



# **Risolvere i problemi di un sistema StorageGRID**

StorageGRID

NetApp  
October 03, 2025

# Sommario

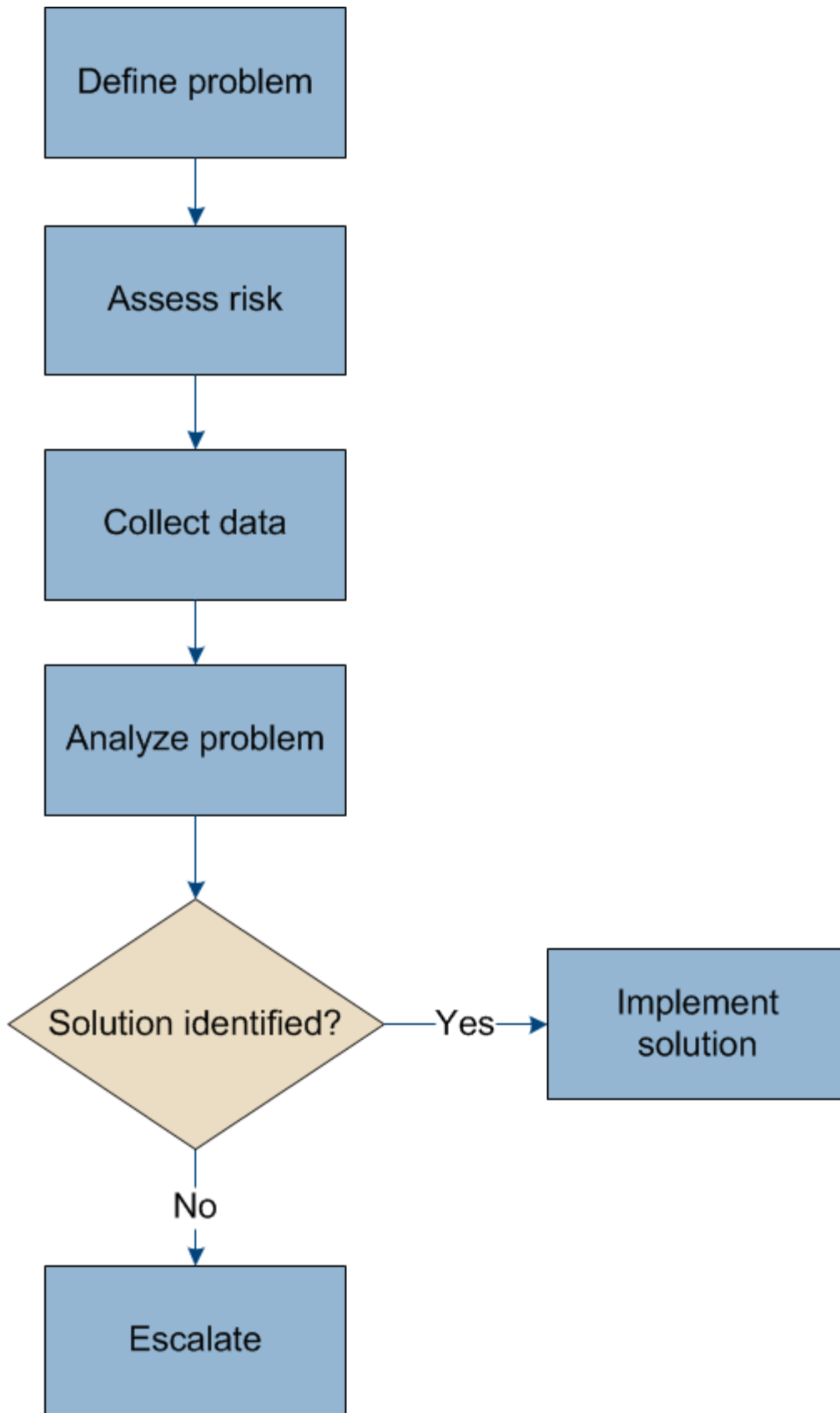
Risolvere i problemi di un sistema StorageGRID .....	1
Panoramica della determinazione del problema .....	1
Definizione del problema .....	2
Valutazione del rischio e dell'impatto sul sistema .....	3
Raccolta di dati .....	4
Analisi dei dati .....	8
Lista di controllo per le informazioni di escalation .....	8
Risoluzione dei problemi relativi a oggetti e storage .....	10
Conferma delle posizioni dei dati degli oggetti .....	10
Errori dell'archivio di oggetti (volume di storage) .....	12
Verifica dell'integrità degli oggetti .....	14
Risoluzione dei problemi relativi ai dati degli oggetti persi e mancanti .....	21
Risoluzione dei problemi relativi all'avviso di storage dei dati a oggetti in esaurimento .....	33
Risoluzione dei problemi relativi all'allarme Storage Status (SST) .....	35
Troubleshooting delivery of platform Services messages (allarme SMTT) .....	39
Risoluzione dei problemi relativi ai metadati .....	40
Risoluzione dei problemi relativi all'avviso di storage metadati in esaurimento .....	40
Risoluzione dei problemi relativi all'allarme Services: Status - Cassandra (SVST) .....	42
Risoluzione dei problemi errori di memoria esaurita di Cassandra (allarme SMTT) .....	46
Risoluzione degli errori del certificato .....	47
Risoluzione dei problemi relativi al nodo di amministrazione e all'interfaccia utente .....	49
Risoluzione dei problemi relativi agli errori di accesso .....	49
Risoluzione dei problemi relativi all'interfaccia utente .....	52
Verifica dello stato di un nodo amministratore non disponibile .....	53
Risoluzione dei problemi di rete, hardware e piattaforma .....	54
Risoluzione degli errori "422: Unprocessable Entity" .....	54
Risoluzione dei problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia .....	55
Risoluzione dei problemi relativi all'allarme NRER (Network Receive Error) .....	57
Risoluzione dei problemi relativi agli errori di sincronizzazione dell'ora .....	59
Linux: Problemi di connettività di rete .....	59
Linux: Stato del nodo "orfano" .....	60
Linux: Risoluzione dei problemi relativi al supporto IPv6 .....	60

# Risolvere i problemi di un sistema StorageGRID

Se si riscontrano problemi durante l'utilizzo di un sistema StorageGRID, consultare i suggerimenti e le linee guida di questa sezione per ottenere assistenza nella determinazione e nella risoluzione del problema.

## Panoramica della determinazione del problema

Se si verifica un problema durante l'amministrazione di un sistema StorageGRID, è possibile utilizzare il processo descritto in questa figura per identificare e analizzare il problema. In molti casi, è possibile risolvere i problemi da soli; tuttavia, potrebbe essere necessario eseguire l'escalation di alcuni problemi al supporto tecnico.



## Definizione del problema

Il primo passo per risolvere un problema è definire il problema in modo chiaro.

Questa tabella fornisce esempi dei tipi di informazioni che è possibile raccogliere per definire un problema:

Domanda	Esempio di risposta
Cosa fa o non fa il sistema StorageGRID? Quali sono i suoi sintomi?	Le applicazioni client segnalano che non è possibile acquisire oggetti in StorageGRID.
Quando è iniziato il problema?	L'acquisizione di oggetti è stata negata per la prima volta alle 14:50 dell'8 gennaio 2020.
Come hai notato il problema per la prima volta?	Notificato dall'applicazione client. Ha ricevuto anche notifiche email di avviso.
Il problema si verifica in modo coerente o solo a volte?	Il problema è in corso.
Se il problema si verifica regolarmente, quali passaggi lo causano	Il problema si verifica ogni volta che un client tenta di acquisire un oggetto.
Se il problema si verifica in modo intermittente, quando si verifica? Registrare i tempi di ciascun incidente di cui si è a conoscenza.	Il problema non è intermittente.
Hai già visto questo problema? Con quale frequenza avete avuto questo problema in passato?	Questa è la prima volta che vedo questo problema.

## Valutazione del rischio e dell'impatto sul sistema

Una volta definito il problema, valutarne il rischio e l'impatto sul sistema StorageGRID. Ad esempio, la presenza di avvisi critici non significa necessariamente che il sistema non stia fornendo servizi di base.

Questa tabella riassume l'impatto del problema di esempio sulle operazioni del sistema:

Domanda	Esempio di risposta
Il sistema StorageGRID è in grado di acquisire contenuti?	No
Le applicazioni client possono recuperare il contenuto?	Alcuni oggetti possono essere recuperati e altri no.
I dati sono a rischio?	No
La capacità di condurre il business è gravemente compromessa?	Sì, perché le applicazioni client non possono memorizzare oggetti nel sistema StorageGRID e i dati non possono essere recuperati in modo coerente.

## Raccolta di dati

Dopo aver definito il problema e averne valutato il rischio e l'impatto, raccogliere i dati per l'analisi. Il tipo di dati più utili da raccogliere dipende dalla natura del problema.

