Monitora e risolvi i problemi

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-120/monitor/index.html on July 23, 2026. Always check docs.netapp.com for the latest.

Sommario

Monitora e risolvi i problemi di un sistema StorageGRID . . . 1
Monitora il sistema StorageGRID . . . 1
Monitora un sistema StorageGRID . . . 1
Visualizza e gestisci la dashboard in StorageGRID . . . 1
Visualizza la pagina dei nodi . . . 4
Informazioni da monitorare regolarmente . . . 37
Gestisci gli avvisi . . . 67
Riferimento ai file di registro . . . 105
Configura la gestione dei log e il server syslog esterno . . . 124
Usa il monitoraggio SNMP . . . 138
Raccogli ulteriori dati StorageGRID . . . 150
Risoluzione dei problemi del sistema StorageGRID . . . 164
Risolvi i problemi di un sistema StorageGRID . . . 164
Risolvi i problemi relativi a oggetti e storage . . . 171
Risolvere i problemi relativi ai metadati in StorageGRID . . . 189
Risolvere gli errori dei certificati in StorageGRID . . . 191
Risolvi i problemi relativi al nodo di amministrazione e all'interfaccia utente in StorageGRID . . . 193
Risolvi i problemi di rete, hardware e piattaforma in StorageGRID . . . 196
Risoluzione dei problemi dei messaggi di errore del server syslog esterno per StorageGRID . . . 204
Scopri i problemi di memorizzazione nella cache del bilanciatore del carico in StorageGRID . . . 207
${post_edited_translations.segment} . . . 208
${post_edited_translations.segment} . . . 208
Come i messaggi di controllo si spostano attraverso il sistema StorageGRID nel file di log audit.log per la conservazione . . . 208
Accedi ai file di log di audit dalla riga di comando del nodo Admin di StorageGRID . . . 211
Scopri la rotazione dei file di log di audit in StorageGRID . . . 212
Formato del file di log di audit . . . 212
Formato del messaggio di audit . . . 224
Messaggi di controllo e ciclo di vita degli oggetti . . . 229
Messaggi di audit . . . 235

Monitora e risolvi i problemi di un sistema StorageGRID

Monitora il sistema StorageGRID

Monitora un sistema StorageGRID

Monitora regolarmente il tuo sistema StorageGRID per assicurarti che funzioni come previsto.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

> Per modificare le unità di misura dei valori di archiviazione visualizzati in Grid Manager, seleziona il menu a discesa utente nell'angolo in alto a destra di Grid Manager, poi seleziona **Preferenze utente**.

Informazioni su questa attività

Queste istruzioni descrivono come:

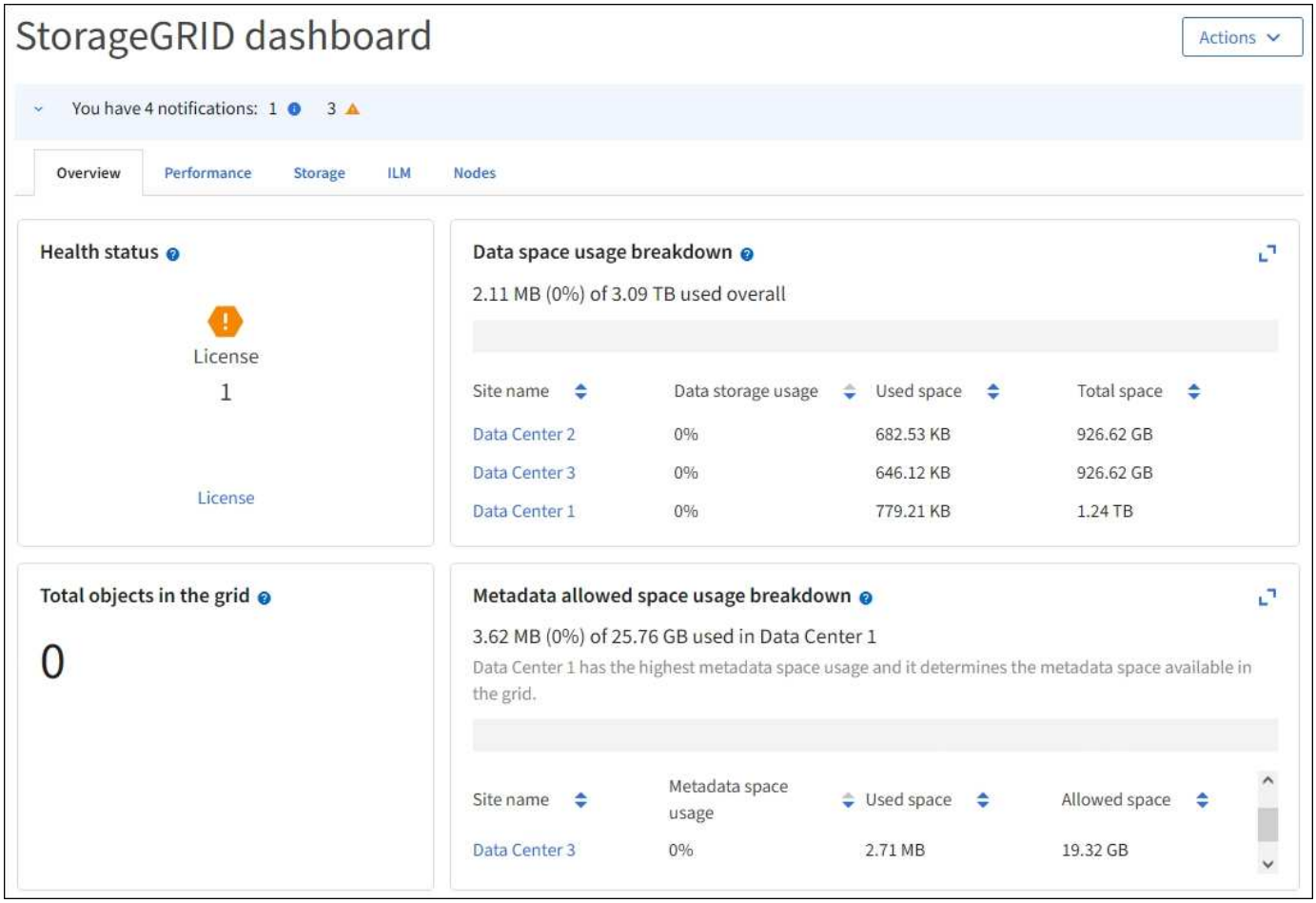
- "Visualizza e gestisci la dashboard"
- "Visualizza la pagina dei nodi"
- "Monitora regolarmente questi aspetti del sistema:"
  - "Stato di salute del sistema"
  - "Capacità di storage"
  - "Gestione del ciclo di vita delle informazioni"
  - "Risorse di rete e di sistema"
  - "Attività tenant"
  - "Operazioni di bilanciamento del carico"
  - "Connessioni di federazione di grid"
- "Gestisci gli avvisi"
- "Visualizza i file di log"
- "Configura la gestione dei log e il server syslog esterno"
- "Usa un server syslog esterno" raccogliere informazioni di audit
- "Usa SNMP per il monitoraggio"
- "Modifica la priorità I/O"per cambiare le priorità relative delle operazioni di I/O

Visualizza e gestisci la dashboard in StorageGRID

Puoi usare la dashboard per monitorare a colpo d'occhio le attività di sistema. Puoi creare dashboard personalizzate per monitorare la tua implementazione di StorageGRID.

Per modificare le unità di misura dei valori di archiviazione visualizzati in Grid Manager, seleziona il menu a discesa utente nell'angolo in alto a destra di Grid Manager, poi seleziona **Preferenze utente**.

La dashboard potrebbe essere diversa in base alla configurazione del sistema.



Visualizza la dashboard

La dashboard è composta da schede che contengono informazioni specifiche sul sistema StorageGRID. Ogni scheda contiene categorie di informazioni visualizzate su delle schede.

Puoi usare la dashboard fornita dal sistema così com'è. Inoltre, puoi creare dashboard personalizzate che contengono solo le schede e le card rilevanti per il monitoraggio della tua implementazione di StorageGRID.

Le schede delle schede del pannello di controllo fornite dal sistema contengono i seguenti tipi di informazioni:

Scheda sul dashboard fornito dal sistema	Contiene
Panoramica	Informazioni generali sulla griglia, come avvisi attivi, utilizzo dello spazio e numero totale di oggetti nella griglia.
Prestazioni	Utilizzo dello spazio, spazio di archiviazione utilizzato nel tempo, operazioni S3, durata della richiesta, tasso di errore.

Scheda sul dashboard fornito dal sistema	Contiene
Storage	Utilizzo delle quote dei tenant e utilizzo dello spazio logico. Previsioni sull'utilizzo dello spazio per i dati utente e i metadati.
ILM	Coda e tasso di valutazione del ciclo di vita delle informazioni.
Nodi	Utilizzo di CPU, dati e memoria per nodo. Operazioni S3 per nodo. Distribuzione da nodo a sito.

Alcune schede possono essere ingrandite per una visualizzazione più agevole. Seleziona l'icona di ingrandimento nell'angolo in alto a destra della scheda. Per chiudere una scheda ingrandita, seleziona l'icona di riduzione oppure seleziona **Close**.

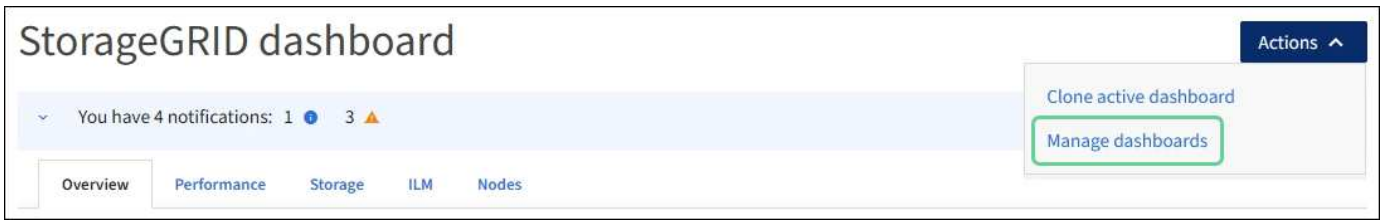
Gestisci dashboard

Se hai l'accesso Root (vedi "Autorizzazioni del gruppo amministratore"), puoi eseguire le seguenti attività di gestione per le dashboard:

- Crea una dashboard personalizzata da zero. Puoi utilizzare le dashboard personalizzate per controllare quali informazioni di StorageGRID vengono visualizzate e come queste informazioni vengono organizzate.
- Clona una dashboard per creare dashboard personalizzate.
- Imposta una dashboard attiva per un utente. La dashboard attiva può essere quella fornita dal sistema o una dashboard personalizzata.
- Imposta una dashboard predefinita, che è quella che tutti gli utenti vedono a meno che non attivino la propria dashboard.
- Modifica il nome di una dashboard.
- Modifica una dashboard per aggiungere o rimuovere schede e riquadri. Puoi avere un minimo di 1 e un massimo di 20 schede.
- Rimuovi una dashboard.

> Se hai qualsiasi altra autorizzazione oltre all'accesso Root, puoi solo impostare una dashboard attiva.

Per gestire le dashboard, seleziona **Azioni** > **Gestisci dashboard**.



