Risoluzione dei problemi relativi a oggetti e storage

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-115/troubleshoot/verifying-object-integrity.html on April 11, 2024. Always check docs.netapp.com for the latest.

Sommario

Risoluzione dei problemi relativi a oggetti e storage

È possibile eseguire diverse attività per determinare l'origine dei problemi di storage e oggetti.

Conferma delle 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.

Di cosa hai bisogno

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
  - **UUID**: Identificativo universalamente 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 e chiave oggetto**: Quando un oggetto viene acquisito tramite l'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 l'interfaccia Swift, l'applicazione client utilizza una combinazione di container e object name 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. Fare clic su **Cerca**.

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

   - Metadati di sistema, tra cui l'ID oggetto (UUID), 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 in cui l'oggetto è stato creato per la prima volta 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",
```


Informazioni correlate

"Gestire gli oggetti con ILM"

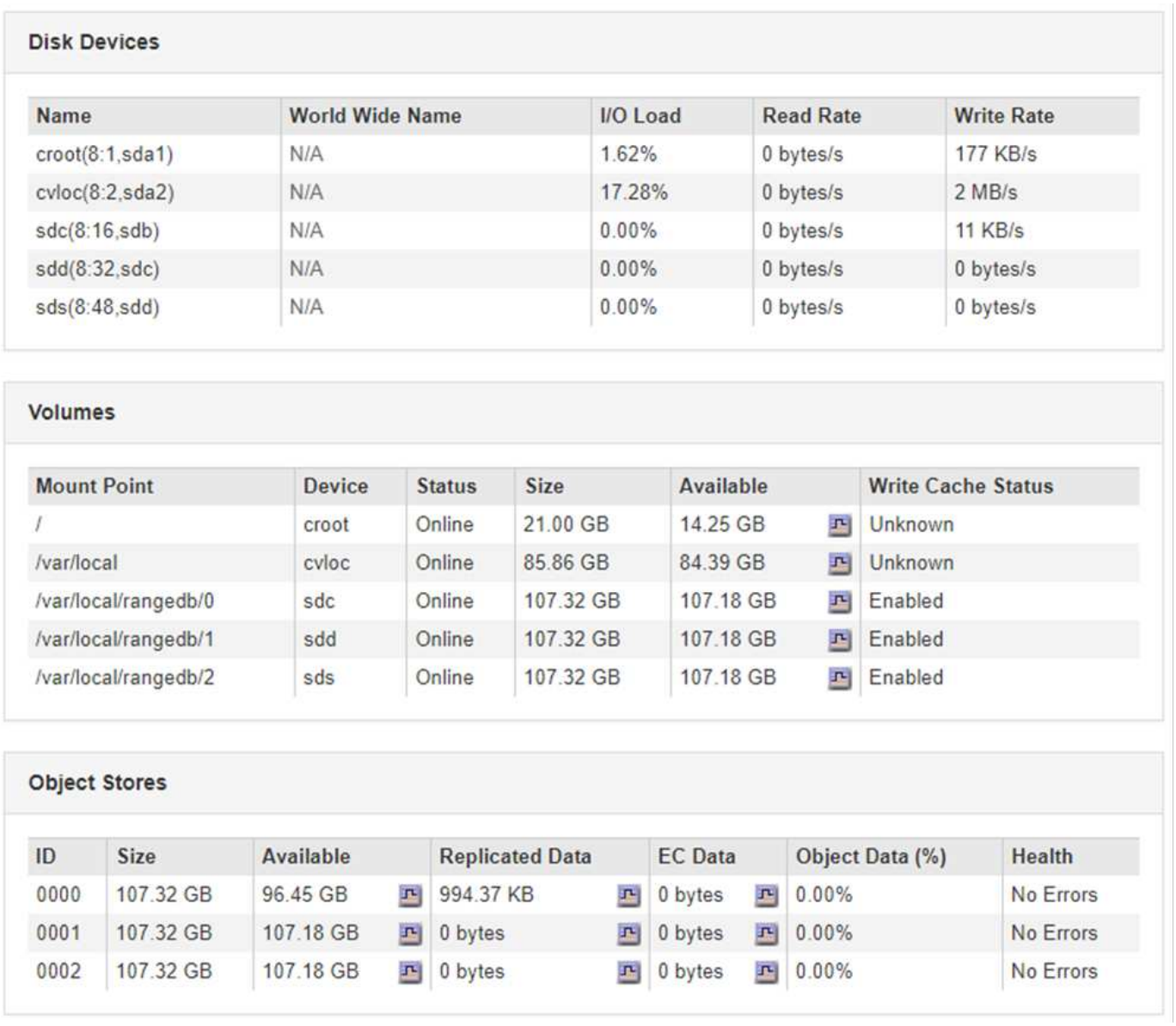
"Utilizzare S3"

"USA Swift"

Errori dell'archivio di oggetti (volume di storage)

Lo storage sottostante su un nodo di storage è diviso in archivi di oggetti. Questi archivi di oggetti sono partizioni fisiche che fungono da punti di montaggio per lo storage del sistema StorageGRID. 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
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s

Volumes

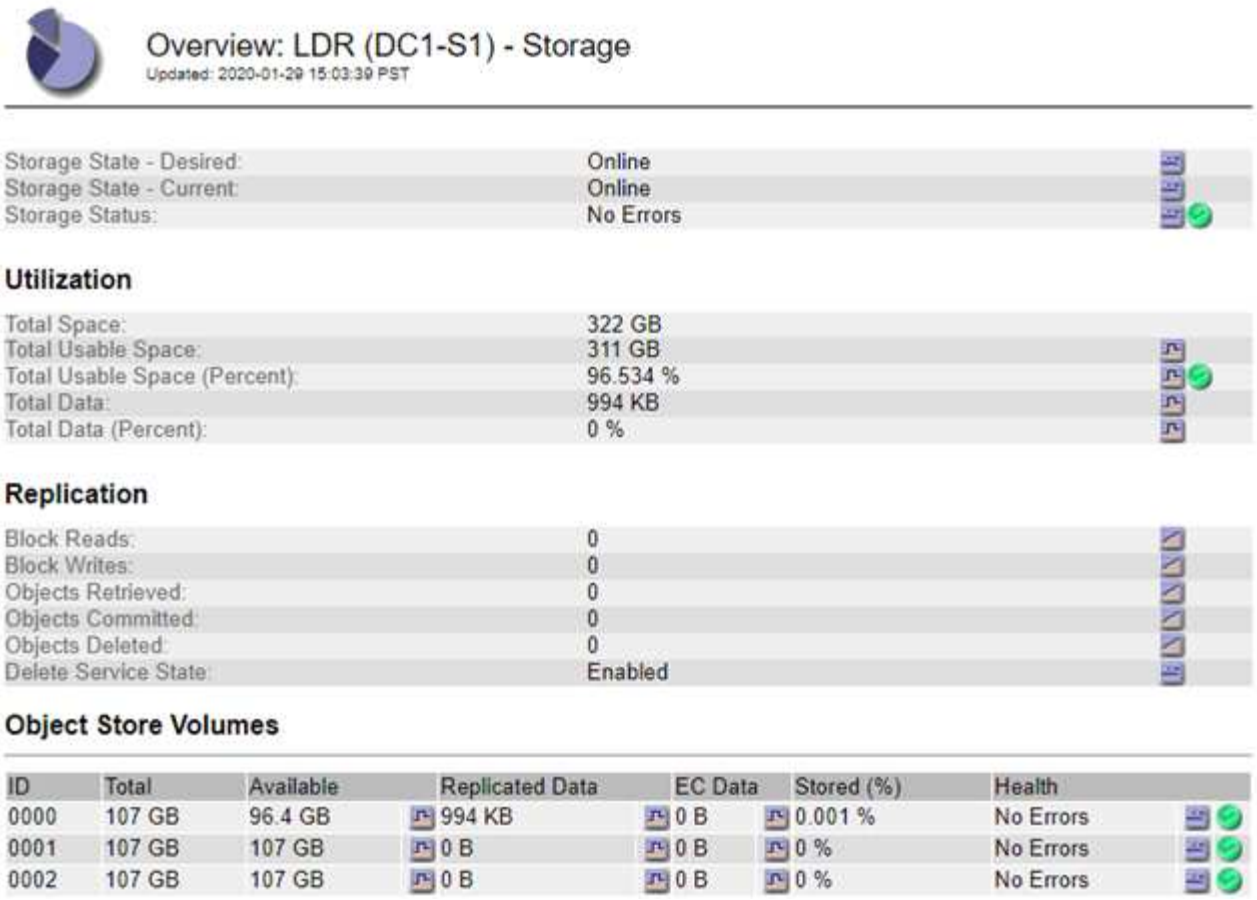
Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	21.00 GB	14.25 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB	Enabled

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB	994.37 KB	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

Per ulteriori informazioni su ciascun nodo di storage, attenersi alla seguente procedura:

1. Selezionare **supporto** > **Strumenti** > **topologia griglia**.
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 mentre si prepara per un ripristino completo del server.

Informazioni correlate

"Mantieni Ripristina"

Verifica dell'integrità degli oggetti

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 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. La verifica in primo piano può essere attivata da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) di 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 una nuova copia non corrotta e posizionata per soddisfare il criterio ILM attivo. 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 non è possibile ricostruire il frammento corrotto, l'attributo Corrupt Copies Detected (ECOR) viene incrementato di uno e si tenta 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, vengono attivati l'avviso **oggetti persi** e l'allarme legacy PERSI (oggetti persi).

Modifica del 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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

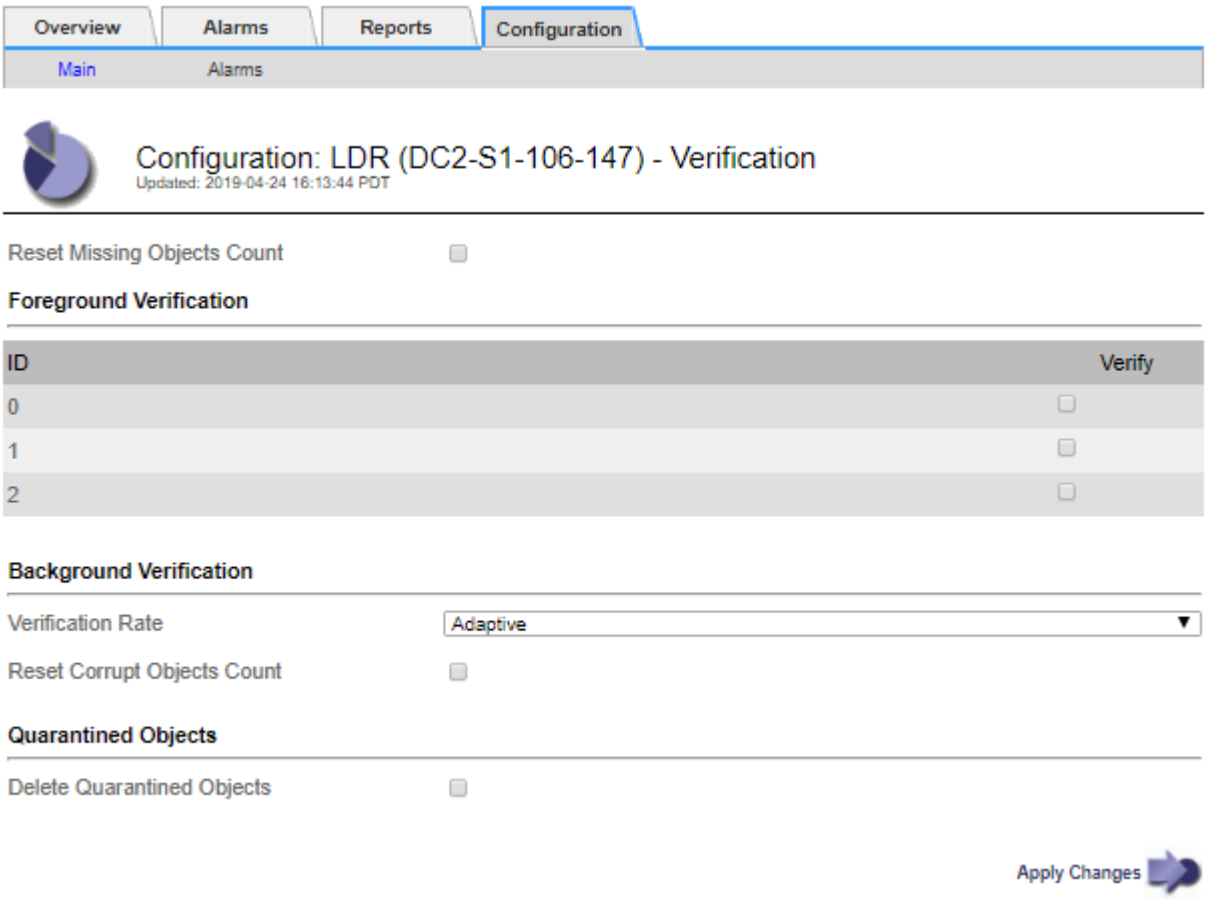
È possibile modificare il tasso di verifica per la verifica in background su un nodo di storage:

- 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 **supporto** > **Strumenti** > **topologia griglia**.
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 High** (tasso di verifica) o **Verification Rate Adaptive** (tasso di verifica).



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

1. Fare clic su **Applica modifiche**.
2. 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 eseguita in qualsiasi punto del sistema StorageGRID che soddisfi la policy ILM attiva.
- 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.

3. 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 **supporto** > **Strumenti** > **topologia griglia**.
   b. Selezionare ***Storage Node* LDR Erasure Coding**.
   c. Nella tabella Verification Results (risultati verifica), monitorare l'attributo corrotto Fragments Detected (ECCD).

