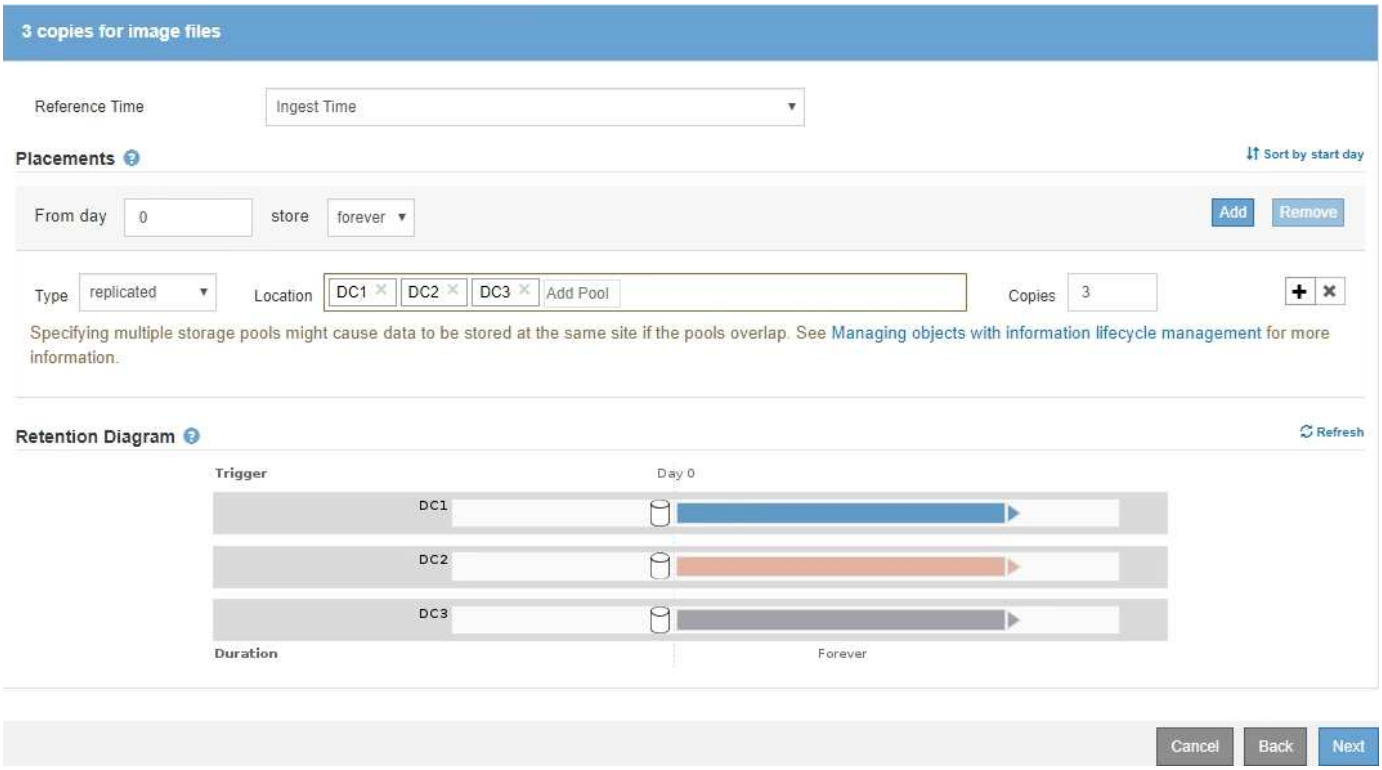
## ILM regola 2 per esempio 3: Replica 3 copie per tutti i file immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file di immagine devono essere replicati.

| Definizione della regola | Valore di esempio |
| --- | --- |
| Nome regola | 3 copie per i file di immagine |
| Tempo di riferimento | Tempo di acquisizione |
| Filtro avanzato per i metadati utente | Il tipo di metadati utente equivale ai file di immagine |
| Posizionamento dei contenuti | Creare 3 copie replicate in tutti i nodi di storage |




Poiché la prima regola del criterio ha già trovato corrispondenza con file di immagine di dimensioni superiori a 200 KB, queste istruzioni di posizionamento si applicano solo ai file di immagine di dimensioni pari o inferiori a 200 KB.

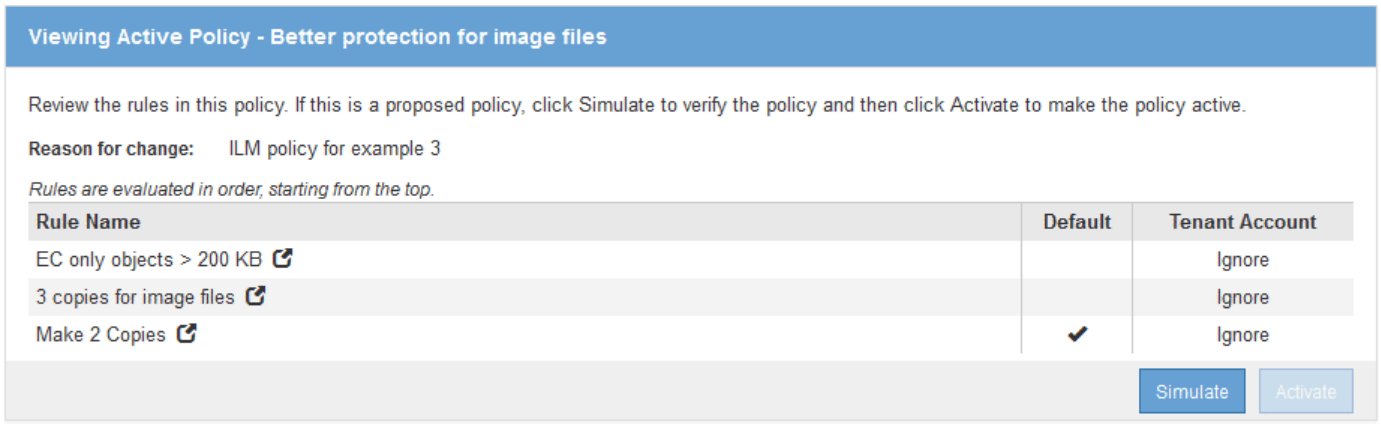



## Policy ILM per esempio 3: Migliore protezione per i file di immagine

In questo esempio, il criterio ILM utilizza tre regole ILM per creare un criterio che erasure i file immagine di dimensioni superiori a 200 KB (0.2 MB), crea copie replicate per i file immagine di dimensioni pari o inferiori a 200 KB e crea due copie replicate per i file non immagine.

Questo esempio di policy ILM include regole che eseguono le seguenti operazioni:

- Erasure coding tutti i file di immagine di dimensioni superiori a 200 KB.
- Creare tre copie dei file immagine rimanenti (ovvero, immagini di dimensioni pari o inferiori a 200 KB).
- Applicare la regola predefinita a tutti gli oggetti rimanenti (ovvero tutti i file non immagine).




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

Se si dispone di un bucket S3 con la versione attivata, è possibile gestire le versioni degli

oggetti non correnti includendo regole nella policy ILM che utilizzano **tempo non corrente** come tempo di riferimento.

Come illustrato in questo esempio, è possibile controllare la quantità di storage utilizzata dagli oggetti con versione utilizzando istruzioni di posizionamento diverse per le versioni degli oggetti non correnti.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

> Se si creano criteri ILM per gestire le versioni degli oggetti non correnti, tenere presente che è necessario conoscere l'UUID o il CBID della versione dell'oggetto per simulare il criterio. Per trovare UUUID e CBID di un oggetto, utilizzare Object Metadata Lookup (Ricerca metadati oggetto) mentre l'oggetto è ancora aggiornato.

