Risolvere i problemi relativi a oggetti e storage

StorageGRID

NetApp
March 21, 2025

Sommario

Risolvere i problemi relativi a oggetti e storage . . . 1
- Confermare le posizioni dei dati degli oggetti . . . 1
- Errori dell'archivio di oggetti (volume di storage) . . . 3
- Verificare l'integrità dell'oggetto . . . 5
  - Che cos'è la verifica in background? . . . 6
  - Che cos'è il controllo dell'esistenza di un oggetto? . . . 8
- Risoluzione dei problemi S3 - Avviso DIMENSIONE oggetto troppo grande . . . 12
- Risolvere i problemi relativi ai dati degli oggetti persi e mancanti . . . 15
  - Risoluzione dei problemi relativi ai dati degli oggetti persi e mancanti: Panoramica . . . 15
  - Esaminare gli oggetti persi . . . 15
  - Cercare e ripristinare oggetti potenzialmente persi . . . 21
  - Ripristinare i conteggi degli oggetti persi e mancanti . . . 27
- Risolvere i problemi relativi all'avviso di storage dei dati a oggetti in esaurimento . . . 28
- Risolvere i problemi relativi agli avvisi di override del watermark di sola lettura bassa . . . 30
  - Comprendere l'avviso . . . 31
  - Risolvere l'avviso . . . 31
- Risolvere i problemi relativi all'allarme Storage Status (SST) . . . 34
- Risoluzione dei problemi relativi all'erogazione dei messaggi dei servizi della piattaforma (allarme SMTT) 38

Risolvere i problemi relativi a oggetti e storage

Confermare le posizioni dei dati degli oggetti

A seconda del problema, potrebbe essere necessario "confermare la posizione in cui vengono memorizzati i dati dell'oggetto". Ad esempio, è possibile verificare che il criterio ILM funzioni come previsto e che i dati degli oggetti vengano memorizzati dove previsto.

Prima di iniziare

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
  - **UUID**: Identificativo universalmente univoco dell'oggetto. Inserire l'UUID in tutte le lettere maiuscole.
  - **CBID**: Identificatore univoco dell'oggetto all'interno di StorageGRID . È possibile ottenere il CBID di un oggetto dal log di audit. Inserire il CBID in tutte le lettere maiuscole.
  - **S3 bucket and object key** (bucket S3 e chiave oggetto): Quando un oggetto viene acquisito tramite "Interfaccia S3", l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto.
  - **Swift container and object name**: Quando un oggetto viene acquisito tramite "Interfaccia Swift", l'applicazione client utilizza una combinazione di container e nome oggetto per memorizzare e identificare l'oggetto.

Fasi

1. Selezionare **ILM** > **Object metadata lookup**.
2. Digitare l'identificativo dell'oggetto nel campo **Identifier**.

   È possibile immettere UUID, CBID, S3 bucket/object-key o Swift container/object-name.

3. Se si desidera cercare una versione specifica dell'oggetto, inserire l'ID versione (facoltativo).

4. Selezionare **Cerca**.

   Il "risultati della ricerca dei metadati degli oggetti" appare. In questa pagina sono elencati i seguenti tipi di informazioni:

   - Metadati di sistema, tra cui l'ID oggetto (UUID), l'ID versione (facoltativo), il nome dell'oggetto, il nome del contenitore, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.
   - Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.

- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
- Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

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

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```

Errori dell’archivio di oggetti (volume di storage)

Lo storage sottostante su un nodo di storage è diviso in archivi di oggetti. Gli archivi di oggetti sono anche noti come volumi di storage.

È possibile visualizzare le informazioni sull’archivio di oggetti per ciascun nodo di storage. Gli archivi di oggetti sono visualizzati nella parte inferiore della pagina **NODE** > ***Storage Node*** > **Storage**.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

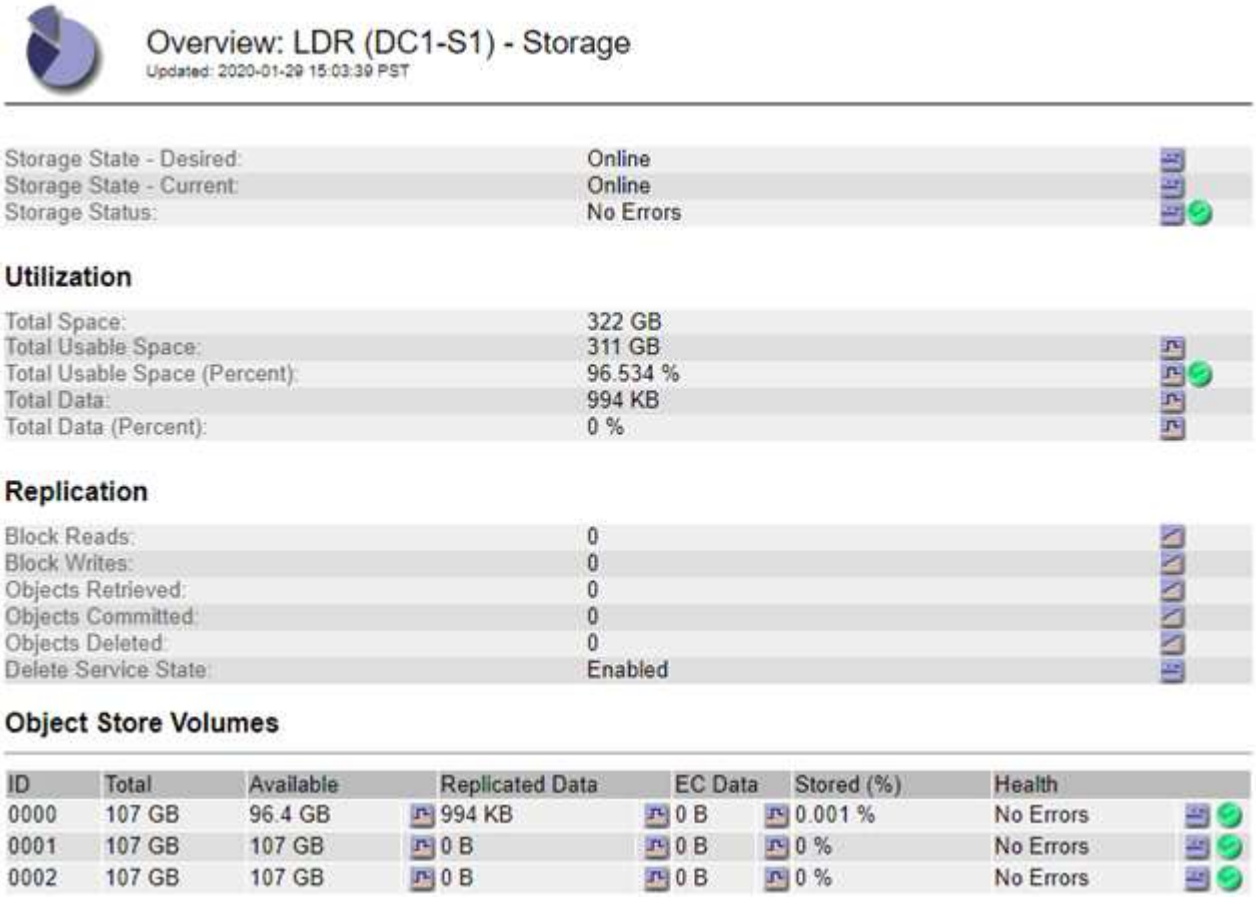
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Per saperne di più "Dettagli su ciascun nodo di storage", attenersi alla seguente procedura:

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Storage** > **Overview** > **Main**.



A seconda della natura del guasto, gli errori di un volume di storage potrebbero essere riflessi in un allarme sullo stato di storage o sullo stato di un archivio di oggetti. In caso di guasto di un volume di storage, è necessario riparare il volume di storage guasto per ripristinare la funzionalità completa del nodo di storage il prima possibile. Se necessario, accedere alla scheda **Configurazione** e. "Posizionare il nodo di storage in uno stato di sola-lettura" In modo che il sistema StorageGRID possa utilizzarlo per il recupero dei dati durante la preparazione per un ripristino completo del server.

Verificare l'integrità dell'oggetto

Il sistema StorageGRID verifica l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti corrotti e mancanti.

Esistono due processi di verifica: Verifica in background e verifica dell'esistenza degli oggetti (in precedenza chiamata verifica in primo piano). Lavorano insieme per garantire l'integrità dei dati. La verifica in background viene eseguita automaticamente e verifica continuamente la correttezza dei dati dell'oggetto. Il controllo dell'esistenza degli oggetti può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) degli oggetti.

Che cos'è la verifica in background?

Il processo di verifica in background verifica automaticamente e continuamente la presenza di copie corrotte dei dati degli oggetti nei nodi di storage e tenta automaticamente di risolvere eventuali problemi rilevati.

La verifica in background verifica l'integrità degli oggetti replicati e degli oggetti con codifica in cancellazione, come segue:

- **Oggetti replicati**: Se il processo di verifica in background trova un oggetto replicato corrotto, la copia corrotta viene rimossa dalla sua posizione e messa in quarantena in un altro punto del nodo di storage. Quindi, viene generata e posizionata una nuova copia non danneggiata per soddisfare le policy ILM attive. La nuova copia potrebbe non essere inserita nel nodo di storage utilizzato per la copia originale.

  > I dati degli oggetti corrotti vengono messi in quarantena invece che cancellati dal sistema, in modo che sia ancora possibile accedervi. Per ulteriori informazioni sull'accesso ai dati degli oggetti in quarantena, contattare il supporto tecnico.

- **Oggetti con codifica di cancellazione**: Se il processo di verifica in background rileva che un frammento di un oggetto con codifica di cancellazione è corrotto, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage, utilizzando i dati rimanenti e i frammenti di parità. Se il frammento danneggiato non può essere ricostruito, viene eseguito un tentativo di recuperare un'altra copia dell'oggetto. Se il recupero ha esito positivo, viene eseguita una valutazione ILM per creare una copia sostitutiva dell'oggetto con codice di cancellazione.

  Il processo di verifica in background controlla solo gli oggetti sui nodi di storage. Non controlla gli oggetti nei nodi di archiviazione o in un pool di storage cloud. Gli oggetti devono avere più di quattro giorni di età per poter essere qualificati per la verifica in background.

La verifica in background viene eseguita a una velocità continua che non interferisce con le normali attività del sistema. Impossibile interrompere la verifica in background. Tuttavia, se si sospetta un problema, è possibile aumentare il tasso di verifica in background per verificare più rapidamente il contenuto di un nodo di storage.

Avvisi e allarmi (legacy) relativi alla verifica in background

Se il sistema rileva un oggetto corrotto che non è in grado di correggere automaticamente (perché il danneggiamento impedisce l'identificazione dell'oggetto), viene attivato l'avviso **rilevato oggetto corrotto non identificato**.

Se la verifica in background non riesce a sostituire un oggetto corrotto perché non riesce a individuare un'altra copia, viene attivato l'avviso **oggetti persi**.