4. Una volta ripristinati automaticamente gli oggetti corrotti dal sistema StorageGRID, ripristinare il numero di oggetti corrotti.
   a. Selezionare **supporto** > **Strumenti** > **topologia griglia**.
   b. Selezionare ***Storage Node* LDR Verification Configuration**.
   c. Selezionare **Ripristina conteggio oggetti corrotti**.
   d. Fare clic su **Applica modifiche**.
5. Se si è certi che gli oggetti in quarantena non sono necessari, è possibile 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.

   1. Selezionare **supporto** > **Strumenti** > **topologia griglia**.
   2. Selezionare ***Storage Node* LDR Verification Configuration**.
   3. Selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).
   4. Fare clic su **Applica modifiche**.

Che cos'è la verifica in primo piano

La verifica in primo piano è un processo avviato dall'utente che verifica l'esistenza di tutti i dati dell'oggetto previsti su un nodo di storage. La verifica in primo piano viene utilizzata per verificare l'integrità di un dispositivo di storage.

La verifica in primo piano è un'alternativa più rapida alla verifica in background che verifica l'esistenza, ma non l'integrità, dei dati dell'oggetto su un nodo di storage. Se la verifica in primo piano rileva la mancanza di molti elementi, potrebbe esserci un problema con tutto o parte di un dispositivo di storage associato al nodo di storage.

La verifica in primo piano verifica sia i dati degli oggetti replicati che quelli con codice di cancellazione, come

segue:

- **Replicated Objects**: Se una copia dei dati degli oggetti replicati risulta mancante, StorageGRID tenta automaticamente di sostituire la copia dalle copie memorizzate 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 la copia mancante non esiste più nella posizione prevista. Viene generata una nuova copia per soddisfare la policy ILM attiva del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa posizione in cui è stata memorizzata la copia mancante.
- **Oggetti con codifica di cancellazione**: Se un frammento di un oggetto con codifica di cancellazione risulta mancante, 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), l'attributo Corrupt Copies Detected (ECOR) (copie corrotte rilevate) viene incrementato di uno. ILM tenta quindi di trovare un'altra copia dell'oggetto, che può utilizzare per generare una nuova copia con codifica di cancellazione.

  Se la verifica in primo piano identifica un problema di erasure coding su un volume di storage, l'attività di verifica in primo piano viene interrotta con un messaggio di errore che identifica il volume interessato. È necessario eseguire una procedura di ripristino per tutti i volumi di storage interessati.

Se nella griglia non vengono trovate altre copie di un oggetto replicato mancante o un oggetto corrotto con codifica in cancellazione, vengono attivati l'allarme **oggetti persi** e l'allarme legacy PERSO (oggetti persi).

Esecuzione della verifica in primo piano

La verifica in primo piano consente di verificare l'esistenza di dati su un nodo di storage. I dati dell'oggetto mancanti potrebbero indicare la presenza di un problema con il dispositivo di storage sottostante.

Di cosa hai bisogno

- Hai verificato che le seguenti attività della griglia non siano in esecuzione:
  - Grid Expansion (espansione griglia): Aggiungere un server (GEXP) quando si aggiunge un nodo di storage
  - Decommissionamento dei nodi di storage (LDCM) sullo stesso nodo di storage se queste attività della griglia sono in esecuzione, attendere il completamento o il rilascio del blocco.
- Hai garantito che lo storage sia online. (Selezionare **supporto Strumenti topologia griglia**. Quindi, selezionare ***Storage Node* LDR Storage Overview Main**. Assicurarsi che lo stato dello storage - corrente* sia online.
- Si è verificato che le seguenti procedure di ripristino non siano in esecuzione sullo stesso nodo di storage:
  - Ripristino di un volume di storage guasto
  - Ripristino di un nodo di storage con un disco di sistema guasto la verifica di Foreground non fornisce informazioni utili durante l'esecuzione delle procedure di ripristino.

A proposito di questa attività

La verifica in primo piano verifica la presenza di dati di oggetti replicati mancanti e di dati di oggetti con codifica di cancellazione mancanti:

- Se la verifica in primo piano rileva grandi quantità di dati dell'oggetto mancanti, è probabile che vi sia un problema con lo storage del nodo di storage che deve essere esaminato e risolto.
- Se la verifica in primo piano rileva un grave errore di storage associato a dati con codifica di cancellazione, viene visualizzato un messaggio di notifica. Per risolvere l'errore, è necessario eseguire il ripristino del volume di storage.

È possibile configurare la verifica in primo piano per controllare tutti gli archivi di oggetti di un nodo di storage o solo gli archivi di oggetti specifici.

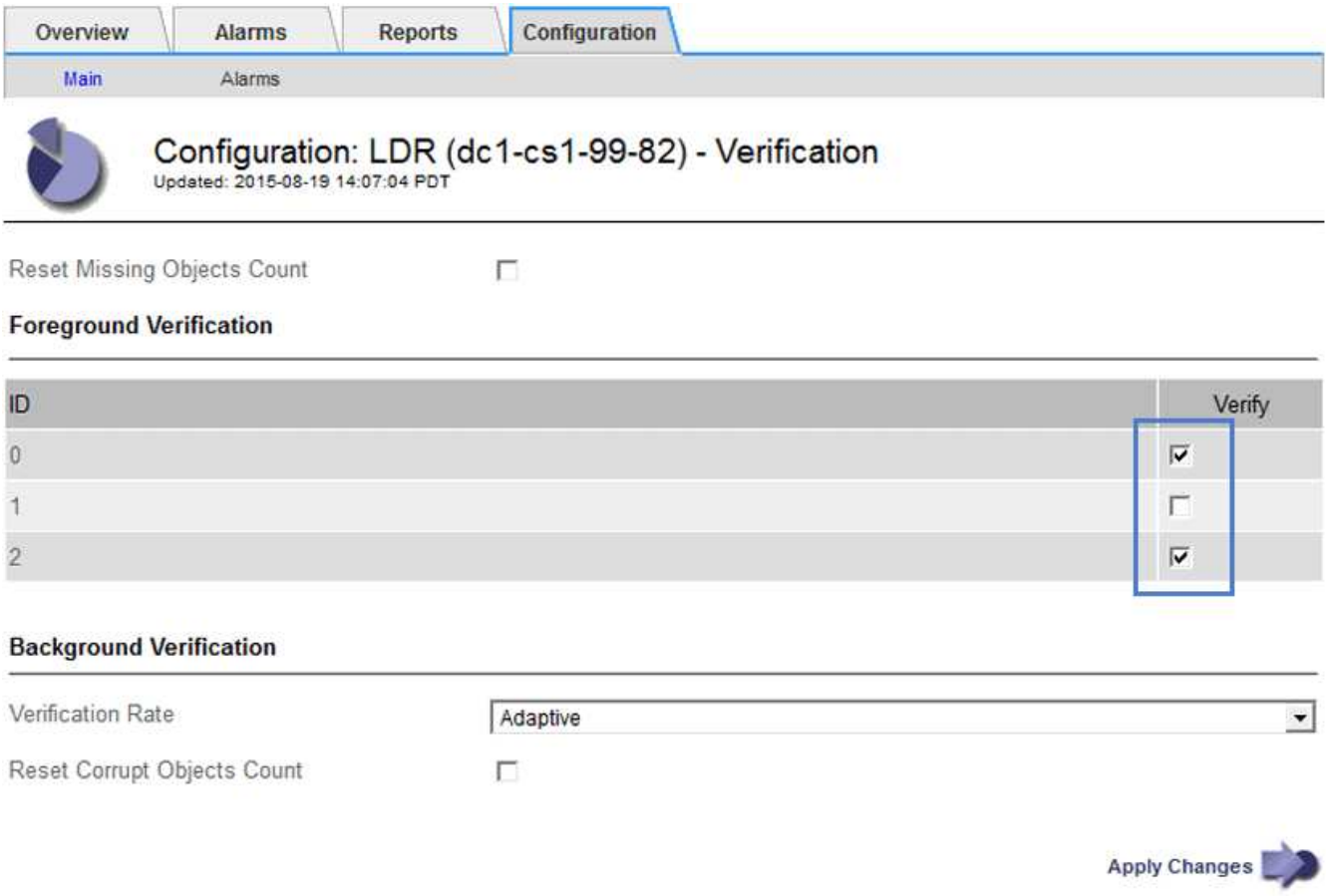
Se la verifica in primo piano rileva dati dell'oggetto mancanti, il sistema StorageGRID tenta di sostituirli. Se non è possibile eseguire una copia sostitutiva, potrebbe essere attivato l'allarme LOST (Lost Objects) (oggetti PERSI).