**Informazioni correlate**

"Modalità di eliminazione degli oggetti con versione S3"

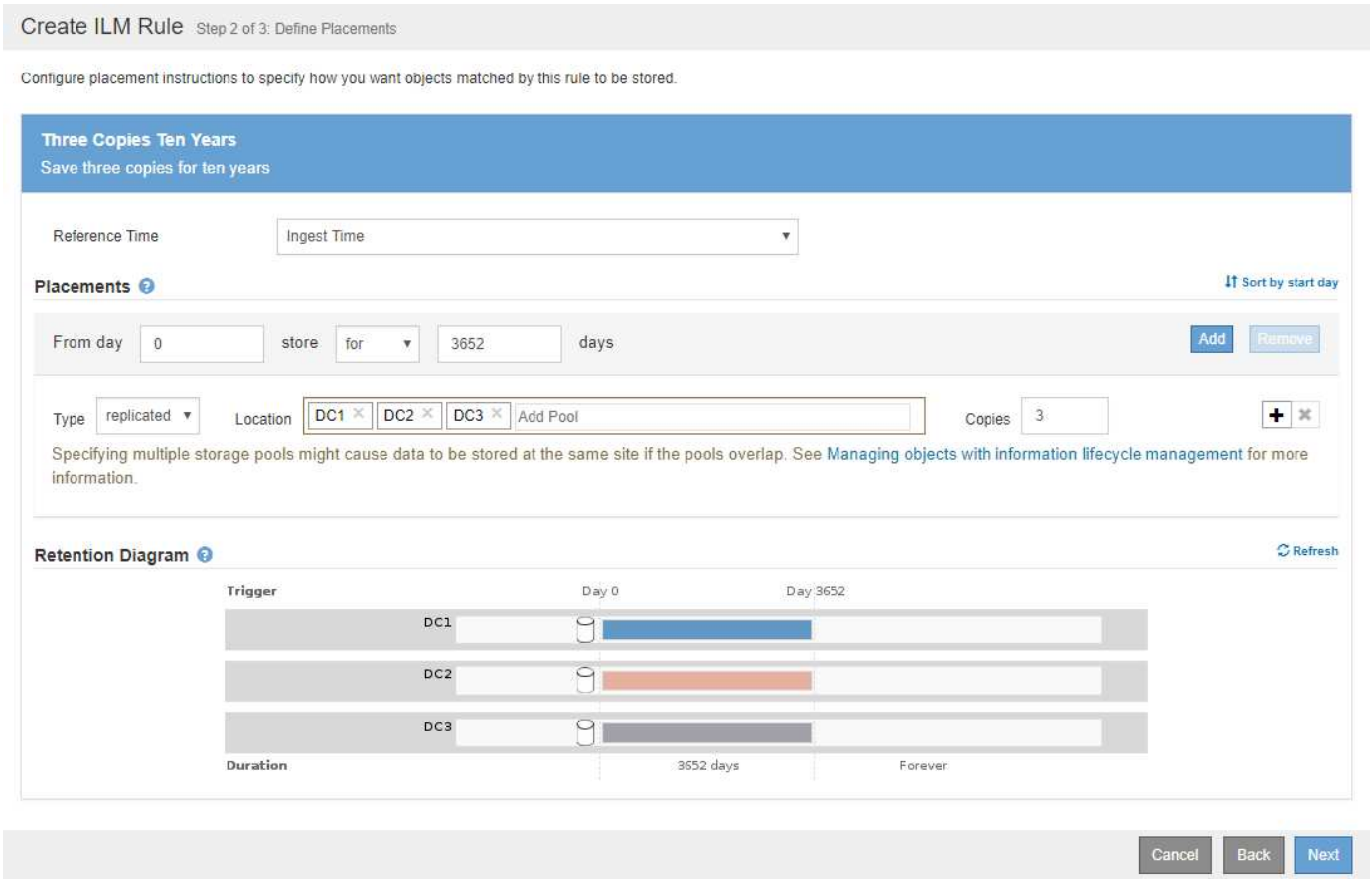
"Verifica di un criterio ILM con la ricerca dei metadati degli oggetti"

## ILM regola 1 per esempio 4: Salva tre copie per 10 anni

Questa regola ILM di esempio memorizza una copia di ciascun oggetto in tre data center per 10 anni.

Questa regola si applica a tutti gli oggetti, indipendentemente dal fatto che siano con versione.

| Definizione della regola | Valore di esempio |
|---|---|
| Pool di storage | Tre pool di storage, ciascuno in diversi data center, denominati DC1, DC2 e DC3. |
| Nome regola | Tre copie dieci anni |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamento dei contenuti | Il giorno 0, conserva tre copie replicate per 10 anni (3,652 giorni), una in DC1, una in DC2 e una in DC3. Alla fine dei 10 anni, eliminare tutte le copie dell'oggetto. |



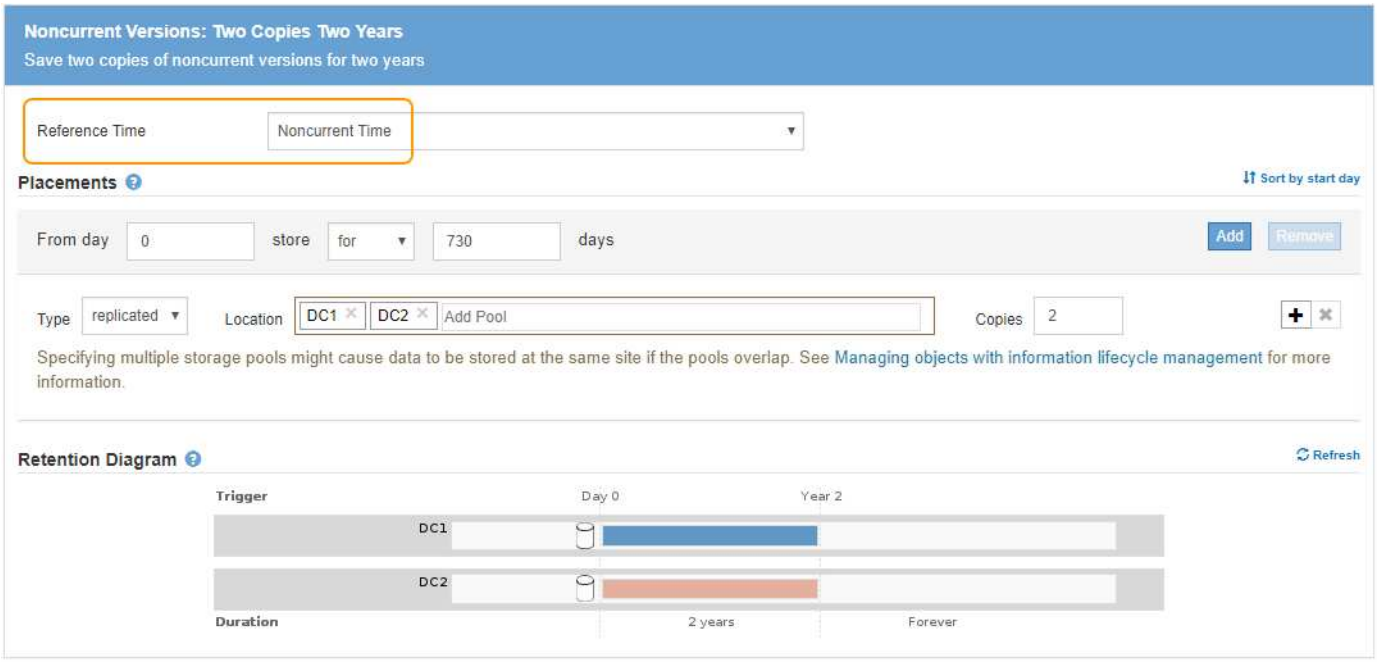

## ILM regola 2 per esempio 4: Salva due copie di versioni non correnti per 2 anni

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

Poiché la regola ILM 1 si applica a tutte le versioni dell'oggetto, è necessario creare un'altra regola per filtrare le versioni non correnti. Questa regola utilizza l'opzione **ora non corrente** per il tempo di riferimento.

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

| Definizione della regola | Valore di esempio |
|---|---|
| Pool di storage | Due pool di storage, ciascuno in diversi data center, denominati DC1 e DC2. |
| Nome regola | Versioni non correnti: Due copie per due anni |
| Tempo di riferimento | Ora non corrente |
| Posizionamento dei contenuti | Il giorno 0 relativo all'ora non corrente (ovvero, a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), mantenere due copie replicate delle versioni dell'oggetto non correnti per 2 anni (730 giorni), una in DC1 e una in DC2. Alla fine di 2 anni, eliminare le versioni non aggiornate. |