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Creare una tempistica delle modifiche recenti	Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	<ul style="list-style-type: none"><li>• <a href="#">Creazione di una cronologia delle modifiche recenti</a></li></ul>
Consente di rivedere avvisi e allarmi	<p>Gli avvisi e gli allarmi possono aiutare a determinare rapidamente la causa principale di un problema fornendo importanti indizi sui problemi sottostanti che potrebbero causarlo.</p> <p>Consultare l'elenco degli avvisi e degli allarmi correnti per verificare se StorageGRID ha identificato la causa principale di un problema.</p> <p>Per ulteriori informazioni, rivedere gli avvisi e gli allarmi attivati in passato.</p>	<ul style="list-style-type: none"><li>• <a href="#">"Visualizzazione degli avvisi correnti"</a></li><li>• <a href="#">"Visualizzazione degli allarmi legacy"</a></li><li>• <a href="#">"Visualizzazione degli avvisi risolti"</a></li><li>• <a href="#">"Revisione della cronologia degli allarmi e della frequenza degli allarmi (sistema precedente)"</a></li></ul>
Monitorare gli eventi	Gli eventi includono qualsiasi errore di sistema o evento di guasto per un nodo, inclusi errori come gli errori di rete. Monitorare gli eventi per ottenere ulteriori informazioni sui problemi o per la risoluzione dei problemi.	<ul style="list-style-type: none"><li>• <a href="#">"Visualizzazione della scheda Eventi"</a></li><li>• <a href="#">"Monitoraggio degli eventi"</a></li></ul>
Identificare i trend utilizzando report a grafico e di testo	Le tendenze possono fornire indizi preziosi su quando sono comparsi i problemi per la prima volta e possono aiutarti a capire quanto rapidamente le cose stanno cambiando.	<ul style="list-style-type: none"><li>• <a href="#">"Utilizzo di grafici e report"</a></li></ul>
Stabilire le linee di base	Raccogliere informazioni sui livelli normali dei vari valori operativi. Questi valori di riferimento, e le deviazioni da queste linee di base, possono fornire indizi preziosi.	<ul style="list-style-type: none"><li>• <a href="#">Definizione delle linee di base</a></li></ul>
Eseguire test di acquisizione e recupero	Per risolvere i problemi di performance con acquisizione e recupero, utilizzare una workstation per memorizzare e recuperare gli oggetti. Confrontare i risultati con quelli osservati durante l'utilizzo dell'applicazione client.	<ul style="list-style-type: none"><li>• <a href="#">"Monitoring PUT e PERFORMANCE"</a></li></ul>

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Esaminare i messaggi di audit	Esaminare i messaggi di audit per seguire in dettaglio le operazioni di StorageGRID. I dettagli nei messaggi di audit possono essere utili per la risoluzione di molti tipi di problemi, inclusi quelli relativi alle performance.	<ul style="list-style-type: none"> <li>• "Revisione dei messaggi di audit"</li> </ul>
Controllare le posizioni degli oggetti e l'integrità dello storage	In caso di problemi di storage, verificare che gli oggetti siano posizionati nel punto previsto. Verificare l'integrità dei dati dell'oggetto su un nodo di storage.	"Monitoraggio delle operazioni di verifica degli oggetti".
Raccogliere i dati per il supporto tecnico	Il supporto tecnico potrebbe richiedere di raccogliere dati o rivedere informazioni specifiche per risolvere i problemi.	<ul style="list-style-type: none"> <li>• "Raccolta di file di log e dati di sistema"</li> <li>• "Attivazione manuale di un messaggio AutoSupport"</li> <li>• "Analisi delle metriche di supporto"</li> </ul>

## Creazione di una cronologia delle modifiche recenti

Quando si verifica un problema, è necessario prendere in considerazione le modifiche apportate di recente e il momento in cui si sono verificate tali modifiche.

- Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.
- Una tempistica delle modifiche può aiutarti a identificare quali modifiche potrebbero essere responsabili di un problema e in che modo ciascuna modifica potrebbe avere influenzato il suo sviluppo.

Creare una tabella di modifiche recenti al sistema che includa informazioni su quando si è verificata ogni modifica e su eventuali dettagli rilevanti relativi alla modifica, ad esempio informazioni su ciò che è accaduto durante l'esecuzione della modifica:

Tempo di cambiamento	Tipo di cambiamento	Dettagli
<p>Ad esempio:</p> <ul style="list-style-type: none"> <li>• Quando è stato avviato il ripristino del nodo?</li> <li>• Quando è stato completato l'aggiornamento del software?</li> <li>• Hai interrotto il processo?</li> </ul>	Che cosa è successo? Cosa hai fatto?	<p>Documentare i dettagli relativi alla modifica. Ad esempio:</p> <ul style="list-style-type: none"> <li>• Dettagli delle modifiche di rete.</li> <li>• Quale hotfix è stato installato.</li> <li>• Come sono cambiati i carichi di lavoro dei client.</li> </ul> <p>Assicurarsi di notare se più di una modifica si è verificata contemporaneamente. Ad esempio, questa modifica è stata apportata mentre era in corso un aggiornamento?</p>

## Esempi di modifiche recenti significative

Ecco alcuni esempi di modifiche potenzialmente significative:

- Il sistema StorageGRID è stato recentemente installato, ampliato o ripristinato?
- Il sistema è stato aggiornato di recente? È stata applicata una correzione rapida?
- L'hardware è stato riparato o modificato di recente?
- La policy ILM è stata aggiornata?
- Il carico di lavoro del client è cambiato?
- L'applicazione client o il suo comportamento sono cambiati?
- Hai modificato i bilanciatori di carico o aggiunto o rimosso un gruppo ad alta disponibilità di nodi di amministrazione o nodi gateway?
- Sono state avviate attività che potrebbero richiedere molto tempo? Alcuni esempi sono:
  - Ripristino di un nodo di storage guasto
  - Disattivazione del nodo di storage
- Sono state apportate modifiche all'autenticazione dell'utente, ad esempio l'aggiunta di un tenant o la modifica della configurazione LDAP?
- La migrazione dei dati è in corso?
- I servizi della piattaforma sono stati abilitati o modificati di recente?
- La compliance è stata abilitata di recente?
- I pool di storage cloud sono stati aggiunti o rimossi?
- Sono state apportate modifiche alla compressione o alla crittografia dello storage?
- Sono state apportate modifiche all'infrastruttura di rete? Ad esempio, VLAN, router o DNS.
- Sono state apportate modifiche alle origini NTP?
- Sono state apportate modifiche alle interfacce Grid, Admin o Client Network?
- Sono state apportate modifiche alla configurazione del nodo di archiviazione?
- Sono state apportate altre modifiche al sistema StorageGRID o al suo ambiente?

## Definizione delle linee di base

È possibile stabilire linee di base per il sistema registrando i livelli normali di diversi valori operativi. In futuro, è possibile confrontare i valori correnti con queste linee di base per rilevare e risolvere i valori anomali.



Proprietà	Valore	Come ottenere
Consumo medio di storage	GB consumati al giorno  Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione).  Nel grafico Storage used - Object Data (Storage utilizzato - dati oggetto), individuare un periodo in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare la quantità di storage consumata ogni giorno  È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Consumo medio di metadati	GB consumati al giorno  Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione).  Nel grafico Storage used - Object Metadata (Storage utilizzato - metadati oggetto), individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per valutare la quantità di storage dei metadati consumata ogni giorno  È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Tasso di operazioni S3/Swift	Operazioni/secondo	Accedere alla dashboard in Grid Manager. Nella sezione Protocol Operations (operazioni protocollo), visualizzare i valori per la velocità S3 e la velocità Swift.  Per visualizzare i tassi di acquisizione e recupero e i conteggi per un sito o nodo specifico, selezionare <b>Nodes Site o Storage Node Objects</b> . Spostare il cursore sul grafico Ingest e Retrieve per S3 o Swift.
Operazioni S3/Swift non riuscite	Operazioni	Selezionare <b>supporto Strumenti topologia griglia</b> . Nella scheda Overview (Panoramica) della sezione API Operations (operazioni API), visualizzare il valore di S3 Operations - Failed (operazioni S3 - non riuscite) o Swift Operations - Failed (operazioni Swift - non riuscite).
Tasso di valutazione ILM	Oggetti/secondo	Dalla pagina nodi, selezionare <b>grid ILM</b> .  Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare un valore di riferimento per <b>tasso di valutazione</b> per il sistema.

Proprietà	Valore	Come ottenere
Velocità di scansione ILM	Oggetti/secondo	Selezionare <b>nodi grid ILM</b> .  Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare un valore di riferimento per <b>velocità di scansione</b> per il sistema.
Oggetti accodati dalle operazioni del client	Oggetti/secondo	Selezionare <b>nodi grid ILM</b> .  Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare un valore di riferimento per <b>oggetti accodati (dalle operazioni client)</b> per il sistema.
Latenza media delle query	Millisecondi	Selezionare <b>nodi nodo di storage oggetti</b> . Nella tabella Query, visualizzare il valore della latenza media.

## Analisi dei dati


Utilizzare le informazioni raccolte per determinare la causa del problema e le potenziali soluzioni.


-analisi dipende dal problema, ma in generale:


- Individuare i punti di guasto e i colli di bottiglia utilizzando gli allarmi.
- Ricostruire la cronologia dei problemi utilizzando la cronologia degli allarmi e i grafici.
- Utilizzare i grafici per individuare le anomalie e confrontare la situazione del problema con il normale funzionamento.

## Lista di controllo per le informazioni di escalation

Se non si riesce a risolvere il problema da solo, contattare il supporto tecnico. Prima di contattare il supporto tecnico, raccogliere le informazioni elencate nella seguente tabella per facilitare la risoluzione del problema.

	Elemento	Note
	Dichiarazione del problema	Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo coerente o intermittente? In caso di intermittenza, quali sono le volte in cui si è verificato il problema?  "Definizione del problema"

	Elemento	Note
	Valutazione dell'impatto	<p>Qual è la gravità del problema? Qual è l'impatto sull'applicazione client?</p> <ul style="list-style-type: none"> <li>• Il client si è connesso correttamente in precedenza?</li> <li>• Il client è in grado di acquisire, recuperare ed eliminare i dati?</li> </ul>
	ID sistema StorageGRID	Selezionare <b>manutenzione sistema licenza</b> . L'ID di sistema StorageGRID viene visualizzato come parte della licenza corrente.
	Versione del software	Fare clic su <b>Guida informazioni</b> per visualizzare la versione di StorageGRID.
	Personalizzazione	<p>Riepilogare la configurazione del sistema StorageGRID. Ad esempio, elencare quanto segue:</p> <ul style="list-style-type: none"> <li>• Il grid utilizza la compressione dello storage, la crittografia dello storage o la conformità?</li> <li>• ILM esegue la replica o la cancellazione di oggetti codificati? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano comportamenti di ingest rigorosi, bilanciati o doppi?</li> </ul>
	File di log e dati di sistema	<p>Raccogliere i file di log e i dati di sistema per il sistema. Selezionare <b>Support Tools Logs</b>.</p> <p>È possibile raccogliere i log per l'intera griglia o per i nodi selezionati.</p> <p>Se si stanno raccogliendo registri solo per i nodi selezionati, assicurarsi di includere almeno un nodo di storage che dispone del servizio ADC. I primi tre nodi di storage di un sito includono il servizio ADC.</p> <p><a href="#">"Raccolta di file di log e dati di sistema"</a></p>
	Informazioni di riferimento	<p>Raccogliere informazioni di riferimento relative alle operazioni di acquisizione, alle operazioni di recupero e al consumo dello storage.</p> <p><a href="#">"Definizione delle linee di base"</a></p>
	Tempistiche delle modifiche recenti	<p>Creare una timeline che riepiloga le modifiche recenti apportate al sistema o al suo ambiente.</p> <p><a href="#">"Creazione di una cronologia delle modifiche recenti"</a></p>

	Elemento	Note
	Cronologia degli sforzi per diagnosticare il problema	Se sono state adottate misure per diagnosticare o risolvere il problema da soli, assicurarsi di registrare i passaggi e il risultato.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

## 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 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 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.

#### Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

Look Up

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": {
      "PAIS": "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**.



## Overview: LDR (DC1-S1) - Storage

Updated: 2020-01-29 15:03:39 PST

Storage State - Desired:	Online	
Storage State - Current:	Online	
Storage Status:	No Errors	

### Utilization

Total Space:	322 GB	
Total Usable Space:	311 GB	
Total Usable Space (Percent):	96.534 %	
Total Data:	994 KB	
Total Data (Percent):	0 %	

### Replication

Block Reads:	0	
Block Writes:	0	
Objects Retrieved:	0	
Objects Committed:	0	
Objects Deleted:	0	
Delete Service State:	Enabled	

### Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health	
0000	107 GB	96.4 GB	994 KB	0 B	0.001 %	No Errors	
0001	107 GB	107 GB	0 B	0 B	0 %	No Errors	
0002	107 GB	107 GB	0 B	0 B	0 %	No Errors	

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).

Overview Alarms Reports Configuration

Main Alarms

Configuration: LDR (DC2-S1-106-147) - Verification  
Updated: 2019-04-24 16:13:44 PDT

Reset Missing Objects Count ☐

**Foreground Verification**

ID	Verify
0	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>

**Background Verification**

Verification Rate

Reset Corrupt Objects Count ☐

**Quarantined Objects**

Delete Quarantined Objects ☐

Apply Changes



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.

Overview Alarms Reports **Configuration**

Main Alarms

 **Configuration: LDR (dc1-cs1-99-82) - Verification**  
Updated: 2015-08-19 14:07:04 PDT

Reset Missing Objects Count ☐


**Foreground Verification**

ID	Verify
0	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>

**Background Verification**

Verification Rate

Reset Corrupt Objects Count ☐

Apply Changes 

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 valid`, 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.

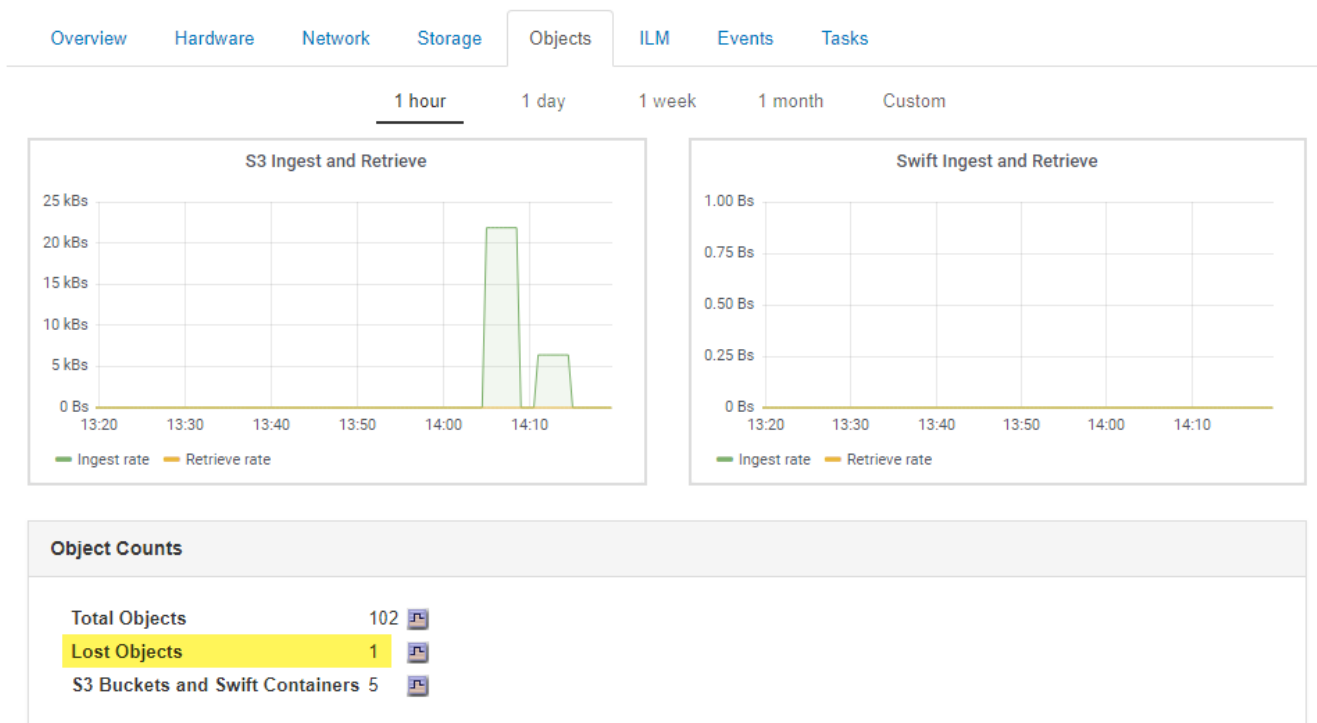
Il numero di oggetti persi può essere visualizzato in Grid Manager.

### 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.

99-97 (Storage Node)