La verifica in primo piano genera un'attività della griglia di verifica in primo piano di LDR che, a seconda del numero di oggetti memorizzati in un nodo di storage, può richiedere giorni o settimane per il completamento. È possibile selezionare più nodi di storage contemporaneamente; tuttavia, queste attività della griglia non vengono eseguite contemporaneamente. Vengono invece messi in coda ed eseguiti uno dopo l'altro fino al completamento. Quando è in corso la verifica in primo piano su un nodo di storage, non è possibile avviare un'altra attività di verifica in primo piano sullo stesso nodo di storage, anche se l'opzione per verificare volumi aggiuntivi potrebbe sembrare disponibile per il nodo di storage.

Se un nodo di storage diverso da quello in cui viene eseguita la verifica in primo piano non è in linea, l'attività Grid continua a essere eseguita fino a quando l'attributo **% complete** non raggiunge il 99.99%. L'attributo **% complete** torna al 50% e attende che il nodo di storage torni allo stato online. Quando lo stato del nodo di storage torna in linea, l'attività della griglia di verifica di primo piano di LDR continua fino al completamento.

Fasi

1. Selezionare ***Storage Node* LDR Verification**.
2. Selezionare **Configurazione principale**.
3. In **Foreground Verification**, selezionare la casella di controllo per ciascun ID del volume di storage che si desidera verificare.



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

   Attendere che la pagina venga aggiornata automaticamente e ricaricata prima di uscire dalla pagina. Una volta aggiornati, gli archivi di oggetti diventano non disponibili per la selezione su quel nodo di storage.

   Viene generata un'attività della griglia LDR Foreground Verification che viene eseguita fino al completamento, alla pausa o all'interruzione.

5. Monitorare gli oggetti mancanti o i frammenti mancanti:

   a. Selezionare ***Storage Node*** **LDR Verification**.

   b. Nella scheda Overview (Panoramica) sotto **Verification Results** (risultati verifica), annotare il valore di **Missing Objects Detected** (oggetti mancanti rilevati).

      Nota: Lo stesso valore viene riportato come **oggetti persi** nella pagina nodi. Accedere a **Nodes** ***Storage Node*** e selezionare la scheda **Objects**.

      Se il numero di **oggetti mancanti rilevati** è elevato (se ci sono centinaia di oggetti mancanti), è probabile che si sia verificato un problema con lo storage del nodo di storage. Contattare il supporto tecnico.

   c. Selezionare ***Storage Node*** **LDR Erasure Coding**.

   d. Nella scheda Overview (Panoramica) sotto **Verification Results** (risultati verifica), annotare il valore **Missing Fragments Detected** (frammenti mancanti rilevati).

      Se il numero di **frammenti mancanti rilevati** è elevato (se vi sono centinaia di frammenti mancanti), è probabile che si sia verificato un problema con lo storage del nodo di storage. Contattare il supporto tecnico.

   Se la verifica in primo piano non rileva un numero significativo di copie di oggetti replicati mancanti o un numero significativo di frammenti mancanti, lo storage funziona normalmente.

6. Monitorare il completamento dell'attività della griglia di verifica in primo piano:

   a. Selezionare **supporto Strumenti topologia griglia**. Quindi selezionare **Site** ***Admin Node*** **CMN Grid Task Overview Main**.

   b. Verificare che l'attività della griglia di verifica in primo piano stia procedendo senza errori.

      Nota: Viene attivato un allarme a livello di avviso sullo stato delle attività della griglia (SCAS) se l'attività della griglia di verifica in primo piano viene interrotta.

   c. Se l'attività della griglia viene interrotta con un `critical storage error`, ripristinare il volume interessato ed eseguire la verifica in primo piano sui volumi rimanenti per verificare la presenza di errori aggiuntivi.

      Attenzione: Se l'attività della griglia di verifica in primo piano viene interrotta con il messaggio `Encountered a critical storage error in volume volID`, è necessario eseguire la procedura per il ripristino di un volume di storage guasto. Consultare le istruzioni di ripristino e manutenzione.

Al termine

Se hai ancora dubbi sull'integrità dei dati, vai a **LDR verifica Configurazione principale** e aumenta la percentuale 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.

Informazioni correlate

"Mantieni Ripristina"

Risoluzione dei problemi relativi ai dati degli oggetti persi e mancanti

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, vengono attivati l'allarme **oggetti persi** e l'allarme legacy PERSI (oggetti persi), come segue:

- Per le copie replicate, se non è possibile recuperare un'altra copia, l'oggetto viene considerato perso e vengono attivati l'avviso e l'allarme.
- Per le copie codificate erasure, se una copia non può essere recuperata dalla posizione prevista, l'attributo Corrupt Copies Detected (ECOR) viene incrementato di uno prima di tentare di recuperare una copia da un'altra posizione. Se non vengono trovate altre copie, vengono attivati l'allarme e l'allarme.

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.

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 Object (oggetti persi) per evitare che oggetti persi noti mascherino eventuali nuovi oggetti persi.

Informazioni correlate

"Analisi degli oggetti smarriti"

"Reimpostazione dei conteggi degli oggetti persi e mancanti"

Analisi degli oggetti smarriti

Quando vengono attivati l'allarme **oggetti persi** e l'allarme legacy PERSI (oggetti persi), è necessario eseguire immediatamente un'analisi. Raccogliere informazioni sugli oggetti interessati e contattare il supporto tecnico.