## Policy ILM per esempio 4: Oggetti con versione S3

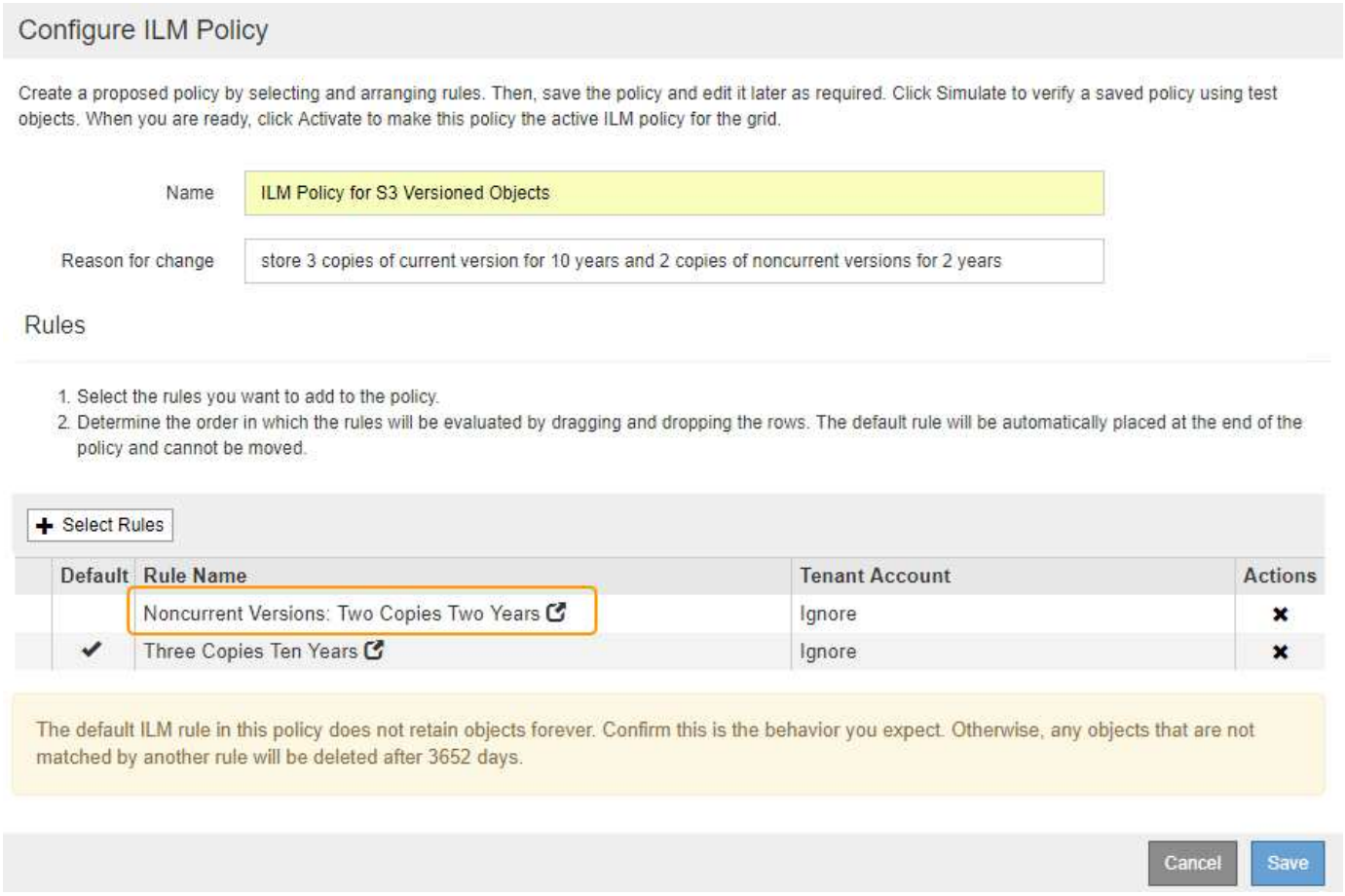
Se si desidera gestire le versioni precedenti di un oggetto in modo diverso dalla versione corrente, le regole che utilizzano **ora non corrente** come ora di riferimento devono essere visualizzate nel criterio ILM prima delle regole che si applicano alla versione corrente dell'oggetto.

Un criterio ILM per gli oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

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

> Le regole dell'ora non corrente devono essere visualizzate nel criterio prima delle regole applicabili alla versione corrente dell'oggetto. In caso contrario, le versioni degli oggetti non correnti non verranno mai associate alla regola dell'ora non corrente.

- Al momento dell'acquisizione, creare tre copie replicate e memorizzare una copia in ciascuno dei tre data center. Conserva le copie della versione corrente dell'oggetto per 10 anni.




Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Qualsiasi versione dell'oggetto non corrente verrebbe associata dalla prima regola. Se una versione dell'oggetto non corrente ha più di 2 anni, viene eliminata in modo permanente da ILM (tutte le copie della versione non corrente vengono rimosse dalla griglia).

> Per simulare versioni di oggetti non correnti, è necessario utilizzare UUID o CBID di tale versione. Mentre l'oggetto è ancora aggiornato, è possibile utilizzare Object Metadata Lookup (Ricerca metadati oggetto) per trovare UUID e CBID.

- La seconda regola corrisponde alla versione corrente dell'oggetto. Quando la versione corrente dell'oggetto è stata memorizzata per 10 anni, il processo ILM aggiunge un indicatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente dell'oggetto "non aggiornata". La prossima volta che si verifica la valutazione ILM, questa versione non corrente corrisponde alla prima regola. Di conseguenza, la copia di DC3 viene eliminata e le due copie di DC1 e DC2 vengono conservate per altri 2 anni.

**Informazioni correlate**

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

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

È possibile utilizzare un filtro di posizione e il rigoroso comportamento di acquisizione in una regola per impedire che gli oggetti vengano salvati in una determinata posizione del

data center.

In questo esempio, un tenant con sede a Parigi non desidera memorizzare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, inclusi tutti gli oggetti di altri account tenant, possono essere memorizzati nel data center di Parigi o nel data center statunitense.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

**Informazioni correlate**

"Modalità di acquisizione degli oggetti"

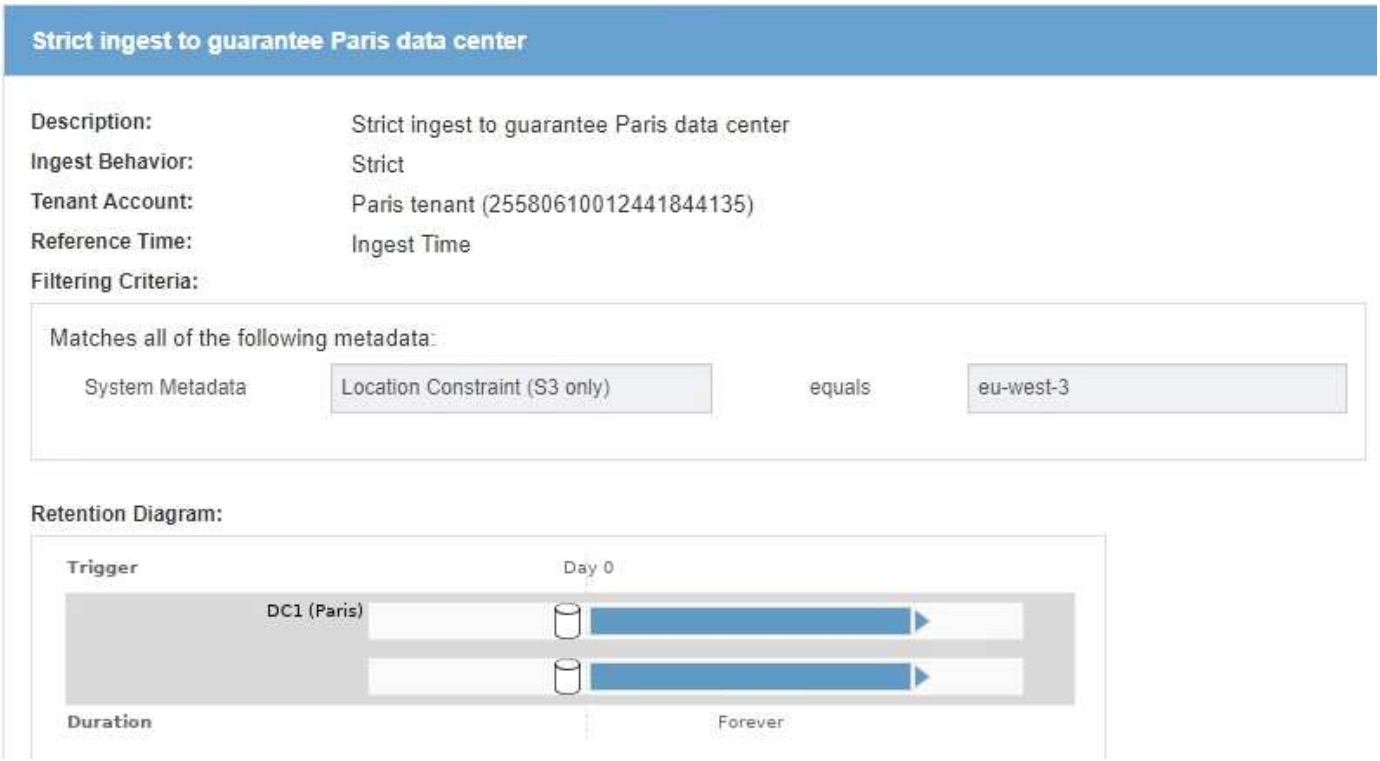
"Fase 3 di 3: Definizione del comportamento di acquisizione"

## ILM regola 1 per esempio 5: Ingest rigoroso per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento rigoroso dell'acquisizione per garantire che gli oggetti salvati da un tenant basato su Parigi nei bucket S3 con la regione impostata su ue-West-3 (Parigi) non vengano mai memorizzati nel data center statunitense.

