



Risolvere i problemi relativi al sistema StorageGRID

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

- Risolvere i problemi relativi al sistema StorageGRID 1
 - Risolvere i problemi di un sistema StorageGRID..... 1
 - Risolvere i problemi relativi a oggetti e storage 8
 - Risolvere i problemi relativi ai metadati 36
 - Risolvere gli errori del certificato 38
 - Risolvere i problemi relativi al nodo di amministrazione e all'interfaccia utente 39
 - Risolvere i problemi di rete, hardware e piattaforma 43
 - Risolvere i problemi di un server syslog esterno 50

Risolvere i problemi relativi al sistema StorageGRID

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.

Spesso è possibile risolvere i problemi da soli; tuttavia, potrebbe essere necessario eseguire l'escalation di alcuni problemi al supporto tecnico.

definire il 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.

Valutare i rischi e l'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.

Raccogliere i 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"> • Creare una tempistica delle modifiche recenti
Rivedere gli avvisi	<p>Gli avvisi possono aiutare a determinare rapidamente la causa principale di un problema fornendo indizi importanti sui problemi sottostanti che potrebbero causarlo.</p> <p>Esaminare l'elenco degli avvisi correnti per verificare se StorageGRID ha identificato la causa principale di un problema.</p> <p>Rivedi gli avvisi attivati in passato per ulteriori informazioni.</p>	<ul style="list-style-type: none"> • "Visualizzare gli avvisi correnti e risolti"
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"> • "Monitorare gli eventi"
Identificare i trend utilizzando grafici e report 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"> • "Utilizzare grafici e grafici" • "Utilizzare report di testo"

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
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"> • Stabilire le linee di base
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"> • "Monitorare L'EFFICIENZA e OTTENERE le performance"
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"> • "Esaminare i messaggi di audit"
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.	<ul style="list-style-type: none"> • "Monitorare le operazioni di verifica degli oggetti" • "Confermare le posizioni dei dati degli oggetti" • "Verificare l'integrità dell'oggetto"
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"> • "Raccogliere i file di log e i dati di sistema" • "Attivare manualmente un pacchetto AutoSupport" • "Rivedere le metriche di supporto"

Crea una timeline di 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"> • Quando è stato avviato il ripristino del nodo? • Quando è stato completato l'aggiornamento del software? • Hai interrotto il processo? 	<p>Che cosa è successo? Cosa hai fatto?</p>	<p>Documentare i dettagli relativi alla modifica. Ad esempio:</p> <ul style="list-style-type: none"> • Dettagli delle modifiche di rete. • Quale hotfix è stato installato. • Come sono cambiati i carichi di lavoro dei client. <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 altre modifiche al sistema StorageGRID o al suo ambiente?

Stabilire le 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 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. Posiziona il cursore sul grafico per stimare 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	Nella dashboard di Grid Manager, selezionare Performance > S3 Operations o Performance > Swift Operations . Per visualizzare i tassi di acquisizione e recupero e i conteggi per un sito o nodo specifico, selezionare NODES > Site o Storage Node > Objects . Posizionare il cursore sul grafico acquisizione e recupero per S3.
Operazioni S3/Swift non riuscite	Operazioni	Selezionare SUPPORT > Tools > Grid topology . 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).

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

Analizzare i 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 avvisi.
- Ricostruire la cronologia dei problemi utilizzando la cronologia e i grafici degli avvisi.
- 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 riesci a risolvere il problema da solo, contatta 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	<p>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?</p> <p>Definire il problema</p>
	Valutazione dell'impatto	<p>Qual è la gravità del problema? Qual è l'impatto sull'applicazione client?</p> <ul style="list-style-type: none"> • Il client si è connesso correttamente in precedenza? • Il client è in grado di acquisire, recuperare ed eliminare i dati?
	ID sistema StorageGRID	<p>Selezionare MANUTENZIONE > sistema > licenza. L'ID di sistema StorageGRID viene visualizzato come parte della licenza corrente.</p>
	Versione del software	<p>Nella parte superiore di Gestione griglia, selezionare l'icona della guida e selezionare About (informazioni su) per visualizzare la versione di StorageGRID.</p>
	Personalizzazione	<p>Riepilogare la configurazione del sistema StorageGRID. Ad esempio, elencare quanto segue:</p> <ul style="list-style-type: none"> • Il grid utilizza la compressione dello storage, la crittografia dello storage o la conformità? • ILM produce oggetti replicati o sottoposti a erasure coding? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano i comportamenti di ingest bilanciato, rigoroso o doppio commit?
	File di log e dati di sistema	<p>Raccogliere i file di log e i dati di sistema per il sistema. Selezionare SUPPORT > Tools > Logs.</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>"Raccogliere i file di log e i dati di sistema"</p>

✓	Elemento	Note
	Informazioni di riferimento	Raccogliere informazioni di riferimento relative alle operazioni di acquisizione, alle operazioni di recupero e al consumo dello storage. Stabilire le linee di base
	Tempistiche delle modifiche recenti	Creare una timeline che riepiloga le modifiche recenti apportate al sistema o al suo ambiente. Creare una tempistica delle modifiche recenti
	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.

Risolvere i problemi relativi a oggetti e storage

Confermare le posizioni dei dati degli oggetti

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

Prima di iniziare

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
 - **UUID**: Identificativo universalmente univoco dell'oggetto. Inserire il 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 oggetto chiave**: Quando un oggetto viene acquisito tramite "[Interfaccia S3](#)", l'applicazione client utilizza una combinazione di chiavi bucket e oggetto per memorizzare e identificare l'oggetto.

Fasi

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

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

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

Object Metadata Lookup

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

Identifier

Version ID (optional)

4. Selezionare **Cerca**.

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

- Metadati di sistema, tra cui l'ID oggetto (UUID), l'ID versione (facoltativo), il nome dell'oggetto, il nome del contenitore, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
- Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

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

System Metadata

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

Replicated Copies

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

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

Errori dell'archivio di oggetti (volume di storage)

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

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

Disk devices

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

Volumes

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

Object stores

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

Per ulteriori informazioni "[Dettagli su ciascun nodo di storage](#)", attenersi alla seguente procedura:

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

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, i guasti relativi a un volume di memorizzazione potrebbero essere riportati in "[avvisi relativi al volume di storage](#)". 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, è possibile 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.

Verificare l'integrità dell'oggetto

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

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

Che cos'è la verifica in background?

Il processo di verifica in background verifica automaticamente e continuamente la presenza di copie corrotte

dei dati degli oggetti nei nodi di storage e tenta automaticamente di risolvere eventuali problemi rilevati.