Configura le dashboard

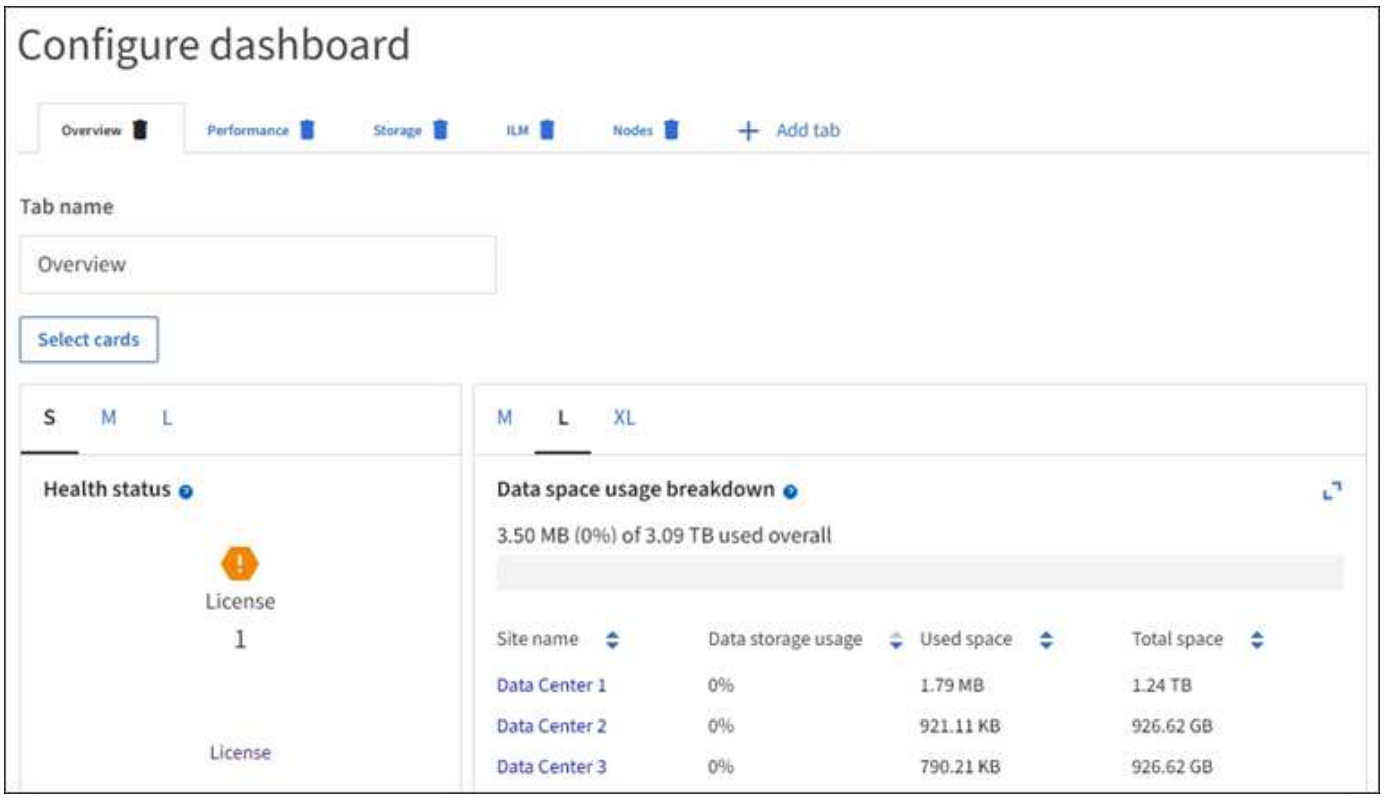
Per creare una nuova dashboard clonando la dashboard attiva, seleziona **Azioni** > **Clona dashboard attiva**.

Per modificare o clonare una dashboard esistente, seleziona **Azioni** > **Gestisci dashboard**.

La dashboard fornita dal sistema non può essere modificata o rimossa.

Quando configuri una dashboard, puoi:

- Aggiungi o rimuovi schede
- Rinomina le schede e dai nomi univoci alle nuove schede
- Aggiungi, rimuovi o riorganizza (trascina) le schede per ogni tab
- Seleziona la taglia per le singole carte scegliendo **S**, **M**, **L** o **XL** in alto sulla carta



Visualizza la pagina dei nodi

Visualizza la pagina dei nodi StorageGRID

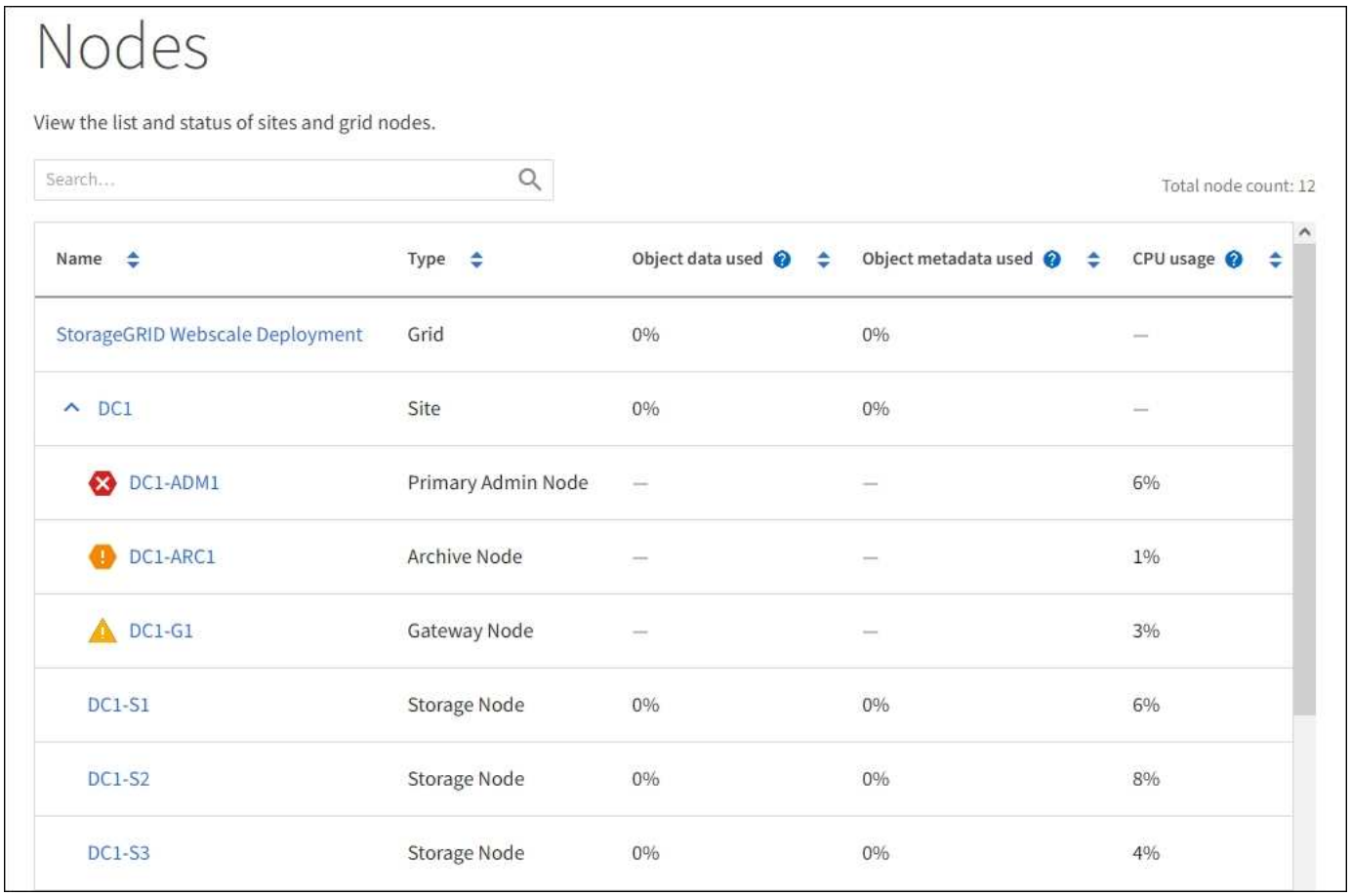
Quando hai bisogno di informazioni più dettagliate sul tuo sistema StorageGRID rispetto a quelle fornite dalla dashboard, puoi utilizzare la pagina Nodi per visualizzare le metriche per l'intera griglia, per ogni sito nella griglia e per ogni nodo in un sito.

La tabella Nodi elenca le informazioni di riepilogo per l'intera griglia, per ogni sito e per ogni nodo. Se un nodo è disconnesso o presenta un avviso attivo, viene visualizzata un'icona accanto al nome del nodo. Se il nodo è connesso e non presenta avvisi attivi, non viene visualizzata alcuna icona.

Quando un nodo non è connesso al grid, ad esempio durante un aggiornamento o in stato di disconnessione, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e del grid. Dopo che un nodo si è riconnesso al grid, aspetta alcuni minuti perché i valori si stabilizzino.

Per modificare le unità di misura dei valori di archiviazione visualizzati in Grid Manager, seleziona il menu a discesa utente nell'angolo in alto a destra di Grid Manager, poi seleziona **Preferenze utente**.

Le schermate mostrate sono esempi. I risultati potrebbero variare a seconda della versione di StorageGRID.



Icone di stato della connessione

Se un nodo viene disconnesso dalla griglia, accanto al nome del nodo viene visualizzata una delle seguenti icone.

Icona	Descrizione	Azione richiesta
	Non connesso - Sconosciuto Per ragioni sconosciute, un nodo risulta disconnesso o i servizi sul nodo risultano inaspettatamente non disponibili. Ad esempio, un servizio sul nodo potrebbe essere stato interrotto oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un guasto imprevisto. Potrebbe anche essere attivato l'avviso **Impossibile comunicare con il nodo**. Potrebbero inoltre essere attivi altri avvisi.	Richiede attenzione immediata. "Seleziona ogni avviso" e segui le azioni consigliate. Ad esempio, potresti dover riavviare un servizio che si è arrestato o riavviare l'host per il nodo. **Nota**: Un nodo potrebbe apparire come Sconosciuto durante le operazioni di arresto gestito. Puoi ignorare lo stato Sconosciuto in questi casi.
	Non connesso - Amministrativamente inattivo Per un motivo prevedibile, il nodo non è connesso al grid. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando oppure il software viene aggiornato. Potrebbero anche essere attivi uno o più avvisi. In base al problema di fondo, questi nodi spesso tornano online senza intervento.	Verifica se ci sono avvisi che interessano questo nodo. Se uno o più avvisi sono attivi, "Seleziona ogni avviso" e segui le azioni consigliate.

Se un nodo è disconnesso dalla griglia, potrebbe avere un avviso sottostante, ma viene visualizzata solo l'icona "Non connesso". Per vedere gli avvisi attivi per un nodo, seleziona il nodo.

Icone di avviso

Se è presente un avviso attivo per un nodo, accanto al nome del nodo viene visualizzata una delle seguenti icone:

Critico: Si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. Devi risolvere immediatamente il problema alla radice. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.

Grave: Si è verificata una condizione anomala che sta influenzando le operazioni in corso o si sta avvicinando alla soglia per un avviso critico. Dovresti esaminare gli avvisi gravi e risolvere eventuali problemi sottostanti per assicurarti che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID.

Minore: Il sistema funziona normalmente, ma è presente una condizione anomala che, se persiste, potrebbe compromettere la capacità del sistema di funzionare. Dovresti monitorare e risolvere gli avvisi minori che non si risolvono da soli per assicurarti che non causino un problema più serio.

Visualizza i dettagli di un sistema, sito o nodo

Per filtrare le informazioni visualizzate nella tabella Nodi, inserisci una stringa di ricerca nel campo **Cerca**. Puoi cercare per nome del sistema, nome visualizzato o tipo (ad esempio, inserisci **gat** per individuare rapidamente tutti i Gateway Nodes).

Per visualizzare le informazioni relative alla griglia, al sito o al nodo:

- Seleziona il nome della griglia per visualizzare un riepilogo aggregato delle statistiche per l'intero sistema StorageGRID.
- Seleziona uno specifico sito del data center per visualizzare un riepilogo aggregato delle statistiche di tutti i nodi in quel sito.
- Seleziona un nodo specifico per visualizzare informazioni dettagliate su quel nodo.