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

| Definizione della regola | Valore di esempio |
|---|---|
| Account tenant | Tenant di Parigi |
| Filtraggio avanzato | Il vincolo di posizione equivale a eu-West-3 |
| Pool di storage | DC1 (Parigi) |
| Nome regola | Un ingest rigoroso per garantire il data center di Parigi |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamento dei contenuti | Il giorno 0, conserva due copie replicate per sempre in DC1 (Parigi) |
| Comportamento di acquisizione | Rigoroso. Utilizza sempre le posizioni di questa regola per l'acquisizione. L'acquisizione non riesce se non è possibile memorizzare due copie dell'oggetto nel data center di Parigi. |




## ILM regola 2 per esempio 5: Acquisizione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciata per fornire un'efficienza ILM ottimale per qualsiasi oggetto non associato alla prima regola. Verranno memorizzate due copie di tutti gli oggetti corrispondenti a questa regola: Una nel data center degli Stati Uniti e una nel data center di Parigi. Se la regola non può essere soddisfatta immediatamente, le copie temporanee vengono memorizzate in qualsiasi posizione disponibile.

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

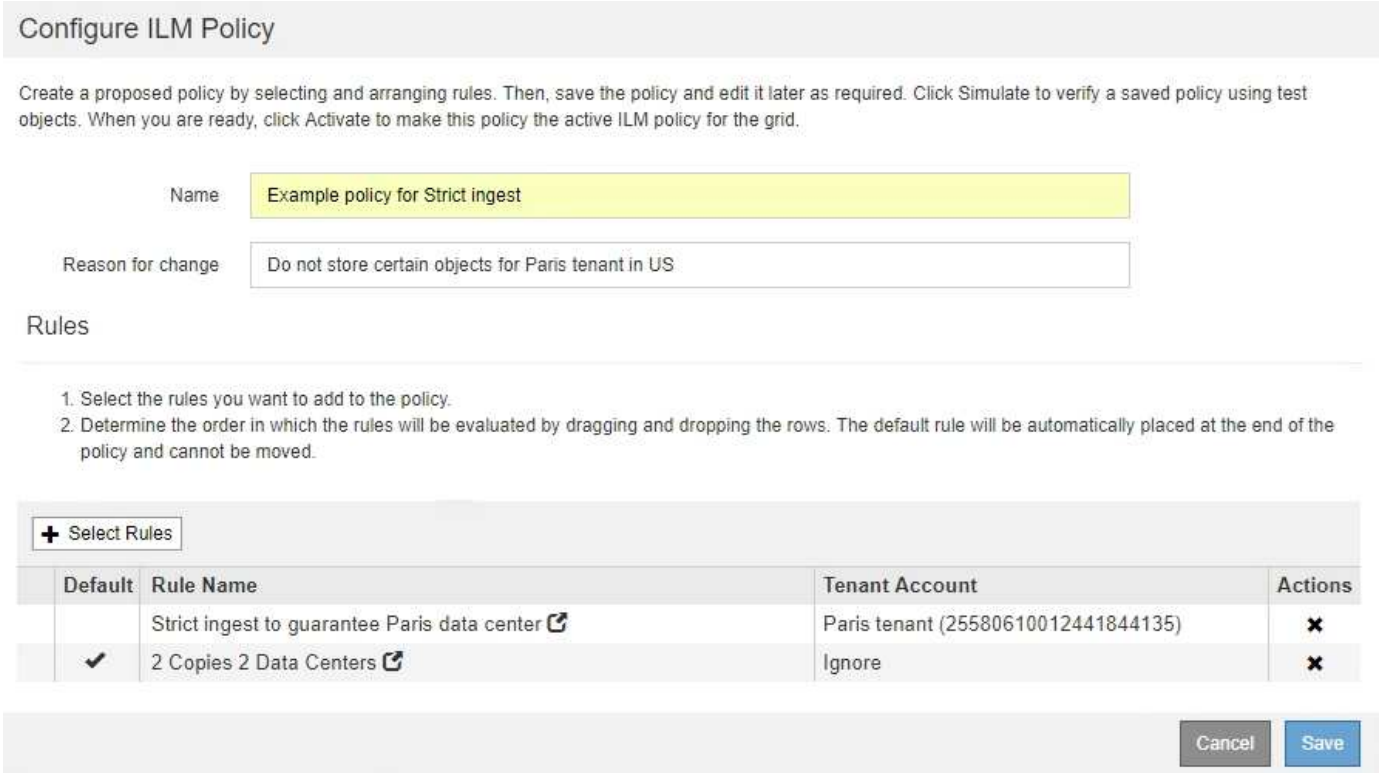
| Definizione della regola | Valore di esempio |
|---|---|
| Account tenant | Ignorare |
| Filtraggio avanzato | *Non specificato* |
| Pool di storage | DC1 (Parigi) e DC2 (Stati Uniti) |
| Nome regola | 2 copie di 2 data center |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamento dei contenuti | Il giorno 0, conserva due copie replicate per sempre in due data center |
| Comportamento di acquisizione | Bilanciato. Gli oggetti che corrispondono a questa regola vengono posizionati in base alle istruzioni di posizionamento della regola, se possibile. In caso contrario, le copie temporanee vengono eseguite in qualsiasi ubicazione disponibile. |

## Policy ILM per esempio 5: Combinazione di comportamenti di acquisizione

Il criterio ILM di esempio include due regole che hanno comportamenti di acquisizione diversi.

Un criterio ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Memorizzare gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 (Parigi) solo nel data center di Parigi. Non eseguire l'acquisizione se il data center di Parigi non è disponibile.
- Memorizzare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) nel data center statunitense e nel data center di Parigi. Se le istruzioni di posizionamento non possono essere soddisfatte, eseguire copie temporanee in qualsiasi ubicazione disponibile.




Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Tutti gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 vengono abbinati alla prima regola e memorizzati nel data center di Parigi. Poiché la prima regola utilizza un ingest rigoroso, questi oggetti non vengono mai memorizzati nel data center statunitense. Se i nodi di storage nel data center di Parigi non sono disponibili, l'acquisizione non riesce.
- Tutti gli altri oggetti sono abbinati dalla seconda regola, inclusi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-West-3. Una copia di ciascun oggetto viene salvata in ciascun data center. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie temporanee in qualsiasi posizione disponibile.

# Esempio 6: Modifica di un criterio ILM

Potrebbe essere necessario creare e attivare una nuova policy ILM se la protezione dei dati deve cambiare o se si aggiungono nuovi siti.

Prima di modificare una policy, è necessario comprendere in che modo le modifiche apportate ai posizionamenti ILM possono influire temporaneamente sulle prestazioni generali di un sistema StorageGRID.

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione e il criterio ILM attivo deve essere rivisto per memorizzare i dati nel nuovo sito.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

## In che modo la modifica di un criterio ILM influisce sulle performance

Quando si attiva un nuovo criterio ILM, le prestazioni del sistema StorageGRID potrebbero risentirne temporaneamente, soprattutto se le istruzioni di posizionamento nel nuovo criterio richiedono lo spostamento di molti oggetti esistenti in nuove posizioni.

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

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

- Applicazione di un profilo di codifica Erasure diverso agli oggetti con codifica erasure esistenti.

  > StorageGRID considera ogni profilo di codifica Erasure unico e non riutilizza i frammenti di codifica Erasure quando viene utilizzato un nuovo profilo.

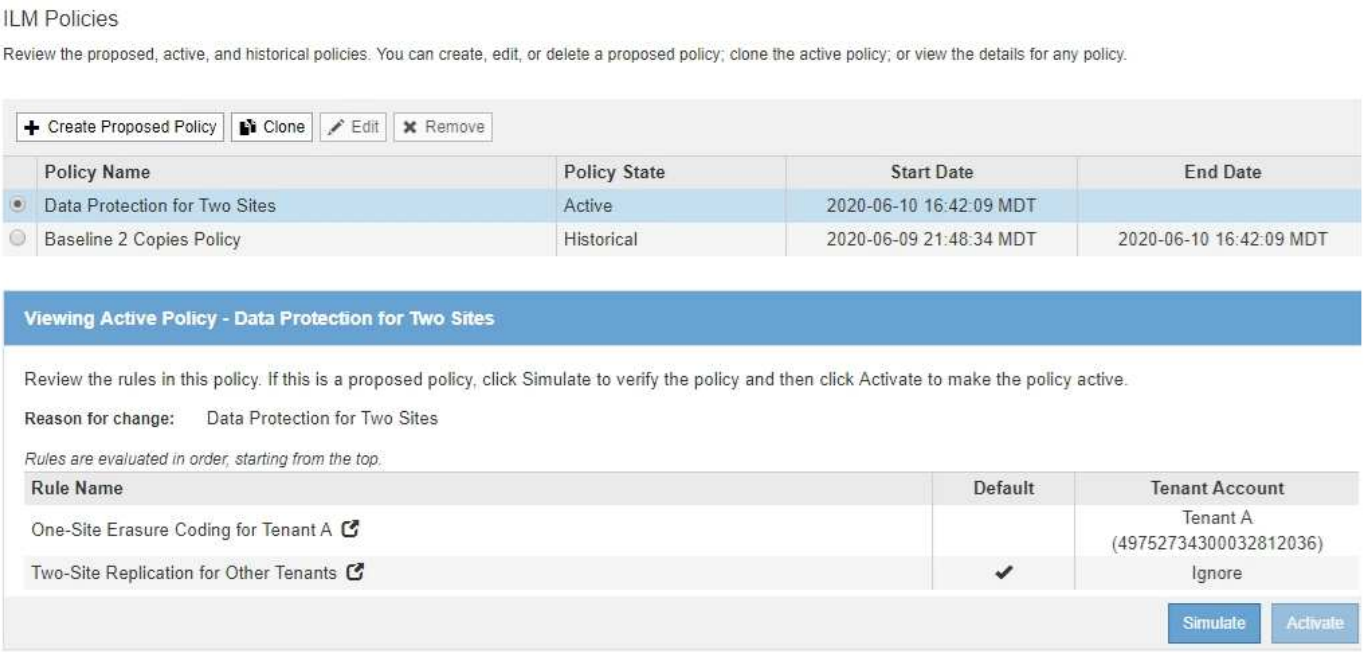
- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, conversione di una grande percentuale di oggetti replicati in oggetti con codifica per la cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un numero elevato di oggetti da o verso un Cloud Storage Pool o da o verso un sito remoto.