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 OLS (Object Lost). Inserire: `grep OLS audit_file_name`
- d. Annotare il valore UUID incluso nel messaggio.

```
>Admin: # grep OLS 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):OLS][ANID(UI32):12448208][AMID(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)": "MD5D0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "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",
        "VOLLI\ (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",
        "VOLLI\ (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":")	<p>Se l'oggetto non viene trovato, viene visualizzato il messaggio "ERROR":.</p> <p>Se l'oggetto non viene trovato, è possibile ignorare l'allarme. La mancanza di un oggetto indica che l'oggetto è stato intenzionalmente cancellato.</p>
Posizioni 0	<p>Se nell'output sono presenti posizioni, l'allarme oggetti persi potrebbe essere un falso positivo.</p> <p>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.</p> <p>La procedura per trovare oggetti potenzialmente persi spiega come utilizzare l'ID nodo per trovare il nodo di storage corretto.</p> <p><a href="#">"Ricerca e ripristino di oggetti potenzialmente persi"</a></p> <p>Se gli oggetti sono presenti, è possibile ripristinare il numero di oggetti persi per annullare l'allarme e l'avviso.</p>
Posizioni = 0	<p>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.</p> <p><a href="#">"Ricerca e ripristino di oggetti potenzialmente persi"</a></p> <p>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 <i>repair-data</i> 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.</p>

## 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 SUDETTO. 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",
    "VOLII\(Volume ID\)": "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",
    "VOLII\(Volume ID\)": "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

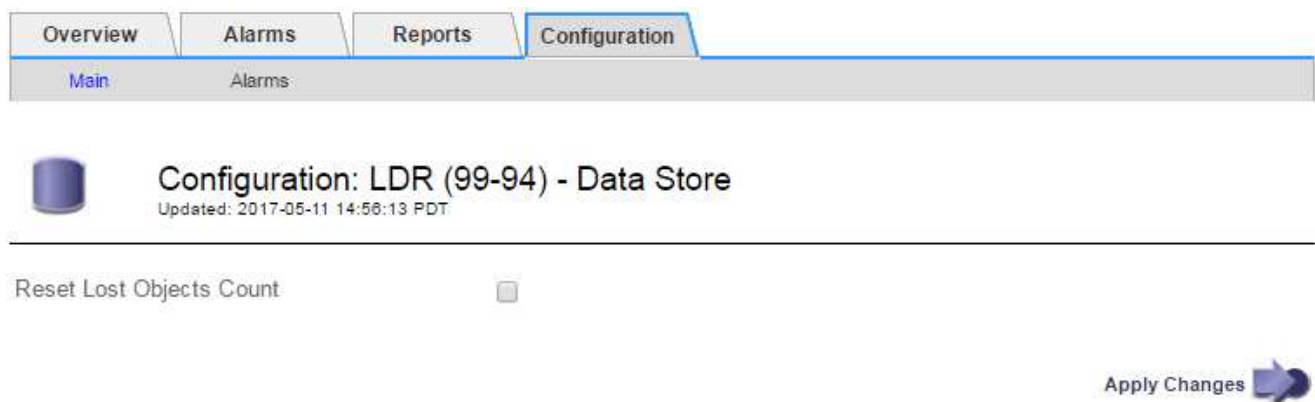
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

- **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 corrupted 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:

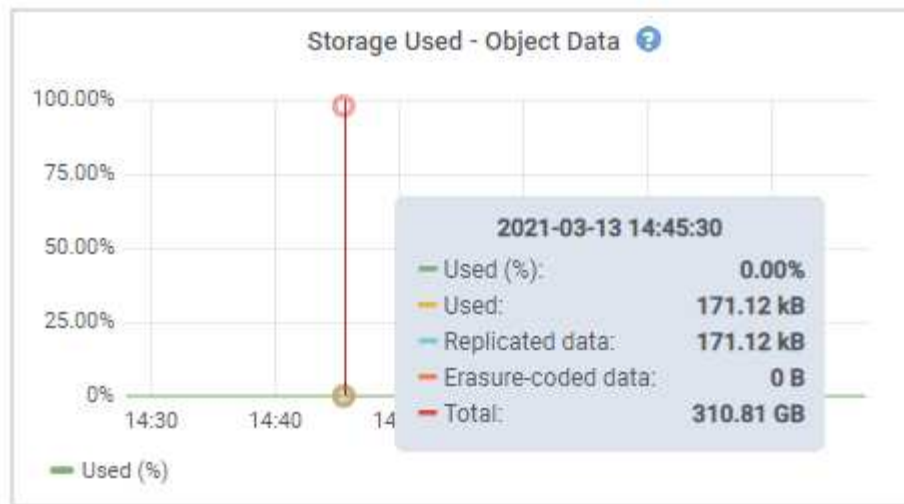
- Tempo di attivazione
- Il nome del sito e del nodo
- I valori correnti delle metriche per questo avviso

### 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.


OverviewAlarmsReportsConfiguration

MainHistory



**Alarms: LDR (DC1-S3-101-195) - Storage**  
Updated: 2019-10-09 12:52:43 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
 Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
 Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
 Normal	SHLH (Health)						<input type="checkbox"/>

Apply Changes 

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).


Overview

Alarms

Reports

Configuration

Main



Overview: LDR (.DC1-S1-101-193) - Storage  
Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:

Online

Storage State - Current:

Read-only

Storage Status:

Insufficient Free Space

Utilization

Total Space:

164 GB

Total Usable Space:

19.6 GB

Total Usable Space (Percent):

11.937 %

Total Data:

139 GB

Total Data (Percent):

84.567 %

Replication

Block Reads:

0

Block Writes:

2,279,881

Objects Retrieved:

0

Objects Committed:

88,882
















Objects Deleted:

16

Delete Service State:

Enabled

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health	
0000	54.7 GB	2.93 GB	 46.2 GB	 0 B	 84.486 %	No Errors	 
0001	54.7 GB	8.32 GB	 46.3 GB	 0 B	 84.644 %	No Errors	 
0002	54.7 GB	8.36 GB	 46.3 GB	 0 B	 84.57 %	No Errors	 

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.

Overview


Alarms

Reports

Configuration

Charts

Text



Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:

Total Usable Space

▼

Quick Query:

Custom Query

▼

Update

Vertical Scaling:

☒

Raw Data:

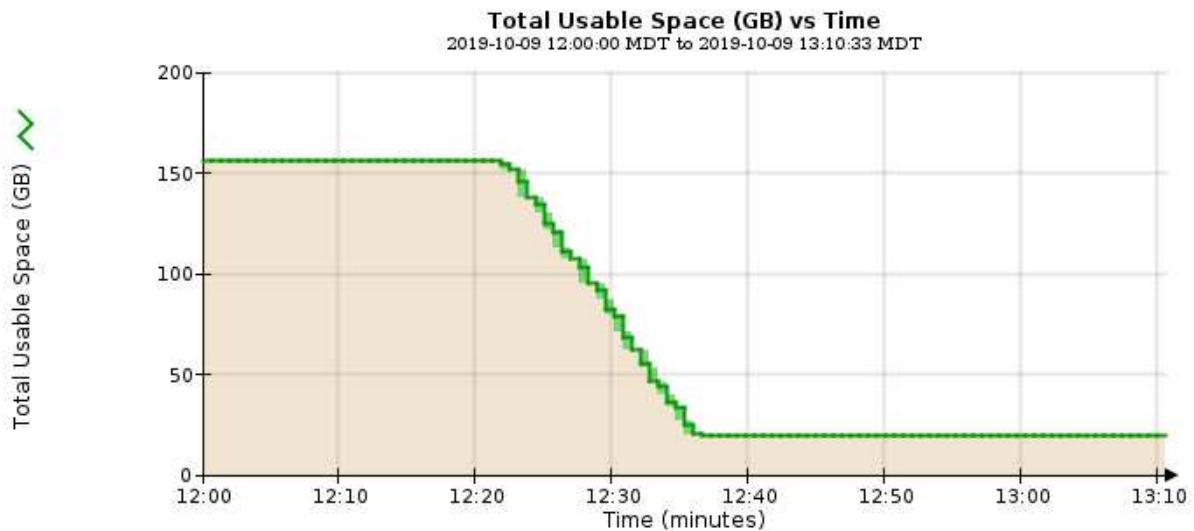
☐

Start Date:

2019/10/09 12:00:00

End Date:

2019/10/09 13:10:33



- 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.



Overview

Alarms

Reports

Configuration

Charts

Text

Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:

Total Usable Space (Percent)

Quick Query:

Custom Query

Update

Vertical Scaling:

☒

Raw Data:

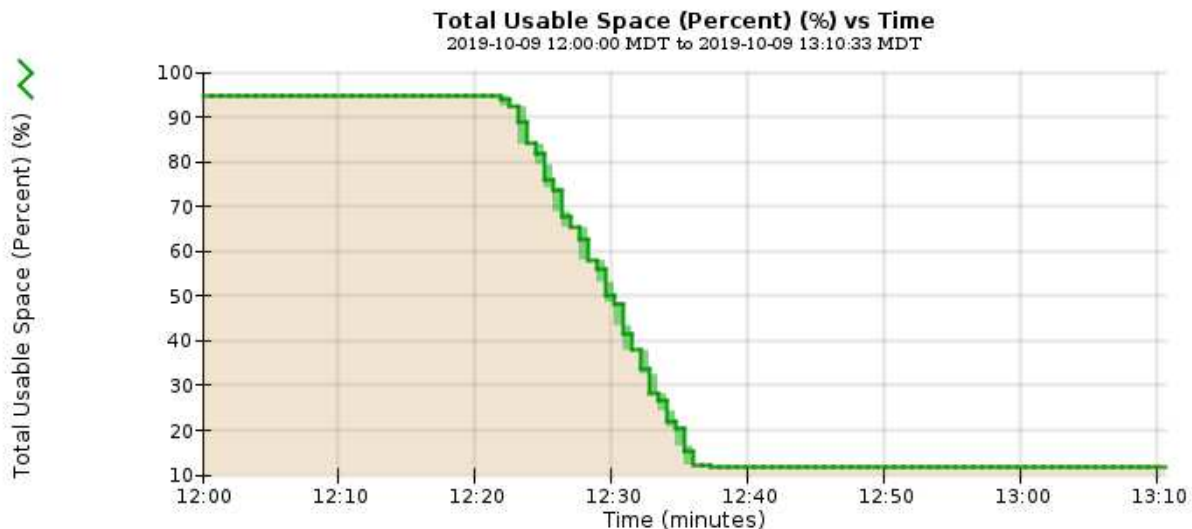
☐

Start Date:

2019/10/09 12:00:00

End Date:

2019/10/09 13:10:33



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/broadcast-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"](#)

## Risoluzione dei problemi relativi ai metadati

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi ai metadati.

### Risoluzione dei problemi relativi all'avviso di storage metadati in esaurimento

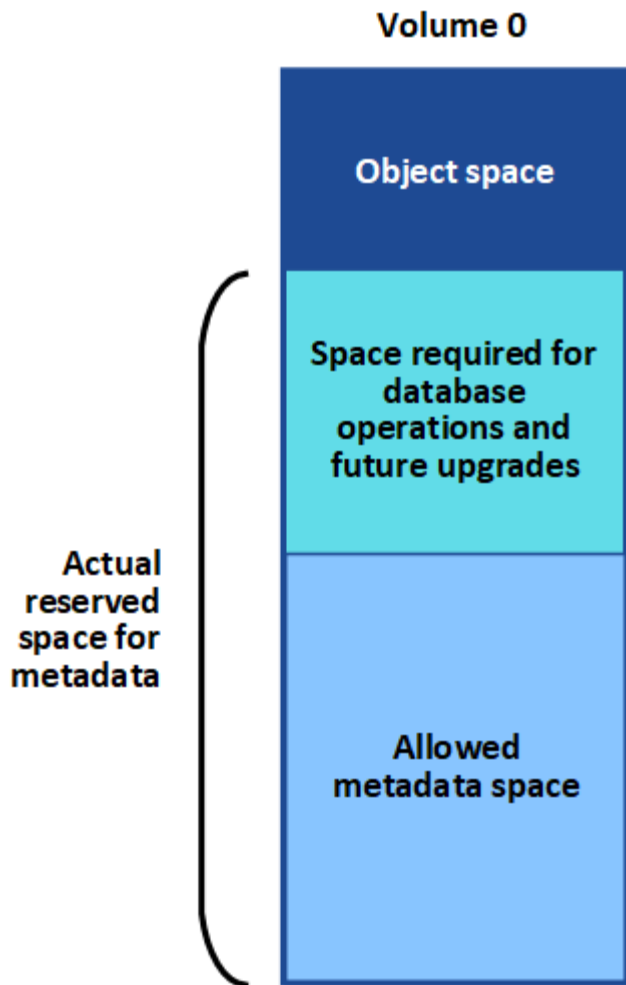
Se viene attivato l'avviso **Low metadata storage**, è necessario aggiungere nuovi nodi di storage.

#### Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.

#### A proposito di questa attività

StorageGRID riserva una certa quantità di spazio sul volume 0 di ciascun nodo di storage per i metadati dell'oggetto. Questo spazio è noto come spazio riservato effettivo e viene suddiviso nello spazio consentito per i metadati dell'oggetto (lo spazio consentito per i metadati) e nello spazio richiesto per le operazioni essenziali del database, come la compattazione e la riparazione. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



Se i metadati degli oggetti consumano più del 100% dello spazio consentito per i metadati, le operazioni del database non possono essere eseguite in modo efficiente e si verificano errori.

StorageGRID utilizza la seguente metrica Prometheus per misurare la quantità di spazio consentito per i metadati:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Quando l'espressione Prometheus raggiunge determinate soglie, viene attivato l'avviso **Low metadata storage**.

- **Minore:** I metadati degli oggetti utilizzano almeno il 70% dello spazio consentito per i metadati. È necessario aggiungere nuovi nodi di storage il prima possibile.
- **Major:** I metadati degli oggetti utilizzano almeno il 90% dello spazio consentito per i metadati. È necessario aggiungere immediatamente nuovi nodi di storage.



Quando i metadati dell'oggetto utilizzano almeno il 90% dello spazio consentito per i metadati, viene visualizzato un avviso nella dashboard. Se viene visualizzato questo avviso, è necessario aggiungere immediatamente nuovi nodi di storage. Non è mai necessario consentire ai metadati degli oggetti di utilizzare più del 100% dello spazio consentito.

- **Critico:** I metadati degli oggetti utilizzano almeno il 100% dello spazio consentito e stanno iniziando a consumare lo spazio necessario per le operazioni essenziali del database. È necessario interrompere l'acquisizione di nuovi oggetti e aggiungere immediatamente nuovi nodi di storage.

Nell'esempio seguente, i metadati degli oggetti utilizzano oltre il 100% dello spazio consentito per i metadati. Si tratta di una situazione critica, che può causare errori e operazioni inefficienti del database.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.



Se la dimensione del volume 0 è inferiore all'opzione di storage Metadata Reserved Space (ad esempio, in un ambiente non in produzione), il calcolo dell'avviso **Low metadata storage** potrebbe essere impreciso.

## Fasi

1. Selezionare **Avvisi corrente**.
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low metadata storage**, se necessario, e selezionare l'avviso specifico che si desidera visualizzare.
3. Esaminare i dettagli nella finestra di dialogo degli avvisi.
4. Se è stato attivato un avviso importante o critico **Low metadata storage**, eseguire un'espansione per aggiungere immediatamente i nodi di storage.



Poiché StorageGRID conserva copie complete di tutti i metadati degli oggetti in ogni sito, la capacità dei metadati dell'intera griglia è limitata dalla capacità dei metadati del sito più piccolo. Se è necessario aggiungere capacità di metadati a un sito, è necessario espandere anche gli altri siti dello stesso numero di nodi di storage.

Dopo aver eseguito l'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti nei nuovi nodi, aumentando così la capacità complessiva dei metadati della griglia. Non è richiesta alcuna azione da parte dell'utente. L'avviso **Low metadata storage** viene cancellato.

## Informazioni correlate

["Monitoraggio della capacità dei metadati degli oggetti per ciascun nodo di storage"](#)

["Espandi il tuo grid"](#)

## Risoluzione dei problemi relativi all'allarme Services: Status - Cassandra (SVST)

L'allarme servizi: Stato - Cassandra (SVST) indica che potrebbe essere necessario ricostruire il database Cassandra per un nodo di storage. Cassandra viene utilizzato come archivio di metadati per StorageGRID.

### 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

Se Cassandra viene arrestato per più di 15 giorni (ad esempio, il nodo di storage viene spento), Cassandra non si avvia quando il nodo viene riportato in linea. È necessario ricostruire il database Cassandra per il servizio DDS interessato.

È possibile utilizzare la pagina Diagnostics (Diagnostica) per ottenere ulteriori informazioni sullo stato corrente della griglia.

### "Esecuzione della diagnostica"




Se due o più servizi di database Cassandra rimangono inutilizzati per più di 15 giorni, contattare il supporto tecnico e non procedere con la procedura riportata di seguito.

### Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Site Storage Node SSM Services Alarms Main** per visualizzare gli allarmi.


Questo esempio mostra che l'allarme SVST è stato attivato.

Overview Alarms Reports Configuration						
Main History						
 <b>Alarms: SSM (DC1-S3) - Services</b> Updated: 2014-08-14 16:29:36 PDT						
Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge
Minor	SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:28 PDT	Not Running	Not Running	<input type="checkbox"/>

La pagina principale dei servizi SSM indica inoltre che Cassandra non è in esecuzione.

Overview
Alarms
Reports
Configuration

Main



**Overview: SSM (DC2-S1) - Services**  
Updated: 2017-03-30 09:53:53 MDT

Operating System:
Linux  
3.16.0-4-amd64

**Services**

Service	Version	Status	Threads	Load	Memory
Account Service	10.4.0-20161224.0333.803cd91	Running	7	0.002 %	12 MB
Administrative Domain Controller (ADC)	10.4.0-20170329.0039.8800cae	Running	52	0.14 %	63.1 MB
Cassandra	4.6.12-1.byc.0-20170308.0109.ba3598a	Not Running	0	0 %	0 B
Content Management System (CMS)	10.4.0-20170220.1846.1a76aed	Running	18	0.055 %	20.6 MB
Distributed Data Store (DDS)	10.4.0-20170329.0039.8800cae	Running	104	1.301 %	76 MB
Identity Service	10.4.0-20170203.2038.a457d45	Running	6	0 %	8.75 MB
Keystone Service	10.4.0-20170104.1815.6e52138	Running	5	0 %	7.77 MB
Local Distribution Router (LDR)	10.4.0-20170329.0039.8800cae	Running	109	0.218 %	96.6 MB
Server Manager	10.4.0-20170306.2303.9649faf	Running	4	3.58 %	19.1 MB

# 1. Provare a riavviare Cassandra dal nodo di storage:

## a. Accedere al nodo Grid:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

## b. Inserire: `/etc/init.d/cassandra status`

## c. Se Cassandra non è in esecuzione, riavviarlo: `/etc/init.d/cassandra restart`

# 2. Se Cassandra non si riavvia, determinare per quanto tempo Cassandra è rimasto inattivo. Se Cassandra è rimasto inattivo per più di 15 giorni, è necessario ricostruire il database Cassandra.



Se due o più servizi di database Cassandra non sono disponibili, contattare il supporto tecnico e non procedere con i passaggi riportati di seguito.

È possibile determinare per quanto tempo Cassandra è rimasta inattiva, inserendolo nella cartella o esaminando il file `servermanager.log`.

# 3. Per inserire il grafico Cassandra:

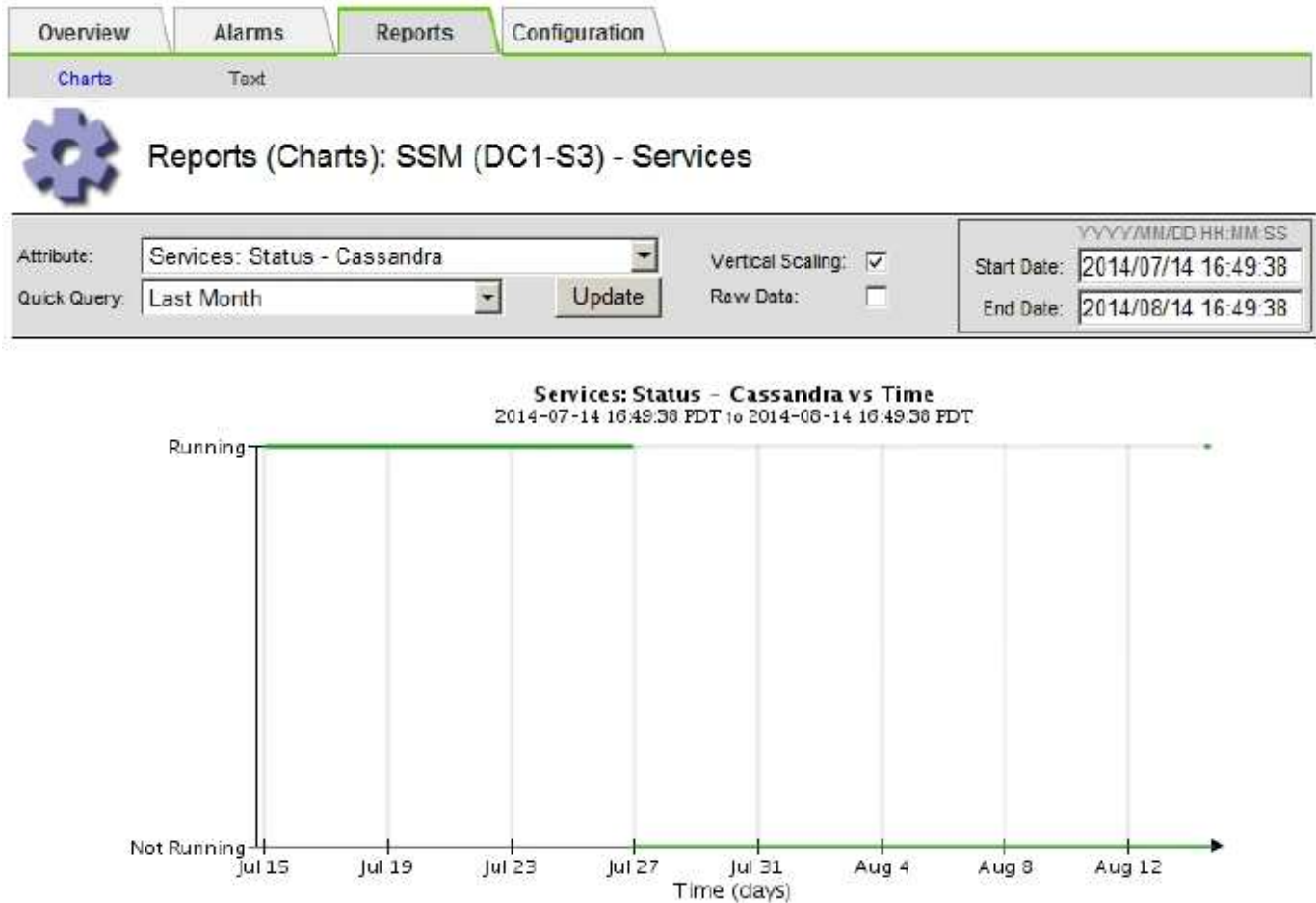
- Selezionare **supporto Strumenti topologia griglia**. Quindi selezionare **Site Storage Node SSM servizi Report grafici**.
- Selezionare **attributo Servizio: Stato - Cassandra**.
- Per **Data di inizio**, immettere una data che sia almeno 16 giorni prima della data corrente. Per **Data di**

**fine**, inserire la data corrente.

d. Fare clic su **Aggiorna**.

e. Se il grafico mostra Cassandra come inattivo per più di 15 giorni, ricostruire il database Cassandra.

L'esempio seguente mostra che Cassandra è rimasta inattiva per almeno 17 giorni.



1. Per esaminare il file `servermanager.log` sul nodo di storage:

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. Inserire: `cat /var/local/log/servermanager.log`

Viene visualizzato il contenuto del file `servermanager.log`.

Se Cassandra rimane inattivo per più di 15 giorni, nel file `servermanager.log` viene visualizzato il seguente messaggio:



```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

- a. Assicurarsi che la data e l'ora del messaggio siano quelle in cui si è tentato di riavviare Cassandra, come indicato al punto [Riavviare Cassandra dal nodo di storage](#).

Per Cassandra possono essere presenti più voci; è necessario individuare la voce più recente.

- b. Se Cassandra è rimasto inattivo per più di 15 giorni, è necessario ricostruire il database Cassandra.

Per istruzioni, vedere “Ripristino da un singolo nodo di storage inattivo per più di 15 giorni” nelle istruzioni di ripristino e manutenzione.

- c. Contattare il supporto tecnico se gli allarmi non vengono disattivati dopo la ricostruzione di Cassandra.

#### Informazioni correlate

["Mantieni Ripristina"](#)

## Risoluzione dei problemi errori di memoria esaurita di Cassandra (allarme SMTT)

Un allarme SMTT (Total Events) viene attivato quando il database Cassandra presenta un errore di memoria esaurita. Se si verifica questo errore, contattare il supporto tecnico per risolvere il problema.

#### A proposito di questa attività

Se si verifica un errore di memoria insufficiente per il database Cassandra, viene creato un dump heap, viene attivato un allarme SMTT (Total Events) e il conteggio degli errori Cassandra Heap out of Memory viene incrementato di uno.

#### Fasi

1. Per visualizzare l'evento, selezionare **Nodes Grid Node Events**.
2. Verificare che il conteggio degli errori di memoria esaurita di Cassandra sia pari o superiore a 1.