Modificare il tasso di verifica in background

È possibile modificare la velocità con cui la verifica in background controlla i dati degli oggetti replicati su un nodo di storage in caso di dubbi sull'integrità dei dati.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

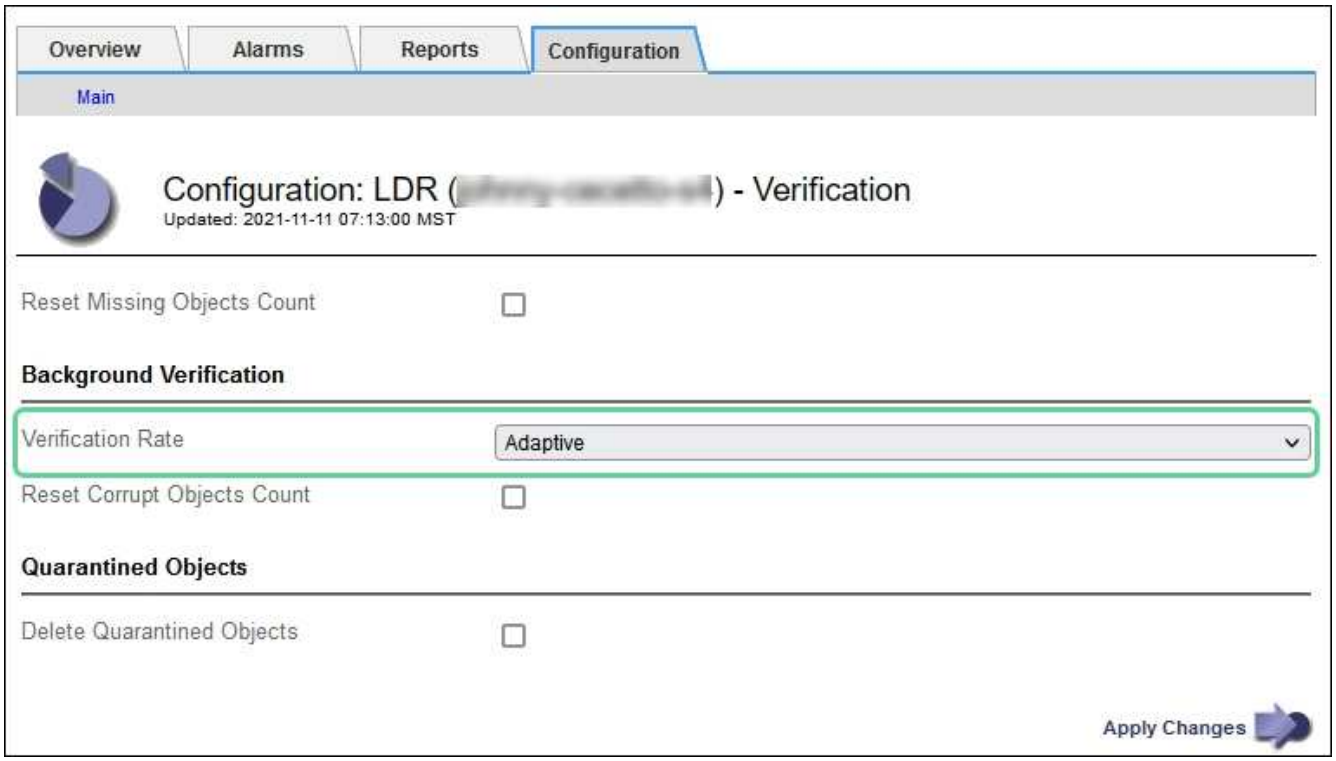
È possibile modificare il tasso di verifica per la verifica in background su un nodo di storage:

- Adattivo: Impostazione predefinita. L'attività è progettata per la verifica a un massimo di 4 MB/s o 10 oggetti/s (a seconda di quale valore viene superato per primo).
- Elevato: La verifica dello storage procede rapidamente, a una velocità che può rallentare le normali attività del sistema.

Utilizzare la frequenza di verifica alta solo quando si sospetta che un errore hardware o software possa avere dati oggetto corrotti. Una volta completata la verifica in background con priorità alta, la velocità di verifica viene ripristinata automaticamente su Adaptive.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Storage Node*** > **LDR** > **Verification**.
3. Selezionare **Configurazione** > **principale**.
4. Accedere a **LDR** > **verifica** > **Configurazione** > **principale**.
5. In background Verification (verifica in background), selezionare **Verification Rate** (tasso di verifica) > **High** (Alto) o **Verification Rate** (tasso di verifica) > **Adaptive** (



Impostando la frequenza di verifica su alta, si attiva l'allarme VPRI (tasso di verifica) legacy a livello di avviso.

6. Fare clic su **Applica modifiche**.
7. Monitorare i risultati della verifica in background per gli oggetti replicati.
   a. Andare a **NODES** > ***Storage Node*** > **Objects**.
   b. Nella sezione verifica, monitorare i valori per **oggetti corrotti** e **oggetti corrotti non identificati**.

      Se la verifica in background trova dati di oggetti replicati corrotti, la metrica **Corrupt Objects** viene incrementata e StorageGRID tenta di estrarre l'identificatore di oggetti dai dati, come segue:

- Se è possibile estrarre l'identificativo dell'oggetto, StorageGRID crea automaticamente una nuova copia dei dati dell'oggetto. La nuova copia può essere effettuata in qualsiasi punto del sistema StorageGRID che soddisfi le policy ILM attive.
- Se l'identificatore dell'oggetto non può essere estratto (perché è stato danneggiato), la metrica **Corrupt Objects Unidentified** viene incrementata e viene attivato l'avviso **Unidentified corrotto object detected**.

c. Se vengono rilevati dati di oggetti replicati corrotti, contattare il supporto tecnico per determinare la causa principale del danneggiamento.

8. Monitorare i risultati della verifica in background per gli oggetti con codifica erasure.

   Se la verifica in background trova frammenti corrotti di dati di oggetti con codifica di cancellazione, l'attributo corrotto Fragments Detected (frammenti corrotti rilevati) viene incrementato. StorageGRID esegue il ripristino ricostruendo il frammento corrotto in posizione sullo stesso nodo di storage.

   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Storage Node*** > **LDR** > **Erasure Coding**.
   c. Nella tabella Verification Results (risultati verifica), monitorare l'attributo corrotto Fragments Detected (ECCD).

9. Una volta ripristinati automaticamente gli oggetti corrotti dal sistema StorageGRID, ripristinare il numero di oggetti corrotti.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
   c. Selezionare **Ripristina conteggio oggetti corrotti**.
   d. Fare clic su **Applica modifiche**.

10. Se sei sicuro che gli oggetti in quarantena non sono necessari, puoi eliminarli.

    > Se viene attivato l'allarme **oggetti persi** o l'allarme legacy PERSI (oggetti persi), il supporto tecnico potrebbe voler accedere agli oggetti in quarantena per eseguire il debug del problema sottostante o tentare il ripristino dei dati.

    a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
    b. Selezionare ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
    c. Selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).
    d. Selezionare **Applica modifiche**.

Che cos'è il controllo dell'esistenza di un oggetto?

Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti non verifica i dati degli oggetti stessi (la verifica in background lo fa), ma fornisce un modo per verificare l'integrità dei dispositivi di storage, soprattutto se un recente problema hardware potrebbe avere influenzato l'integrità dei dati.

A differenza della verifica in background, che si verifica automaticamente, è necessario avviare manualmente un lavoro di verifica dell'esistenza di un oggetto.

Il controllo dell'esistenza degli oggetti legge i metadati di ogni oggetto memorizzato in StorageGRID e verifica

l'esistenza di copie di oggetti replicate e frammenti di oggetti codificati per la cancellazione. I dati mancanti vengono gestiti come segue:

- **Copie replicate**: Se manca una copia dei dati degli oggetti replicati, StorageGRID tenta automaticamente di sostituire la copia da una copia memorizzata altrove nel sistema. Il nodo di storage esegue una copia esistente attraverso una valutazione ILM, che determina che il criterio ILM corrente non è più soddisfatto per questo oggetto perché manca un'altra copia. Viene generata e posizionata una nuova copia per soddisfare i criteri ILM attivi del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa posizione in cui è stata memorizzata la copia mancante.
- **Frammenti con codifica di cancellazione**: Se manca un frammento di un oggetto con codifica di cancellazione, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage utilizzando i frammenti rimanenti. Se il frammento mancante non può essere ricostruito (perché sono stati persi troppi frammenti), ILM tenta di trovare un'altra copia dell'oggetto, che può utilizzare per generare un nuovo frammento con codifica di cancellazione.

Eseguire il controllo dell'esistenza dell'oggetto

Viene creato ed eseguito un job di controllo dell'esistenza di un oggetto alla volta. Quando si crea un processo, selezionare i nodi di archiviazione e i volumi che si desidera verificare. È inoltre possibile selezionare la coerenza per il lavoro.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Hai garantito che i nodi di storage che desideri controllare siano online. Selezionare **NODES** per visualizzare la tabella dei nodi. Assicurarsi che non venga visualizzata alcuna icona di avviso accanto al nome del nodo per i nodi che si desidera controllare.
- Si è verificato che le seguenti procedure siano **non** in esecuzione sui nodi che si desidera controllare:
  - Espansione della griglia per aggiungere un nodo di storage
  - Decommissionare il nodo di storage
  - Ripristino di un volume di storage guasto
  - Ripristino di un nodo di storage con un disco di sistema guasto
  - Ribilanciamento EC
  - Clone del nodo dell'appliance

Il controllo dell'esistenza degli oggetti non fornisce informazioni utili durante l'esecuzione di queste procedure.

A proposito di questa attività

Il completamento di un processo di verifica dell'esistenza di un oggetto può richiedere giorni o settimane, in base al numero di oggetti nella griglia, ai volumi e ai nodi di storage selezionati e alla coerenza selezionata. È possibile eseguire un solo processo alla volta, ma è possibile selezionare più nodi e volumi di storage contemporaneamente.

Fasi

1. Selezionare **MANUTENZIONE** > **attività** > **controllo dell'esistenza dell'oggetto**.
2. Selezionare **Crea job**. Viene visualizzata la procedura guidata Crea un processo di verifica dell'esistenza di un oggetto.
3. Selezionare i nodi contenenti i volumi che si desidera verificare. Per selezionare tutti i nodi online, selezionare la casella di controllo **Node name** (Nome nodo) nell'intestazione della colonna.

È possibile eseguire la ricerca in base al nome del nodo o al sito.

Non è possibile selezionare nodi che non sono connessi alla griglia.

4. Selezionare **continua**.
5. Selezionare uno o più volumi per ciascun nodo dell'elenco. È possibile cercare i volumi utilizzando il numero del volume di storage o il nome del nodo.

   Per selezionare tutti i volumi per ciascun nodo selezionato, selezionare la casella di controllo **Storage volume** nell'intestazione della colonna.

6. Selezionare **continua**.
7. Selezionare la coerenza per il lavoro.

   La coerenza determina il numero di copie dei metadati degli oggetti utilizzate per il controllo dell'esistenza dell'oggetto.

   - **Strong-site**: Due copie di metadati in un singolo sito.
   - **Strong-Global**: Due copie di metadati in ogni sito.
   - **Tutti** (impostazione predefinita): Tutte e tre le copie dei metadati di ciascun sito.

     Per ulteriori informazioni sulla coerenza, vedere le descrizioni nella procedura guidata.

8. Selezionare **continua**.
9. Controllare e verificare le selezioni. È possibile selezionare **Previous** (precedente) per passare a una fase precedente della procedura guidata e aggiornare le selezioni.