**Informazioni correlate**

"Creazione di un criterio ILM"

## Policy ILM attiva ad esempio 6: Protezione dei dati in due siti

In questo esempio, la policy ILM attiva è stata inizialmente progettata per un sistema StorageGRID a due siti e utilizza due regole ILM.



In questa policy ILM, gli oggetti appartenenti al tenant A sono protetti da una codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti in due siti utilizzando la replica a 2 copie.

> La prima regola di questo esempio utilizza un filtro avanzato per garantire che la codifica erasure non venga utilizzata per oggetti di piccole dimensioni. Qualsiasi oggetto del tenant A di dimensioni inferiori a 200 KB sarà protetto dalla seconda regola, che utilizza la replica.

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

| Definizione della regola | Valore di esempio |
|---|---|
| Nome regola | Codifica di cancellazione one-site per il tenant A. |
| Account tenant | Tenant A. |
| Pool di storage | Data center 1 |
| Posizionamento dei contenuti | 2+1 erasure coding in Data Center 1 dal giorno 0 a per sempre |

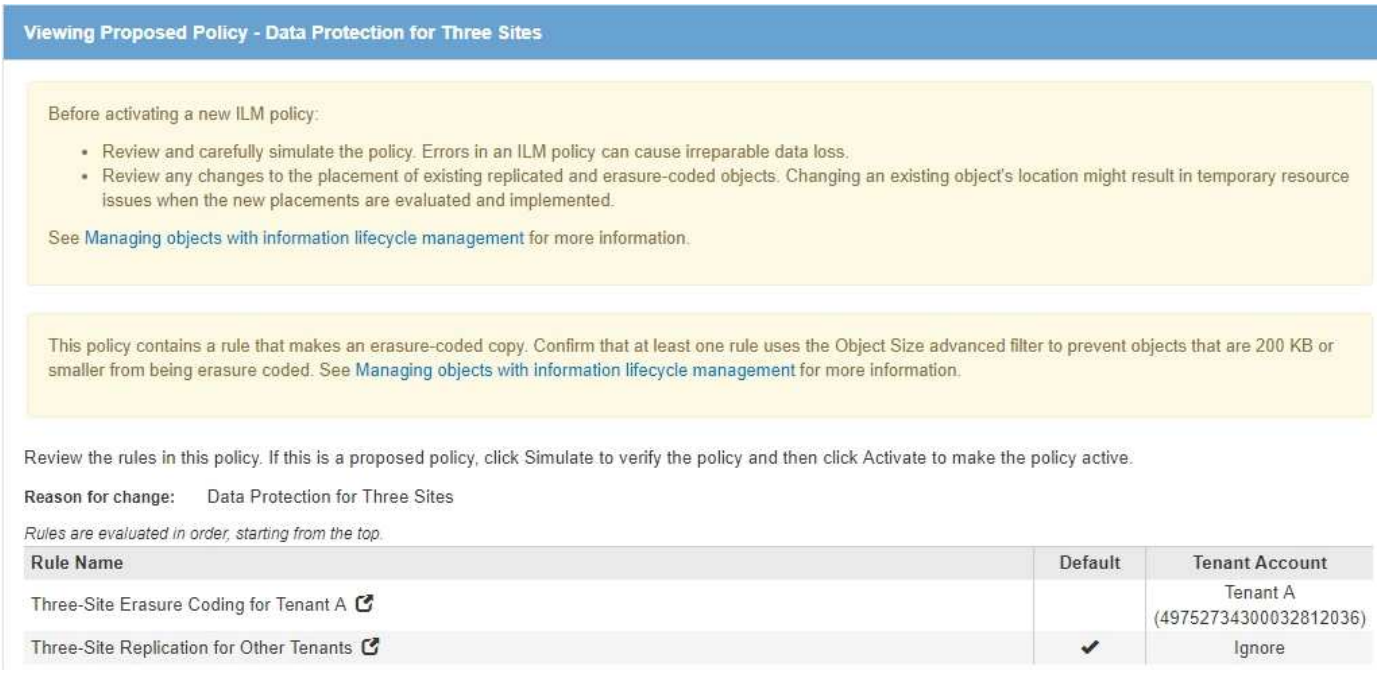
**Regola 2: Replica a due siti per altri tenant**

| Definizione della regola | Valore di esempio |
|---|---|
| Nome regola | Replica a due siti per altri tenant |
| Account tenant | Ignorare |
| Pool di storage | Data Center 1 e Data Center 2 |
| Posizionamento dei contenuti | Due copie replicate dal giorno 0 all'infinito: Una copia nel data center 1 e una copia nel data center 2. |

## Policy ILM proposta per esempio 6: Protezione dei dati in tre siti

In questo esempio, il criterio ILM viene aggiornato per un sistema StorageGRID a tre siti.

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore del grid ha creato due nuovi pool di storage: Un pool di storage per Data Center 3 e un pool di storage contenente tutti e tre i siti (non lo stesso del pool di storage predefinito di tutti i nodi di storage). Quindi, l'amministratore ha creato due nuove regole ILM e una nuova policy ILM proposta, progettata per proteggere i dati in tutti e tre i siti.




Quando viene attivata questa nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti da una cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e gli oggetti più piccoli appartenenti al tenant A) saranno protetti in tre siti utilizzando la replica a 3 copie.

**Regola 1: Erasure coding a tre siti per il tenant A.**

| Definizione della regola | Valore di esempio |
|---|---|
| Nome regola | Codifica di cancellazione a tre siti per il tenant A. |
| Account tenant | Tenant A. |
| Pool di storage | Tutti e 3 i data center (inclusi data center 1, data center 2 e data center 3) |
| Posizionamento dei contenuti | 2+1 erasure coding in tutti e 3 i data center, dal giorno 0 fino all'eterno |

**Regola 2: Replica a tre siti per altri tenant**

| Definizione della regola | Valore di esempio |
|---|---|
| Nome regola | Replica a tre siti per altri tenant |
| Account tenant | Ignorare |
| Pool di storage | Data Center 1, Data Center 2 e Data Center 3 |
| Posizionamento dei contenuti | Tre copie replicate dal giorno 0 a sempre: Una copia presso il data center 1, una copia presso il data center 2 e una copia presso il data center 3. |

## Attivazione della policy ILM proposta, ad esempio 6

Quando si attiva un nuovo criterio ILM proposto, gli oggetti esistenti potrebbero essere spostati in nuove posizioni oppure potrebbero essere create nuove copie degli oggetti per gli oggetti esistenti, in base alle istruzioni di posizionamento in qualsiasi regola nuova o aggiornata.

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

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

### Cosa succede quando cambiano le istruzioni di erasure coding

Nella policy ILM attualmente attiva, per questo esempio, gli oggetti appartenenti al tenant A sono protetti utilizzando la codifica di cancellazione 2+1 nel data center 1. Nella nuova policy ILM proposta, gli oggetti appartenenti al tenant A verranno protetti utilizzando la codifica di cancellazione 2+1 nei data center 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- I nuovi oggetti acquisiti dal tenant A vengono suddivisi in due frammenti di dati e viene aggiunto un frammento di parità. Quindi, ciascuno dei tre frammenti viene memorizzato in un data center diverso.
- Gli oggetti esistenti appartenenti al tenant A vengono rivalutati durante il processo di scansione ILM in corso. Poiché le istruzioni di posizionamento di ILM utilizzano un nuovo profilo di codifica Erasure, vengono creati e distribuiti frammenti completamente nuovi con codifica erasure nei tre data center.

> I frammenti 2+1 esistenti nel data center 1 non vengono riutilizzati. StorageGRID considera ogni profilo di codifica Erasure unico e non riutilizza i frammenti di codifica Erasure quando viene utilizzato un nuovo profilo.