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

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



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

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

Il processo di verifica in background controlla solo gli oggetti sui nodi di storage. Non controlla gli oggetti in un Cloud Storage Pool. 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 relativi alla verifica in background

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

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

Modificare il tasso di verifica in background

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

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone 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:

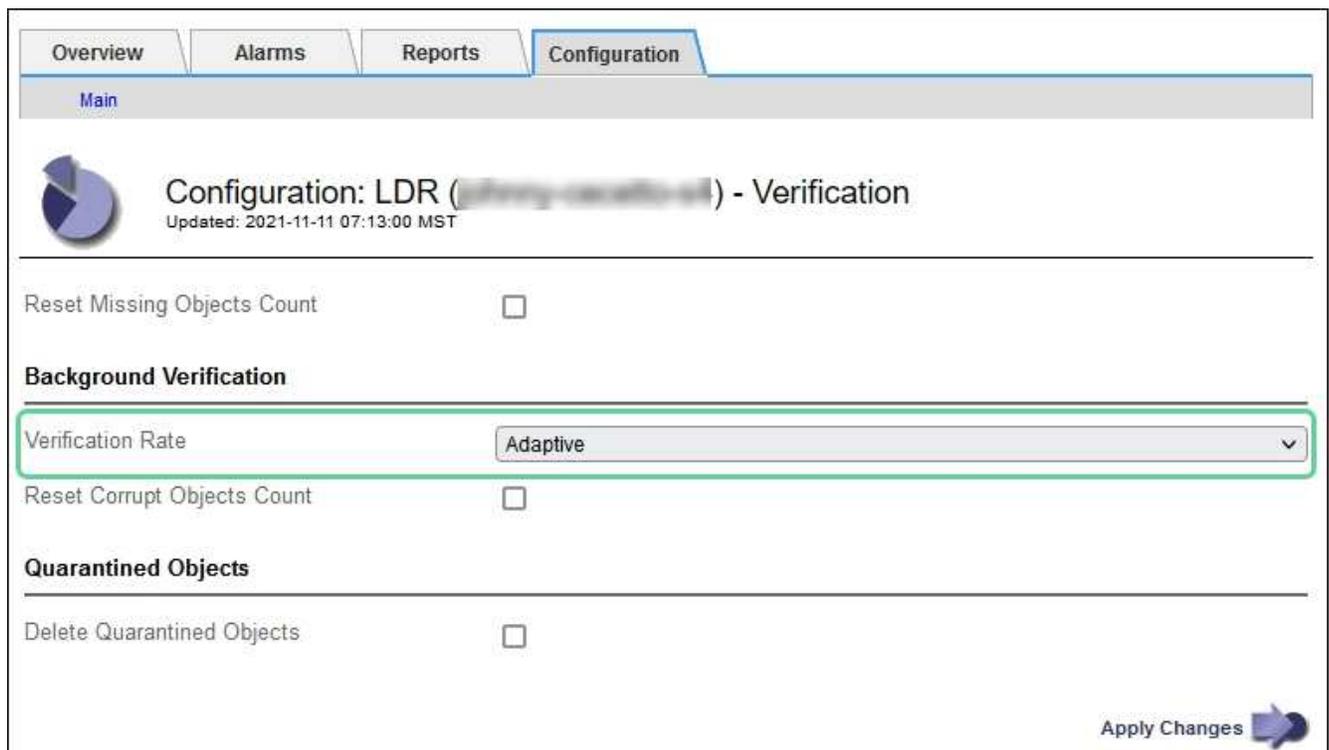
- **Adattivo:** Impostazione predefinita. L'attività è progettata per la verifica a un massimo di 4 MB/s o 10 oggetti/s (a seconda di quale valore viene superato per primo).
- **Elevato:** La verifica dello storage procede rapidamente, a una velocità che può rallentare le normali attività

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



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

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

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

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

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

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

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

9. Una volta ripristinati automaticamente gli oggetti corrotti dal sistema StorageGRID, ripristinare il numero di oggetti corrotti.

- a. Selezionare **SUPPORT > Tools > Grid topology**.
- b. Selezionare **Storage Node > LDR > Verification > Configuration**.
- c. Selezionare **Ripristina conteggio oggetti corrotti**.
- d. Fare clic su **Applica modifiche**.

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



Se l'avviso **oggetti persi** è stato attivato, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena per agevolare il debug del problema sottostante o tentare il ripristino dei dati.

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

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

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

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

Il controllo dell'esistenza degli oggetti legge i metadati di ogni oggetto memorizzato in StorageGRID e verifica l'esistenza di copie di oggetti replicate e frammenti di oggetti codificati per la cancellazione. I dati mancanti vengono gestiti come segue:

- **Copie replicate:** Se manca una copia dei dati degli oggetti replicati, StorageGRID tenta automaticamente di sostituire la copia da una copia memorizzata altrove nel sistema. Il nodo di storage esegue una copia esistente attraverso una valutazione ILM, che determina che il criterio ILM corrente non è più soddisfatto per questo oggetto perché manca un'altra copia. Viene generata e posizionata una nuova copia per soddisfare i criteri ILM attivi del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa

posizione in cui è stata memorizzata la copia mancante.

- **Frammenti con codifica di cancellazione:** Se manca un frammento di un oggetto con codifica di cancellazione, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage utilizzando i frammenti rimanenti. Se il frammento mancante non può essere ricostruito (perché sono stati persi troppi frammenti), ILM tenta di trovare un'altra copia dell'oggetto, che può utilizzare per generare un nuovo frammento con codifica di cancellazione.

Eeguire il controllo dell'esistenza dell'oggetto

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

Prima di iniziare

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

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

A proposito di questa attività

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

Fasi

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

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

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

4. Selezionare **continua**.
5. Selezionare uno o più volumi per ciascun nodo dell'elenco. È possibile cercare i volumi utilizzando il

numero del volume di storage o il nome del nodo.

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

6. Selezionare **continua**.

7. Selezionare la coerenza per il lavoro.

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

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

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

8. Selezionare **continua**.

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

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

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



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

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

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

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

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

The screenshot displays the 'Object existence check' interface. At the top, there are two tabs: 'Active job' (selected) and 'Job history'. Below the tabs, the job status is 'Accepted' with Job ID '2334602652907829302'. A green box highlights the 'Missing object copies detected' field, which shows '0'. The progress bar is at 0%. There are 'Pause' and 'Cancel' buttons. Below the job details, there is a table with columns for 'Selected node', 'Selected storage volumes', and 'Site'.

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Una volta completato il lavoro, eseguire eventuali azioni aggiuntive richieste:

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

Questa procedura è simile a quella per "[analisi degli oggetti smarriti](#)", anche se per le copie degli oggetti si cerca LLST invece di OLSST .