   Viene generato un job di controllo dell'esistenza di un oggetto che viene eseguito fino a quando non si verifica una delle seguenti condizioni:

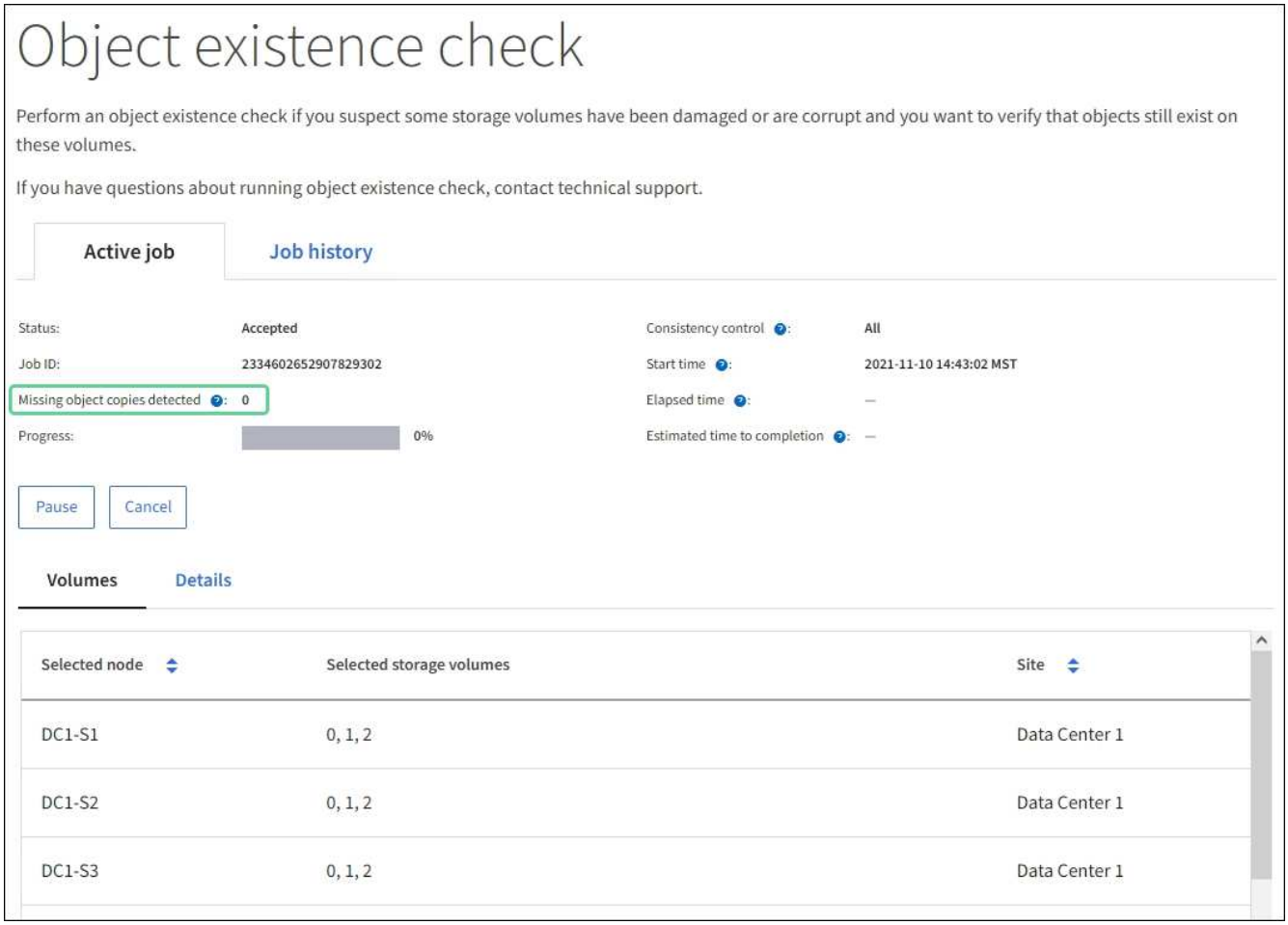
   - Il lavoro viene completato.
   - Il processo viene sospeso o annullato. È possibile riprendere un lavoro che è stato messo in pausa, ma non è possibile riprendere un lavoro che è stato annullato.
   - Il lavoro si blocca. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto bloccato**. Seguire le azioni correttive specificate per l'avviso.
   - Il lavoro non riesce. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto non riuscito**. Seguire le azioni correttive specificate per l'avviso.
   - Viene visualizzato il messaggio "Servizio non disponibile" o "errore interno del server". Dopo un minuto, aggiornare la pagina per continuare a monitorare il lavoro.

     > Se necessario, è possibile allontanarsi dalla pagina di controllo dell'esistenza dell'oggetto e tornare indietro per continuare a monitorare il lavoro.

10. Durante l'esecuzione del processo, visualizzare la scheda **lavoro attivo** e annotare il valore di copie oggetto mancanti rilevate.

    Questo valore rappresenta il numero totale di copie mancanti di oggetti replicati e di oggetti con codifica di cancellazione con uno o più frammenti mancanti.

    Se il numero di copie di oggetti mancanti rilevate è superiore a 100, potrebbe esserci un problema con lo storage del nodo di storage.



11. Una volta completato il lavoro, eseguire eventuali azioni aggiuntive richieste:
    - Se le copie oggetto mancanti rilevate sono pari a zero, non sono stati rilevati problemi. Non è richiesta alcuna azione.
    - Se vengono rilevate copie di oggetti mancanti maggiori di zero e l'avviso **oggetti persi** non è stato attivato, tutte le copie mancanti sono state riparate dal sistema. Verificare che eventuali problemi hardware siano stati corretti per evitare danni futuri alle copie degli oggetti.
    - Se le copie degli oggetti mancanti rilevate sono superiori a zero e viene attivato l'avviso **oggetti persi**, l'integrità dei dati potrebbe risentirne. Contattare il supporto tecnico.
    - È possibile analizzare le copie degli oggetti persi utilizzando grep per estrarre i messaggi di audit LLST: `grep LLST audit_file_name`.

      Questa procedura è simile a quella per "analisi degli oggetti smarriti", anche se per le copie di oggetto cercate `LLST` invece di `OLST`.

12. Se è stata selezionata la coerenza globale forte o strong-Site per il lavoro, attendere circa tre settimane per la coerenza dei metadati, quindi rieseguire nuovamente il lavoro sugli stessi volumi.

    Quando StorageGRID ha avuto il tempo di ottenere la coerenza dei metadati per i nodi e i volumi inclusi nel processo, la riesecuzione del processo potrebbe eliminare le copie degli oggetti mancanti segnalate erroneamente o causare il controllo di altre copie degli oggetti in caso di mancata esecuzione.

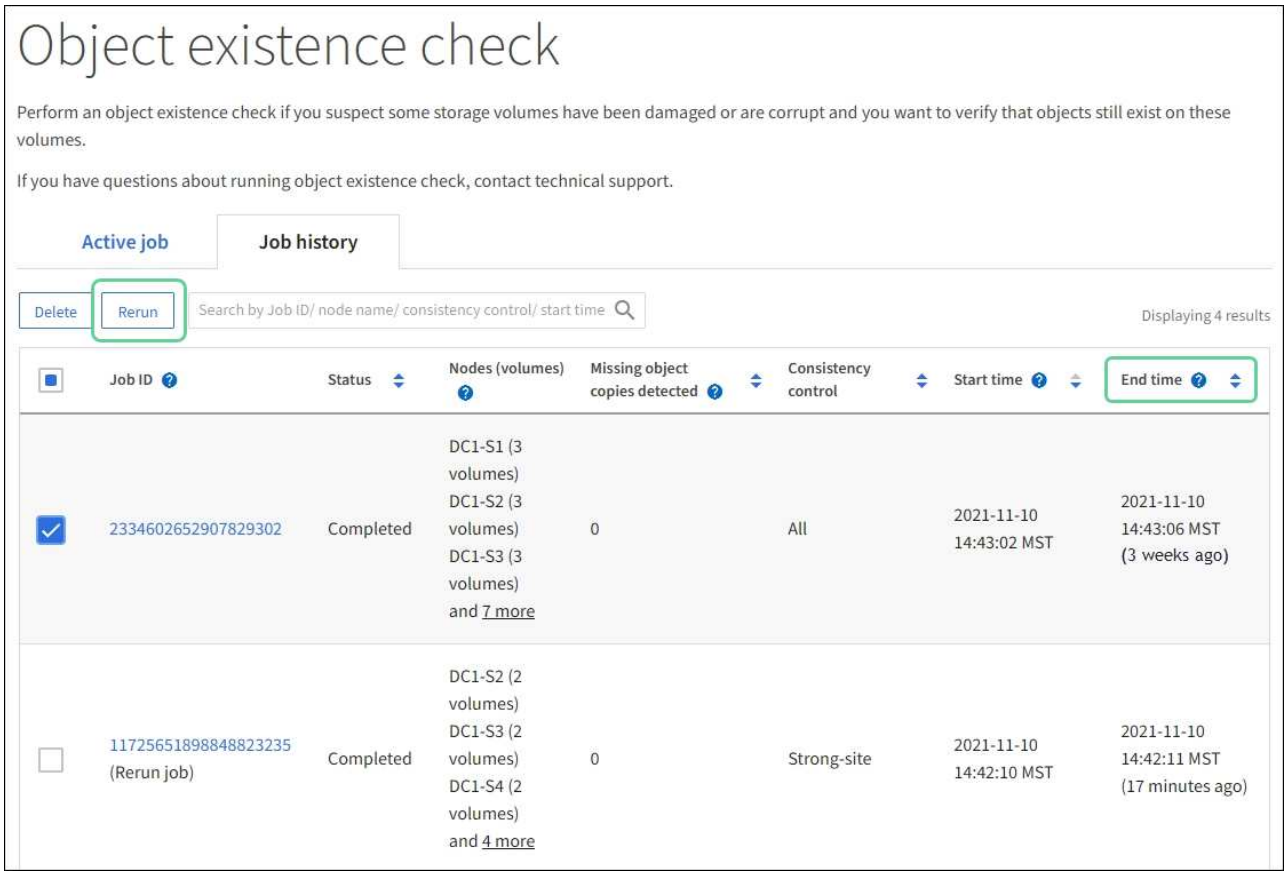
    a. Selezionare **MANUTENZIONE** > **verifica dell'esistenza dell'oggetto** > **Cronologia lavori**.

    b. Determinare quali lavori sono pronti per essere rieseguiti:

i. Esaminare la colonna **ora di fine** per determinare quali lavori sono stati eseguiti più di tre settimane fa.

ii. Per questi lavori, eseguire la scansione della colonna di controllo della coerenza per individuare la presenza di un sito forte o globale forte.

c. Selezionare la casella di controllo per ciascun processo che si desidera rieseguire, quindi selezionare **Rerun**.



d. Nella procedura guidata Riesegui lavori, esaminare i nodi e i volumi selezionati e la coerenza.

e. Quando si è pronti per rieseguire i lavori, selezionare **Rerun**.

Viene visualizzata la scheda lavoro attivo. Tutti i lavori selezionati vengono rieseguiti come un unico lavoro con una consistenza di sito sicuro. Un campo **lavori correlati** nella sezione Dettagli elenca gli ID lavoro per i lavori originali.

Al termine

Se hai ancora dubbi sull'integrità dei dati, vai a **SUPPORT** > **Tools** > **Grid topology** > ***Site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **Main** e aumenta il tasso di verifica in background. La verifica in background verifica la correttezza di tutti i dati degli oggetti memorizzati e ripara eventuali problemi rilevati. L'individuazione e la riparazione di potenziali problemi il più rapidamente possibile riduce il rischio di perdita di dati.