È possibile utilizzare la pagina Diagnostics (Diagnostica) per ottenere ulteriori informazioni sullo stato corrente della griglia.

["Esecuzione della diagnostica"](#)

3. Passare a `/var/local/core/`, comprimere `Cassandra.hprof` e inviarla al supporto tecnico.
4. Eseguire un backup di `Cassandra.hprof` ed eliminarlo da `/var/local/core/` directory.

Questo file può avere una dimensione massima di 24 GB, quindi è necessario rimuoverlo per liberare spazio.

5. Una volta risolto il problema, fare clic su **Reset event count** (Ripristina conteggi eventi).



Per reimpostare i conteggi degli eventi, è necessario disporre dell'autorizzazione Grid Topology Page Configuration (Configurazione pagina topologia griglia).

#### Informazioni correlate



## Risoluzione degli errori del certificato

Se si verifica un problema di sicurezza o certificato quando si tenta di connettersi a StorageGRID utilizzando un browser Web, un client S3 o Swift o uno strumento di monitoraggio esterno, controllare il certificato.

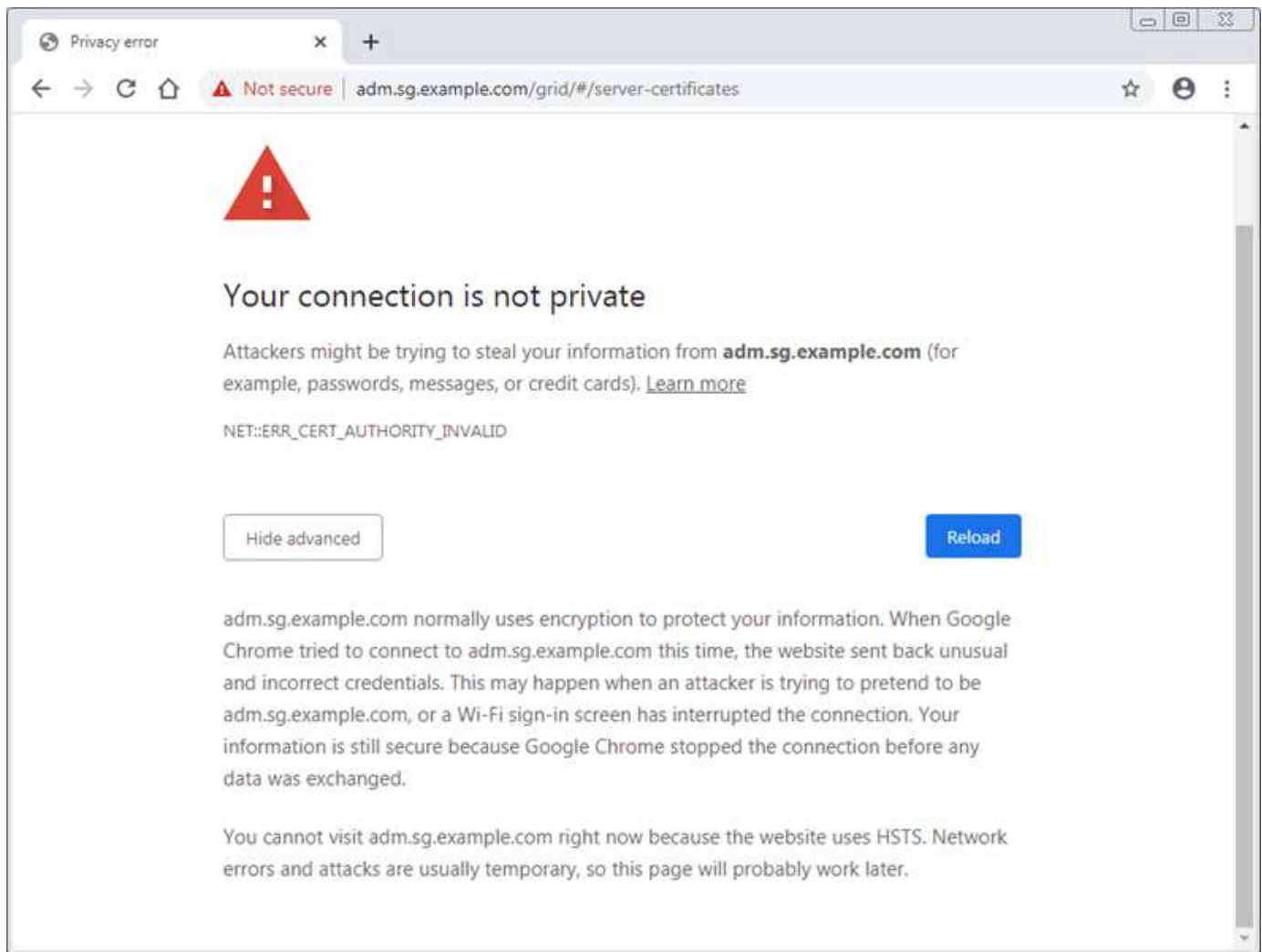
### A proposito di questa attività

Gli errori dei certificati possono causare problemi quando si tenta di connettersi a StorageGRID utilizzando Gestione griglia, API di gestione griglia, Gestore tenant o API di gestione tenant. Gli errori di certificato possono verificarsi anche quando si tenta di connettersi a un client S3 o Swift o a uno strumento di monitoraggio esterno.

Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato del server dell'interfaccia di gestione personalizzata scade.
- Viene ripristinato il certificato del server di un'interfaccia di gestione personalizzata al certificato del server predefinito.

L'esempio seguente mostra un errore di certificato quando il certificato del server dell'interfaccia di gestione personalizzata è scaduto:



Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** viene attivato quando il certificato del server sta per scadere.

Quando si utilizzano certificati client per l'integrazione esterna di Prometheus, gli errori dei certificati possono essere causati dal certificato del server dell'interfaccia di gestione StorageGRID o dai certificati client. L'avviso **scadenza dei certificati configurati nella pagina certificati client** viene attivato quando un certificato client sta per scadere.

### Fasi

1. Se si riceve una notifica di avviso relativa a un certificato scaduto, accedere ai dettagli del certificato:
  - Per un certificato server, selezionare **Configurazione Impostazioni di rete certificati server**.
  - Per un certificato client, selezionare **Configuration Access Control Client Certificates**.
2. Controllare il periodo di validità del certificato.

Alcuni browser Web e client S3 o Swift non accettano certificati con un periodo di validità superiore a 398 giorni.

3. Se il certificato è scaduto o scadrà a breve, caricare o generare un nuovo certificato.
  - Per un certificato server, consultare la procedura per la configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager nelle istruzioni per l'amministrazione di

StorageGRID.

- Per un certificato client, consultare la procedura per la configurazione di un certificato client nelle istruzioni per l'amministrazione di StorageGRID.

4. In caso di errori del certificato del server, provare una o entrambe le seguenti opzioni:

- Assicurarsi che il campo Subject alternative Name (SAN) del certificato sia compilato e che LA SAN corrisponda all'indirizzo IP o al nome host del nodo a cui si sta effettuando la connessione.
- Se si sta tentando di connettersi a StorageGRID utilizzando un nome di dominio:
  - i. Inserire l'indirizzo IP del nodo di amministrazione invece del nome di dominio per evitare l'errore di connessione e accedere a Grid Manager.
  - ii. In Grid Manager, selezionare **Configuration Network Settings Server Certificates** per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
  - iii. Nelle istruzioni per l'amministrazione di StorageGRID, consultare la procedura per la configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

## Risoluzione dei problemi relativi al nodo di amministrazione e all'interfaccia utente

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi ai nodi di amministrazione e all'interfaccia utente di StorageGRID.

### Risoluzione dei problemi relativi agli errori di accesso

Se si verifica un errore durante l'accesso a un nodo amministrativo StorageGRID, il sistema potrebbe avere un problema con la configurazione della federazione delle identità, un problema di rete o hardware, un problema con i servizi del nodo amministrativo o un problema con il database Cassandra sui nodi di storage connessi.

#### Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` file.
- È necessario disporre di autorizzazioni di accesso specifiche.

#### A proposito di questa attività

Utilizzare queste linee guida per la risoluzione dei problemi se viene visualizzato uno dei seguenti messaggi di errore quando si tenta di accedere a un nodo amministratore:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start...`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page...`

#### Fasi

1. Attendere 10 minuti e riprovare a effettuare l'accesso.

Se l'errore non viene risolto automaticamente, passare alla fase successiva.

2. Se il sistema StorageGRID dispone di più di un nodo amministratore, provare ad accedere al gestore della griglia da un altro nodo amministratore.
  - Se sei in grado di effettuare l'accesso, puoi utilizzare le opzioni **Dashboard, Nodes, Alerts e Support** per determinare la causa dell'errore.
  - Se si dispone di un solo nodo di amministrazione o non si riesce ancora ad accedere, passare alla fase successiva.
3. Determinare se l'hardware del nodo non è in linea.
4. Se il sistema StorageGRID è abilitato per l'accesso singolo (SSO), fare riferimento alla procedura per la configurazione dell'accesso singolo nelle istruzioni per l'amministrazione di StorageGRID.

Potrebbe essere necessario disattivare temporaneamente e riattivare SSO per un singolo nodo di amministrazione per risolvere eventuali problemi.



Se SSO è attivato, non è possibile accedere utilizzando una porta con restrizioni. È necessario utilizzare la porta 443.

5. Determinare se l'account in uso appartiene a un utente federato.

Se l'account utente federated non funziona, provare ad accedere a Grid Manager come utente locale, ad esempio root.

- Se l'utente locale può effettuare l'accesso:
    - i. Esaminare gli eventuali allarmi visualizzati.
    - ii. Selezionare **Configuration Identity Federation**.
    - iii. Fare clic su **Test Connection** (verifica connessione) per convalidare le impostazioni di connessione per il server LDAP.
    - iv. Se il test non riesce, risolvere eventuali errori di configurazione.
  - Se l'utente locale non riesce ad accedere e si è certi che le credenziali siano corrette, passare alla fase successiva.
6. Utilizzare Secure Shell (ssh) per accedere al nodo di amministrazione:
    - a. Immettere il seguente comando: `ssh admin@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 #.

7. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

Assicurarsi che i servizi api nms, mi, nginx e mgmt siano tutti in esecuzione.