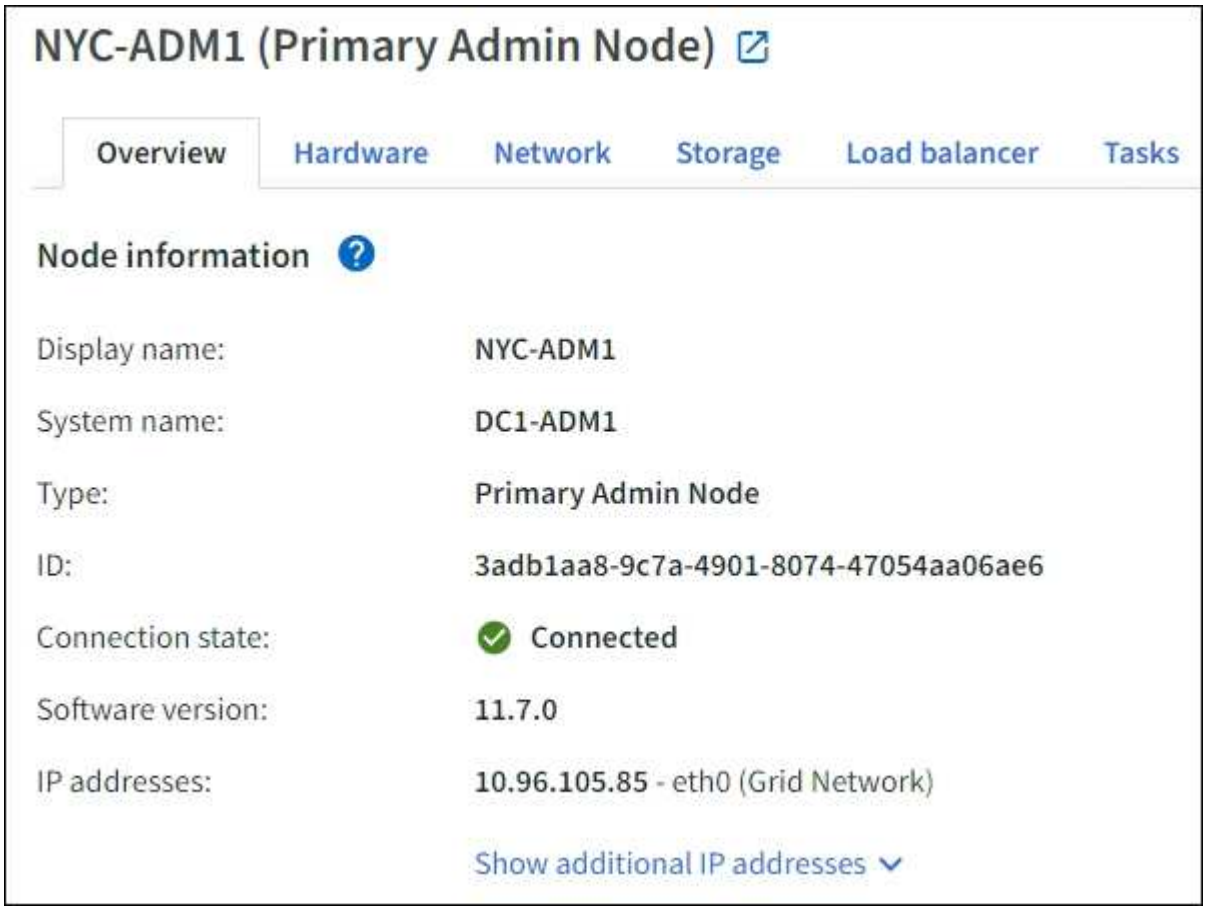
Visualizza la scheda Panoramica di StorageGRID

La scheda Panoramica fornisce informazioni di base su ciascun nodo. Mostra anche eventuali avvisi che attualmente interessano il nodo.

La scheda Panoramica viene mostrata per tutti i nodi.

Informazioni sul nodo

La sezione Informazioni sul nodo della scheda Panoramica elenca le informazioni di base sul nodo.



Le informazioni generali relative a un nodo includono quanto segue:

- **Nome visualizzato** (mostrato solo se il nodo è stato rinominato): Il nome visualizzato corrente del nodo. Usa la procedura "Rinomina la griglia, i siti e i nodi" per aggiornare questo valore.
- **Nome del sistema**: Il nome che hai inserito per il nodo durante l'installazione. I nomi del sistema vengono utilizzati per le operazioni interne di StorageGRID e non possono essere modificati.
- **Tipo**: Il tipo di nodo: Admin Node, primary Admin Node, Storage Node o Gateway Node.
- **ID**: L'identificativo univoco del nodo, noto anche come UUID.
- **Stato della connessione**: Uno dei tre stati. L'icona per lo stato più grave viene mostrata.
  - **Sconosciuto**: Per un motivo sconosciuto, il nodo non è connesso alla grid oppure uno o più servizi sono inaspettatamente non disponibili. Ad esempio, la connessione di rete tra i nodi è stata persa, manca l'alimentazione o un servizio non è disponibile. Potrebbe anche essere attivato l'avviso **Unable to communicate with node**. Potrebbero essere attivi anche altri avvisi. Questa situazione richiede un intervento immediato.

    > Durante le operazioni di arresto gestito, un nodo potrebbe apparire come "Sconosciuto". Puoi ignorare lo stato "Sconosciuto" in questi casi.

  - **Inattivo per motivi amministrativi**: Il nodo non è connesso alla grid per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando oppure il software viene aggiornato. Potrebbero anche essere attivi uno o più avvisi.
  - **Connesso**: Il nodo è connesso alla griglia.
- **Spazio di archiviazione utilizzato**: Solo per Storage Nodes.
  - **Dati oggetto**: la percentuale dello spazio totale utilizzabile per i dati oggetto che è stata utilizzata sullo Storage Node.
  - **Metadati degli oggetti**: la % dello spazio totale consentito per i metadati degli oggetti che hai utilizzato sullo Storage Node.
- **Versione del software**: La versione di StorageGRID installata sul nodo.
- **Gruppi HA**: Solo per Admin Node e Gateway Nodes. Mostrato se un'interfaccia di rete sul nodo è inclusa in un gruppo ad alta disponibilità e se tale interfaccia è l'interfaccia primaria.
- **Indirizzi IP**: Gli indirizzi IP del nodo. Fai clic su **Mostra indirizzi IP aggiuntivi** per visualizzare gli indirizzi IPv4 e IPv6 del nodo e le mappature delle interfacce.

Avvisi

La sezione Avvisi della scheda Panoramica elenca tutti gli avvisi "avvisi che attualmente interessano questo nodo e che non sono stati silenziati". Seleziona il nome dell'avviso per visualizzare ulteriori dettagli e azioni consigliate.

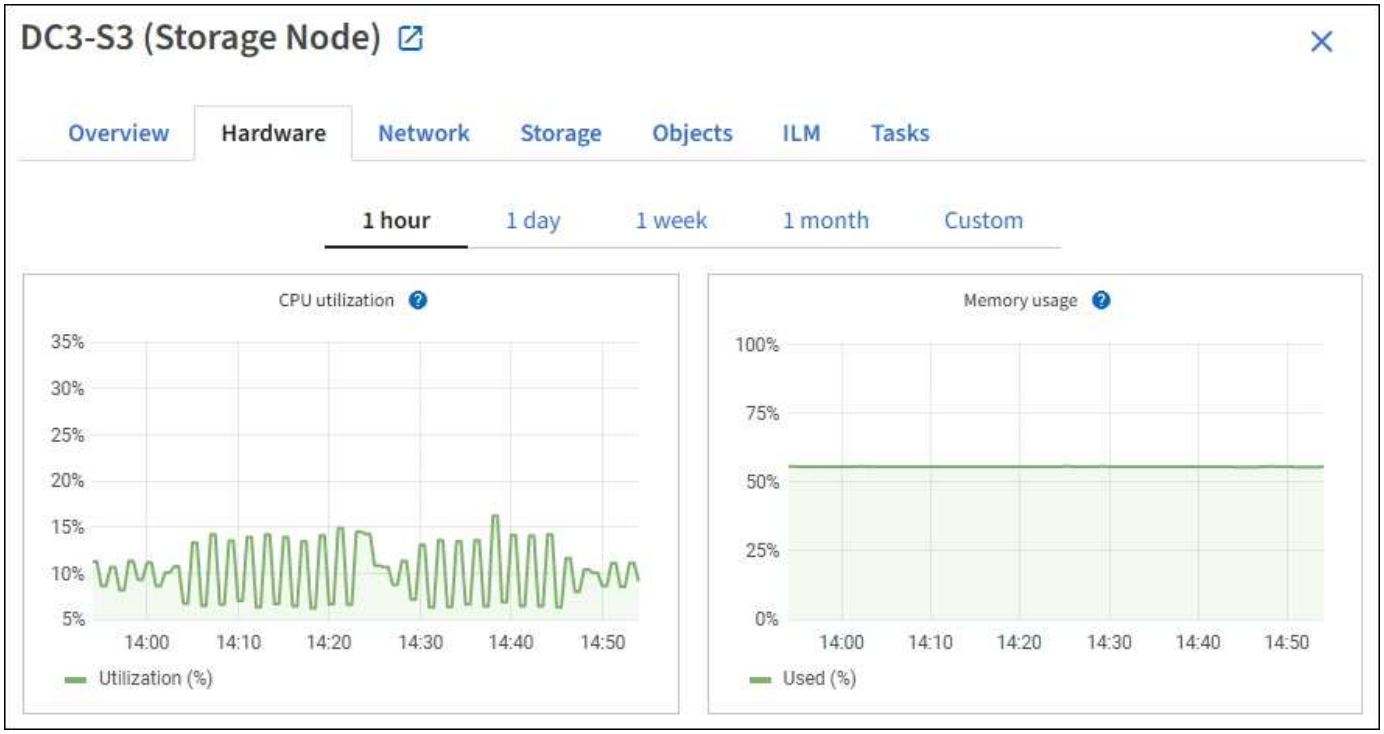
Sono inclusi anche gli avvisi per "stati di connessione del nodo".

Visualizza la scheda Hardware di StorageGRID

La scheda Hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo e ulteriori informazioni sull'hardware dei dispositivi.

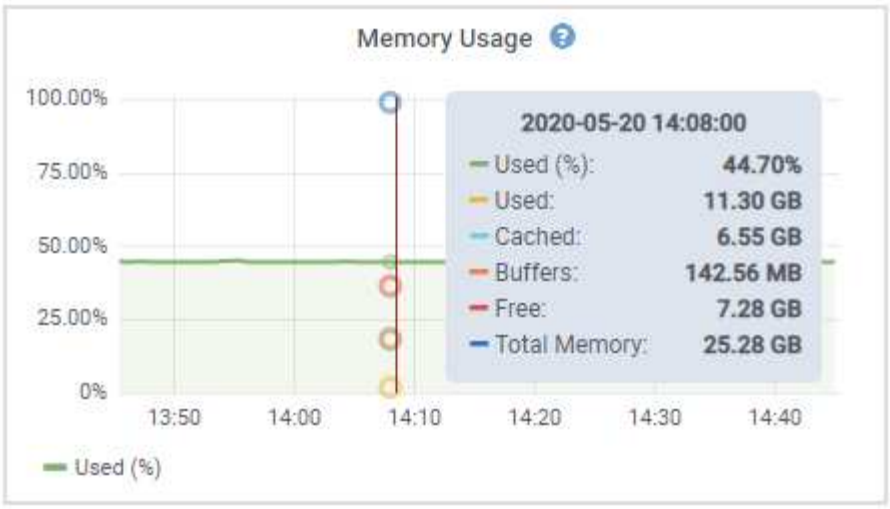
> Il Grid Manager viene aggiornato a ogni release e potrebbe non corrispondere alle schermate di esempio presenti in questa pagina.

La scheda Hardware viene visualizzata per tutti i nodi.



Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. Puoi visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. Puoi anche impostare un intervallo personalizzato, che ti permette di specificare intervalli di date e orari.

Per vedere i dettagli sull'utilizzo della CPU e della memoria, posiziona il cursore su ciascun grafico.



Se il nodo è un nodo appliance, questa scheda include anche una sezione con ulteriori informazioni sull'hardware dell'appliance.