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

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

- Selezionare **MANUTENZIONE > verifica dell'esistenza dell'oggetto > Cronologia lavori**.
- Determinare quali lavori sono pronti per essere rieseguiti:

- i. Esaminare la colonna **ora di fine** per determinare quali lavori sono stati eseguiti più di tre settimane fa.
 - ii. Per questi lavori, eseguire la scansione della colonna di controllo della coerenza per individuare la presenza di un sito forte o globale forte.
- c. Selezionare la casella di controllo per ciascun processo che si desidera rieseguire, quindi selezionare **Rerun**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job | Job history

Delete | **Rerun** | Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

<input type="checkbox"/>	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
<input checked="" type="checkbox"/>	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
<input type="checkbox"/>	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. Nella procedura guidata Riesegui lavori, esaminare i nodi e i volumi selezionati e la coerenza.
- e. Quando si è pronti per rieseguire i lavori, selezionare **Rerun**.

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

Al termine

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

Risoluzione dei problemi S3 - Avviso DIMENSIONE oggetto troppo grande

L'avviso S3 PUT object size too large viene attivato se un tenant tenta un'operazione PutObject non multipart che supera il limite di dimensione S3 di 5 GiB.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

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

Fasi

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

- a. Invio `ssh admin@primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

- e. Invio `cd /var/local/log`



["Informazioni sulle destinazioni per le informazioni di verifica"](#).

- f. Identificare i tenant che utilizzano oggetti di dimensioni superiori a 5 GiB.
 - i. Invio `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9] {9}"`
 - ii. Per ciascun messaggio di controllo nei risultati, esaminare il `S3AI` campo per determinare l'ID account tenant. Utilizzare gli altri campi del messaggio per determinare l'indirizzo IP utilizzato dal client, dal bucket e dall'oggetto:

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

Esempio di risultati del registro di controllo

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

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

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

b. Estrarre il file e andare a `broadcast.log`:

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

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

Esempio di `broadcast.log`

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

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

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

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Risolvere i 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, viene attivato l'avviso **oggetti persi**, come segue:

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

È necessario esaminare immediatamente tutti gli avvisi **oggetti smarriti** per determinare la causa principale della perdita e per determinare se l'oggetto potrebbe ancora esistere in un nodo di archiviazione non in linea o non attualmente disponibile. Vedere ["Esaminare gli oggetti persi"](#).

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

Esaminare gli oggetti persi

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

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- È necessario disporre del `Passwords.txt` file.

A proposito di questa attività

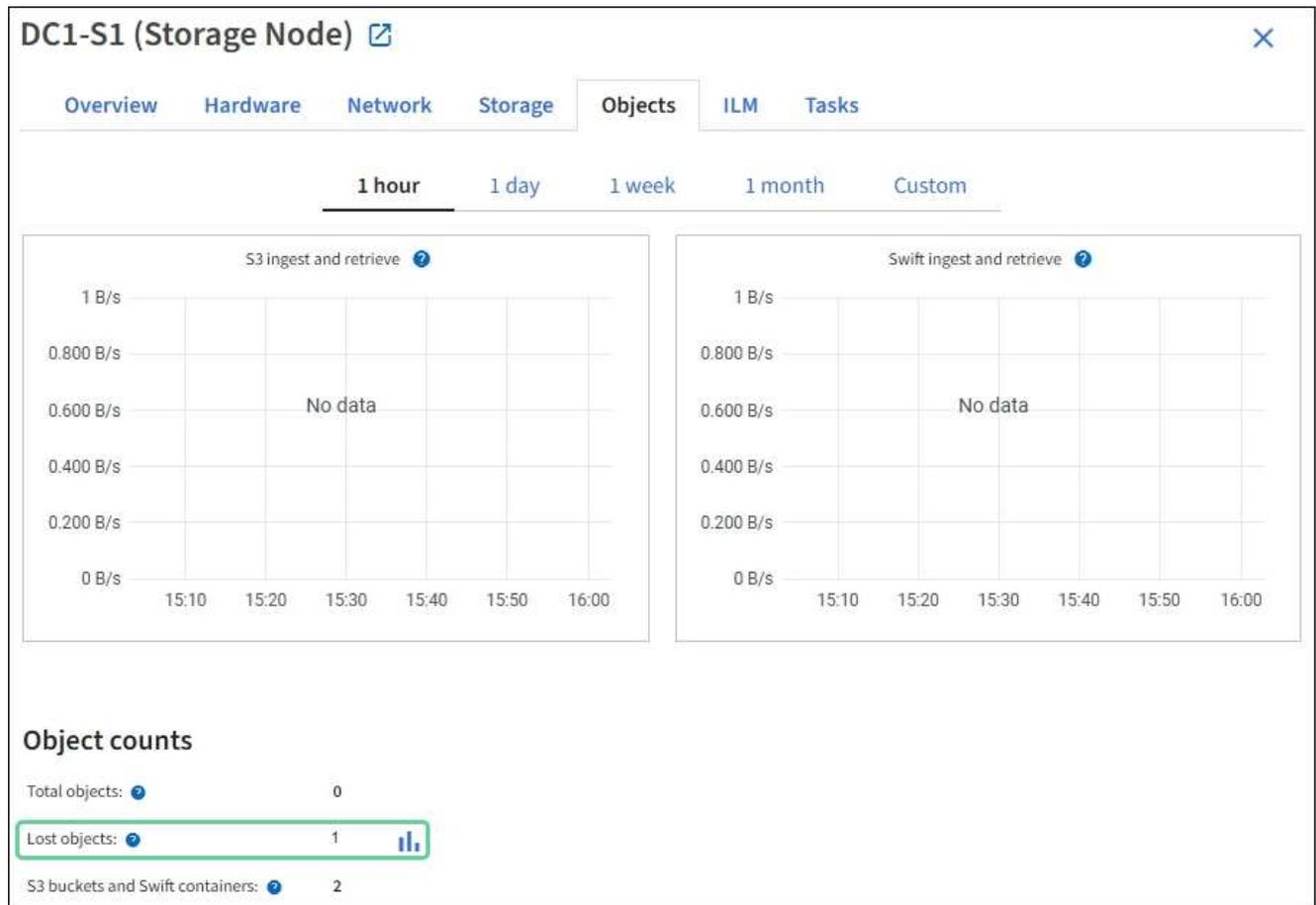
L'avviso **oggetti persi** indica che StorageGRID ritiene che non vi siano copie di un oggetto nella griglia. I dati potrebbero essere stati persi in modo permanente.