L'output viene aggiornato immediatamente se lo stato di un servizio cambia.

```

$ storagegrid-status
Host Name                99-211
IP Address                10.96.99.211
Operating System Kernel  4.19.0                Verified
Operating System Environment Debian 10.1            Verified
StorageGRID Webscale Release 11.4.0                Verified
Networking                Verified
Storage Subsystem        Verified
Database Engine           5.5.9999+default      Running
Network Monitoring        11.4.0                Running
Time Synchronization      1:4.2.8p10+dfsg      Running
ams                        11.4.0                Running
cmn                        11.4.0                Running
nms                        11.4.0                Running
ssm                        11.4.0                Running
mi                        11.4.0                Running
dynip                     11.4.0                Running
nginx                     1.10.3                Running
tomcat                    9.0.27                Running
grafana                   6.4.3                Running
mgmt api                  11.4.0                Running
prometheus                11.4.0                Running
persistence               11.4.0                Running
ade exporter              11.4.0                Running
alertmanager              11.4.0                Running
attrDownPurge             11.4.0                Running
attrDownSamp1             11.4.0                Running
attrDownSamp2             11.4.0                Running
node exporter              0.17.0+ds            Running
sg snmp agent             11.4.0                Running

```

8. Verificare che il server Web Apache sia in esecuzione: `# service apache2 status`

1. Utilizzare Lumberjack per raccogliere i registri: `# /usr/local/sbin/lumberjack.rb`

Se l'autenticazione non è riuscita in passato, è possibile utilizzare le opzioni di script `--start` e `--end` Lumberjack per specificare l'intervallo di tempo appropriato. Utilizzare `lumberjack -h` per i dettagli su queste opzioni.

L'output sul terminale indica dove è stato copiato l'archivio di log.

1. Esaminare i seguenti registri:

- ° `/var/local/log/bycast.log`
- ° `/var/local/log/bycast-err.log`
- ° `/var/local/log/nms.log`

- `**/*commands.txt`

2. Se non si riesce a identificare alcun problema con il nodo di amministrazione, eseguire uno dei seguenti comandi per determinare gli indirizzi IP dei tre nodi di storage che eseguono il servizio ADC presso la propria sede. In genere, si tratta dei primi tre nodi di storage installati nel sito.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

I nodi di amministrazione utilizzano il servizio ADC durante il processo di autenticazione.

3. Dal nodo di amministrazione, accedere a ciascuno dei nodi di storage ADC, utilizzando gli indirizzi IP identificati.
  - a. Immettere il seguente comando: `ssh admin@grid_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 #.

4. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

Assicurarsi che i servizi `idnt`, `acct`, `nginx` e `cassandra` siano tutti in esecuzione.

5. Ripetere i passaggi [Utilizzare Lumberjack per raccogliere i registri](#) e [Esaminare i registri](#) Per rivedere i log sui nodi di storage.
6. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

Fornire al supporto tecnico i registri raccolti.

## Informazioni correlate

["Amministrare StorageGRID"](#)

["Riferimenti ai file di log"](#)

## Risoluzione dei problemi relativi all'interfaccia utente

Dopo l'aggiornamento a una nuova versione del software StorageGRID, potrebbero verificarsi problemi con Grid Manager o con il tenant manager.

### L'interfaccia Web non risponde come previsto

Dopo l'aggiornamento del software StorageGRID, il gestore di rete o il tenant manager potrebbero non rispondere come previsto.

In caso di problemi con l'interfaccia Web:

- Assicurarsi di utilizzare un browser supportato.



Il supporto del browser è cambiato per StorageGRID 11.5. Confermare che si sta utilizzando una versione supportata.

- Cancellare la cache del browser Web.

La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare nuovamente correttamente. Per istruzioni, consultare la documentazione del browser Web.

#### Informazioni correlate

["Requisiti del browser Web"](#)

["Amministrare StorageGRID"](#)

## Verifica dello stato di un nodo amministratore non disponibile

Se il sistema StorageGRID include più nodi di amministrazione, è possibile utilizzare un altro nodo di amministrazione per controllare lo stato di un nodo di amministrazione non disponibile.

#### Di cosa hai bisogno

È necessario disporre di autorizzazioni di accesso specifiche.

#### Fasi

1. Da un nodo Admin disponibile, accedere a Grid Manager utilizzando un browser supportato.
2. Selezionare **supporto > Strumenti > topologia griglia**.
3. Selezionare **Site non disponibile Admin Node SSM servizi Panoramica principale**.
4. Cercare i servizi con stato non in esecuzione e che potrebbero essere visualizzati anche in blu.

Operating System: Linux 3.16.0-4-amd64

## Services

Service	Version	Status	Threads	Load	Memory
Audit Management System (AMS)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.043 %	35.7 MB
CIFS Filesharing (nmbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	5.5 MB
CIFS Filesharing (smbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	14.5 MB
CIFS Filesharing (winbindd)	2:4.2.14+dfsg-0+deb8u2	Not Running	0	0 %	0 B
Configuration Management Node (CMN)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.055 %	41.3 MB
Database Engine	5.5.53-0+deb8u1	Running	47	0.354 %	1.33 GB
Grid Deployment Utility Server	10.4.0-20170112.2125.c4253bb	Running	3	0 %	32.8 MB
Management Application Program Interface (mgmt-api)	10.4.0-20170113.2136.07c4997	Not Running	0	0 %	0 B
NFS Filesharing	10.4.0-20161224.0333.803cd91	Not Running	0	0 %	0 B
NMS Data Cleanup	10.4.0-20161224.0333.803cd91	Running	22	0.008 %	52.4 MB
NMS Data Downsampler 1	10.4.0-20161224.0333.803cd91	Running	22	0.049 %	195 MB
NMS Data Downsampler 2	10.4.0-20161224.0333.803cd91	Running	22	0.009 %	157 MB
NMS Processing Engine	10.4.0-20161224.0333.803cd91	Running	40	0.132 %	200 MB

- Determinare se gli allarmi sono stati attivati.
- Intraprendere le azioni appropriate per risolvere il problema.

### Informazioni correlate

["Amministrare StorageGRID"](#)

## Risoluzione dei problemi di rete, hardware e piattaforma

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi a problemi di rete, hardware e piattaforma StorageGRID.

### Risoluzione degli errori “422: Unprocessable Entity”

L'errore 422: Unprocessable Entity può verificarsi in diverse circostanze. Controllare il messaggio di errore per determinare la causa del problema.

Se viene visualizzato uno dei messaggi di errore elencati, eseguire l'azione consigliata.



Messaggio di errore	Causa principale e azione correttiva
<p>422: Unprocessable Entity</p> <p>Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839</p>	<p>Questo messaggio potrebbe essere visualizzato se si seleziona l'opzione <b>non utilizzare TLS</b> per Transport Layer Security (TLS) durante la configurazione della federazione delle identità utilizzando Windows Active Directory (ad).</p> <p>L'utilizzo dell'opzione <b>non utilizzare TLS</b> non è supportato per l'utilizzo con i server ad che applicano la firma LDAP. Selezionare l'opzione <b>Use STARTTLS</b> (Usa STARTTLS*) o l'opzione <b>Use LDAPS</b> (Usa LDAPS* per TLS).</p>
<p>422: Unprocessable Entity</p> <p>Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</p>	<p>Questo messaggio viene visualizzato se si tenta di utilizzare una crittografia non supportata per stabilire una connessione TLS (Transport Layer Security) da StorageGRID a un sistema esterno utilizzato per identificare la federazione o i pool di storage cloud.</p> <p>Controllare le cifre offerte dal sistema esterno. Il sistema deve utilizzare uno dei cifrari supportati da StorageGRID per le connessioni TLS in uscita, come illustrato nelle istruzioni per l'amministrazione di StorageGRID.</p>

#### Informazioni correlate

["Amministrare StorageGRID"](#)

## Risoluzione dei problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia

L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato quando l'impostazione Maximum Transmission Unit (MTU) per l'interfaccia Grid Network (eth0) differisce significativamente tra i nodi della griglia.

## A proposito di questa attività

Le differenze nelle impostazioni MTU potrebbero indicare che alcune, ma non tutte, reti eth0 sono configurate per i frame jumbo. Una mancata corrispondenza delle dimensioni MTU superiore a 1000 potrebbe causare problemi di performance di rete.

### Fasi

1. Elencare le impostazioni MTU per eth0 su tutti i nodi.
  - Utilizzare la query fornita in Grid Manager.
  - Selezionare *primary Admin Node IP address/metrics/graph* e immettere la seguente query:  
`node_network_mtu_bytes{interface='eth0'}`
2. Modificare le impostazioni MTU in base alle necessità per assicurarsi che siano le stesse per l'interfaccia Grid Network (eth0) su tutti i nodi.
  - Per i nodi dell'appliance, consultare le istruzioni di installazione e manutenzione dell'appliance.
  - Per i nodi basati su Linux e VMware, utilizzare il seguente comando: `/usr/sbin/change-mtu.py [-h] [-n node] mtu network [network...]`

**Esempio:** `change-mtu.py -n node 1500 grid admin`

**Nota:** Nei nodi basati su Linux, se il valore MTU desiderato per la rete nel container supera il valore già configurato sull'interfaccia host, è necessario prima configurare l'interfaccia host in modo che abbia il valore MTU desiderato, quindi utilizzare `change-mtu.py` Script per modificare il valore MTU della rete nel container.

Utilizzare i seguenti argomenti per modificare la MTU su nodi basati su Linux o VMware.

Argomenti di posizione	Descrizione
mtu	MTU da impostare. Deve essere compreso tra 1280 e 9216.
network	Le reti a cui applicare la MTU. Includere uno o più dei seguenti tipi di rete: <ul style="list-style-type: none"><li>• griglia</li><li>• amministratore</li><li>• client</li></ul>

+

Argomenti facoltativi	Descrizione
-h, - help	Visualizzare il messaggio della guida e uscire.
-n node, --node node	Il nodo. L'impostazione predefinita è il nodo locale.

### Informazioni correlate

["SG100 SG1000 Services appliance"](#)

"Appliance di storage SG6000"

"Appliance di storage SG5700"

"Appliance di storage SG5600"

## Risoluzione dei problemi relativi all'allarme NRER (Network Receive Error)

Gli allarmi NRER (Network Receive Error) possono essere causati da problemi di connettività tra StorageGRID e l'hardware di rete. In alcuni casi, gli errori NRER possono essere corretti senza l'intervento manuale. Se gli errori non si cancellano, eseguire le azioni consigliate.