Risoluzione dei problemi S3 - Avviso DIMENSIONE oggetto troppo grande

L'avviso S3 PUT object size too large viene attivato se un tenant tenta un'operazione

PutObject non multiparte che supera il limite di dimensione S3 di 5 GiB.

Prima di iniziare

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

Determinare quali tenant utilizzano oggetti di dimensioni superiori a 5 GiB, in modo da poterli notificare.

Fasi

1. Accedere a **CONFIGURAZIONE** > **monitoraggio** > **server di audit e syslog**.
2. Se le scritture del client sono normali, accedere al registro di controllo:

   a. Invio `ssh admin@primary_Admin_Node_IP`

   b. Immettere la password elencata in `Passwords.txt` file.

   c. Immettere il seguente comando per passare a root: `su -`

   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

   e. Passare alla directory in cui si trovano i registri di controllo.

   La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	`/var/local/log/localaudit.log`
Nodi amministrativi/nodi locali	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
Server syslog esterno	`/var/local/log/localaudit.log`

   In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log` O. `/var/local/audit/export/`

   Per ulteriori informazioni, fare riferimento a "Selezionare le destinazioni delle informazioni di audit".

   f. Identificare i tenant che utilizzano oggetti di dimensioni superiori a 5 GiB.

      i. Invio `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

      ii. Per ogni messaggio di audit nei risultati, consultare `S3AI` Per determinare l'ID account tenant. Utilizzare gli altri campi del messaggio per determinare l'indirizzo IP utilizzato dal client, dal bucket e dall'oggetto:

Codice	Descrizione
SAIP	IP di origine
S3AI	ID tenant
S3BK	Bucket
S3KY	Oggetto
CSIZ	Dimensione (byte)

Esempio di risultati del registro di controllo

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"933908492661540043 43"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::933908492661540043 43:root"][SBAI(CSTR):"933908492661540043 43"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Se le scritture del client non sono normali, utilizzare l'ID tenant dell'avviso per identificare il tenant:

   a. Accedere a **SUPPORT** > **Tools** > **Logs**. Raccogliere i log delle applicazioni per il nodo di storage nell'avviso. Specificare 15 minuti prima e dopo l'avviso.

   b. Estrarre il file e accedere a. `bycast.log`:

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. Cercare nel registro `method=PUT` e identificare il client in `clientIP` campo.

      Esempio di bycast.log

      ```
      Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
      2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
      EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
      name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
      ```

4. Informare i locatari che la dimensione massima di PutObject è di 5 GiB e di utilizzare caricamenti multiparte per oggetti superiori a 5 GiB.

5. Ignorare l'avviso per una settimana se l'applicazione è stata modificata.

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Risoluzione dei problemi relativi ai dati degli oggetti persi e mancanti: Panoramica

Gli oggetti possono essere recuperati per diversi motivi, tra cui le richieste di lettura da un'applicazione client, le verifiche in background dei dati degli oggetti replicati, le rivalutazioni ILM e il ripristino dei dati degli oggetti durante il ripristino di un nodo di storage.

Il sistema StorageGRID utilizza le informazioni sulla posizione nei metadati di un oggetto per determinare da quale posizione recuperare l'oggetto. Se una copia dell'oggetto non viene trovata nella posizione prevista, il sistema tenta di recuperare un'altra copia dell'oggetto da un'altra parte del sistema, supponendo che il criterio ILM contenga una regola per eseguire due o più copie dell'oggetto.

Se il recupero riesce, il sistema StorageGRID sostituisce la copia mancante dell'oggetto. In caso contrario, viene attivato l'avviso **oggetti persi**, come segue:

- Per le copie replicate, se non è possibile recuperare un'altra copia, l'oggetto viene considerato perso e viene attivato l'avviso.
- Per le copie con erasure coding, se non è possibile recuperare una copia dalla posizione prevista, l'attributo copie danneggiate rilevate (ECOR) viene incrementato di uno prima di tentare di recuperare una copia da un'altra posizione. Se non viene trovata alcuna altra copia, viene attivato l'avviso.

Esaminare immediatamente tutti gli avvisi **oggetti persi** per determinare la causa principale della perdita e determinare se l'oggetto potrebbe ancora esistere in un nodo di storage o in un nodo di archivio offline o al momento non disponibile. Vedere "Esaminare gli oggetti persi".

Nel caso in cui i dati degli oggetti senza copie vadano persi, non esiste una soluzione di recovery. Tuttavia, è necessario reimpostare il contatore Lost Objects (oggetti persi) per evitare che oggetti persi noti mascherino eventuali nuovi oggetti persi. Vedere "Ripristinare i conteggi degli oggetti persi e mancanti".

Esaminare gli oggetti persi

Quando viene attivato l'avviso **oggetti persi**, è necessario eseguire un'analisi immediata. Raccogliere informazioni sugli oggetti interessati e contattare il supporto tecnico.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

L'avviso **oggetti persi** indica che StorageGRID ritiene che non vi siano copie di un oggetto nella griglia. I dati potrebbero essere stati persi in modo permanente.

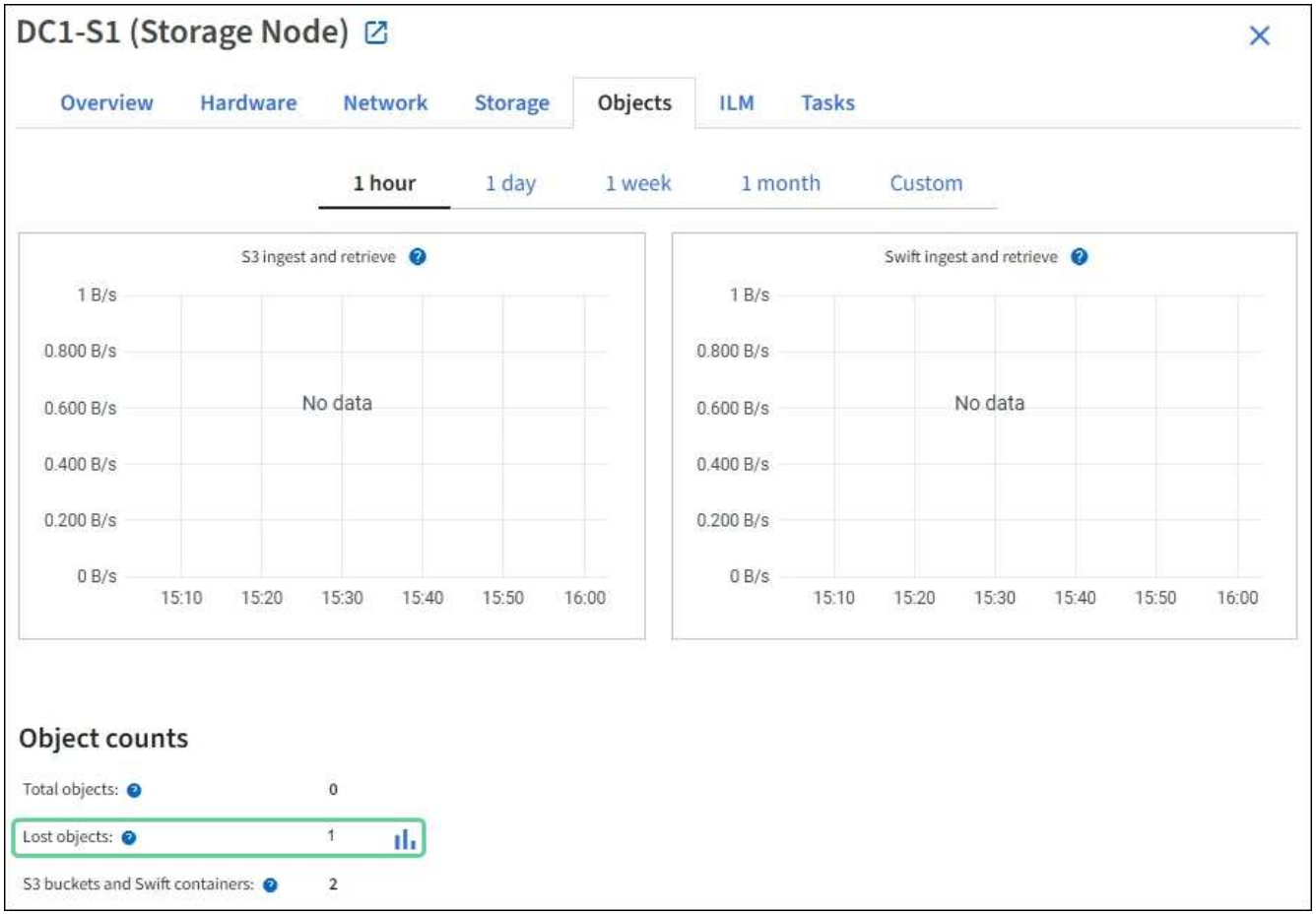
Esaminare immediatamente gli avvisi di oggetti smarriti. Potrebbe essere necessario intervenire per evitare ulteriori perdite di dati. In alcuni casi, potrebbe essere possibile ripristinare un oggetto perso se si esegue

un’azione rapida.

Fasi

1. Selezionare **NODI**.
2. Selezionare ***Storage Node*** > **Objects**.
3. Esaminare il numero di oggetti persi visualizzato nella tabella dei conteggi degli oggetti.

   Questo numero indica il numero totale di oggetti che il nodo della griglia rileva come mancanti dall’intero sistema StorageGRID. Il valore è la somma dei contatori Lost Objects del componente Data Store all’interno dei servizi LDR e DDS.



4. Da un nodo Admin, "accedere al registro di controllo" Per determinare l’identificatore univoco (UUID) dell’oggetto che ha attivato l’avviso **oggetti persi**:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l’accesso come root, il prompt cambia da `$` a. `#`.
   b. Passare alla directory in cui si trovano i registri di controllo.

      La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	`/var/local/log/localaudit.log`
Nodi amministrativi/nodi locali	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
Server syslog esterno	`/var/local/log/localaudit.log`

In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log` O. `/var/local/audit/export/`

Per ulteriori informazioni, fare riferimento a "Selezionare le destinazioni delle informazioni di audit".

c. Utilizzare grep per estrarre i messaggi di audit OLST (Object Lost). Inserire: `grep OLST audit_file_name`

d. Annotare il valore UUID incluso nel messaggio.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Utilizzare `ObjectByUUID` Comando per trovare l'oggetto in base al relativo identificatore (UUID), quindi determinare se i dati sono a rischio.

a. Utilizzare SSH per accedere a qualsiasi nodo storage. Quindi accedere alla console LDR digitando "telnet 0 1402".

b. Inserire: `/proc/OBRP/ObjectByUUID UUID_value`

In questo primo esempio, l'oggetto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` ha due posizioni elencate.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
```

```
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
```

```
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

Nel secondo esempio, l'oggetto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` non ha posizioni elencate.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Esaminare l'output di /proc/OBRP/ObjectByUUID e intraprendere l'azione appropriata:

Metadati	Conclusione
Nessun oggetto trovato ("ERRORE":"")	Se l'oggetto non viene trovato, viene visualizzato il messaggio "ERROR":". Se l'oggetto non viene trovato, è possibile azzerare il numero di **oggetti persi** per eliminare l'avviso. La mancanza di un oggetto indica che l'oggetto è stato intenzionalmente cancellato.
Posizioni > 0	Se nell'output sono presenti posizioni, l'avviso **oggetti persi** potrebbe essere un falso positivo. Verificare che gli oggetti esistano. Utilizzare l'ID nodo e il percorso del file elencati nell'output per confermare che il file a oggetti si trova nella posizione indicata. (La procedura per "ricerca di oggetti potenzialmente persi" Spiega come utilizzare l'ID nodo per trovare il nodo di storage corretto). Se gli oggetti sono presenti, è possibile ripristinare il numero di **oggetti persi** per cancellare l'avviso.
Posizioni = 0	Se nell'output non sono presenti posizioni, l'oggetto potrebbe essere mancante. Puoi provare "cercare e ripristinare l'oggetto" oppure puoi contattare il supporto tecnico. Il supporto tecnico potrebbe richiedere di determinare se è in corso una procedura di ripristino dello storage. Consultare le informazioni su "Ripristino dei dati degli oggetti mediante Grid Manager" e. "ripristino dei dati degli oggetti in un volume di storage".