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

Fasi

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

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



4. Da un nodo amministrativo, "accedere al registro di controllo" per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **oggetti persi**:

a. Accedere al nodo Grid:

- i. Immettere il seguente comando: `ssh admin@grid_node_IP`
- ii. Immettere la password elencata nel `Passwords.txt` file.
- iii. Immettere il seguente comando per passare alla directory principale: `su -`
- iv. Immettere la password elencata nel `Passwords.txt` file. Quando si è collegati come root, il prompt cambia da `$` a `#`.

b. Passare alla directory in cui si trovano i registri di controllo. Immettere: `cd /var/local/log/`



"Informazioni sulle destinazioni per le informazioni di verifica".

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

d. Annotare il valore UUID incluso nel messaggio.

```
>Admin: # grep OLSM 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):OLSM][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Cercare i metadati per l'oggetto perso utilizzando l'UUID:

- a. Selezionare **ILM > Object metadata lookup**.
- b. Immettere l'UUID e selezionare **Cerca**.
- c. Esaminare le posizioni nei metadati e intraprendere l'azione appropriata:

Metadati	Conclusione
<object_identifier> oggetto non trovato	<p>Se l'oggetto non viene trovato, viene visualizzato il messaggio "ERROR":.</p> <p>Se l'oggetto non viene trovato, è possibile azzerare il numero di oggetti persi per eliminare l'avviso. La mancanza di un oggetto indica che l'oggetto è stato intenzionalmente cancellato.</p>
Posizioni > 0	<p>Se nell'output sono presenti posizioni, l'avviso 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 "ricerca di oggetti potenzialmente persi" spiega come utilizzare l'ID nodo per trovare il nodo di archiviazione corretto).</p> <p>Se gli oggetti sono presenti, è possibile ripristinare il numero di oggetti persi per cancellare l'avviso.</p>
Posizioni = 0	<p>Se nell'output non sono presenti posizioni, l'oggetto potrebbe essere mancante. È possibile provare "cercare e ripristinare l'oggetto" da soli o contattare il supporto tecnico.</p> <p>Il supporto tecnico potrebbe richiedere di determinare se è in corso una procedura di ripristino dello storage. Vedere le informazioni su "Ripristino dei dati degli oggetti mediante Grid Manager" e "ripristino dei dati degli oggetti in un volume di storage".</p>

Cercare e ripristinare oggetti potenzialmente persi

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

Prima di iniziare

- Si dispone dell'UUID di qualsiasi oggetto perso, come identificato in ["Esaminare gli oggetti persi"](#).
- Si dispone del `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 nel `Passwords.txt` file.
- iii. Immettere il seguente comando per passare alla directory principale: `su -`
- iv. Immettere la password elencata nel `Passwords.txt` file. Quando si è collegati come root, il prompt cambia da `$` a `#`.

b. Passare alla directory in cui si trovano i registri di controllo: `cd /var/local/log/`



["Informazioni sulle destinazioni per le informazioni di verifica"](#).

c. Utilizzare `grep` per estrarre **"messaggi di audit associati all'oggetto potenzialmente perso"** e inviarli a un file di output. Immettere: `grep uuid-value audit_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. Immettere: `grep LLST output_file_name`

Ad esempio:

```
Admin: # grep LLST messages_about_lost_objects.txt
```

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

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

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

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

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

a. Accedere al nodo Grid:

- i. Immettere il seguente comando: `ssh admin@grid_node_IP`
- ii. Immettere la password elencata nel `Passwords.txt` file.
- iii. Immettere il seguente comando per passare alla directory principale: `su -`
- iv. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

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

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

Ad esempio, immettere:

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



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

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

ripristinare l'oggetto trovato in StorageGRID.

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

Ad esempio, immettere:

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

L'emissione del `Object_Found` comando notifica alla griglia la posizione dell'oggetto. Attiva inoltre i criteri ILM attivi, che eseguono copie aggiuntive come specificato in ciascun criterio.



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

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

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

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

Passare alla fase successiva.

4. Se l'oggetto è stato ripristinato correttamente in StorageGRID, verificare che siano state create le nuove posizioni:
 - a. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
 - b. Selezionare **ILM > Object metadata lookup**.
 - c. Immettere l'UUID e selezionare **Cerca**.
 - d. Rivedere i metadati e verificare le nuove posizioni.
5. Da un nodo di amministrazione, cercare nei registri di controllo il messaggio di audit ORLM relativo a questo oggetto per confermare che ILM (Information Lifecycle Management) ha inserito le copie come richiesto.

- a. Accedere al nodo Grid:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`
 - iv. Immettere la password elencata nel `Passwords.txt` file. Quando si è collegati come root, il prompt cambia da `$` a `#`.
- b. Passare alla directory in cui si trovano i registri di controllo: `cd /var/local/log/`
- c. Utilizzare `grep` per estrarre i messaggi di audit associati all'oggetto in un file di output. Immettere: `grep uuid-value audit_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. Immettere: `grep ORLM output_file_name`

Ad esempio:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

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

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

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

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

6. ["Ripristinare i conteggi degli oggetti persi e mancanti"](#) In Grid Manager.

Ripristinare i conteggi degli oggetti persi e mancanti

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

azzerare il valore dell'attributo oggetti persi.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".

A proposito di questa attività

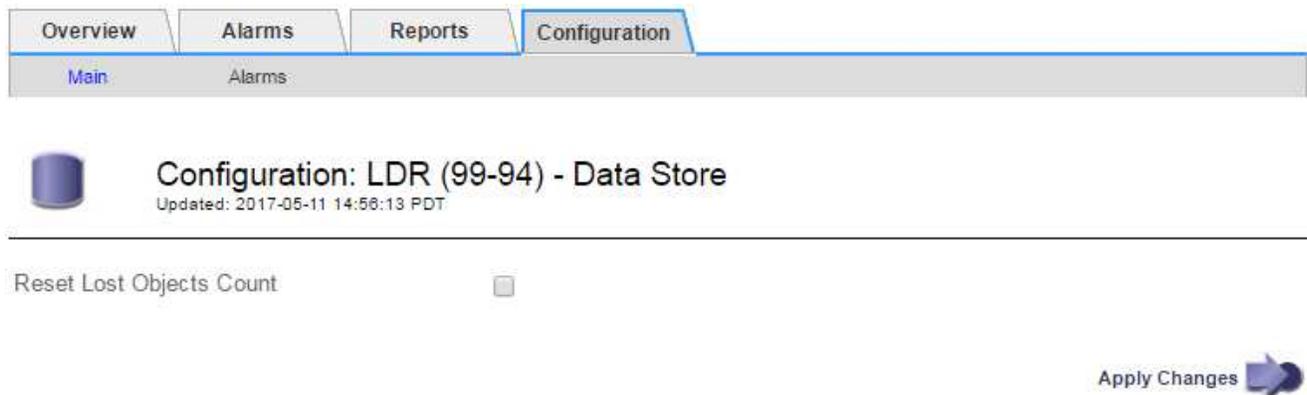
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

- **SUPPORTO > Strumenti > topologia griglia > Sito > nodo di archiviazione > LDR > Archivio dati > Panoramica > principale**
- **SUPPORTO > Strumenti > topologia griglia > Sito > nodo di archiviazione > DDS > Archivio dati > Panoramica > principale**

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

Fasi

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



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

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

5. Facoltativamente, reimpostare altri valori degli attributi correlati che potrebbero essere stati incrementati durante il processo di identificazione dell'oggetto perso.
 - a. Selezionare **Site > Storage Node > LDR > Erasure Coding > Configuration**.
 - b. Selezionare **Reset Reads Failure Count** e **Reset corrotto copies Detected Count**.
 - c. Fare clic su **Applica modifiche**.
 - d. Selezionare **Site > Storage Node > LDR > Verification > Configuration**.
 - e. Selezionare **Reset Missing Objects Count** e **Reset Corrupt Objects Count**.
 - f. Se si è certi che gli oggetti in quarantena non siano necessari, selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).

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

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

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

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

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[autorizzazioni di accesso specifiche](#)".

A proposito di questa attività

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

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

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

In questa condizione:

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

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

Fasi

1. Selezionare **ALERTS > current**.

Viene visualizzata la pagina Avvisi.

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

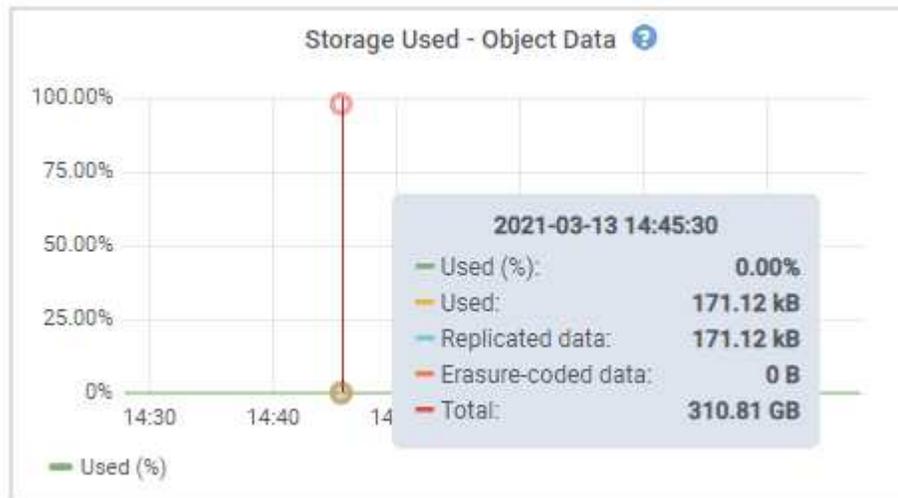


Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.

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

Vengono visualizzati i seguenti valori:

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



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

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

7. Il più presto possibile, ["aggiungere capacità di storage"](#) alla vostra griglia.

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



Per ulteriori informazioni, vedere ["Gestire nodi storage completi"](#).

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

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

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

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

- Il sistema è vicino alla capacità e non è in grado di accettare nuovi dati se sono state applicate filigrane ottimizzate. In questo caso, StorageGRID non modificherà le impostazioni della filigrana.
- In precedenza, le filigrane dei volumi di storage sono state impostate su un valore personalizzato. StorageGRID non sovrascrive le impostazioni personalizzate del watermark con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso di sovrascrittura filigrana di sola lettura * bassa se il valore personalizzato per la filigrana di sola lettura soft del volume di archiviazione è troppo piccolo.

Comprendere l'avviso

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

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

Ad esempio, si supponga di aver precedentemente impostato il watermark soft di sola lettura del volume di archiviazione su 5 GB. Supponiamo ora che StorageGRID abbia calcolato i seguenti valori ottimizzati per i quattro volumi di storage nel nodo di storage A:

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

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

Risolvere l'avviso

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

Prima di iniziare

- L'aggiornamento a StorageGRID 11.6 o versione successiva è stato completato.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