Di cosa hai bisogno

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

A proposito di questa attività

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

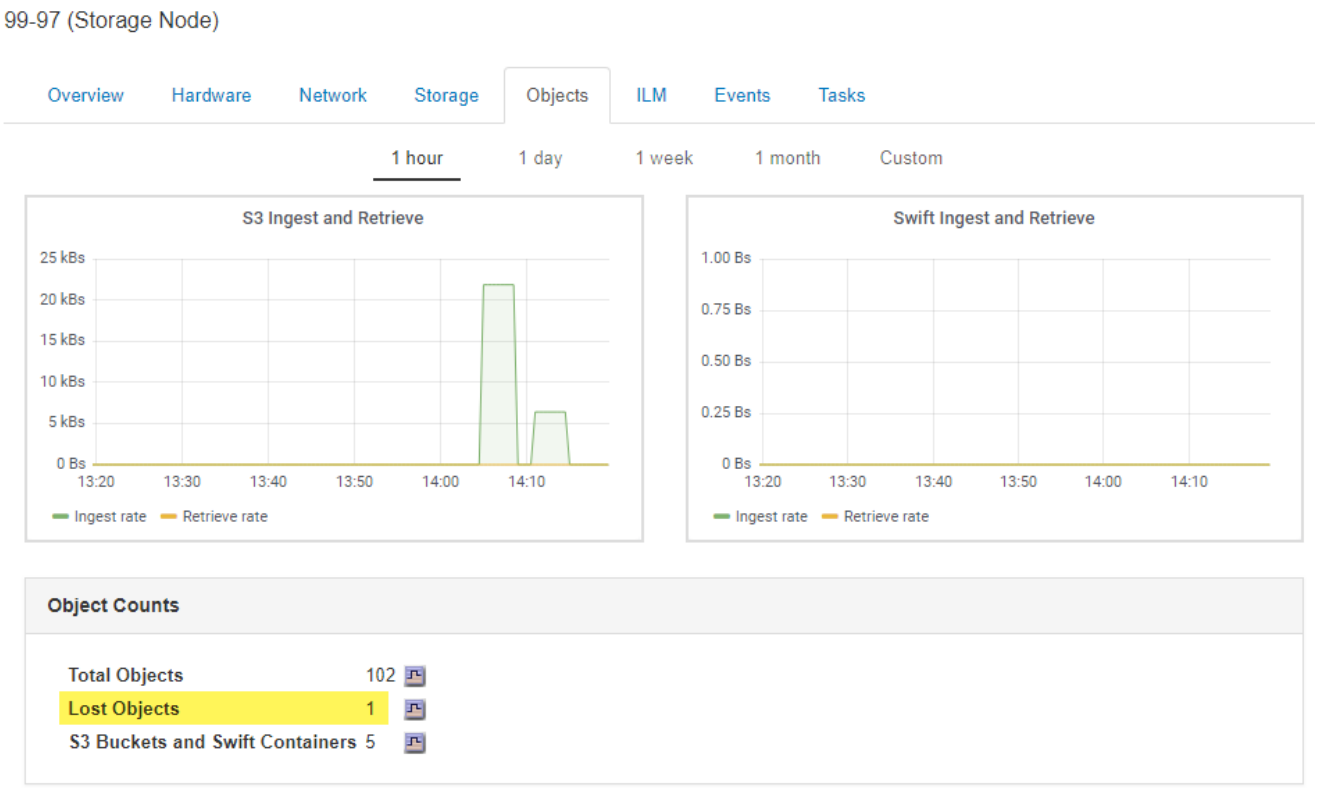
Esaminare immediatamente gli allarmi o gli avvisi di oggetti smarriti. Potrebbe essere necessario intervenire per evitare ulteriori perdite di dati. In alcuni casi, potrebbe essere possibile ripristinare un oggetto perso se si esegue un'azione rapida.

Il numero di oggetti persi può essere visualizzato in Grid Manager.

Fasi

1. Selezionare **nodi**.
2. Selezionare ***Storage Node* Objects**.
3. Esaminare il numero di oggetti persi visualizzato nella tabella Conteggio 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 amministratore, accedere al registro di controllo per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **oggetti persi** e l'allarme PERSO:
   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. Inserire: `cd /var/local/audit/export/`

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. Telnet all'host locale 1402 per accedere alla console LDR.

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 ignorare l'allarme. La mancanza di un oggetto indica che l'oggetto è stato intenzionalmente cancellato.
Posizioni 0	Se nell'output sono presenti posizioni, l'allarme 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 trovare oggetti potenzialmente persi spiega come utilizzare l'ID nodo per trovare il nodo di storage corretto. "Ricerca e ripristino di oggetti potenzialmente persi" Se gli oggetti sono presenti, è possibile ripristinare il numero di oggetti persi per annullare l'allarme e l'avviso.
Posizioni = 0	Se nell'output non sono presenti posizioni, l'oggetto potrebbe essere mancante. È possibile cercare e ripristinare l'oggetto da soli oppure contattare il supporto tecnico. "Ricerca e ripristino di oggetti potenzialmente persi" Il supporto tecnico potrebbe richiedere di determinare se è in corso una procedura di ripristino dello storage. Vale a dire, è stato emesso un comando *repair-data* su qualsiasi nodo di storage e il ripristino è ancora in corso? Consultare le informazioni relative al ripristino dei dati degli oggetti in un volume di storage nelle istruzioni di ripristino e manutenzione.

Informazioni correlate

"Mantieni Ripristina"

"Esaminare i registri di audit"

Ricerca e ripristino di 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.

Di cosa hai bisogno

- È necessario disporre dell'UUID di qualsiasi oggetto perso, come indicato in "analisi degli oggetti persi".
- È necessario disporre di `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: `cd /var/local/audit/export/`
   c. Utilizzare grep per estrarre i messaggi di controllo 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 >
      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 messages_about_lost_objects.txt
      ```

      Un messaggio di audit 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):
      1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
      SM]
      [ATID(UI64):7086871083190743409]]
      ```

   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.

f. Individuare il nodo di storage per questo ID nodo LDR.

Esistono due modi per utilizzare l'ID del nodo per trovare il nodo di storage:

- In Grid Manager, selezionare **Support Tools Grid Topology**. Quindi selezionare ***Data Center Storage Node* LDR**. L'ID del nodo 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.
- Scaricare e decomprimere il pacchetto di ripristino per la griglia. Esiste una directory */docs* nel pacchetto SUDDETTO. Se si apre il file index.html, il Riepilogo server mostra tutti gli ID dei nodi per tutti i nodi della griglia.

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'
```

Nota: 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, andare al passo Ripristinare l'oggetto su StorageGRID. È possibile tentare di ripristinare l'oggetto trovato in StorageGRID.

1. 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. Telnet all'host locale 1402 per accedere alla console LDR. Inserire: `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 anche il criterio ILM attivo, che crea copie aggiuntive come specificato nel criterio.