### Cosa succede quando cambiano le istruzioni di replica

Nel criterio ILM attualmente attivo per questo esempio, gli oggetti appartenenti ad altri tenant vengono protetti utilizzando due copie replicate nei pool di storage dei data center 1 e 2. Nella nuova policy ILM proposta, gli oggetti appartenenti ad altri tenant verranno protetti utilizzando tre copie replicate nei pool di storage dei data center 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID crea tre copie e salva una copia in ogni data center.
- Gli oggetti esistenti appartenenti a questi altri tenant vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie di oggetti esistenti nel data center 1 e nel data center 2 continuano a soddisfare i requisiti di replica della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il data center 3.

**Impatto delle performance dell'attivazione di questa policy**

Quando viene attivata la policy ILM proposta in questo esempio, le prestazioni generali di questo sistema StorageGRID saranno temporaneamente compromesse. Per creare nuovi frammenti erasure-coded per gli oggetti esistenti del tenant A e nuove copie replicate nel data center 3 per gli oggetti esistenti degli altri tenant saranno necessari livelli di risorse grid superiori al normale.

Come conseguenza della modifica del criterio ILM, le richieste di lettura e scrittura del client potrebbero temporaneamente riscontrare latenze superiori al normale. Le latenze torneranno ai livelli normali dopo che le istruzioni di posizionamento sono state completamente implementate nella griglia.

Per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui il nuovo criterio verrà applicato per garantire che gli oggetti esistenti non vengano spostati inutilmente.

Contattare il supporto tecnico se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

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

È possibile utilizzare il bucket S3, le regole ILM e il criterio ILM in questo esempio come punto di partenza quando si definisce un criterio ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con blocco oggetti S3 attivato.

Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti di StorageGRID, puoi anche utilizzare questo esempio per gestire qualsiasi bucket esistente con la funzionalità di conformità legacy attivata.

Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

**Informazioni correlate**

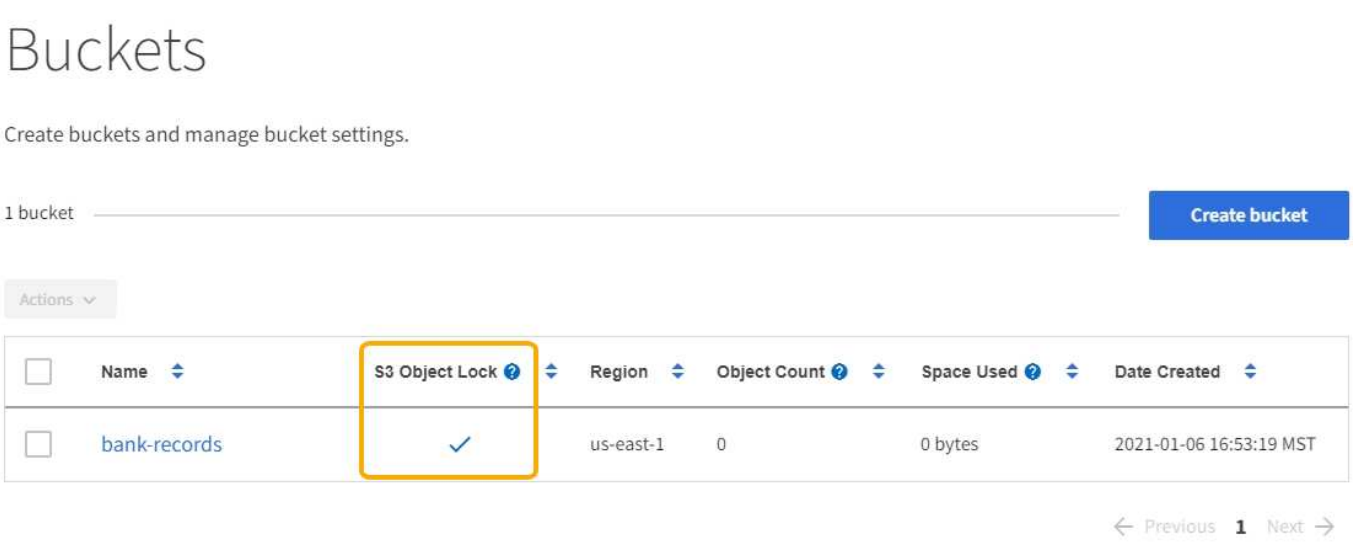
"Gestione degli oggetti con S3 Object Lock"

"Creazione di un criterio ILM"

## Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato il tenant Manager per creare un bucket con blocco oggetti S3 abilitato per memorizzare i record bancari critici.

| Definizione del bucket | Valore di esempio |
| --- | --- |
| Nome account tenant | Banca di ABC |
| Nome bucket | banca-record |
| Area bucket | us-east-1 (impostazione predefinita) |




Ogni versione di oggetto e oggetto aggiunta al bucket dei record bancari utilizzerà i seguenti valori per `retain-until-date` e. `legal hold` impostazioni.

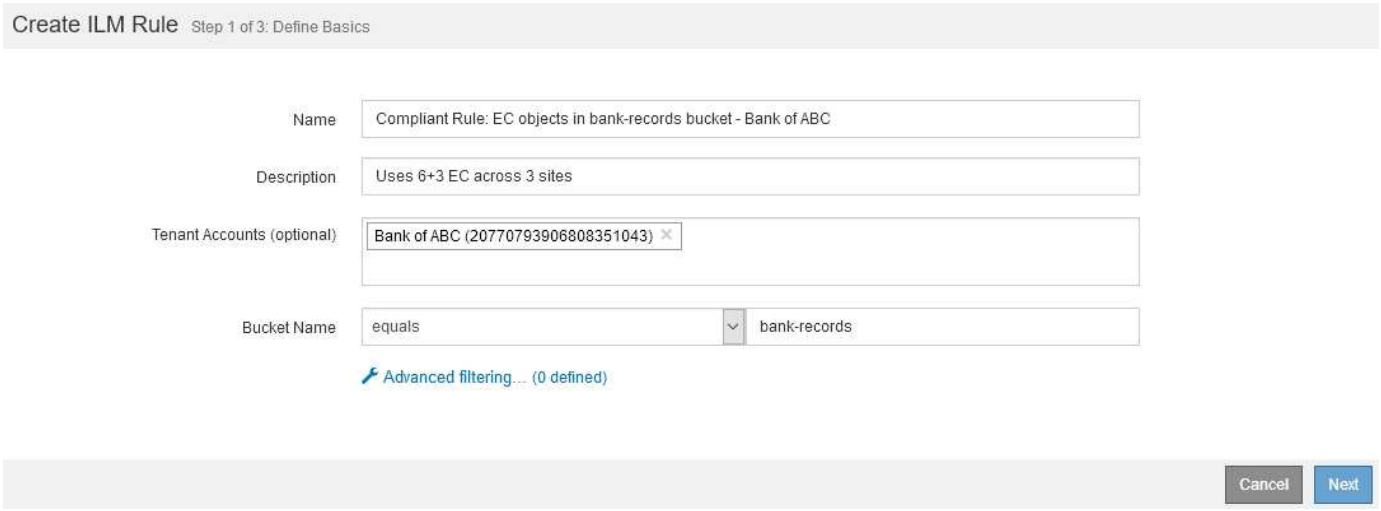
| Impostazione per ciascun oggetto | Valore di esempio |
|---|---|
| `retain-until-date` | `"2030-12-30T23:59:59Z"` (30 dicembre 2030)<br><br>Ogni versione dell'oggetto ha il proprio `retain-until-date` impostazione. Questa impostazione può essere aumentata, ma non ridotta. |
| `legal hold` | `"OFF"` (Non in vigore)<br><br>È possibile mettere o revocare un blocco legale su qualsiasi versione oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è sottoposto a un blocco legale, non è possibile eliminarlo anche se `retain-until-date` è stato raggiunto. |