Cercare e ripristinare oggetti potenzialmente persi

Potrebbe essere possibile trovare e ripristinare oggetti che hanno attivato un allarme Lost Objects (LOST Objects, oggetti persi) e un avviso **Object Lost** e che sono stati identificati come potenzialmente persi.

Prima di iniziare

- Si dispone dell'UUID di qualsiasi oggetto perso, come identificato nella "Esaminare gli oggetti persi".
- Hai il `Passwords.txt` file.

A proposito di questa attività

È possibile seguire questa procedura per cercare copie replicate dell'oggetto perso in un altro punto della griglia. Nella maggior parte dei casi, l'oggetto perso non viene trovato. Tuttavia, in alcuni casi, potrebbe essere possibile trovare e ripristinare un oggetto replicato perso se si esegue un'azione rapida.

Contattare il supporto tecnico per assistenza con questa procedura.

Fasi

1. Da un nodo amministratore, cercare nei registri di controllo le posizioni possibili degli oggetti:

a. Accedere al nodo Grid:

   i. Immettere il seguente comando: `ssh admin@grid_node_IP`

   ii. Immettere la password elencata in `Passwords.txt` file.

   iii. Immettere il seguente comando per passare a root: `su -`

   iv. Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

b. passare alla directory in cui si trovano i registri di controllo.

   La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	`/var/local/log/localaudit.log`
Nodi amministrativi/nodi locali	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
Server syslog esterno	`/var/local/log/localaudit.log`

   In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log` O. `/var/local/audit/export/`

   Per ulteriori informazioni, fare riferimento a "Selezionare le destinazioni delle informazioni di audit".

c. Utilizzare grep per estrarre "messaggi di audit associati all'oggetto potenzialmente perso" e inviarli a un file di output. Inserire: `grep uuid-valueaudit_file_name > output_file_name`

   Ad esempio:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

d. Utilizzare grep per estrarre i messaggi di controllo LLST (Location Lost) da questo file di output. Inserire: `grep LLST output_file_name`

   Ad esempio:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

   Un messaggio di controllo LLST è simile a questo messaggio di esempio.

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

e. Individuare il campo PCLD e IL campo NOID nel messaggio LLST.

Se presente, il valore di PCLD è il percorso completo sul disco verso la copia dell'oggetto replicato mancante. IL valore DI NOID è l'id del nodo dell'LDR in cui è possibile trovare una copia dell'oggetto.

Se si trova una posizione dell'oggetto, potrebbe essere possibile ripristinarlo.

a. Trova il nodo di storage associato a questo ID nodo LDR. In Grid Manager, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Data Center*** > ***Storage Node*** > **LDR**.

L'ID nodo per il servizio LDR si trova nella tabella Node Information (informazioni nodo). Esaminare le informazioni relative a ciascun nodo di storage fino a individuare quello che ospita questo LDR.

2. Determinare se l'oggetto esiste sul nodo di storage indicato nel messaggio di audit:

a. Accedere al nodo Grid:

i. Immettere il seguente comando: `ssh admin@grid_node_IP`

ii. Immettere la password elencata in `Passwords.txt` file.

iii. Immettere il seguente comando per passare a root: `su -`

iv. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

b. Determinare se il percorso del file per l'oggetto esiste.

Per il percorso file dell'oggetto, utilizzare il valore PCLD del messaggio di audit LLST.

Ad esempio, immettere:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Racchiudere sempre il percorso del file oggetto tra virgolette singole nei comandi per escapire eventuali caratteri speciali.

- Se il percorso dell'oggetto non viene trovato, l'oggetto viene perso e non può essere ripristinato utilizzando questa procedura. Contattare il supporto tecnico.
- Se viene trovato il percorso dell'oggetto, passare alla fase successiva. È possibile tentare di ripristinare l'oggetto trovato in StorageGRID.

3. Se il percorso dell'oggetto è stato trovato, tentare di ripristinare l'oggetto in StorageGRID:
   a. Dallo stesso nodo di storage, modificare la proprietà del file a oggetti in modo che possa essere gestito da StorageGRID. Inserire: `chown ldr-user:bycast 'file_path_of_object'`
   b. Utilizzare SSH per accedere a qualsiasi nodo storage. Quindi accedere alla console LDR digitando "telnet 0 1402".
   c. Inserire: `cd /proc/STOR`
   d. Inserire: `Object_Found 'file_path_of_object'`

      Ad esempio, immettere:

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Emissione di `Object\_Found` il comando notifica alla griglia la posizione dell'oggetto. Attiva inoltre i criteri ILM attivi, che eseguono copie aggiuntive come specificato in ciascun criterio.

      > Se il nodo di storage in cui è stato trovato l'oggetto non è in linea, è possibile copiare l'oggetto in qualsiasi nodo di storage in linea. Posizionare l'oggetto in qualsiasi directory /var/local/rangedb del nodo di storage online. Quindi, eseguire il `Object\_Found` utilizzando il percorso del file all'oggetto.

      - Se l'oggetto non può essere ripristinato, il `Object\_Found` comando non riuscito. Contattare il supporto tecnico.
      - Se l'oggetto è stato ripristinato correttamente in StorageGRID, viene visualizzato un messaggio di esito positivo. Ad esempio:

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

        Passare alla fase successiva.

4. Se l'oggetto è stato ripristinato correttamente in StorageGRID, verificare che siano state create nuove posizioni.
   a. Inserire: `cd /proc/OBRP`
   b. Inserire: `ObjectByUUID UUID_value`

      L'esempio seguente mostra che sono presenti due posizioni per l'oggetto con UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