Visualizza informazioni sui nodi di storage dell'appliance

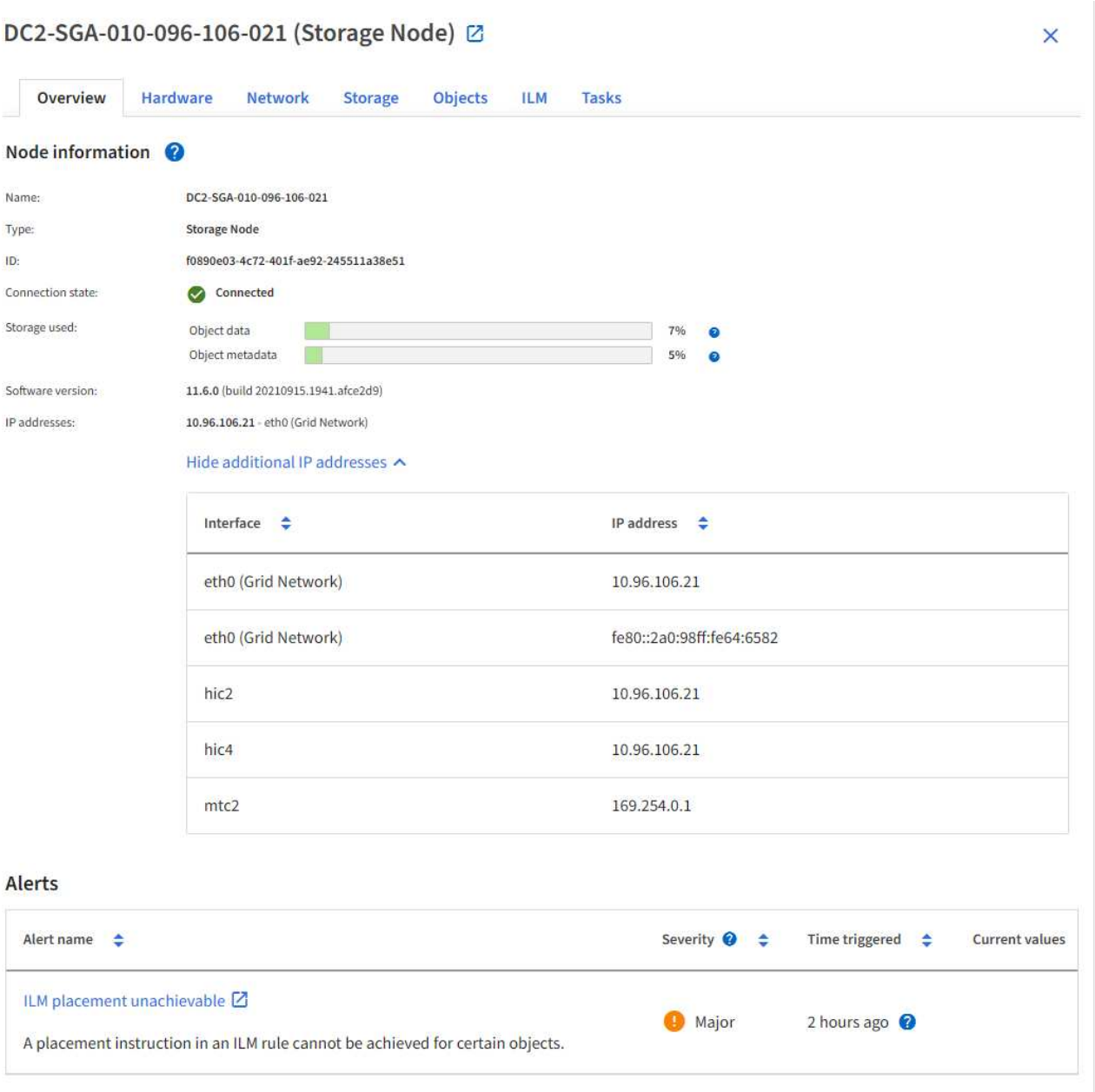
La pagina Nodi elenca le informazioni sullo stato del servizio e su tutte le risorse di calcolo, i dispositivi disco e le risorse di rete per ciascun Storage Node dell'appliance. Puoi anche vedere memoria, hardware di storage, versione del firmware del controller, risorse di rete, interfacce di rete, indirizzi di rete e dati ricevuti e trasmessi.

Passaggi

1. Dalla pagina Nodi, seleziona un nodo di storage dell'appliance.
2. Seleziona **Overview**.

   La sezione Informazioni nodo della scheda Panoramica visualizza informazioni di riepilogo relative al nodo, come il nome, il tipo, l'ID e lo stato della connessione. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

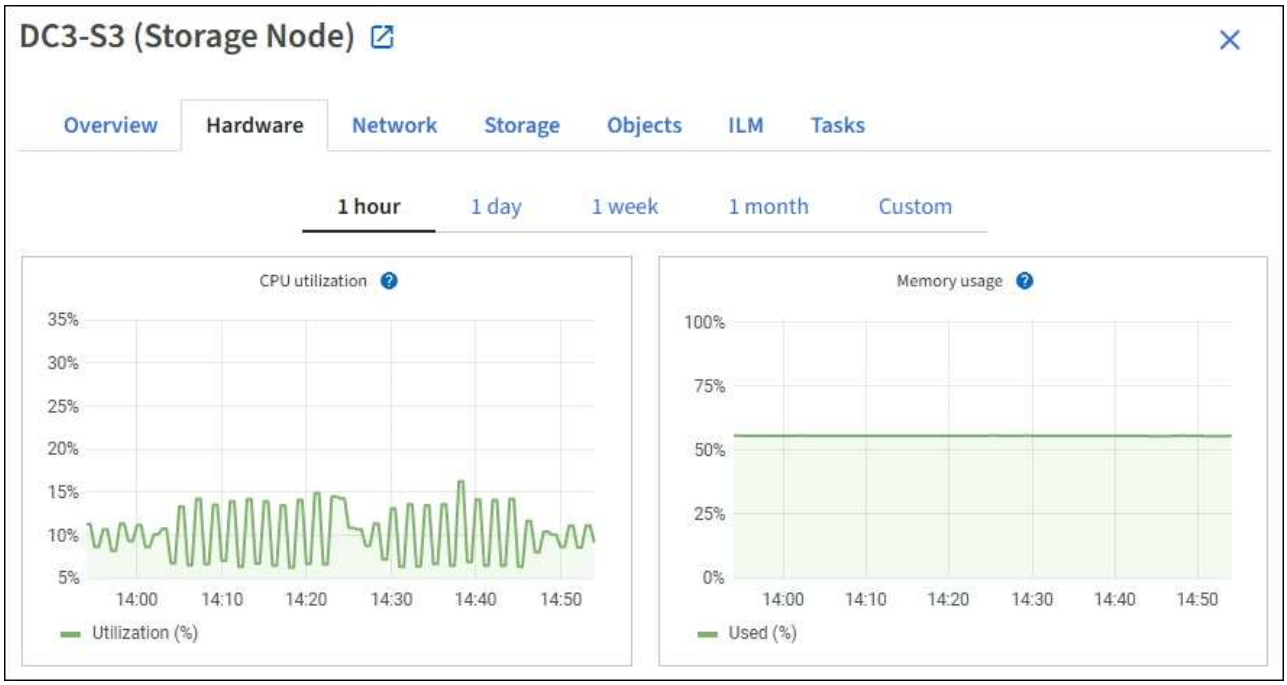
   - **eth**: La Grid Network, l'Admin Network o la Client Network.
   - **hic**: Una delle porte fisiche da 10, 25 o 100 GbE presenti sull'appliance. Queste porte possono essere aggregate e connesse alla StorageGRID Grid Network (eth0) e alla Client Network (eth2).
   - **mtc**: Una delle porte fisiche da 1 GbE presenti sull'appliance. Una o più interfacce mtc sono aggregate per formare l'interfaccia di rete di amministrazione di StorageGRID (eth1). Puoi lasciare disponibili altre interfacce mtc per la connettività locale temporanea di un tecnico nel data center.



La sezione Avvisi della scheda Panoramica visualizza eventuali avvisi attivi per il nodo.

3. Seleziona **Hardware** per vedere altre informazioni sull'appliance.

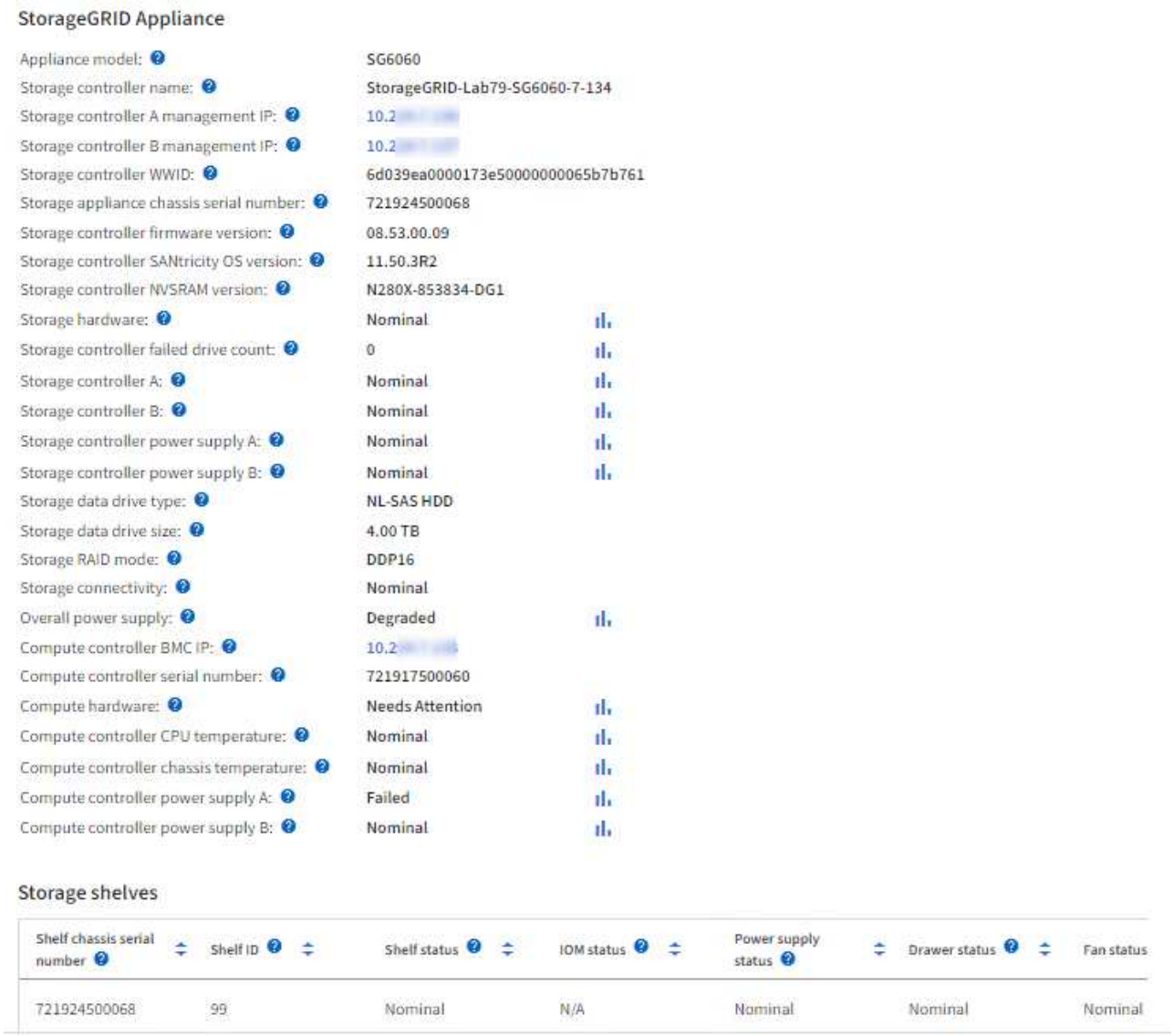
   a. Visualizza i grafici di utilizzo della CPU e della memoria per determinare le percentuali di utilizzo di CPU e memoria nel tempo. Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. Puoi visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. Puoi anche impostare un intervallo personalizzato, che ti permette di specificare intervalli di date e orari.



b. Scorri verso il basso per visualizzare la tabella dei componenti dell'appliance. Questa tabella contiene informazioni quali il nome del modello dell'appliance, i nomi dei controller, i numeri di serie e gli indirizzi IP, nonché lo stato di ciascun componente.

> Alcuni campi, come Compute controller BMC IP e Compute hardware, vengono visualizzati solo per gli appliance che dispongono di questa funzionalità.

I componenti per gli shelf di storage e gli shelf di espansione, se fanno parte dell'installazione, compaiono in una tabella separata sotto la tabella dell'appliance.



Campo nella tabella Appliance	Descrizione
Modello dell'appliance	Il numero di modello di questo appliance StorageGRID viene visualizzato in SANtricity OS.
Nome dello storage controller	Il nome di questa appliance StorageGRID visualizzato in SANtricity OS.
IP di gestione dello storage controller A	Indirizzo IP per la porta di gestione 1 sullo storage controller A. Usi questo IP per accedere a SANtricity OS per risolvere i problemi di storage.
IP di gestione dello storage controller B	Indirizzo IP per la porta di gestione 1 sullo storage controller B. Usi questo IP per accedere a SANtricity OS per risolvere i problemi di storage. Alcuni modelli di appliance non dispongono di uno storage controller B.