### A proposito di questa attività

Gli allarmi NRER possono essere causati dai seguenti problemi relativi all'hardware di rete che si collega a StorageGRID:

- La funzione FEC (Forward Error Correction) è obbligatoria e non in uso
- Mancata corrispondenza tra porta dello switch e MTU della scheda NIC
- Elevati tassi di errore di collegamento
- Buffer di anello NIC scaduto

### Fasi

1. Seguire i passaggi per la risoluzione dei problemi relativi a tutte le potenziali cause dell'allarme NRER in base alla configurazione di rete.

- Se l'errore è causato da una mancata corrispondenza FEC, attenersi alla seguente procedura:

**Nota:** Questi passaggi sono applicabili solo per gli errori NRER causati dalla mancata corrispondenza FEC sulle appliance StorageGRID.

- i. Controllare lo stato FEC della porta dello switch collegato all'appliance StorageGRID.
- ii. Controllare l'integrità fisica dei cavi che collegano l'apparecchio allo switch.
- iii. Se si desidera modificare le impostazioni FEC per tentare di risolvere l'allarme NRER, assicurarsi innanzitutto che l'appliance sia configurata per la modalità **auto** nella pagina di configurazione del collegamento del programma di installazione dell'appliance StorageGRID (consultare le istruzioni di installazione e manutenzione dell'appliance). Quindi, modificare le impostazioni FEC sulle porte dello switch. Le porte dell'appliance StorageGRID regoleranno le impostazioni FEC in modo che corrispondano, se possibile.

Non è possibile configurare le impostazioni FEC sulle appliance StorageGRID. Le appliance tentano invece di rilevare e duplicare le impostazioni FEC sulle porte dello switch a cui sono collegate. Se i collegamenti sono forzati a velocità di rete 25-GbE o 100-GbE, lo switch e la NIC potrebbero non riuscire a negoziare un'impostazione FEC comune. Senza un'impostazione FEC comune, la rete torna alla modalità "no-FEC". Quando la funzione FEC non è attivata, le connessioni sono più soggette a errori causati da disturbi elettrici.

**Nota:** Le appliance StorageGRID supportano Firecode (FC) e Reed Solomon (RS) FEC, oltre che FEC.

- Se l'errore è causato da una mancata corrispondenza tra la porta dello switch e la MTU della NIC, verificare che le dimensioni MTU configurate sul nodo corrispondano all'impostazione MTU per la porta dello switch.

La dimensione MTU configurata sul nodo potrebbe essere inferiore all'impostazione sulla porta dello switch a cui è connesso il nodo. Se un nodo StorageGRID riceve un frame Ethernet più grande del relativo MTU, cosa possibile con questa configurazione, potrebbe essere segnalato l'allarme NRER. Se si ritiene che questo sia quanto accade, modificare la MTU della porta dello switch in modo che corrisponda alla MTU dell'interfaccia di rete StorageGRID oppure modificare la MTU dell'interfaccia di rete StorageGRID in modo che corrisponda alla porta dello switch, in base agli obiettivi o ai requisiti della MTU end-to-end.



Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.



Per modificare l'impostazione MTU, consultare la guida all'installazione e alla manutenzione dell'appliance.

- Se l'errore è causato da un elevato tasso di errori di collegamento, attenersi alla seguente procedura:
  - i. Attivare FEC, se non è già attivato.
  - ii. Verificare che il cablaggio di rete sia di buona qualità e non sia danneggiato o collegato in modo errato.
  - iii. Se i cavi non sembrano essere il problema, contattare il supporto tecnico.



In un ambiente con elevati livelli di rumore elettrico, potrebbero verificarsi errori elevati.

- Se l'errore è un buffer di anello della scheda di rete in eccesso, contattare il supporto tecnico.

Il buffer circolare può essere sovraccarico quando il sistema StorageGRID è sovraccarico e non è in grado di elaborare gli eventi di rete in modo tempestivo.

2. Dopo aver risolto il problema sottostante, reimpostare il contatore degli errori.
  - a. Selezionare **supporto > Strumenti > topologia griglia**.
  - b. Selezionare **Site Grid Node SSM risorse Configurazione principale**.
  - c. Selezionare **Ripristina conteggio errori di ricezione** e fare clic su **Applica modifiche**.

#### Informazioni correlate

["Risoluzione dei problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia"](#)

["Riferimento allarmi \(sistema legacy\)"](#)

["Appliance di storage SG6000"](#)

["Appliance di storage SG5700"](#)

["Appliance di storage SG5600"](#)

["SG100 SG1000 Services appliance"](#)

## Risoluzione dei problemi relativi agli errori di sincronizzazione dell'ora

Potrebbero verificarsi problemi con la sincronizzazione dell'ora nella griglia.

Se si verificano problemi di sincronizzazione dell'ora, verificare di aver specificato almeno quattro origini NTP esterne, ciascuna con uno strato 3 o un riferimento migliore, e che tutte le origini NTP esterne funzionino normalmente e siano accessibili dai nodi StorageGRID.



Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time sulle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'utilizzo in ambienti ad alta precisione, come StorageGRID.

### Informazioni correlate

["Mantieni Ripristina"](#)

## Linux: Problemi di connettività di rete

Potrebbero verificarsi problemi con la connettività di rete per i grid node StorageGRID ospitati su host Linux.

### Clonazione indirizzo MAC

In alcuni casi, i problemi di rete possono essere risolti utilizzando la clonazione dell'indirizzo MAC. Se si utilizzano host virtuali, impostare il valore della chiave di clonazione dell'indirizzo MAC per ciascuna rete su "true" nel file di configurazione del nodo. Questa impostazione fa in modo che l'indirizzo MAC del container StorageGRID utilizzi l'indirizzo MAC dell'host. Per creare i file di configurazione dei nodi, consultare le istruzioni nella guida all'installazione della piattaforma in uso.



Creare interfacce di rete virtuali separate per l'utilizzo da parte del sistema operativo host Linux. L'utilizzo delle stesse interfacce di rete per il sistema operativo host Linux e per il container StorageGRID potrebbe rendere il sistema operativo host irraggiungibile se la modalità promiscua non è stata attivata sull'hypervisor.

Per ulteriori informazioni sull'attivazione della clonazione MAC, consultare le istruzioni nella guida all'installazione della piattaforma.

### Modalità promiscua

Se non si desidera utilizzare la clonazione dell'indirizzo MAC e si desidera consentire a tutte le interfacce di ricevere e trasmettere dati per indirizzi MAC diversi da quelli assegnati dall'hypervisor, Assicurarsi che le proprietà di sicurezza a livello di switch virtuale e gruppo di porte siano impostate su **Accept** per modalità promiscuous, modifiche indirizzo MAC e trasmissione forgiata. I valori impostati sullo switch virtuale possono essere sovrascritti dai valori a livello di gruppo di porte, quindi assicurarsi che le impostazioni siano le stesse in entrambe le posizioni.

### Informazioni correlate

["Installare Red Hat Enterprise Linux o CentOS"](#)

["Installare Ubuntu o Debian"](#)

## Linux: Stato del nodo “orfano”

Un nodo Linux in uno stato orfano di solito indica che il servizio StorageGRID o il daemon del nodo StorageGRID che controlla il contenitore del nodo sono morti inaspettatamente.

### A proposito di questa attività

Se un nodo Linux segnala che si trova in uno stato orfano, è necessario:

- Controllare i registri per verificare la presenza di errori e messaggi.
- Tentare di riavviare il nodo.
- Se necessario, utilizzare i comandi Docker per arrestare il contenitore di nodi esistente.
- Riavviare il nodo.

### Fasi

1. Controllare i log sia per il daemon di servizio che per il nodo orfano per verificare la presenza di errori evidenti o messaggi relativi all'uscita imprevista.
2. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
3. Tentare di riavviare il nodo eseguendo il seguente comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Se il nodo è orfano, la risposta è

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Da Linux, arrestare il container Docker e qualsiasi processo di controllo del nodo storagegrid: `sudo docker stop --time secondscontainer-name`

Per `seconds`, immettere il numero di secondi che si desidera attendere per l'arresto del container (in genere 15 minuti o meno).

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Riavviare il nodo: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

## Linux: Risoluzione dei problemi relativi al supporto IPv6

Potrebbe essere necessario abilitare il supporto IPv6 nel kernel se sono stati installati nodi StorageGRID su host Linux e si nota che gli indirizzi IPv6 non sono stati assegnati ai contenitori di nodi come previsto.

### A proposito di questa attività

È possibile visualizzare l'indirizzo IPv6 assegnato a un nodo Grid nelle seguenti posizioni in Grid Manager:

- Selezionare **nodi** e selezionare il nodo. Quindi, fare clic su **Mostra altri** accanto a **indirizzi IP** nella scheda Panoramica.

### DC1-S1 (Storage Node)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Events](#)

**Node Information** ?

<b>Name</b>	DC1-S1
<b>Type</b>	Storage Node
<b>Software Version</b>	11.1.0 (build 20180606.2152.b3bbe9d)
<b>IP Addresses</b>	10.96.106.102 <a href="#">Show less</a> ^

Interface	IP Address
eth0	10.96.106.102
eth0	fe80::250:56ff:fea7:5c83

- Selezionare **supporto Strumenti topologia griglia**. Quindi, selezionare **node SSM Resources**. Se è stato assegnato un indirizzo IPv6, questo viene elencato sotto l'indirizzo IPv4 nella sezione **indirizzi di rete**.

Se l'indirizzo IPv6 non viene visualizzato e il nodo è installato su un host Linux, seguire questa procedura per abilitare il supporto IPv6 nel kernel.

#### Fasi

1. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
2. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Il risultato deve essere 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Se il risultato non è 0, consultare la documentazione relativa al sistema operativo in uso per le modifiche `sysctl` impostazioni. Quindi, modificare il valore su 0 prima di continuare.

3. Inserire il contenitore di nodi StorageGRID: `storagegrid node enter node-name`
4. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Il risultato deve essere 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Se il risultato non è 1, questa procedura non si applica. Contattare il supporto tecnico.

5. Uscire dal container: `exit`

```
root@DC1-S1:~ # exit
```

6. Come root, modificare il seguente file: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Individuare le due righe seguenti e rimuovere i tag di commento. Quindi, salvare e chiudere il file.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Eseguire questi comandi per riavviare il container StorageGRID:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```



## Informazioni sul copyright

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

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.