Nota: 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'
```

Andare al passo Verificare che siano state create nuove posizioni

1. 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`

2. 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: `cd /var/local/audit/export/`

   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 >
      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 messages_about_restored_object.txt
      ```

      Un messaggio di audit 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.

b. Ripristinare il numero di oggetti persi in Grid Manager.

Informazioni correlate

"Analisi degli oggetti smarriti"

"Conferma delle posizioni dei dati degli oggetti"

"Reimpostazione dei conteggi degli oggetti persi e mancanti"

"Esaminare i registri di audit"

Reimpostazione dei 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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

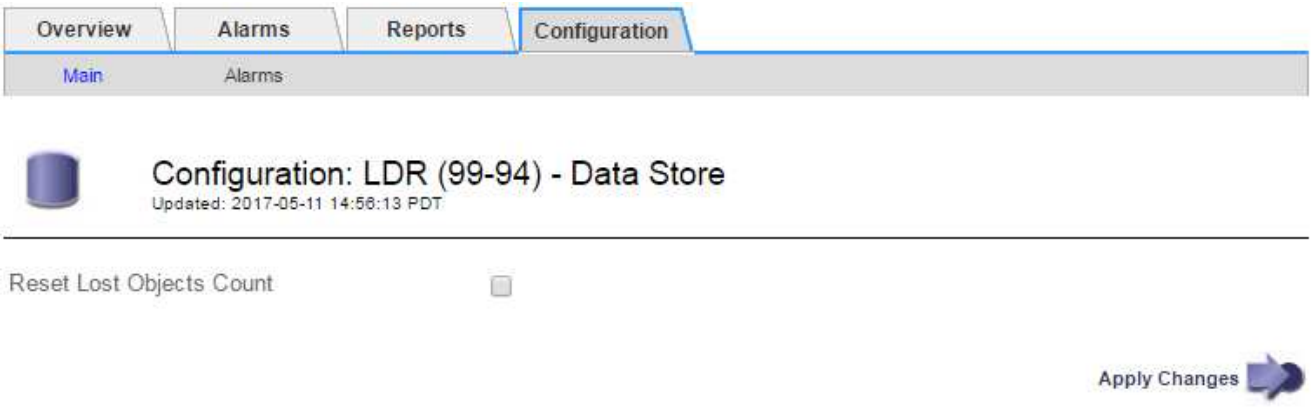
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

- **Supporto Strumenti topologia griglia *nodo di storage del sito* LDR Archivio dati Panoramica principale**
- **Supporto Strumenti topologia griglia *nodo di storage del sito* DDS Data Store Panoramica principale**

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

Fasi

1. Selezionare **supporto** > **Strumenti** > **topologia griglia**.
2. Selezionare ***Site Storage Node* LDR Data Store Configuration** per il nodo di storage con 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.

Informazioni correlate

"Amministrare StorageGRID"

Risoluzione dei 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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Lo spazio di archiviazione dei dati **Low Object Data Storage** viene attivato quando la quantità totale di dati degli oggetti codificati replicati ed erasure 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 della dimensione totale dei dati degli oggetti replicati ed erasure coded per un nodo di 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 **Avvisi corrente**.

   Viene visualizzata la pagina Avvisi.

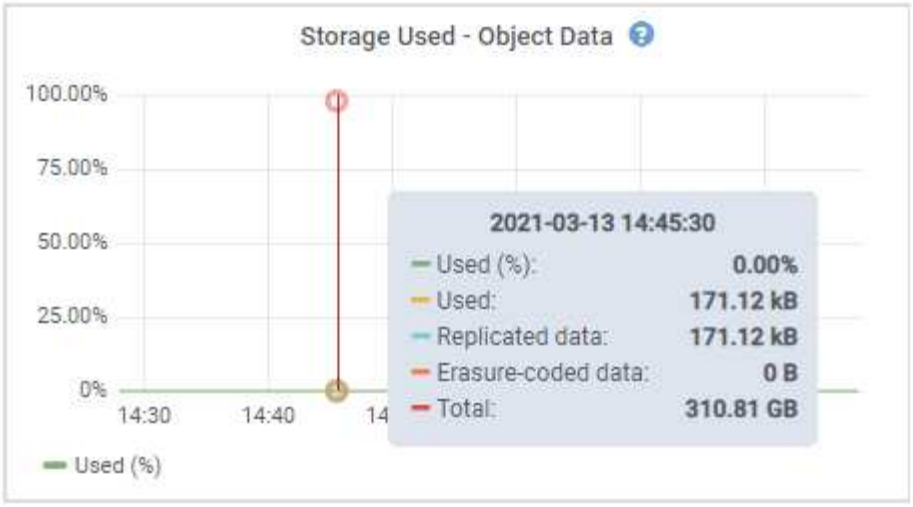
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low Object Data Storage**, se necessario, e selezionare l'avviso che si desidera visualizzare.

   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 o Site* Storage**.
5. Spostare 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. Non appena possibile, eseguire una procedura di espansione per aggiungere capacità di storage.

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

   > Per gestire un nodo di storage completo, consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

"Risoluzione dei problemi relativi all'allarme Storage Status (SST)"

"Espandi il tuo grid"

"Amministrare StorageGRID"

Risoluzione dei 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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

L'allarme SST (Storage Status) viene attivato a livello di notifica quando la quantità di spazio libero su ogni volume in un nodo di storage scende al di sotto del valore del watermark di sola lettura del volume di storage (**Configuration Storage Options Overview**).