Campo nella tabella Appliance	Descrizione
WWID dello storage controller	L'identificativo mondiale dello storage controller visualizzato in SANtricity OS.
Numero di serie dello chassis dell'appliance di storage	Il numero di serie del chassis dell'apparecchio.
Versione firmware dello storage controller	La versione del firmware sullo storage controller per questo appliance.
Versione del sistema operativo SANtricity dello storage controller	La versione SANtricity OS dello storage controller A.
Versione NVSRAM dello storage controller	Versione NVSRAM dello storage controller come riportato da SANtricity System Manager. Per SG6060 e SG6160, se c'è una discrepanza nella versione della NVSRAM tra i due controller, viene visualizzata la versione del controller A. Se il controller A non è installato o operativo, viene visualizzata la versione del controller B.
Hardware di storage	Lo stato generale dell'hardware dello storage controller. Se SANtricity System Manager segnala uno stato di Needs Attention per l'hardware di storage, anche il sistema StorageGRID riporta questo valore. Se lo stato è "richiede attenzione", innanzitutto controlla lo storage controller utilizzando SANtricity OS. Poi assicurati che non siano presenti altri avvisi relativi al compute controller.
Conteggio delle unità guaste dello storage controller	Il numero di unità che non sono ottimali.
Storage controller A	Lo stato dello storage controller A.
Storage controller B	Lo stato dello storage controller B. Alcuni modelli di appliance non hanno uno storage controller B.
Alimentatore dello storage controller A	Stato dell'alimentatore A per lo storage controller.
Alimentatore dello storage controller B	Stato dell'alimentatore B per lo storage controller.
Tipo di unità dati di storage	Il tipo di drive presenti nell'appliance, come HDD (hard drive) o SSD (solid state drive).

Campo nella tabella Appliance	Descrizione
Dimensione dell'unità dati di storage	La dimensione effettiva di un'unità dati. Per l'SG6160, viene visualizzata anche la dimensione dell'unità cache. **Nota**: Per i nodi con shelf di espansione, usa Dimensioni dell'unità dati per ogni shelf invece. La dimensione effettiva del disco potrebbe variare a seconda dello shelf.
Modalità RAID dello storage	La modalità RAID configurata per l'appliance.
Connettività dello storage	Lo stato della connettività dello storage.
Alimentazione elettrica complessiva	Lo stato di tutti gli alimentatori dell'appliance.
IP del BMC del controller di calcolo	L'indirizzo IP della porta BMC (baseboard management controller) nel compute controller. Usi questo IP per connetterti all'interfaccia BMC e monitorare o diagnosticare l'hardware dell'appliance. Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.
Hardware di calcolo	Stato dell'hardware del controller di elaborazione. Questo campo non viene visualizzato per i modelli di appliance che non dispongono di hardware di elaborazione e di archiviazione separati.
Temperatura della CPU del compute controller	Lo stato della temperatura della CPU del compute controller.
Temperatura dello chassis del controller di calcolo	Stato della temperatura del compute controller.

+

Colonna nella tabella degli shelf di storage	Descrizione
Numero di serie dello chassis dello shelf	Il numero di serie dello chassis dello shelf di espansione.

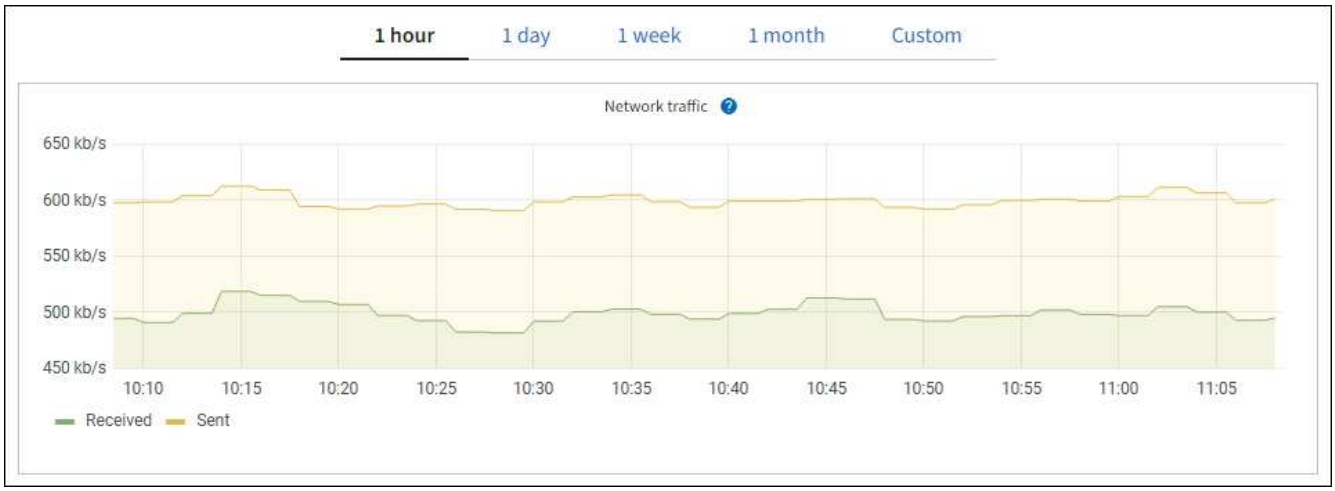
Colonna nella tabella degli shelf di storage	Descrizione
ID shelf	L'identificativo numerico dello shelf di storage. • 99: Shelf dello storage controller • 0: Primo shelf di espansione • 1: Secondo shelf di espansione **Nota:** Gli shelf di espansione si applicano solo a SG6060 e SG6160.
Stato dello shelf	Stato generale dello shelf di espansione.
Stato dell'IOM	Lo stato dei moduli di input/output (IOM) presenti in qualsiasi shelf di espansione. N/D se non si tratta di uno shelf di espansione.
stato dell'alimentazione	Stato generale degli alimentatori per lo shelf di storage.
Stato del cassetto	Stato dei cassetti nello shelf di espansione. N/D se lo shelf non contiene cassetti.
Stato della ventola	Stato generale delle ventole di raffreddamento nello shelf di espansione.
Slot per unità	Il numero totale di alloggiamenti per unità disco nello shelf di storage.
Unità dati	Il numero di unità nello shelf di storage utilizzate per l'archiviazione dei dati.
Dimensione dell'unità dati	La dimensione effettiva di un'unità dati nello shelf di archiviazione.
Unità cache	Il numero di unità nello shelf di archiviazione utilizzate come cache.
Dimensione dell'unità cache	La dimensione dell'unità cache più piccola presente nello shelf di espansione. Normalmente, le unità cache hanno tutte le stesse dimensioni.
Stato della configurazione	Stato di configurazione dello shelf di storage.

a. Conferma che tutti gli stati siano "Nominali".

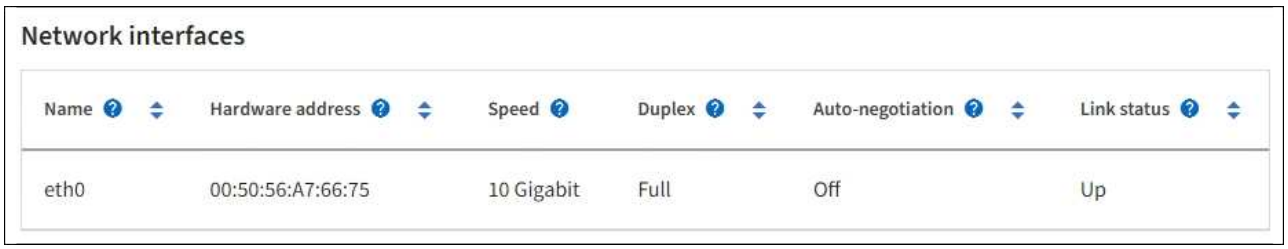
   Se lo stato non è "Nominale", controlla gli avvisi correnti. Puoi anche usare SANtricity System Manager per saperne di più su alcuni di questi valori hardware. Consulta le istruzioni per installare e mantenere il tuo appliance.

4. Seleziona **Network** per visualizzare le informazioni relative a ciascuna rete.

Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo.



a. Esamina la sezione Interfacce di rete.



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

Usa la seguente tabella con i valori nella colonna **Velocità** della tabella Interfacce di rete per determinare se le porte di rete 10/25-GbE sull'appliance sono state configurate per utilizzare la modalità attivo/backup o la modalità LACP.

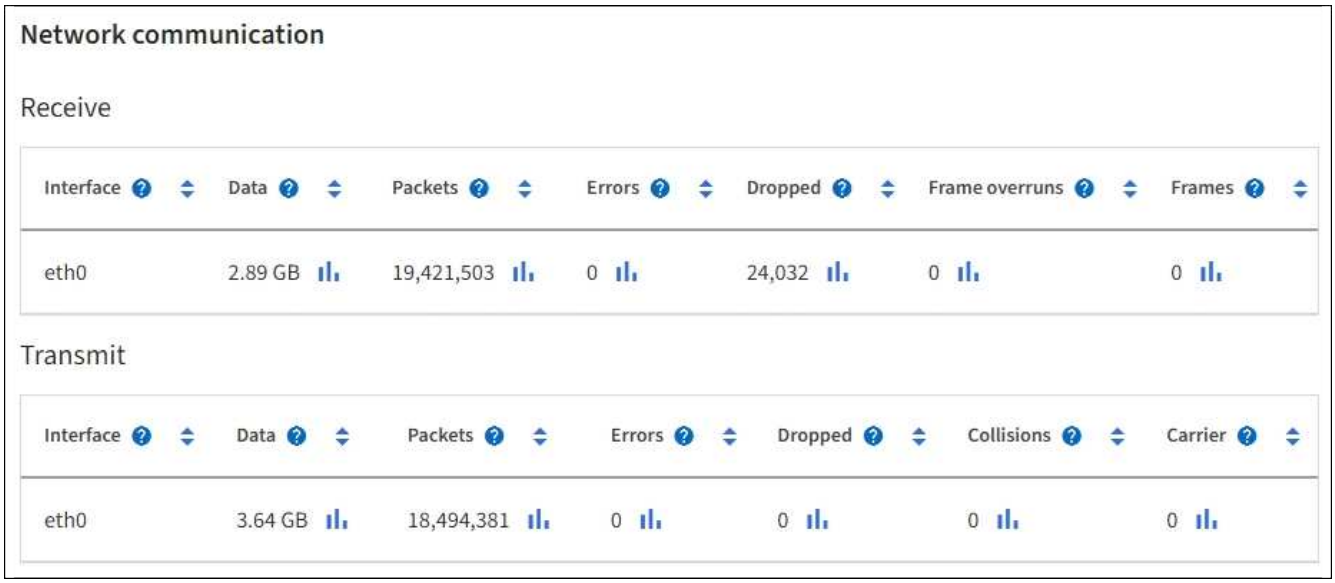
I valori riportati nella tabella presuppongono l'utilizzo di tutti e quattro i collegamenti.

Modalità di collegamento	Modalità bond	Velocità di collegamento HIC individuale (hic1, hic2, hic3, hic4)	Velocità prevista della rete Grid/Client (eth0,eth2)
Aggregato	LACP	25	100
Fisso	LACP	25	50
Fisso	Attivo/Backup	25	25
Aggregato	LACP	10	40
Fisso	LACP	10	20
Fisso	Attivo/Backup	10	10

Consulta "Configura i collegamenti di rete" per ulteriori informazioni sulla configurazione delle porte 10/25-GbE.

b. Consulta la sezione Comunicazione di rete.

Le tabelle Ricezione e Trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, oltre ad altre metriche di ricezione e trasmissione.