      ```
      ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
      ```

```
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
```

```
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Disconnettersi dalla console LDR. Inserire: `exit`

5. Da un nodo di amministrazione, cercare nei registri di controllo il messaggio di audit ORLM relativo a questo oggetto per confermare che ILM (Information Lifecycle Management) ha inserito le copie come richiesto.

   a. Accedere al nodo Grid:

      i. Immettere il seguente comando: `ssh admin@grid_node_IP`

      ii. Immettere la password elencata in `Passwords.txt` file.

      iii. Immettere il seguente comando per passare a root: `su -`

      iv. Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

   b. Passare alla directory in cui si trovano i registri di controllo. Fare riferimento alla sottosezione 1. b.

   c. Utilizzare grep per estrarre i messaggi di audit associati all'oggetto in un file di output. Inserire: `grep uuid-valueaudit_file_name > output_file_name`

      Ad esempio:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      /var/local/tmp/messages_about_restored_object.txt
      ```

   d. Utilizzare grep per estrarre i messaggi di audit ORLM (Object Rules Met) da questo file di output. Inserire: `grep ORLM output_file_name`

      Ad esempio:

      ```
      Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
      ```

      Un messaggio di controllo ORLM è simile a questo messaggio di esempio.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Individuare il campo LOCS (POSIZIONI) nel messaggio di audit.

   Se presente, il valore di CLDI in LOCS è l'ID del nodo e l'ID del volume in cui è stata creata una copia dell'oggetto. Questo messaggio indica che l'ILM è stato applicato e che sono state create due copie di oggetti in due posizioni nella griglia.

6. "Ripristinare i conteggi degli oggetti persi e mancanti" In Grid Manager.

Ripristinare i conteggi degli oggetti persi e mancanti

Dopo aver esaminato il sistema StorageGRID e aver verificato che tutti gli oggetti persi registrati vengano persi in modo permanente o che si tratti di un falso allarme, è possibile azzerare il valore dell'attributo oggetti persi.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

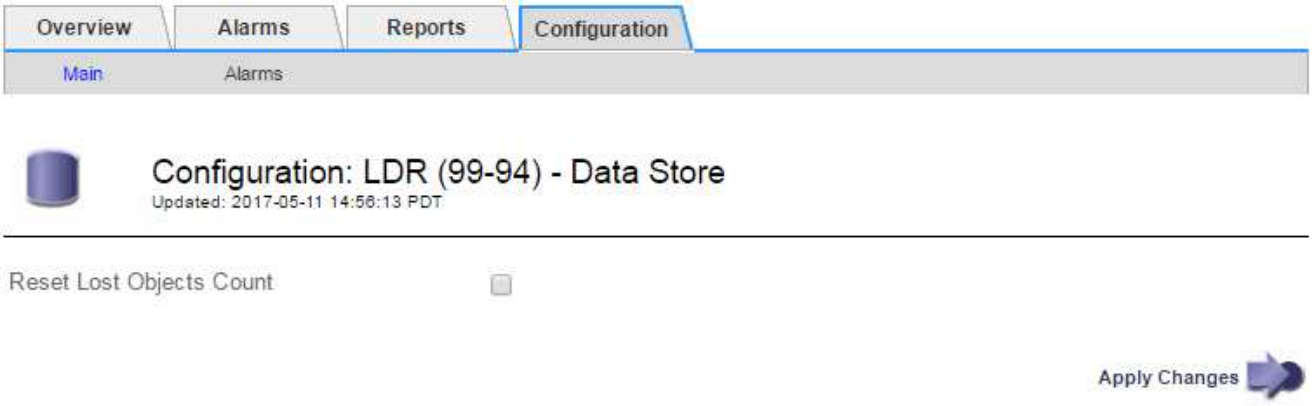
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

- **SUPPORT** > **Tools** > **Grid topology** > ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Overview** > **Main**
- **SUPPORTO** > **Strumenti** > **topologia griglia** > ***Sito*** > ***nodo di archiviazione*** > **DDS** > **Archivio dati** > **Panoramica** > **principale**

Queste istruzioni mostrano come azzerare il contatore dalla pagina **LDR** > **Data Store**.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Data Store** > **Configuration** per il nodo di storage che presenta l'avviso **Objects Lost** o l'allarme LOST.
3. Selezionare **Reset Lost Objects Count** (Ripristina conteggio oggetti persi).



4. Fare clic su **Applica modifiche**.

   L'attributo Lost Objects (oggetti persi) viene reimpostato su 0 e l'avviso **Objects lost** (oggetti persi) e l'allarme LOST (PERSO) vengono eliminati, che possono richiedere alcuni minuti.

5. Facoltativamente, reimpostare altri valori degli attributi correlati che potrebbero essere stati incrementati durante il processo di identificazione dell'oggetto perso.

   a. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Erasure Coding** > **Configuration**.

   b. Selezionare **Reset Reads Failure Count** e **Reset corrotto copies Detected Count**.

   c. Fare clic su **Applica modifiche**.

   d. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration**.

   e. Selezionare **Reset Missing Objects Count** e **Reset Corrupt Objects Count**.

   f. Se si è certi che gli oggetti in quarantena non siano necessari, selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).

      Gli oggetti in quarantena vengono creati quando la verifica in background identifica una copia di oggetti replicati corrotta. Nella maggior parte dei casi, StorageGRID sostituisce automaticamente l'oggetto corrotto ed è sicuro eliminare gli oggetti in quarantena. Tuttavia, se viene attivato l'allarme **oggetti persi** o L'allarme PERSO, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena.

   g. Fare clic su **Applica modifiche**.

   Dopo aver fatto clic su **Apply Changes** (Applica modifiche), il ripristino degli attributi può richiedere alcuni istanti.

Risolvere i problemi relativi all'avviso di storage dei dati a oggetti in esaurimento

L'avviso **Low Object Data Storage** monitora lo spazio disponibile per memorizzare i dati degli oggetti su ciascun nodo di storage.

Prima di iniziare

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

A proposito di questa attività

L'avviso **archiviazione dati oggetto bassa** viene attivato quando la quantità totale di dati oggetto replicati e con erasure coding su un nodo di archiviazione soddisfa una delle condizioni configurate nella regola di avviso.

Per impostazione predefinita, viene attivato un avviso importante quando questa condizione viene valutata come true:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In questa condizione:

- `storagegrid_storage_utilization_data_bytes` È una stima delle dimensioni totali dei dati di oggetti replicati e con erasure coding per un nodo storage.
- `storagegrid_storage_utilization_usable_space_bytes` È la quantità totale di spazio di storage a oggetti rimanente per un nodo di storage.

Se viene attivato un avviso **Low Object Data Storage** maggiore o minore, è necessario eseguire una procedura di espansione il prima possibile.

Fasi

1. Selezionare **ALERTS** > **current**.

   Viene visualizzata la pagina Avvisi.

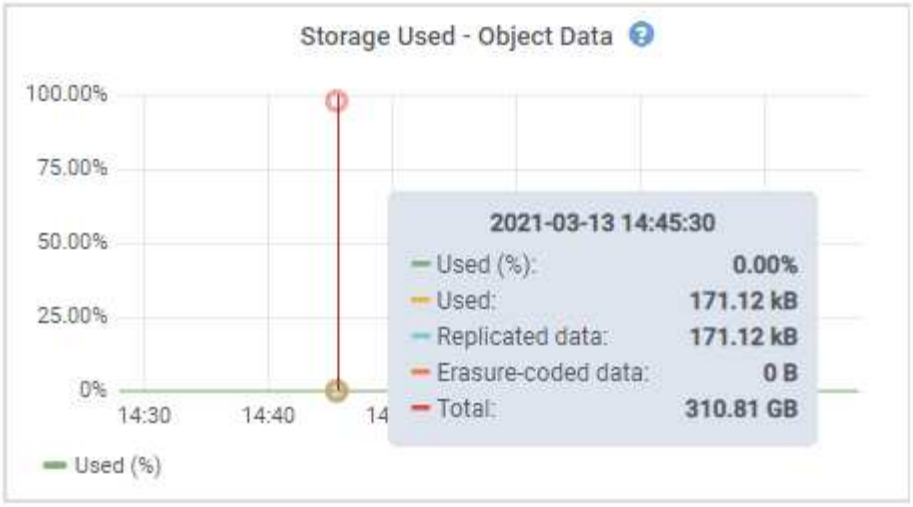
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low Object Data Storage**, se necessario, e selezionare l'avviso che si desidera visualizzare.

   Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.

3. Esaminare i dettagli nella finestra di dialogo e prendere nota di quanto segue:
   - Tempo di attivazione
   - Il nome del sito e del nodo
   - I valori correnti delle metriche per questo avviso
4. Selezionare **NODES** > ***Storage Node or Site*** > **Storage**.
5. Posizionare il cursore sul grafico Storage Used - Object Data (Storage utilizzato - dati oggetto).

   Vengono visualizzati i seguenti valori:

   - **Used (%)**: Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto.
   - **Used**: Quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
   - **Dati replicati**: Stima della quantità di dati degli oggetti replicati su questo nodo, sito o griglia.