## ILM regola 1 per S3 Object Lock esempio: Erasure coding profile with bucket matching

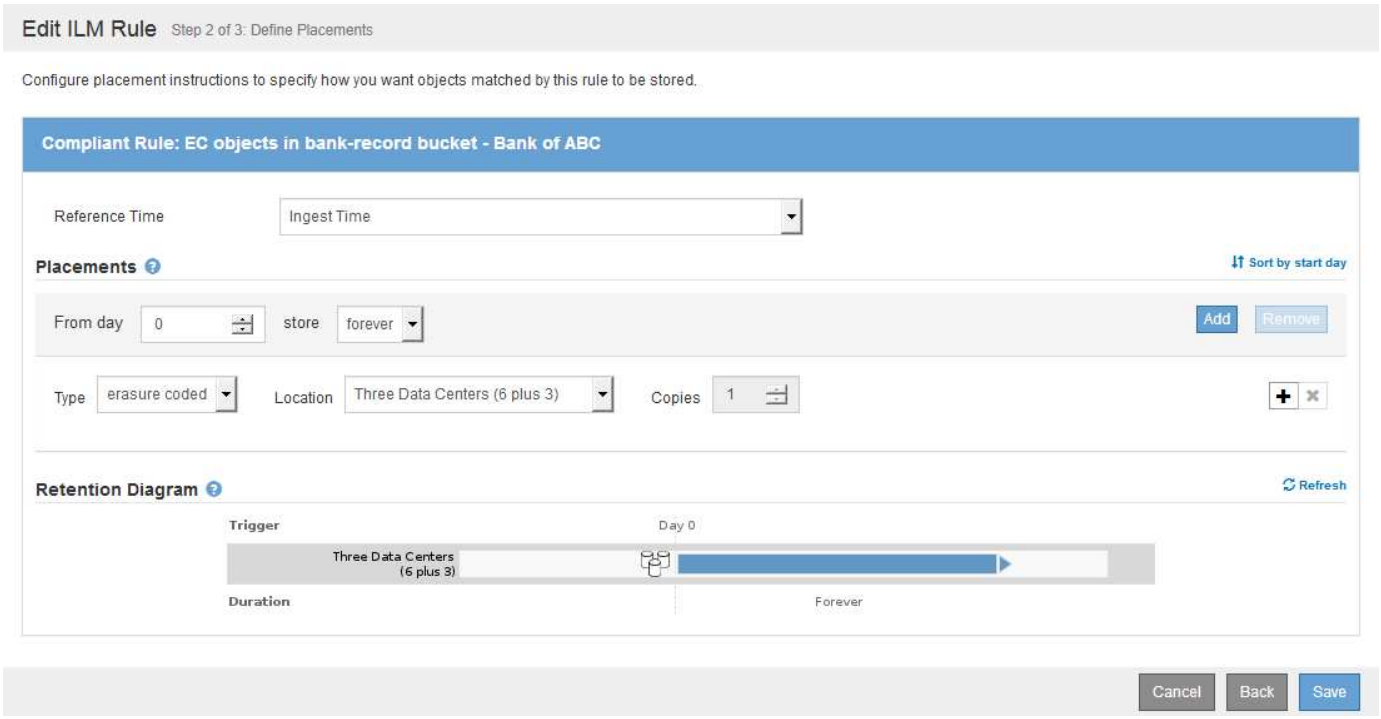
Questa regola ILM di esempio si applica solo all'account tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto in `bank-records` Quindi utilizza la codifica di cancellazione per memorizzare l'oggetto su nodi di storage in tre siti del data center utilizzando un profilo di codifica Erasure 6+3. Questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato: Una copia codificata in cancellazione viene conservata nei nodi di storage dal giorno 0 all'eterno, utilizzando l'ora di Ingest come ora di riferimento.

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

| Definizione della regola | Valore di esempio |
| --- | --- |
| Nome bucket | `bank-records` |
| Filtraggio avanzato | Dimensione oggetto (MB) maggiore di 0.20<br><br>**Nota:** questo filtro garantisce che la codifica erasure non venga utilizzata per oggetti di dimensioni pari o inferiori a 200 KB. |



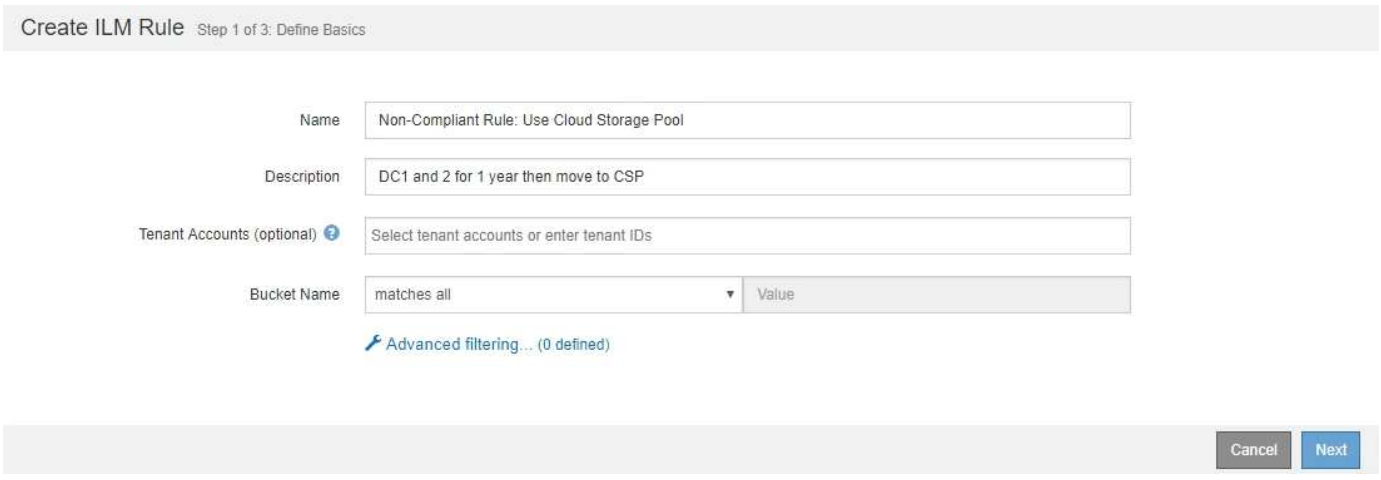

| Definizione della regola | Valore di esempio |
| --- | --- |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamenti | Dal giorno 0 memorizzare per sempre |
| Erasure Coding Profile (erasure Coding Profile | • Creare una copia con codifica di cancellazione sui nodi di storage in tre siti del data center<br>• Utilizza uno schema di erasure coding 6+3 |




## ILM regola 2 per S3 Object Lock esempio: Regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie di oggetti replicate sui nodi di storage. Dopo un anno, memorizza una copia su un Cloud Storage Pool per sempre. Poiché questa regola utilizza un Cloud Storage Pool, non è conforme e non si applica agli oggetti nei bucket con S3 Object Lock attivato.

| Definizione della regola | Valore di esempio |
|---|---|
| Nome regola | Regola non conforme: Utilizza il pool di storage cloud |
| Account tenant | Non specificato |
| Nome bucket | Non specificato, ma si applica solo ai bucket che non hanno S3 Object Lock (o la funzione Compliance legacy) abilitato. |
| Filtraggio avanzato | Non specificato |

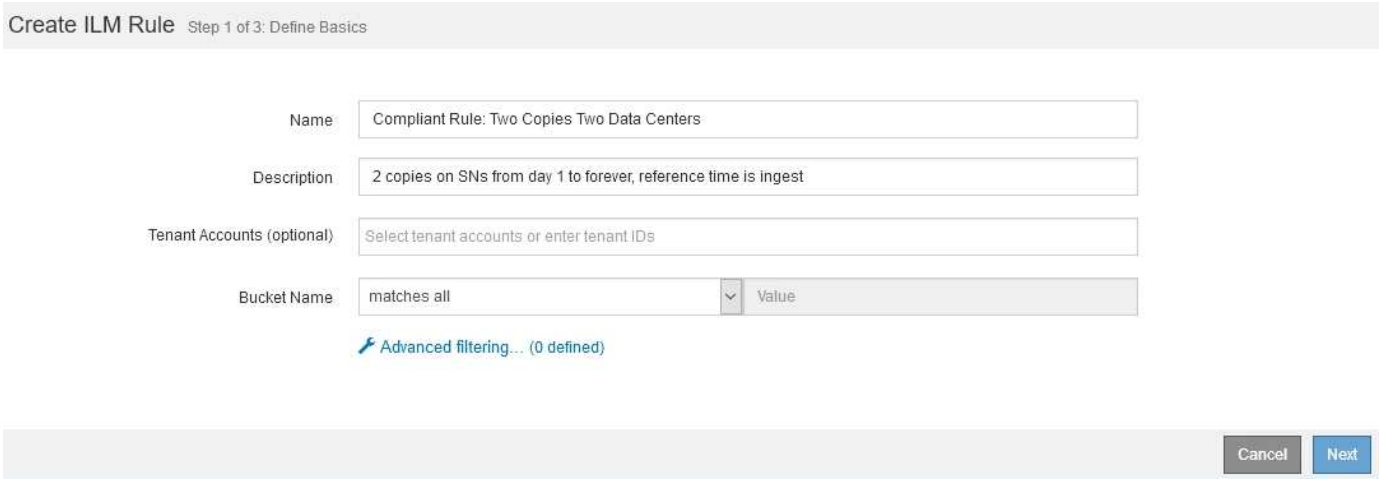


| Definizione della regola | Valore di esempio |
| --- | --- |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamenti | • Il giorno 0, conserva due copie replicate sui nodi di storage nel data center 1 e nel data center 2 per 365 giorni<br>• Dopo 1 anno, conserva per sempre una copia replicata in un Cloud Storage Pool |