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

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

Fasi

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

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Seguire la procedura appropriata:

- Se nessuno dei nodi di storage è quasi pieno (ad esempio, tutti i valori **dati oggetto utilizzati** sono inferiori al 80%), è possibile iniziare a utilizzare le impostazioni di override. Andare a [Utilizzare filigrane ottimizzate](#).
- Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se i pool di storage specifici sono quasi completi, eseguire i passaggi in [Visualizza filigrane di storage ottimizzate](#) e [Determinare se è possibile utilizzare filigrane ottimizzate](#).

Visualizza filigrane di memorizzazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati calcolati per il watermark soft di sola lettura del volume di archiviazione. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

Fasi

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

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato del watermark di sola lettura soft per tutti i volumi di

archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per il watermark soft di sola lettura del volume di archiviazione, viene attivato l'avviso **low Read-only watermark override** per il nodo di archiviazione.

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

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore massimo ottimizzato del watermark di sola lettura soft per tutti i volumi di archiviazione su ciascun nodo di archiviazione.

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

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

Fasi

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

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

4. Se è necessario continuare a utilizzare i valori personalizzati per le filigrane del volume di archiviazione ["silenzio"](#) o ["disattiva"](#) l'avviso **Ignora filigrana di sola lettura bassa**.



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

utilizza filigrane ottimizzate

Fasi

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

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

Risolvere i problemi relativi ai metadati

Se si verificano problemi relativi ai metadati, gli avvisi ti informeranno sull'origine dei problemi e sulle azioni consigliate da intraprendere. In particolare, è necessario aggiungere nuovi nodi di archiviazione se viene attivato l'avviso archiviazione metadati bassa.

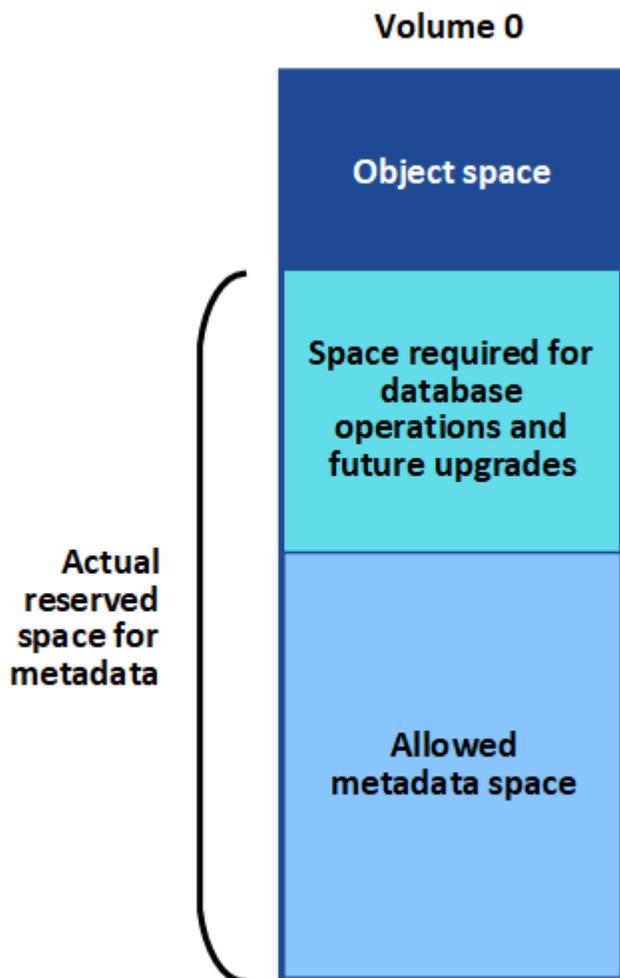
Prima di iniziare

L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

Seguire le azioni consigliate per ogni avviso relativo ai metadati attivato. Se viene attivato l'avviso **Low metadata storage**, è necessario aggiungere nuovi nodi di storage.

StorageGRID riserva una certa quantità di spazio sul volume 0 di ciascun nodo di storage per i metadati dell'oggetto. Questo spazio, noto come *spazio riservato effettivo*, è suddiviso nello spazio consentito per i metadati dell'oggetto (lo spazio dei metadati consentito) 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.

Puoi "[Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage](#)" aiutarti ad anticipare gli errori e correggerli prima che si verifichino.

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 sul 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.



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 **ALERTS > current**.
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 utilizzare anche "[espandere qualsiasi altro sito](#)" lo stesso numero di nodi di archiviazione.

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.

Risolvere gli 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 uno strumento di monitoraggio esterno, è necessario controllare il certificato.

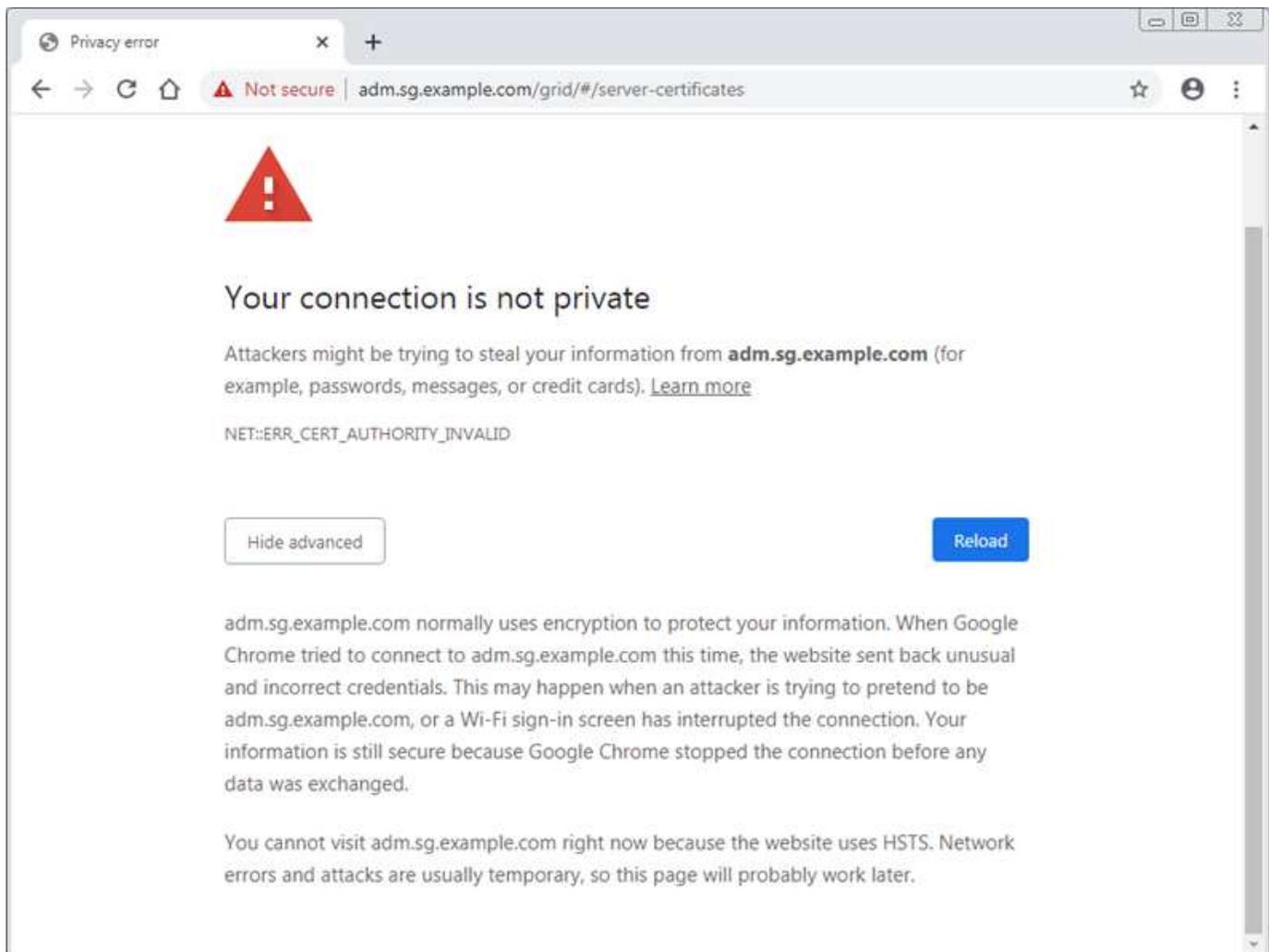
A proposito di questa attività

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 dei certificati possono verificarsi anche quando si tenta di connettersi a un client S3 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 dell'interfaccia di gestione personalizzata scade.
- Viene ripristinato da un certificato dell'interfaccia di gestione personalizzata al certificato del server predefinito.

L'esempio seguente mostra un errore di certificato quando il certificato 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 dell'interfaccia di gestione di StorageGRID o dai certificati client. L'avviso **scadenza dei certificati client configurati nella pagina certificati** viene attivato quando un certificato client sta per scadere.

Fasi

Se si riceve una notifica di avviso relativa a un certificato scaduto, accedere ai dettagli del certificato: . Selezionare **CONFIGURAZIONE > sicurezza > certificati** e quindi ["selezionare la scheda del certificato appropriata"](#).

1. Controllare il periodo di validità del certificato. + alcuni browser web e client S3 non accettano certificati con un periodo di validità superiore a 398 giorni.
2. Se il certificato è scaduto o scadrà a breve, caricare o generare un nuovo certificato.
 - Per un certificato server, vedere la procedura per ["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#).
 - Per un certificato client, vedere la procedura per ["configurazione di un certificato client"](#).
3. 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. Da Grid Manager, selezionare **CONFIGURAZIONE > sicurezza > certificati**, quindi ["selezionare la scheda del certificato appropriata"](#) per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
 - iii. Nelle istruzioni per l'amministrazione di StorageGRID, vedere la procedura per ["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#).

Risolvere i problemi relativi al nodo di amministrazione e all'interfaccia utente

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

Errori di accesso al nodo amministrativo

Se si verifica un errore durante l'accesso a un nodo amministrativo StorageGRID, il sistema potrebbe presentare un problema relativo a ["networking"](#) o ["hardware"](#), a ["Servizi del nodo di amministrazione"](#) o a ["Problema con il database Cassandra"](#) nodi di archiviazione connessi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone del `Passwords.txt` file.

- Si dispone 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 amministrativo, provare ad accedere al Grid Manager da un altro nodo amministrativo per verificare lo stato di un nodo amministrativo non disponibile.
 - 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 Single Sign-on (SSO) è attivato per il sistema StorageGRID, fare riferimento alla procedura per "[configurazione del single sign-on](#)".

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. Rivedere gli avvisi.
 - ii. Selezionare **CONFIGURATION > Access Control > 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 nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

7. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo griglia: `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 servizio nginx-gw sia in esecuzione `# service nginx-gw status`
9. 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.

10. Rivedi i seguenti log:
 - `/var/local/log/bycast.log`
 - `/var/local/log/bycast-err.log`
 - `/var/local/log/nms.log`
 - `**/*commands.txt`
11. 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
```

```
# gpt-list-services adc
```