Network communication

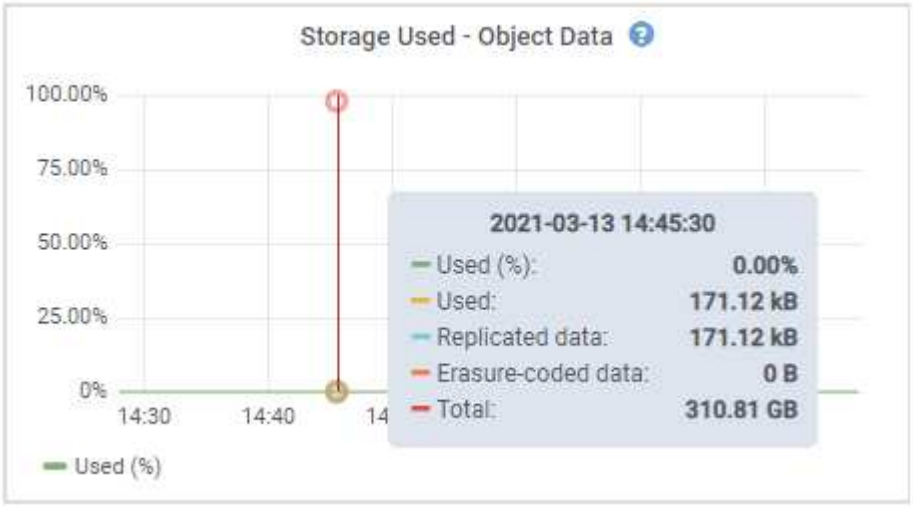
Receive

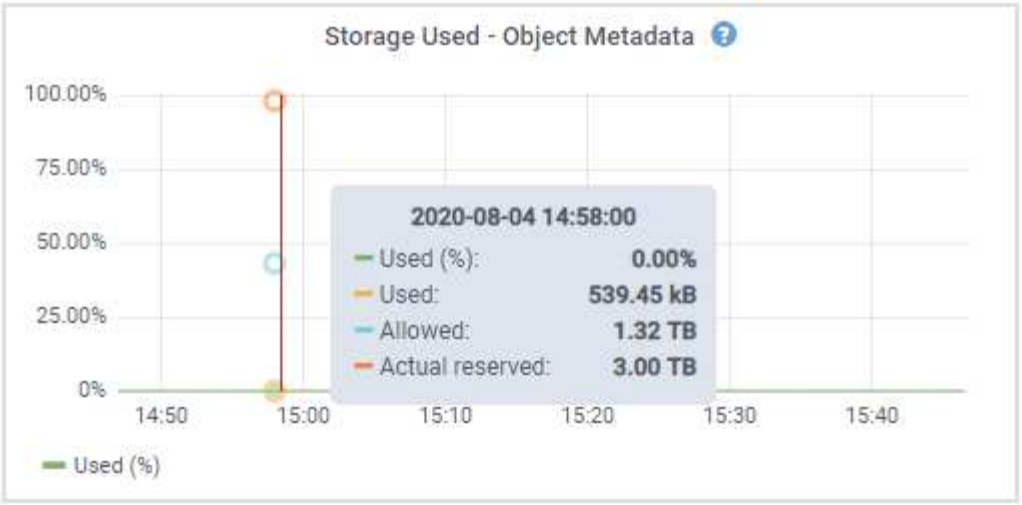
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

5. Seleziona **Archiviazione** per visualizzare i grafici che mostrano le % di storage utilizzato nel tempo per i dati degli oggetti e i metadati degli oggetti, oltre a informazioni su dispositivi disco, volumi e object store.

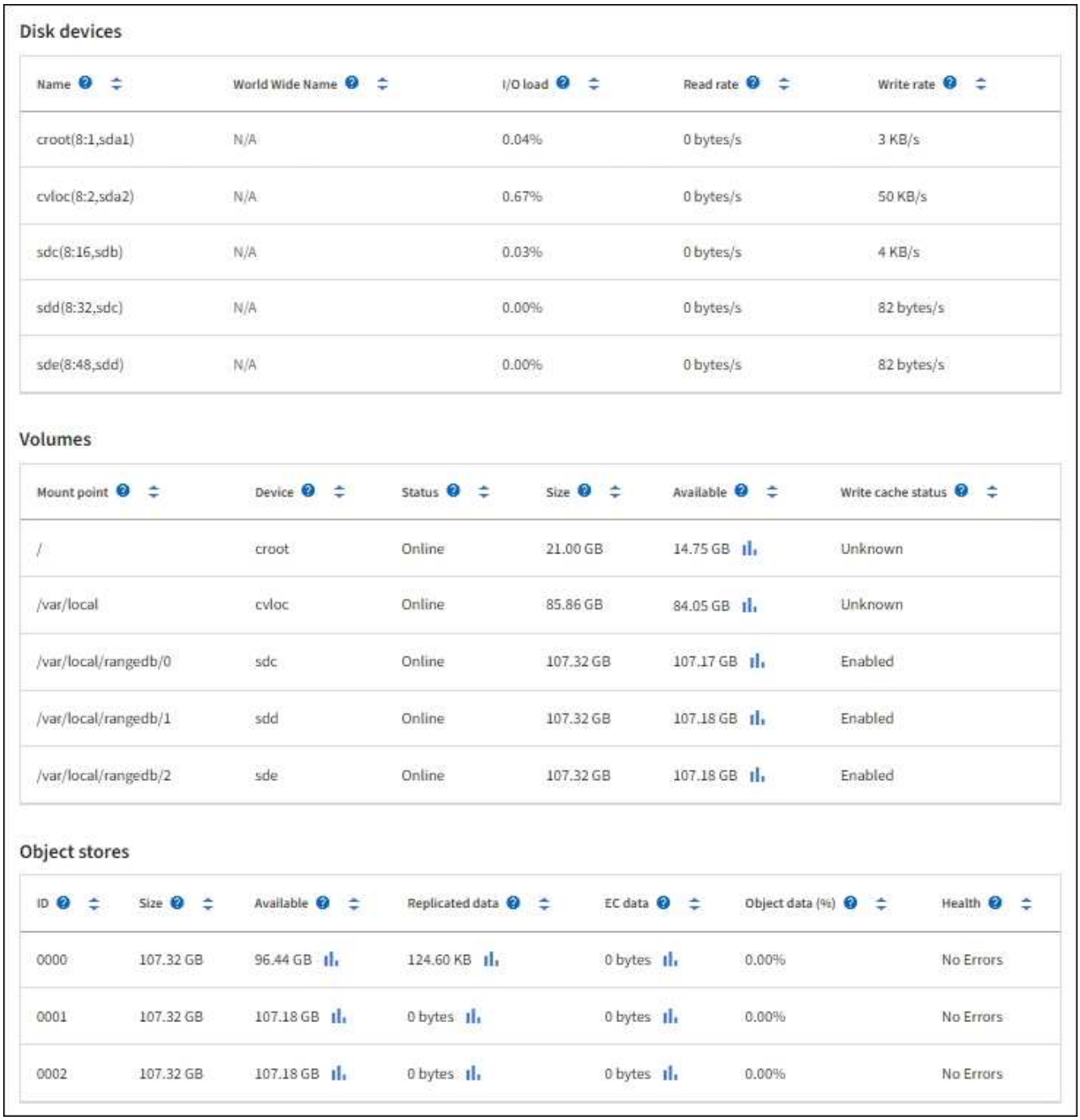




a. Scorri verso il basso per visualizzare la quantità di spazio di storage disponibile per ciascun volume e archivio di oggetti.

   Il Worldwide Name di ciascun disco corrisponde all'identificatore globale del volume (WWID) che appare quando visualizzi le proprietà standard del volume in SANtricity OS (il management software connesso allo storage controller).

   Per aiutarti a interpretare le statistiche di lettura e scrittura del disco relative ai punti di montaggio dei volumi, la prima parte del nome mostrato nella colonna **Nome** della tabella Dispositivi disco (cioè *sdc*, *sdd*, *sde* e così via) corrisponde al valore mostrato nella colonna **Dispositivo** della tabella Volumi.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Visualizza le informazioni sui nodi Admin e sui nodi Gateway dell'appliance

La pagina Nodi elenca le informazioni sullo stato del servizio e su tutte le risorse di calcolo, i dispositivi disco e le risorse di rete per ogni appliance di servizio utilizzata come Admin Node o Gateway Node. Puoi anche vedere memoria, hardware di storage, risorse di rete, interfacce di rete, indirizzi di rete e dati ricevuti e trasmessi.

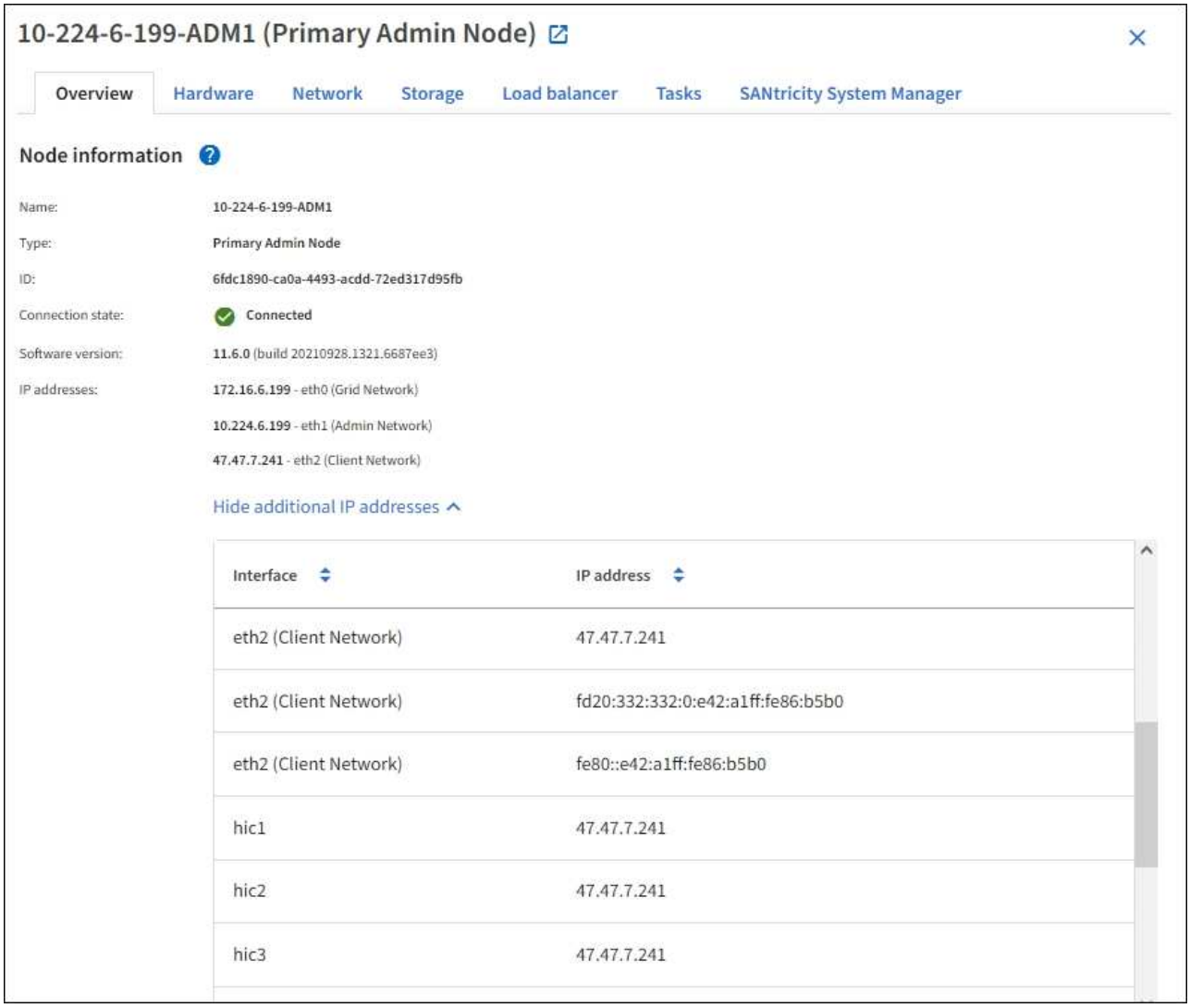
Passaggi

1. Dalla pagina Nodi, seleziona un appliance Admin Node o un appliance Gateway Node.
2. Seleziona **Overview**.

   La sezione Informazioni nodo della scheda Panoramica visualizza informazioni di riepilogo relative al nodo,

come il nome, il tipo, l'ID e lo stato della connessione. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