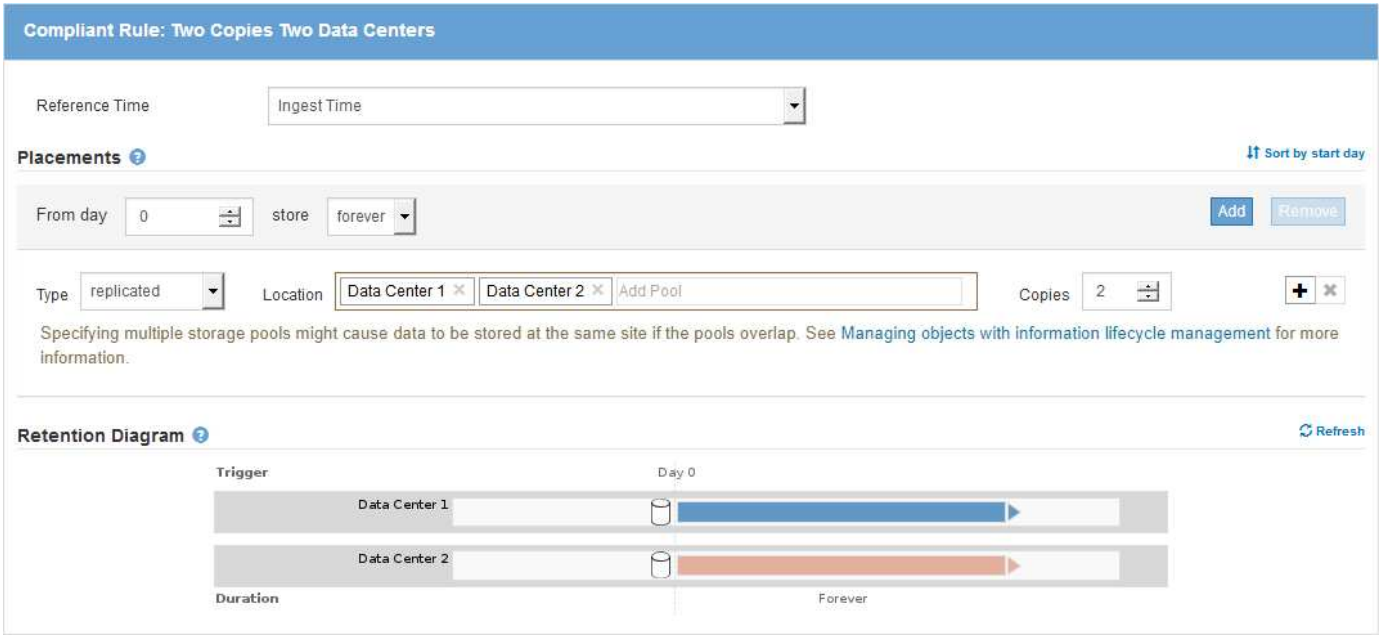
## ILM regola 3 per S3 Object Lock esempio: Regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due data center. Questa regola di conformità è stata progettata per essere la regola predefinita nel criterio ILM. Non include alcun filtro e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: Due copie di oggetti vengono conservate sui nodi di storage dal giorno 0 all'eterno, utilizzando Ingest come tempo di riferimento.

| Definizione della regola | Valore di esempio |
| --- | --- |
| Nome regola | Default CompacCompacant Rule: Due copie di due data center |
| Account tenant | Non specificato |
| Nome bucket | Non specificato |
| Filtraggio avanzato | Non specificato |




| Definizione della regola | Valore di esempio |
| --- | --- |
| Tempo di riferimento | Tempo di acquisizione |
| Posizionamenti | Dal giorno 0 all'anno, conserva due copie replicate, una sui nodi di storage nel data center 1 e una sui nodi di storage nel data center 2. |



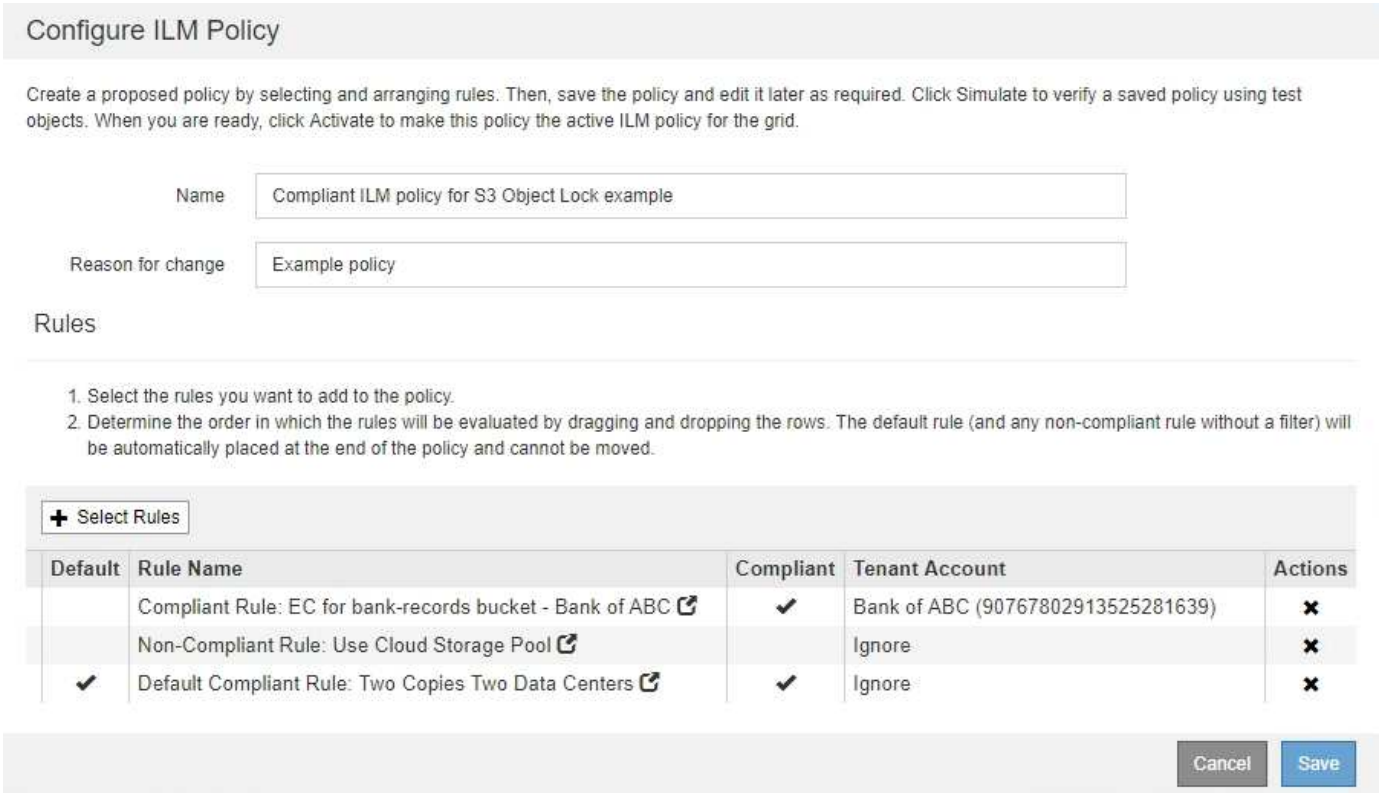

## Esempio di policy ILM conforme per S3 Object Lock

Per creare un criterio ILM che protegga efficacemente tutti gli oggetti del sistema, inclusi quelli nei bucket con S3 Object Lock attivato, è necessario selezionare le regole ILM che soddisfano i requisiti di storage per tutti gli oggetti. Quindi, è necessario simulare e attivare la policy proposta.

### Aggiunta di regole al criterio

In questo esempio, il criterio ILM include tre regole ILM, nel seguente ordine:

1. Regola conforme che utilizza la codifica erasure per proteggere oggetti di dimensioni superiori a 200 KB in un bucket specifico con blocco oggetti S3 attivato. Gli oggetti vengono memorizzati nei nodi di storage dal giorno 0 a sempre.
2. Una regola non conforme che crea due copie di oggetti replicate sui nodi di storage per un anno e sposta una copia di oggetto in un pool di storage cloud per sempre. Questa regola non si applica ai bucket con blocco oggetti S3 attivato perché utilizza un pool di storage cloud.
3. La regola di conformità predefinita che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a per sempre.




### Simulazione della policy proposta

Dopo aver aggiunto le regole nella policy proposta, aver scelto una regola di conformità predefinita e aver disposto le altre regole, è necessario simulare la policy testando gli oggetti dal bucket con S3 Object Lock abilitato e da altri bucket. Ad esempio, quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- La prima regola corrisponde solo agli oggetti di test di dimensioni superiori a 200 KB nei record bancari bucket per il tenant Bank of ABC.
- La seconda regola corrisponde a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri account tenant.
- La regola predefinita corrisponde ai seguenti oggetti:
  - Oggetti di 200 KB o inferiori nei bucket bank-record per il tenant Bank of ABC.
  - Oggetti in qualsiasi altro bucket con S3 Object Lock attivato per tutti gli altri account tenant.

### Attivazione del criterio

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

## Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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