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

12. Dal nodo Admin, utilizzare ssh per accedere a ciascuno dei nodi di archiviazione ADC, utilizzando gli indirizzi IP identificati.
13. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo griglia: `storagegrid-status`

Assicurarsi che i servizi `idnt`, `acct`, `nginx` e `cassandra` siano tutti in esecuzione.
14. Ripetere i passaggi [Utilizzare Lumberjack per raccogliere i registri](#) e [Esaminare i registri](#) per rivedere i registri sui nodi di archiviazione.
15. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

Fornire al supporto tecnico i registri raccolti. Vedere anche ["Riferimenti ai file di log"](#).

Problemi dell'interfaccia utente

L'interfaccia utente di Grid Manager o Tenant Manager potrebbe non rispondere come previsto dopo l'aggiornamento del software StorageGRID.

Fasi

1. Assicurarsi di utilizzare un ["browser web supportato"](#).
2. 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.

Risolvere i 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.

Errori "422: Entità non elaborabile"

L'errore 422: Unprocessable Entity può verificarsi per diversi motivi. 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
<pre>422: Unprocessable Entity 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</pre>	<p>Questo messaggio potrebbe essere visualizzato se si seleziona l'opzione non utilizzare TLS per Transport Layer Security (TLS) durante la configurazione della federazione delle identità utilizzando Windows Active Directory (ad).</p> <p>L'utilizzo dell'opzione non utilizzare TLS non è supportato per l'utilizzo con i server ad che applicano la firma LDAP. Selezionare l'opzione Use STARTTLS (Usa STARTTLS*) o l'opzione Use LDAPS (Usa LDAPS* per TLS).</p>

Messaggio di errore	Causa principale e azione correttiva
<pre>422: Unprocessable Entity 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)</pre>	<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 una delle "Crittografia supportata da StorageGRID" per le connessioni TLS in uscita, come illustrato nelle istruzioni per l'amministrazione di StorageGRID.</p>

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.
 - Passare alla *primary Admin Node IP address/metrics/graph* query seguente e immetterla: `node_network_mtu_bytes{device="eth0"}`
2. "[Modificare le impostazioni MTU](#)" Se necessario, per garantire che siano uguali per l'interfaccia di rete della griglia (eth0) su tutti i nodi.
 - Per i nodi basati su Linux e VMware, utilizzare il seguente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

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

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

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

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

+

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

Avviso errore frame di ricezione rete nodo

Gli avvisi **errore frame di ricezione rete nodo** possono essere causati da problemi di connettività tra StorageGRID e l'hardware di rete. Questo avviso viene cancellato da solo dopo aver risolto il problema sottostante.

A proposito di questa attività

Gli avvisi **errore frame di ricezione rete nodo** possono essere causati dai seguenti problemi con l'hardware di rete che si connette 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 la procedura di risoluzione dei problemi per tutte le cause potenziali di questo avviso, data la configurazione della rete in uso.
2. A seconda della causa dell'errore, attenersi alla seguente procedura:

Mancata corrispondenza FEC



Questi passaggi sono applicabili solo agli avvisi **Node network reception frame error** causati dalla mancata corrispondenza FEC sulle apparecchiature StorageGRID.

- a. Controllare lo stato FEC della porta dello switch collegato all'appliance StorageGRID.
- b. Controllare l'integrità fisica dei cavi che collegano l'apparecchio allo switch.
- c. Se si desidera modificare le impostazioni FEC per tentare di risolvere l'avviso, verificare innanzitutto che il dispositivo sia configurato per la modalità **Auto** nella pagina di configurazione del collegamento del programma di installazione del dispositivo StorageGRID (consultare le istruzioni per il dispositivo in uso:
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 e SG1100"
 - "SG100 e SG1000"
- d. 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.



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

Mancata corrispondenza tra porta dello switch e MTU della scheda NIC

Se l'avviso è causato da una porta dello switch e da una mancata corrispondenza della MTU della NIC, verificare che la dimensione MTU configurata sul nodo corrisponda 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 della sua MTU, cosa possibile con questa configurazione, potrebbe essere segnalato l'avviso **Node network reception frame error**. 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 ulteriori informazioni, vedere [Risolvere i problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia](#).



Vedere anche "[Modificare l'impostazione MTU](#)".

Elevati tassi di errore di collegamento

- a. Attivare FEC, se non è già attivato.
- b. Verificare che il cablaggio di rete sia di buona qualità e non sia danneggiato o collegato in modo errato.
- c. 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.