   - **Erasure-coded data**: Stima della quantità di dati dell'oggetto con codifica di cancellazione su questo nodo, sito o griglia.
   - **Total**: Quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è `storagegrid_storage_utilization_data_bytes` metrico.



6. Selezionare i controlli dell'ora sopra il grafico per visualizzare l'utilizzo dello storage in diversi periodi di tempo.

   L'utilizzo dello storage nel tempo può aiutarti a capire la quantità di storage utilizzata prima e dopo l'attivazione dell'avviso e può aiutarti a stimare il tempo necessario per lo spazio rimanente del nodo.

7. Il più presto possibile, "aggiungere capacità di storage" alla tua griglia.

   È possibile aggiungere volumi di storage (LUN) ai nodi di storage esistenti oppure aggiungere nuovi nodi di storage.

   Per ulteriori informazioni, vedere "Gestire nodi storage completi".

Informazioni correlate

"Risoluzione dei problemi relativi all'allarme dello stato dello storage (SST) (legacy)"

Risolvere i problemi relativi agli avvisi di override del watermark di sola lettura bassa

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, potrebbe essere necessario risolvere l'avviso **bassa sostituzione filigrana di sola lettura**. Se possibile, aggiornare il sistema per iniziare a utilizzare i valori ottimizzati.

Nelle release precedenti, le tre "filigrane dei volumi di storage" Erano impostazioni globali e n. 8212; gli stessi valori applicati a ogni volume di storage su ogni nodo di storage. A partire da StorageGRID 11.6, il software può ottimizzare queste filigrane per ogni volume di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

Quando si esegue l'aggiornamento a StorageGRID 11.6 o versioni successive, le filigrane ottimizzate di sola lettura e di lettura/scrittura vengono applicate automaticamente a tutti i volumi di storage, a meno che non si verifichino le seguenti condizioni:

- Il sistema è vicino alla capacità e non è in grado di accettare nuovi dati se sono state applicate filigrane ottimizzate. In questo caso, StorageGRID non modificherà le impostazioni della filigrana.
- In precedenza, le filigrane dei volumi di storage sono state impostate su un valore personalizzato.

StorageGRID non sovrascrive le impostazioni personalizzate del watermark con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso **override filigrana di sola lettura bassa** se il valore personalizzato per la filigrana di sola lettura morbida del volume di storage è troppo piccolo.

Comprendere l'avviso

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, l'avviso **Low Read-only watermark override** potrebbe essere attivato per uno o più nodi di storage.

Ogni istanza dell'avviso indica che il valore personalizzato di **Storage Volume Soft Read-Only Watermark** è inferiore al valore minimo ottimizzato per quel nodo di storage. Se si continua a utilizzare l'impostazione personalizzata, lo spazio del nodo di storage potrebbe essere molto basso prima di poter passare in sicurezza allo stato di sola lettura. Alcuni volumi di storage potrebbero diventare inaccessibili (automaticamente smontati) quando il nodo raggiunge la capacità.

Ad esempio, si supponga di aver precedentemente impostato la filigrana di sola lettura **Storage Volume Soft** su 5 GB. Supponiamo ora che StorageGRID abbia calcolato i seguenti valori ottimizzati per i quattro volumi di storage nel nodo di storage A:

Volume 0	12 GB
Volume 1	12 GB
Volume 2	11 GB
Volume 3	15 GB

L'avviso **Low Read-only watermark override** viene attivato per il nodo di storage A perché il watermark personalizzato (5 GB) è inferiore al valore minimo ottimizzato per tutti i volumi in quel nodo (11 GB). Se si continua a utilizzare l'impostazione personalizzata, lo spazio del nodo potrebbe essere estremamente ridotto prima di poter passare in sicurezza allo stato di sola lettura.

Risolvere l'avviso

Seguire questa procedura se sono stati attivati uno o più avvisi **Low Read-only watermark override**. È inoltre possibile utilizzare queste istruzioni se si utilizzano impostazioni personalizzate per la filigrana e si desidera iniziare a utilizzare impostazioni ottimizzate anche se non sono stati attivati avvisi.

Prima di iniziare

- L'aggiornamento a StorageGRID 11.6 o versione successiva è stato completato.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

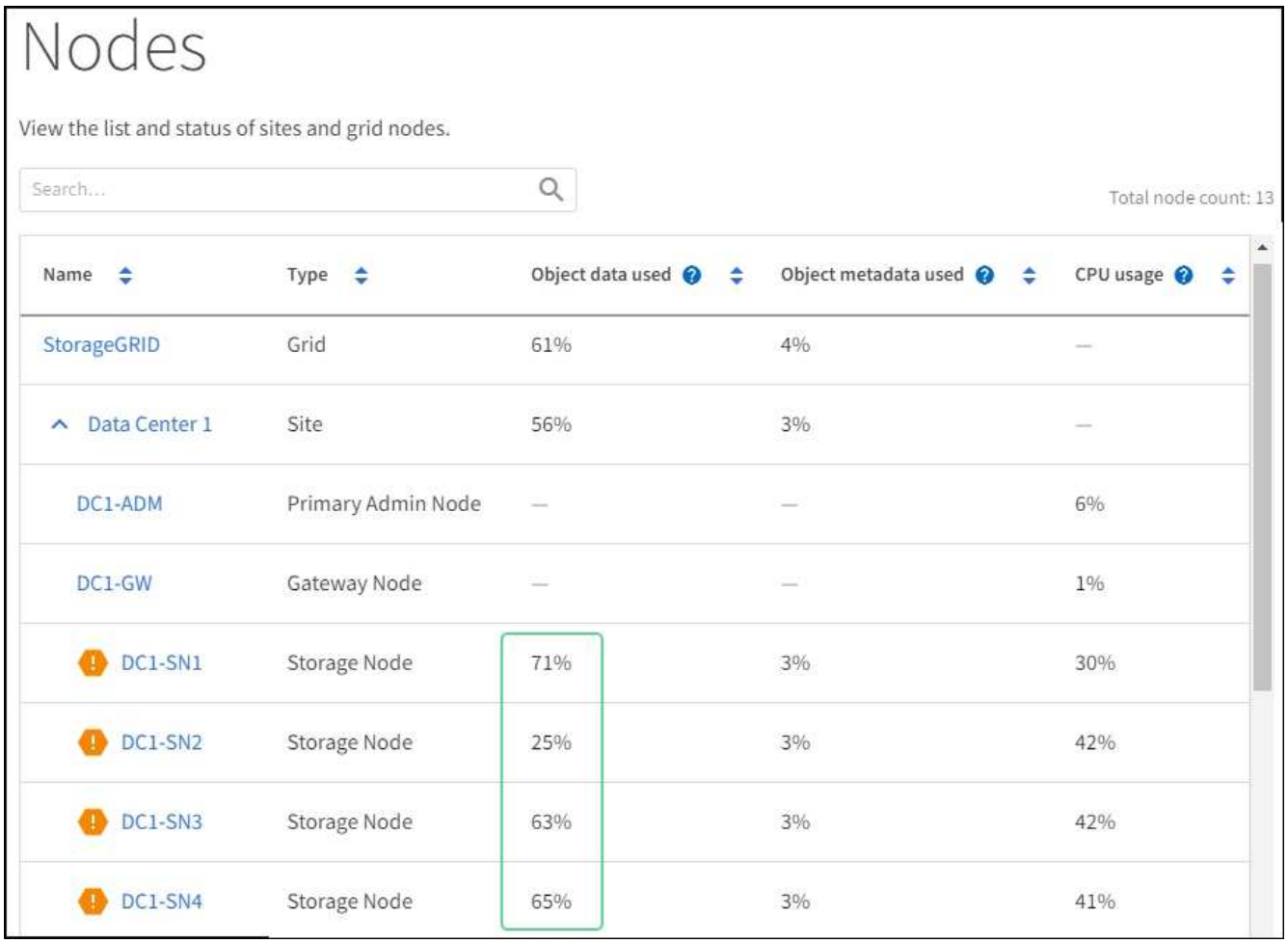
A proposito di questa attività

È possibile risolvere l'avviso **deroga filigrana di sola lettura bassa** aggiornando le impostazioni di filigrana personalizzate con le nuove sostituzioni della filigrana. Tuttavia, se uno o più nodi di storage sono quasi pieni o si hanno requisiti ILM speciali, è necessario prima visualizzare le filigrane di storage ottimizzate e determinare se è sicuro utilizzarle.

Valutare l'utilizzo dei dati a oggetti per l'intero grid

Fasi

1. Selezionare **NODI**.
2. Per ogni sito nella griglia, espandere l'elenco dei nodi.
3. Esaminare i valori percentuali mostrati nella colonna **dati oggetto utilizzati** per ciascun nodo di storage in ogni sito.



4. Seguire la procedura appropriata:
   a. Se nessuno dei nodi di storage è quasi pieno (ad esempio, tutti i valori **dati oggetto utilizzati** sono inferiori al 80%), è possibile iniziare a utilizzare le impostazioni di override. Passare a. Utilizzare filigrane ottimizzate.
   b. Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se i pool di storage specifici sono quasi completi, eseguire i passaggi descritti in Visualizza filigrane di storage ottimizzate e. Determinare se è possibile utilizzare filigrane ottimizzate.

Visualizza filigrane di memorizzazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati che ha calcolato per la filigrana di sola lettura del volume di storage **Soft Read-only**. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Metrics**.
2. Nella sezione Prometheus, selezionare il collegamento per accedere all'interfaccia utente Prometheus.
3. Per visualizzare la filigrana minima di sola lettura soft consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore minimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage. Se questo valore è superiore all'impostazione personalizzata per **Storage Volume Soft Read-Only Watermark**, viene attivato l'avviso **Low Read-only watermark override** per il nodo di storage.

4. Per visualizzare la filigrana di sola lettura soft massima consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore massimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage.

5. Nota sul valore massimo ottimizzato per ciascun nodo di storage.

[[determina-filigrane ottimizzate]]determinare se è possibile utilizzare filigrane ottimizzate

Fasi