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

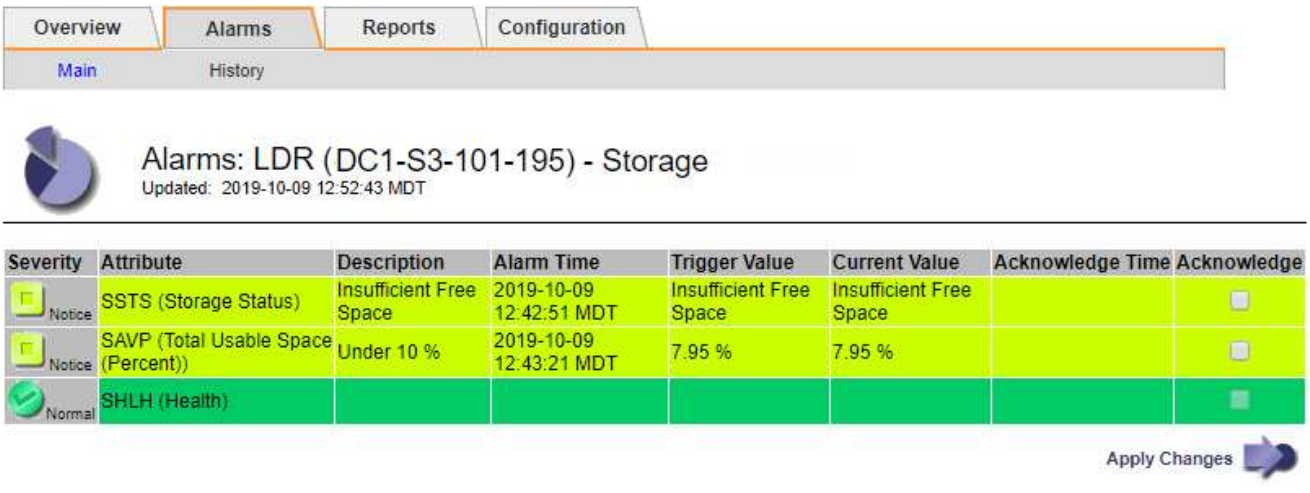
Ad esempio, si supponga che la filigrana Storage Volume Soft Read-Only sia impostata su 10 GB, che è il valore predefinito. L'allarme SSTS viene attivato se su ciascun volume di storage nel nodo di storage rimangono meno di 10 GB di spazio utilizzabile. Se uno dei volumi dispone di almeno 10 GB di spazio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

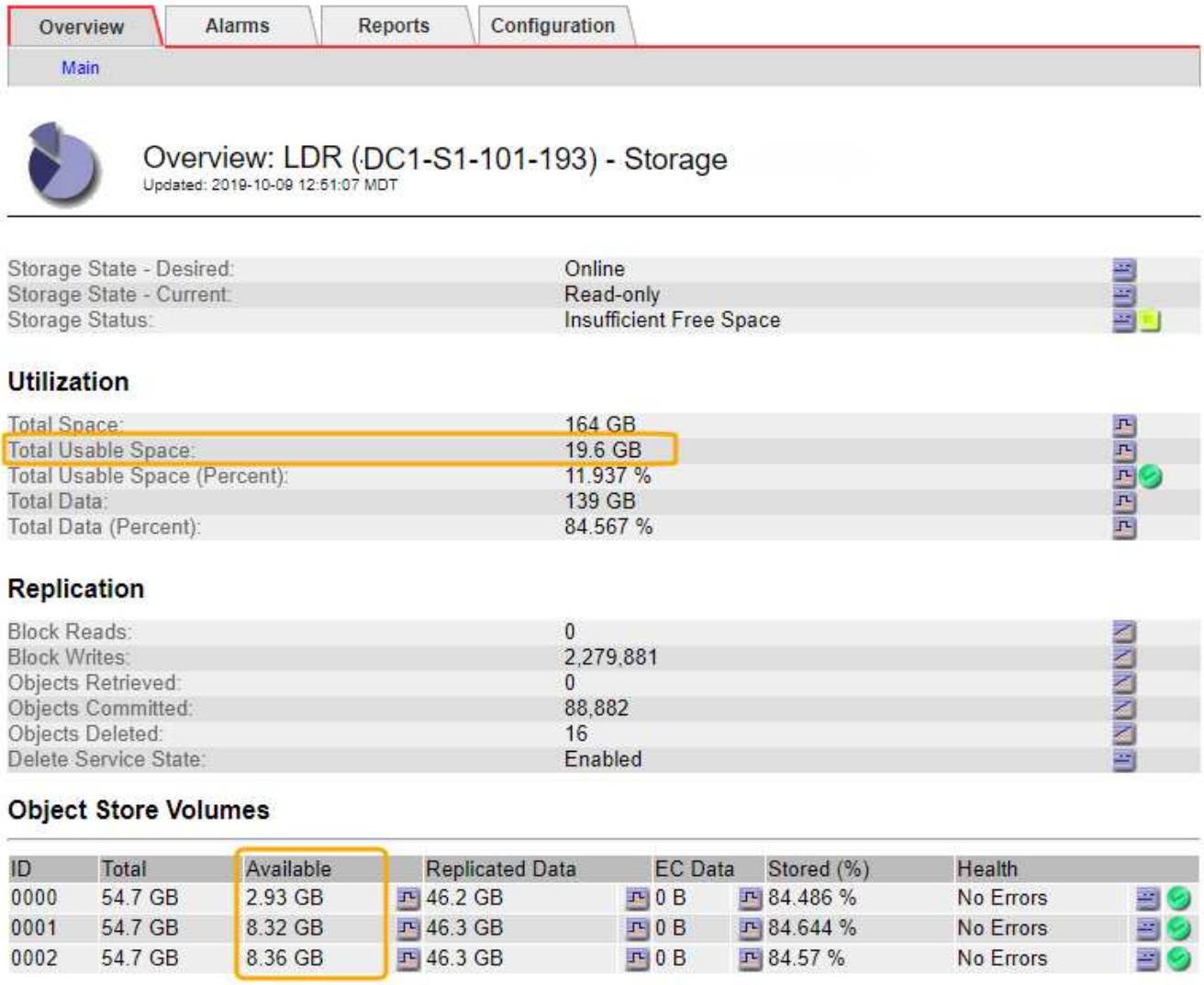
   Viene visualizzata la pagina Grid Topology (topologia griglia). La scheda Allarmi mostra gli allarmi attivi per il nodo e il servizio selezionato.



   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.

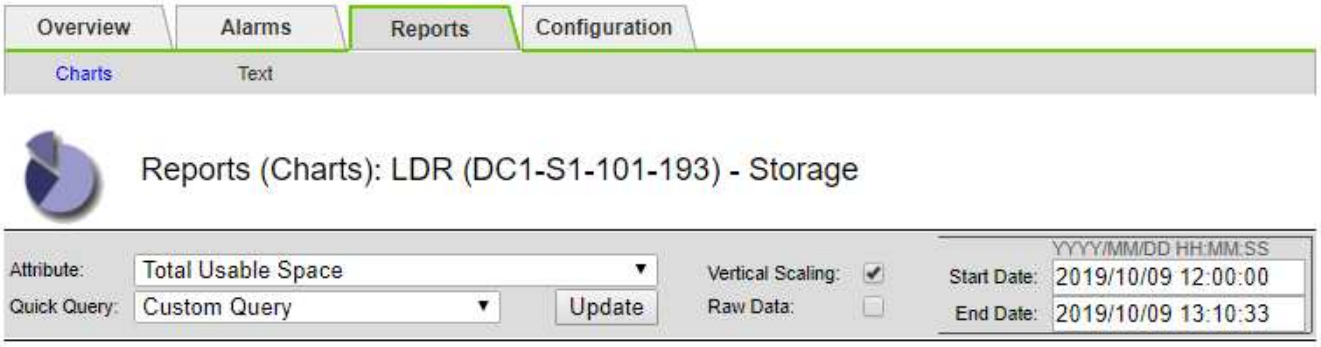
3. Per determinare la quantità di spazio utilizzabile effettivamente disponibile, selezionare **LDR Storage Overview** e individuare l'attributo Total Usable Space (STAS).