Buffer di anello NIC scaduto

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.

3. Monitorare il problema e contattare l'assistenza tecnica se l'avviso non risolve il problema.

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.



"Specifica dell'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.

Linux: Problemi di connettività di rete

Potrebbero verificarsi problemi di connettività di rete per i nodi 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, vedere le istruzioni per ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#).



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, vedere le istruzioni per ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#).

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.

Per ulteriori informazioni sull'uso della modalità promiscua, vedere le istruzioni per ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#).

Linux: Lo stato del nodo è "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 del motore dei container 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 motore dei container e qualsiasi processo di controllo del nodo storagegrid. Ad esempio:
`sudo docker stop --time secondscontainer-name`

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

```
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

Per visualizzare l'indirizzo IPv6 assegnato a un nodo griglia:

1. Selezionare **NODI** e selezionare il nodo.
2. Selezionare **Mostra indirizzi IP aggiuntivi** accanto a **indirizzi IP** nella scheda Panoramica.

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 del sistema operativo per modificare `sysctl` le impostazioni. Quindi, modificare il valore su 0 prima di continuare.

3. Inserisci il contenitore del nodo 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 contenitore: `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
```

Risolvere i problemi di un server syslog esterno

La tabella seguente descrive i messaggi di errore che potrebbero essere correlati a un server syslog esterno ed elenca le azioni correttive.

Per ulteriori informazioni sull'invio di informazioni di audit a un server syslog esterno, consultare:

- "Considerazioni sull'utilizzo di un server syslog esterno"
- "Configurare i messaggi di controllo e il server syslog esterno"

Messaggio di errore	Descrizione e azioni consigliate
Impossibile risolvere il nome host	<p>Impossibile risolvere l'FQDN immesso per il server syslog in un indirizzo IP.</p> <ol style="list-style-type: none"> 1. Controllare il nome host immesso. Se è stato immesso un indirizzo IP, assicurarsi che sia un indirizzo IP valido con la notazione W.X.Y.Z ("decimale separato da punti"). 2. Verificare che i server DNS siano configurati correttamente. 3. Verificare che ciascun nodo possa accedere agli indirizzi IP del server DNS.
Connessione rifiutata	<p>Una connessione TCP o TLS al server syslog è stata rifiutata. Sulla porta TCP o TLS dell'host potrebbe non essere presente alcun servizio o un firewall potrebbe bloccare l'accesso.</p> <ol style="list-style-type: none"> 1. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Verificare che l'host del servizio syslog stia eseguendo un daemon syslog in attesa sulla porta specificata. 3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi all'IP e alla porta del server syslog.
Rete non raggiungibile	<p>Il server syslog non si trova su una subnet collegata direttamente. Un router ha restituito un messaggio di errore ICMP per indicare che non è stato possibile inoltrare i messaggi di test dai nodi elencati al server syslog.</p> <ol style="list-style-type: none"> 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per instradare il traffico al server syslog attraverso l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host non raggiungibile	<p>Il server syslog si trova su una subnet collegata direttamente (subnet utilizzata dai nodi elencati per gli indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di test, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del server syslog.</p> <ol style="list-style-type: none"> 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Verificare che l'host che esegue il servizio syslog sia attivo.

Messaggio di errore	Descrizione e azioni consigliate
Timeout della connessione	<p>È stato eseguito un tentativo di connessione TCP/TLS, ma non è stata ricevuta alcuna risposta dal server syslog per molto tempo. Potrebbe esserci un errore di configurazione del routing o un firewall potrebbe interrompere il traffico senza inviare alcuna risposta (una configurazione comune).</p> <ol style="list-style-type: none"> 1. Verificare di aver immesso l’FQDN o l’indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per indirizzare il traffico al server syslog utilizzando l’interfaccia di rete e il gateway (Grid, Admin o Client) su cui si prevede di raggiungere il server syslog. 3. Verificare che un firewall non blocchi l’accesso alle connessioni TCP/TLS dai nodi elencati all’IP e alla porta del server syslog.
Connessione chiusa dal partner	<p>Una connessione TCP al server syslog è stata stabilita correttamente, ma in seguito è stata chiusa. I motivi potrebbero includere:</p> <ul style="list-style-type: none"> • Il server syslog potrebbe essere stato riavviato o riavviato. • Il nodo e il server syslog potrebbero avere impostazioni TCP/TLS diverse. • Un firewall intermedio potrebbe chiudere le connessioni TCP inattive. • Un server non syslog in ascolto sulla porta del server syslog potrebbe aver chiuso la connessione. <p>Per risolvere questo problema:</p> <ol style="list-style-type: none"> 1. Verificare di aver immesso l’FQDN o l’indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Se si utilizza il protocollo TLS, verificare che anche il server syslog utilizzi il protocollo TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. 3. Verificare che un firewall intermedio non sia configurato per chiudere le connessioni TCP inattive.
Errore certificato TLS	<p>Il certificato del server ricevuto dal server syslog non era compatibile con il bundle di certificati CA e con il certificato client forniti.</p> <ol style="list-style-type: none"> 1. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server sul server syslog. 2. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.
Inoltro sospeso	<p>I record syslog non vengono più inoltrati al server syslog e StorageGRID non è in grado di rilevare il motivo.</p> <p>Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale.</p>

Messaggio di errore	Descrizione e azioni consigliate
Sessione TLS terminata	<p data-bbox="472 153 1446 222">Il server syslog ha terminato la sessione TLS e StorageGRID non è in grado di rilevare il motivo.</p> <ol data-bbox="472 254 1484 695" style="list-style-type: none"> <li data-bbox="472 254 1484 323">1. Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale. <li data-bbox="472 338 1409 407">2. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. <li data-bbox="472 422 1458 527">3. Se si utilizza il protocollo TLS, verificare che anche il server syslog utilizzi il protocollo TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. <li data-bbox="472 541 1414 611">4. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server dal server syslog. <li data-bbox="472 625 1484 695">5. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.
Query dei risultati non riuscita	<p data-bbox="472 747 1458 842">Il nodo di amministrazione utilizzato per la configurazione e il test del server syslog non è in grado di richiedere i risultati del test dai nodi elencati. Uno o più nodi potrebbero non essere attivi.</p> <ol data-bbox="472 873 1471 989" style="list-style-type: none"> <li data-bbox="472 873 1471 942">1. Seguire le procedure standard per la risoluzione dei problemi per assicurarsi che i nodi siano online e che tutti i servizi previsti siano in esecuzione. <li data-bbox="472 957 1057 989">2. Riavviare il servizio miscd sui nodi elencati.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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