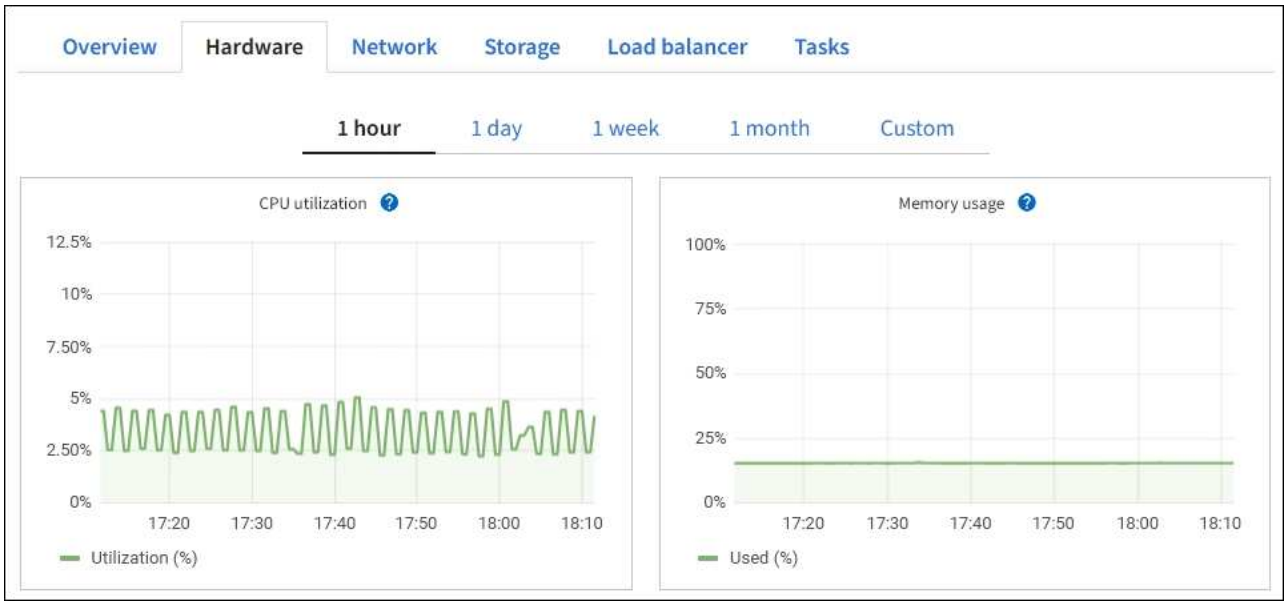
- **adllb** e **adlli**: visualizzati se viene utilizzato il bonding attivo/backup per l'interfaccia Admin Network
- **eth**: La Grid Network, l'Admin Network o la Client Network.
- **hic**: Una delle porte fisiche da 10, 25 o 100 GbE presenti sull'appliance. Queste porte possono essere aggregate e connesse alla StorageGRID Grid Network (eth0) e alla Client Network (eth2).
- **mtc**: Una delle porte fisiche da 1 GbE presenti sull'appliance. Una o più interfacce mtc sono aggregate per formare l'interfaccia Admin Network (eth1). Puoi lasciare disponibili altre interfacce mtc per la connettività locale temporanea di un tecnico nel data center.



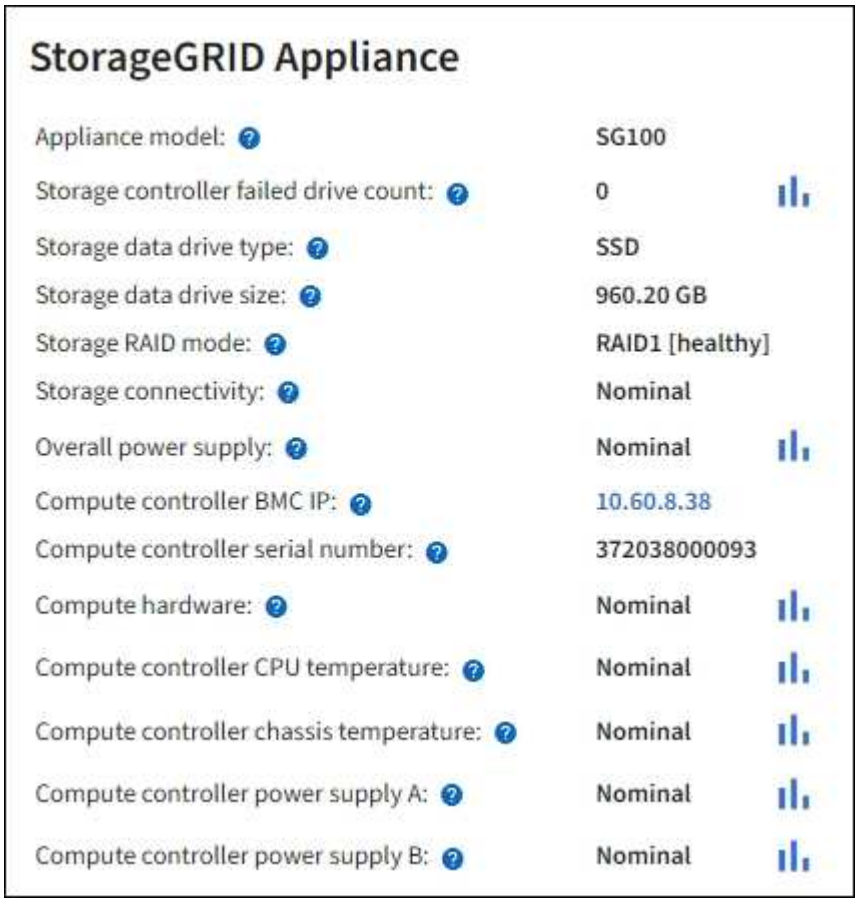
La sezione Avvisi della scheda Panoramica visualizza eventuali avvisi attivi per il nodo.

3. Seleziona **Hardware** per vedere altre informazioni sull'appliance.

   a. Visualizza i grafici di utilizzo della CPU e della memoria per determinare le percentuali di utilizzo di CPU e memoria nel tempo. Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. Puoi visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. Puoi anche impostare un intervallo personalizzato, che ti permette di specificare intervalli di date e orari.



b. Scorri verso il basso per visualizzare la tabella dei componenti dell'appliance. Questa tabella contiene informazioni quali il nome del modello, il numero di serie, la versione del firmware del controller e lo stato di ciascun componente.



Campo nella tabella Appliance	Descrizione
Modello dell'appliance	Il numero di modello di questo appliance StorageGRID.

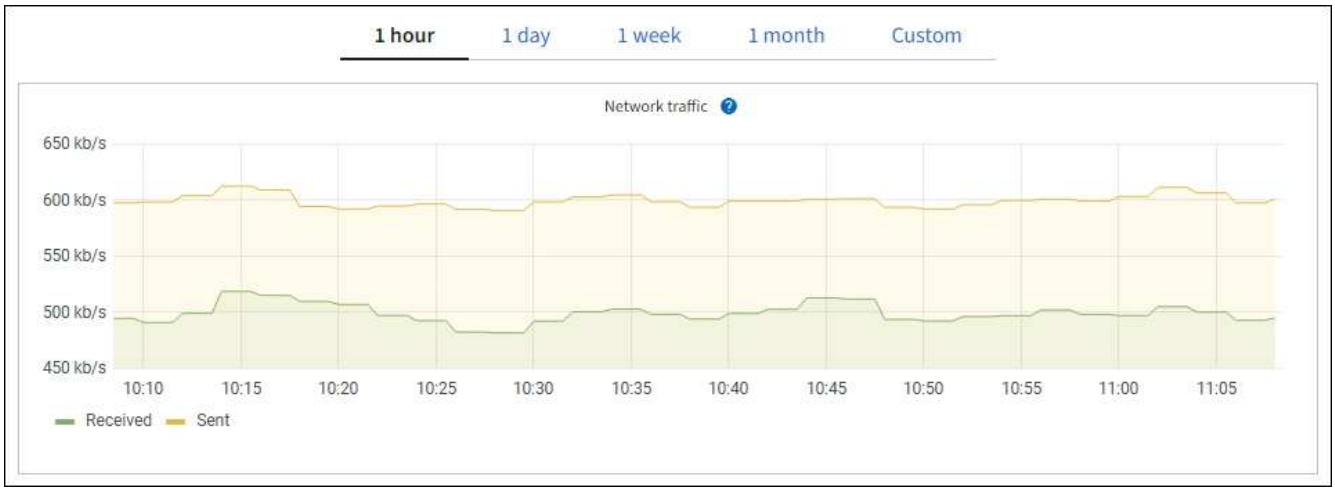
Campo nella tabella Appliance	Descrizione
Conteggio delle unità guaste dello storage controller	Il numero di unità che non sono ottimali.
Tipo di unità dati di storage	Il tipo di drive presenti nell'appliance, come HDD (hard drive) o SSD (solid state drive).
Dimensione dell'unità dati di storage	La dimensione effettiva di un'unità dati.
Modalità RAID dello storage	La modalità RAID per il dispositivo.
Alimentazione elettrica complessiva	Lo stato di tutti gli alimentatori presenti nell'apparecchio.
IP del BMC del controller di calcolo	L'indirizzo IP della porta del baseboard management controller (BMC) nel compute controller. Puoi usare questo IP per connetterti all'interfaccia BMC e monitorare e diagnosticare l'hardware dell'appliance. Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.
Hardware di calcolo	Stato dell'hardware del controller di calcolo.
Temperatura della CPU del compute controller	Lo stato della temperatura della CPU del compute controller.
Temperatura dello chassis del controller di calcolo	Stato della temperatura del compute controller.

a. Conferma che tutti gli stati siano "Nominali".

   Se lo stato non è "Nominale", controlla gli avvisi correnti.

4. Seleziona **Network** per visualizzare le informazioni relative a ciascuna rete.

   Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo.



a. Esamina la sezione Interfacce di rete.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

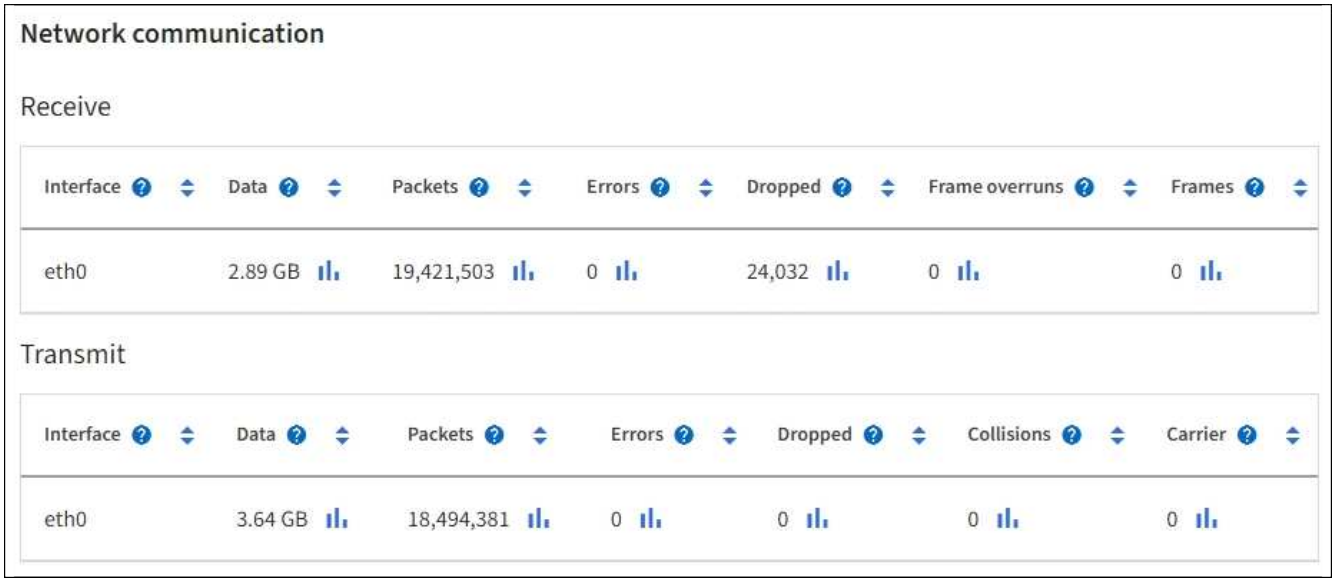
Usa la seguente tabella con i valori nella colonna **Velocità** della tabella Interfacce di rete per capire se le quattro porte di rete 40/100-GbE sull'appliance sono state configurate per usare la modalità attivo/backup o la modalità LACP.

I valori riportati nella tabella presuppongono l'utilizzo di tutti e quattro i collegamenti.