1. Selezionare **NODI**.
2. Ripetere questi passaggi per ogni nodo di storage online:
   a. Selezionare ***Storage Node*** > **Storage**.
   b. Scorrere verso il basso fino alla tabella degli archivi di oggetti.
   c. Confrontare il valore **Available** per ciascun archivio di oggetti (volume) con il watermark ottimizzato massimo annotato per quel nodo di storage.
3. Se almeno un volume su ogni nodo di storage online ha più spazio disponibile rispetto al watermark ottimizzato massimo per quel nodo, visitare il sito Web Utilizzare filigrane ottimizzate per iniziare a utilizzare le filigrane ottimizzate.

   In caso contrario, espandere la griglia il prima possibile. Entrambi "aggiungere volumi di storage" a un nodo esistente o. "Aggiungere nuovi nodi di storage". Quindi, passare a. Utilizzare filigrane ottimizzate per aggiornare le impostazioni della filigrana.

4. Se è necessario continuare a utilizzare valori personalizzati per le filigrane del volume di storage, "silenzio" oppure "disattiva" L'avviso **deroga filigrana di sola lettura bassa**.

   > Gli stessi valori di watermark personalizzati vengono applicati a ogni volume di storage su ogni nodo di storage. L'utilizzo di valori inferiori a quelli consigliati per le filigrane dei volumi di storage potrebbe causare l'inaccessibilità di alcuni volumi di storage (automaticamente smontati) quando il nodo raggiunge la capacità.

utilizza filigrane ottimizzate

Fasi

1. Andare a **SUPPORT** > **other** > **Storage Watermarks**.
2. Selezionare la casella di controllo **Usa valori ottimizzati**.
3. Selezionare **Salva**.

Le impostazioni ottimizzate del watermark del volume di storage sono ora attive per ciascun volume di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

Risolvere i problemi relativi all'allarme Storage Status (SST)

L'allarme Storage Status (SST) viene attivato se un nodo di storage non dispone di spazio libero sufficiente per lo storage a oggetti.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

L'allarme SSTS (Storage Status) viene attivato a livello di Notice quando la quantità di spazio libero su ogni volume in un nodo di storage scende al di sotto del valore del watermark Storage Volume Soft Read Only (**CONFIGURATION** > **System** > **Storage options**).

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

Ad esempio, si supponga che la filigrana Storage Volume Soft Read-Only sia impostata su 10 GB, che è il valore predefinito. L'allarme SSTS viene attivato se su ciascun volume di storage nel nodo di storage rimangono meno di 10 GB di spazio utilizzabile. Se uno dei volumi dispone di almeno 10 GB di spazio disponibile, l'allarme non viene attivato.

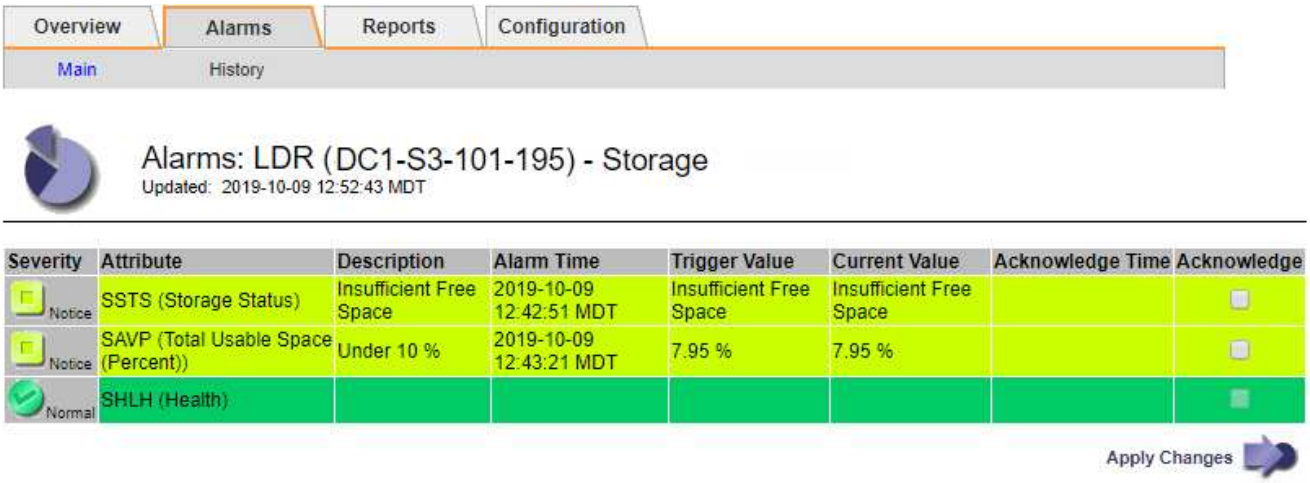
Se è stato attivato un allarme SSTS, è possibile seguire questa procedura per comprendere meglio il problema.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.

2. Dalla colonna Service (Servizio), selezionare il data center, il nodo e il servizio associati all'allarme SSTS.

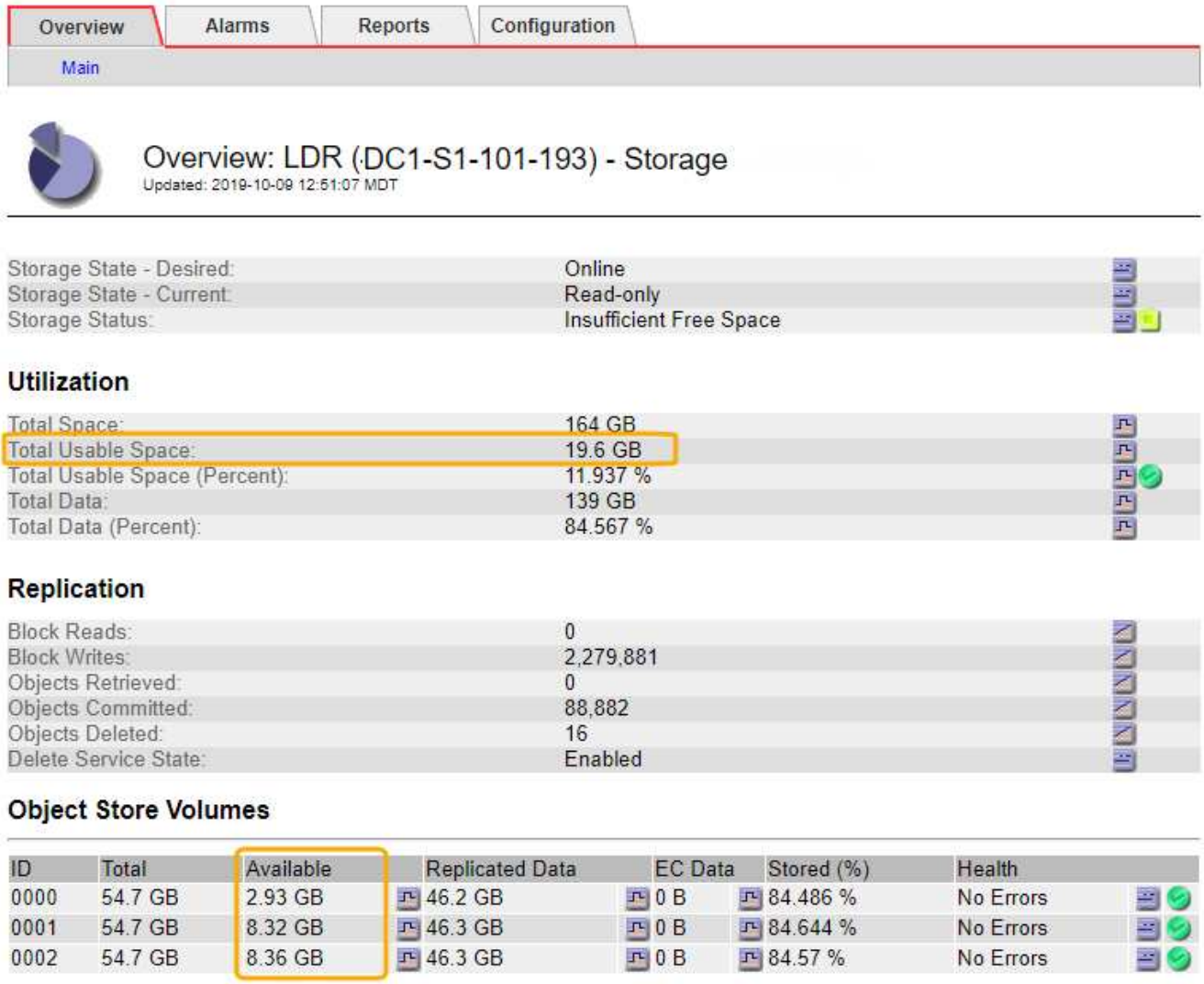
   Viene visualizzata la pagina Grid Topology (topologia griglia). La scheda Allarmi mostra gli allarmi attivi per il nodo e il servizio selezionato.



   In questo esempio, gli allarmi SST (Storage Status) e SAVP (Total usable Space (Percent)) sono stati attivati a livello di notifica.

   > In genere, sia l'allarme SSTS che l'allarme SAVP vengono attivati circa contemporaneamente; tuttavia, l'attivazione di entrambi gli allarmi dipende dall'impostazione del watermark in GB e dall'impostazione dell'allarme SAVP in percentuale.

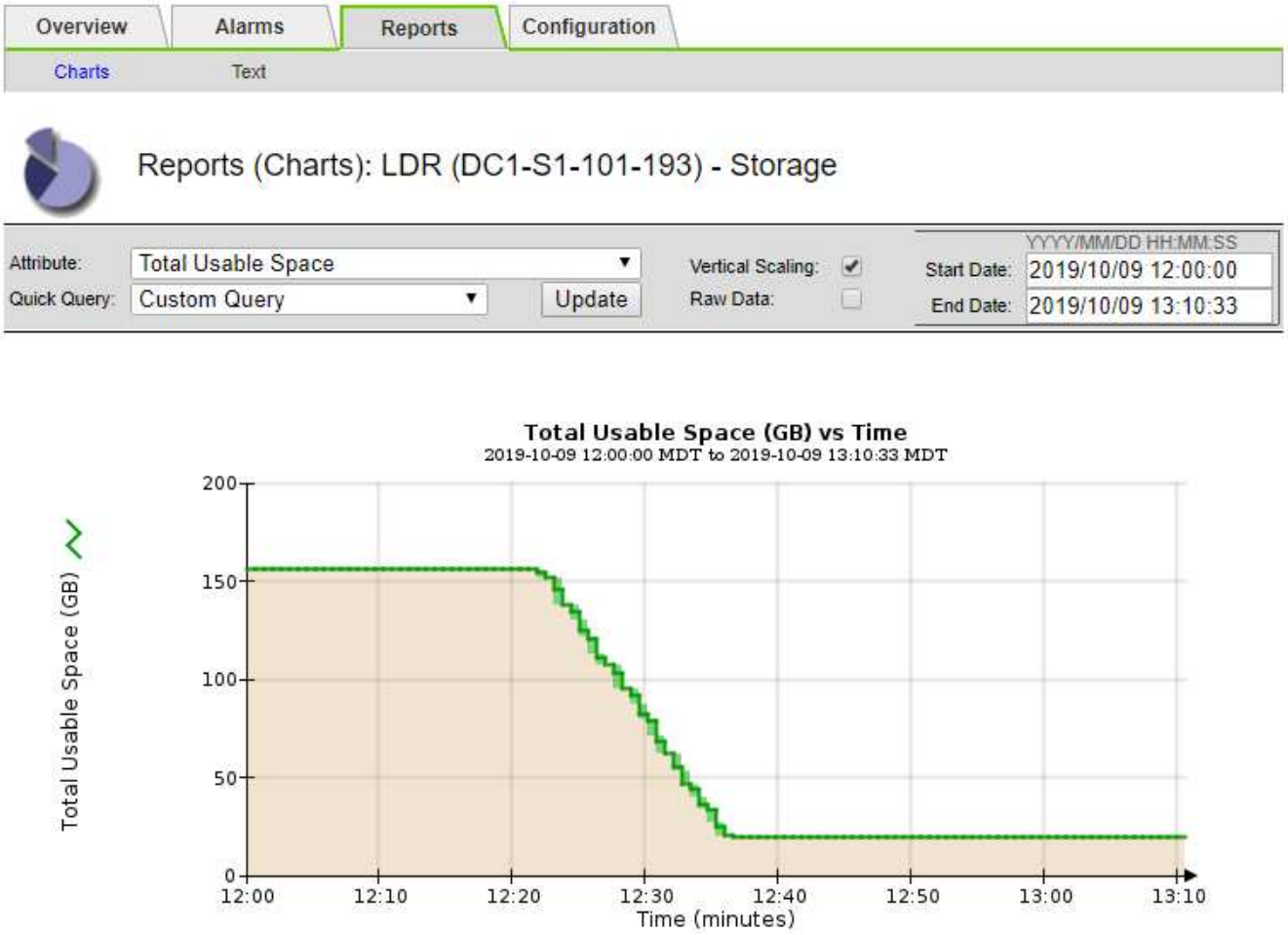
3. Per determinare la quantità di spazio utilizzabile effettivamente disponibile, selezionare **LDR** > **Storage** > **Overview** e individuare l'attributo Total Usable Space (STAS).



In questo esempio, rimangono disponibili solo 19.6 GB dei 164 GB di spazio su questo nodo di storage. Si noti che il valore totale è la somma dei valori **Available** per i tre volumi dell'archivio di oggetti. L'allarme SSTS è stato attivato perché ciascuno dei tre volumi di storage aveva meno di 10 GB di spazio disponibile.

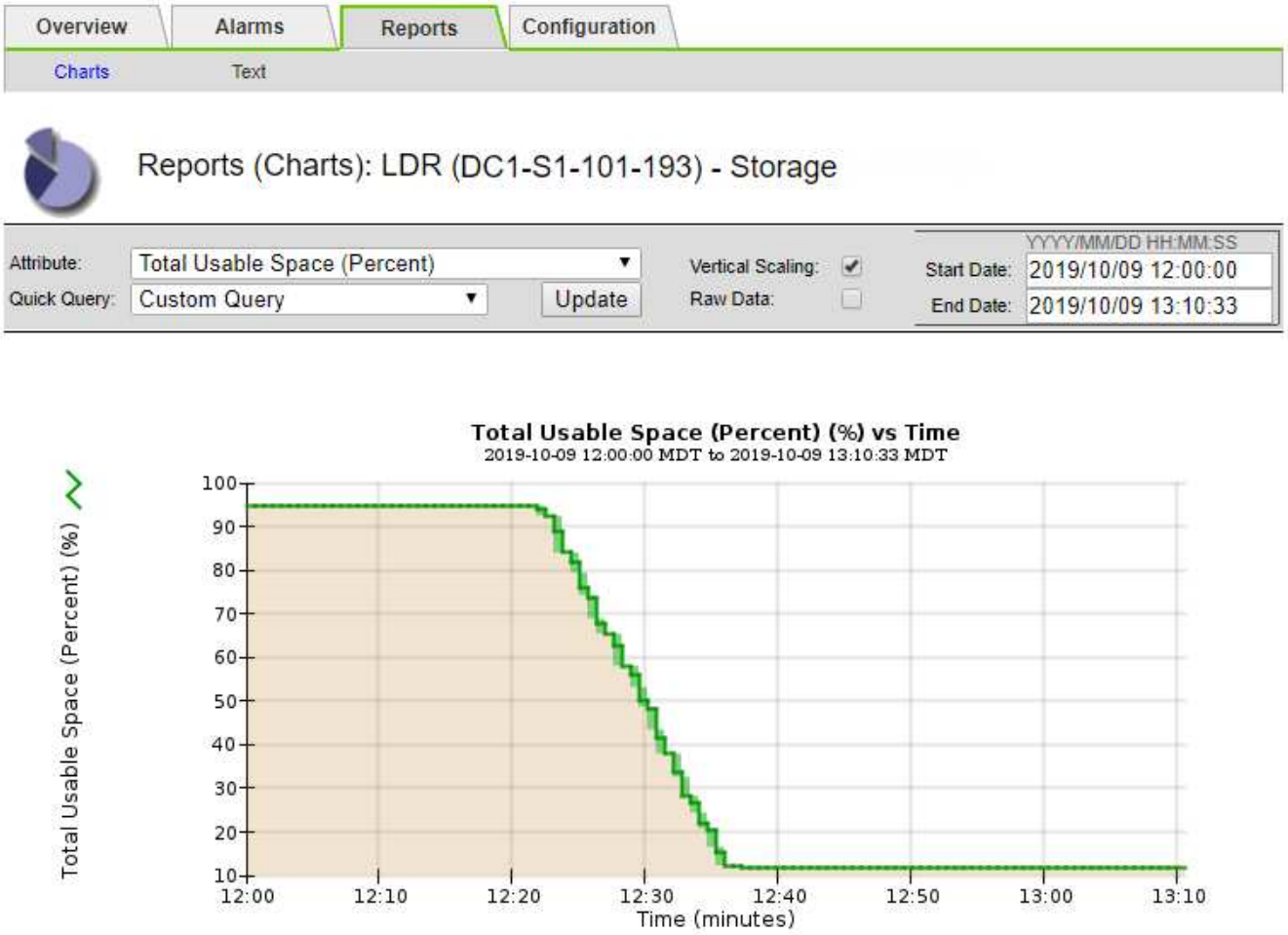
4. Per capire come lo storage è stato utilizzato nel tempo, selezionare la scheda **Report** e tracciare lo spazio utilizzabile totale nelle ultime ore.

   In questo esempio, lo spazio utilizzabile totale è sceso da circa 155 GB a 12:00 a 20 GB a 12:35, il che corrisponde al momento in cui è stato attivato l'allarme SSTS.



5. Per comprendere come lo storage viene utilizzato come percentuale del totale, tracciare lo spazio utilizzabile totale (percentuale) nelle ultime ore.

   In questo esempio, lo spazio utilizzabile totale è sceso dal 95% a poco più del 10% circa contemporaneamente.



6. Secondo necessità, "aggiungere capacità di storage".

   Vedere anche "Gestire nodi storage completi".

Risoluzione dei problemi relativi all'erogazione dei messaggi dei servizi della piattaforma (allarme SMTT)

L'allarme SMTT (Total Events) viene attivato in Grid Manager se un messaggio di servizio della piattaforma viene inviato a una destinazione che non può accettare i dati.

A proposito di questa attività

Ad esempio, il caricamento di un S3 multipart può avere successo anche se la replica o il messaggio di notifica associati non possono essere inviati all'endpoint configurato. In alternativa, un messaggio per la replica di CloudMirror potrebbe non essere recapitato se i metadati sono troppo lunghi.

L'allarme SMTT contiene un messaggio Last Event (ultimo evento) che indica: `Failed to publish notifications for` *`bucket-name object key`* per l'ultimo oggetto la cui notifica non è riuscita.

I messaggi degli eventi sono elencati anche in `/var/local/log/bycast-err.log` file di log. Vedere "Riferimenti ai file di log".

Per ulteriori informazioni, consultare "Risolvere i problemi relativi ai servizi della piattaforma". Potrebbe essere necessario "Accedere al tenant dal tenant manager" per eseguire il debug di un errore del servizio della

piattaforma.

Fasi

1. Per visualizzare l'allarme, selezionare **NODES** > ***Site*** > ***Grid Node*** > **Events**.
2. Visualizza ultimo evento nella parte superiore della tabella.

   I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

3. Seguire le indicazioni fornite nel contenuto degli allarmi SMTT per correggere il problema.
4. Selezionare **Reset event count** (Ripristina conteggi eventi).
5. Notificare al tenant gli oggetti i cui messaggi dei servizi della piattaforma non sono stati recapitati.
6. Chiedere al tenant di attivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto.

Informazioni sul copyright

Informazioni sul marchio commerciale