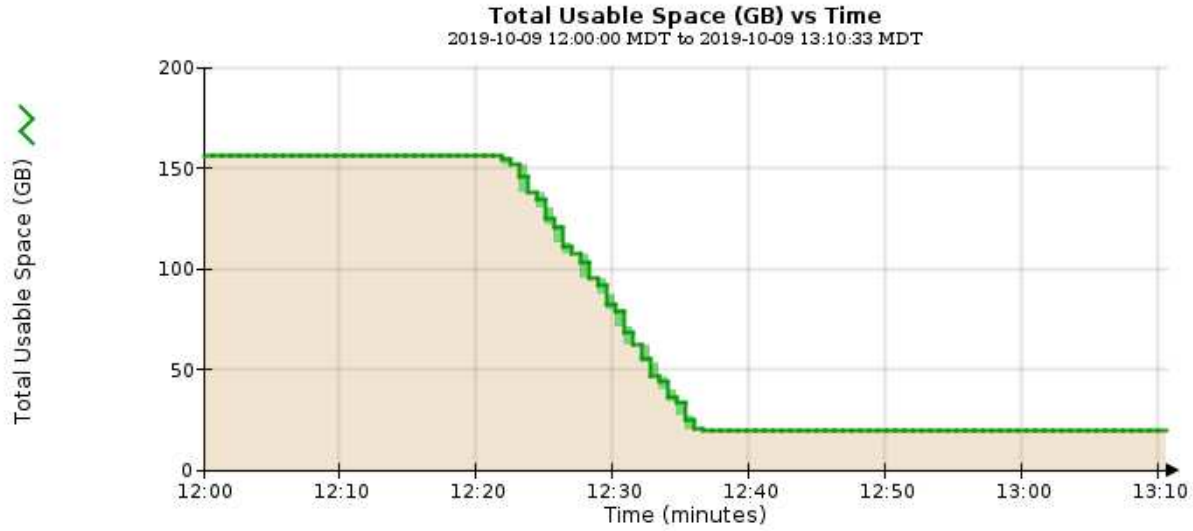


In questo esempio, rimangono disponibili solo 19.6 GB dei 164 GB di spazio su questo nodo di storage. Si noti che il valore totale è la somma dei valori **Available** per i tre volumi dell'archivio di oggetti. L'allarme SSTS è stato attivato perché ciascuno dei tre volumi di storage aveva meno di 10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

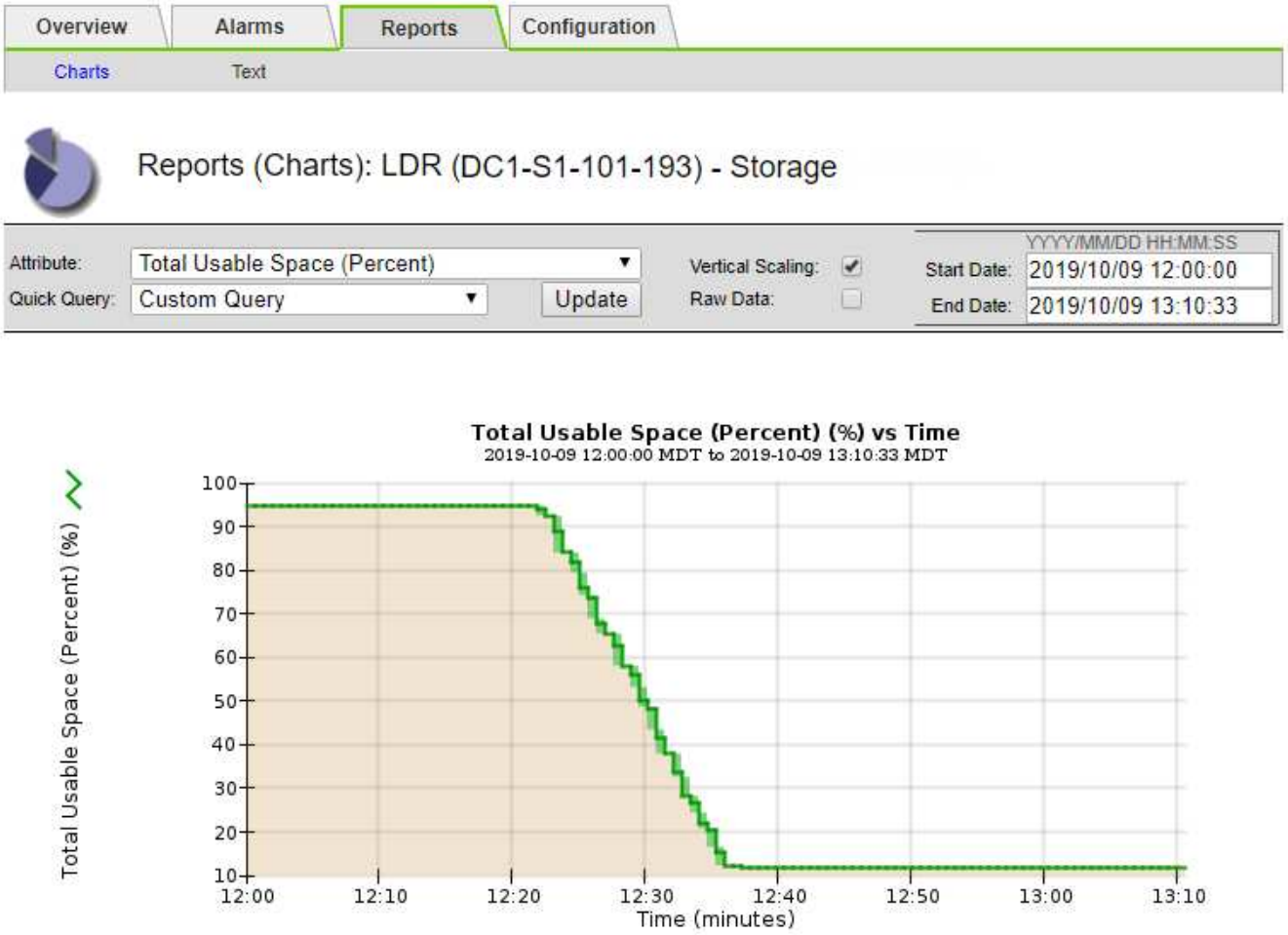
   In questo esempio, lo spazio utilizzabile totale è sceso da circa 155 GB a 12:00 a 20 GB a 12:35, il che corrisponde al momento in cui è stato attivato l'allarme SSTS.





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. Se necessario, aggiungere capacità di storage espandendo il sistema StorageGRID.

   Per le procedure su come gestire un nodo di storage completo, vedere le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

"Espandi il tuo grid"

"Amministrare StorageGRID"

Troubleshooting delivery of platform Services messages (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, un caricamento di S3 multiparte 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.

Per ulteriori informazioni sulla risoluzione dei problemi relativi ai servizi della piattaforma, consultare le istruzioni per l'amministrazione di StorageGRID. Potrebbe essere necessario accedere al tenant da 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. Fare clic su **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 correlate

"Amministrare StorageGRID"

"Utilizzare un account tenant"

"Riferimenti ai file di log"

"Reimpostazione dei conteggi degli eventi"

Informazioni sul copyright

Copyright © 2024 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.