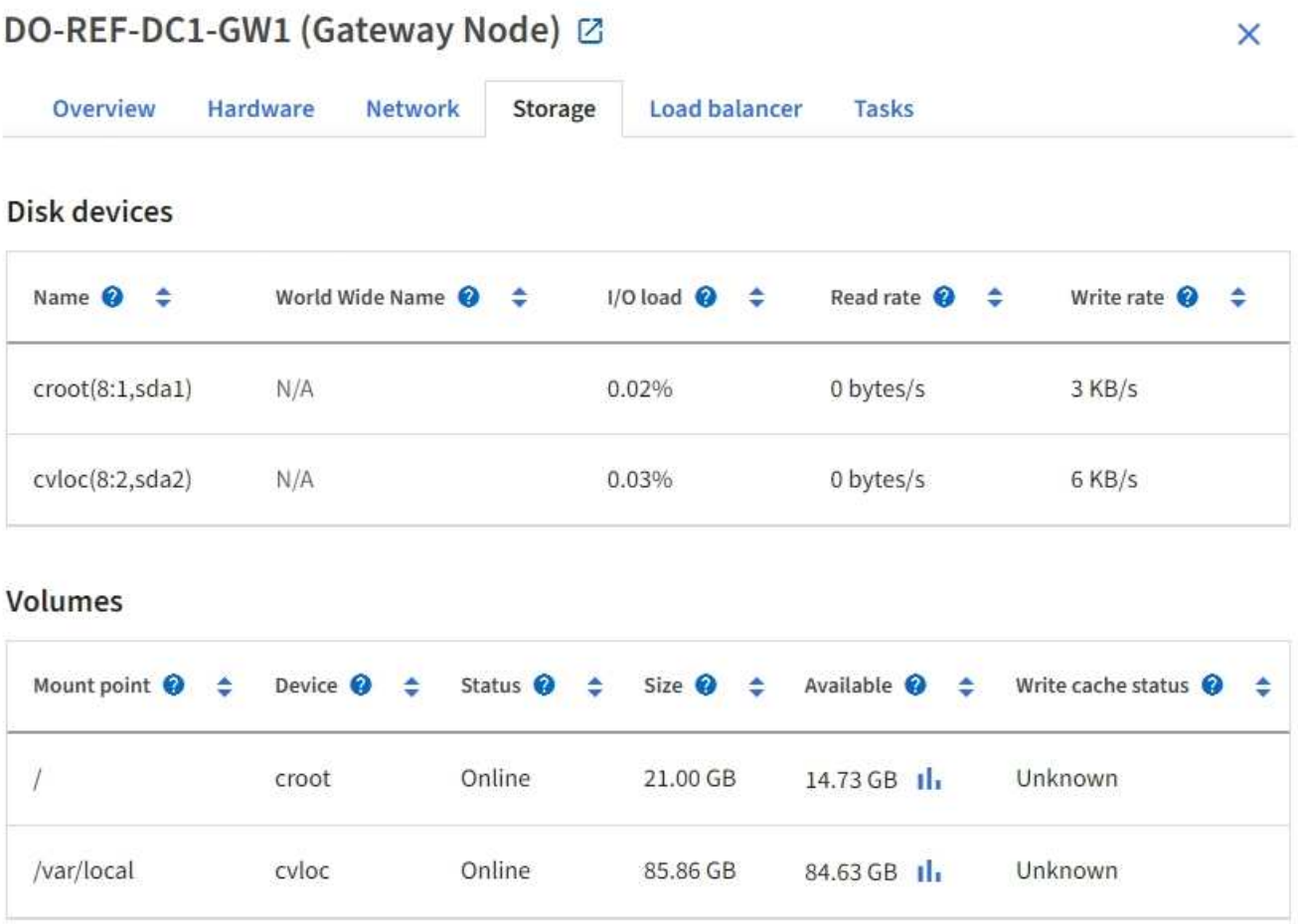
Modalità di collegamento	Modalità bond	Velocità di collegamento HIC individuale (hic1, hic2, hic3, hic4)	Velocità prevista della rete Grid/Client (eth0, eth2)
Aggregato	LACP	100	400
Fisso	LACP	100	200
Fisso	Attivo/Backup	100	100
Aggregato	LACP	40	160
Fisso	LACP	40	80
Fisso	Attivo/Backup	40	40

b. Consulta la sezione Comunicazione di rete.

Le tabelle Ricezione e Trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, oltre ad altre metriche di ricezione e trasmissione.



5. Seleziona **Storage** per visualizzare le informazioni sui dispositivi disco e sui volumi presenti sull'appliance di servizio.



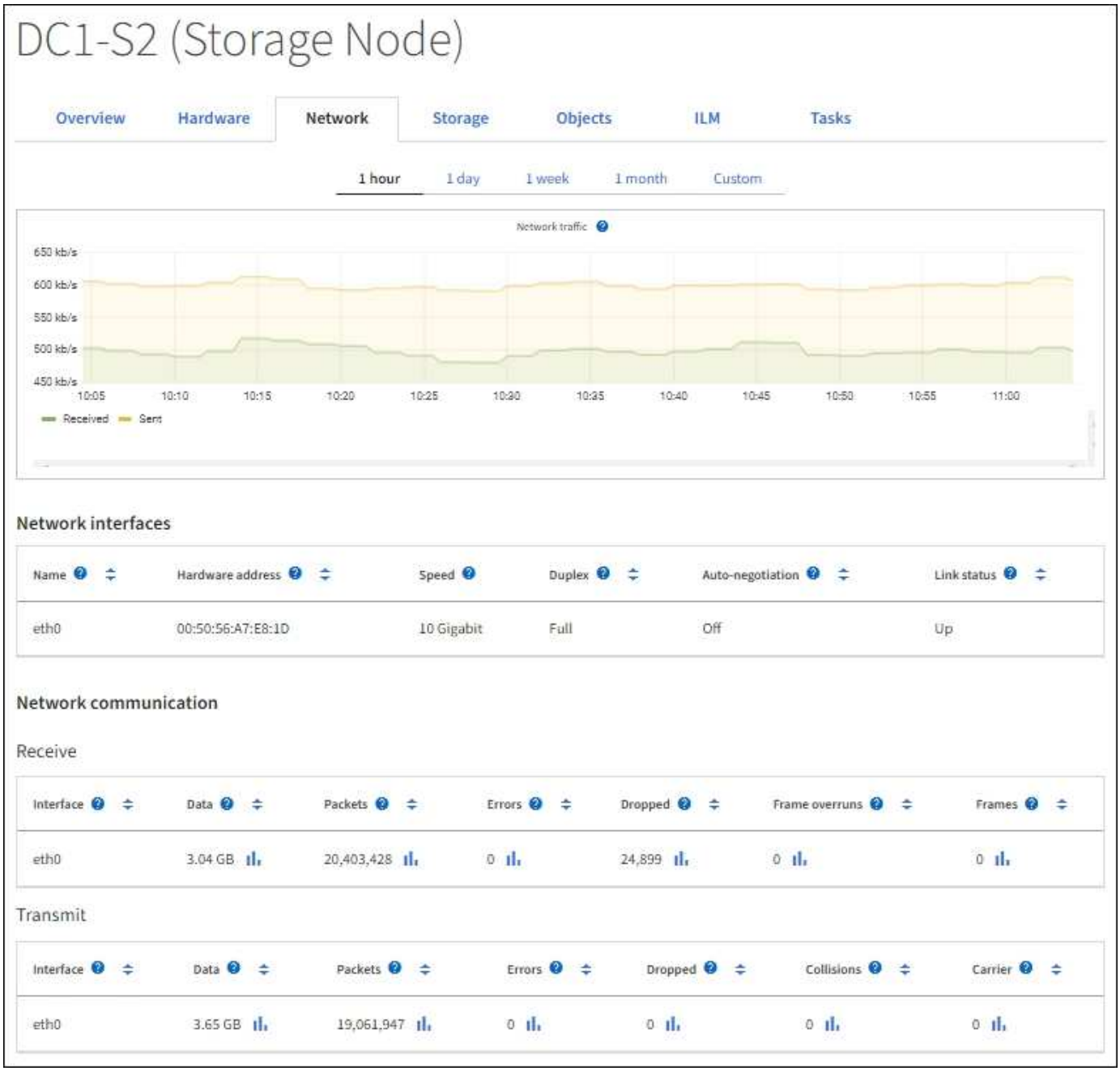
Visualizza la scheda Rete di StorageGRID

La scheda Rete visualizza un grafico che mostra il traffico di rete ricevuto e inviato attraverso tutte le interfacce di rete del nodo, del sito o della griglia.

La scheda Rete viene visualizzata per tutti i nodi, per ciascun sito e per l'intera griglia.

Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. Puoi visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. Puoi anche impostare un intervallo personalizzato, che ti permette di specificare intervalli di date e orari.

Per i nodi, la tabella Interfacce di rete fornisce informazioni sulle porte di rete fisiche di ciascun nodo. La tabella Comunicazioni di rete fornisce dettagli sulle operazioni di ricezione e trasmissione di ciascun nodo e su eventuali contatori di errore segnalati dal driver.



Informazioni correlate

"Monitora le connessioni di rete e le prestazioni"

Visualizza la scheda Storage della StorageGRID

La scheda Archiviazione riassume la disponibilità dello storage e altre metriche dello storage.

La scheda Archiviazione viene visualizzata per tutti i nodi, per ogni sito e per l'intera griglia.

Grafici dello storage utilizzato

Per i nodi di archiviazione, per ogni sito e per l'intera griglia, la scheda Archiviazione include grafici che mostrano la quantità di storage utilizzato dai dati degli oggetti e dai metadati degli oggetti nel tempo.

Quando un nodo non è connesso al grid, ad esempio durante un aggiornamento o in stato di disconnessione, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e del grid. Dopo che un nodo si è riconnesso al grid, aspetta alcuni minuti perché i valori si stabilizzino.

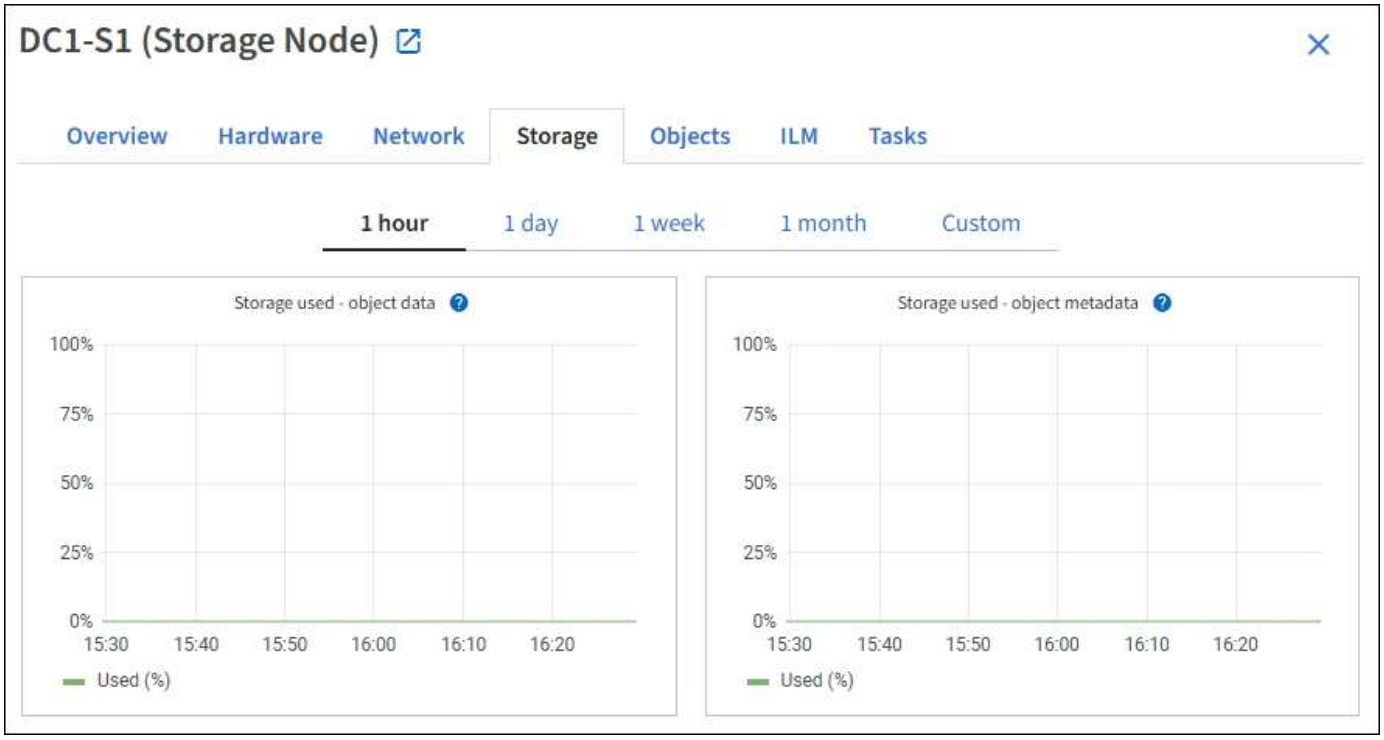
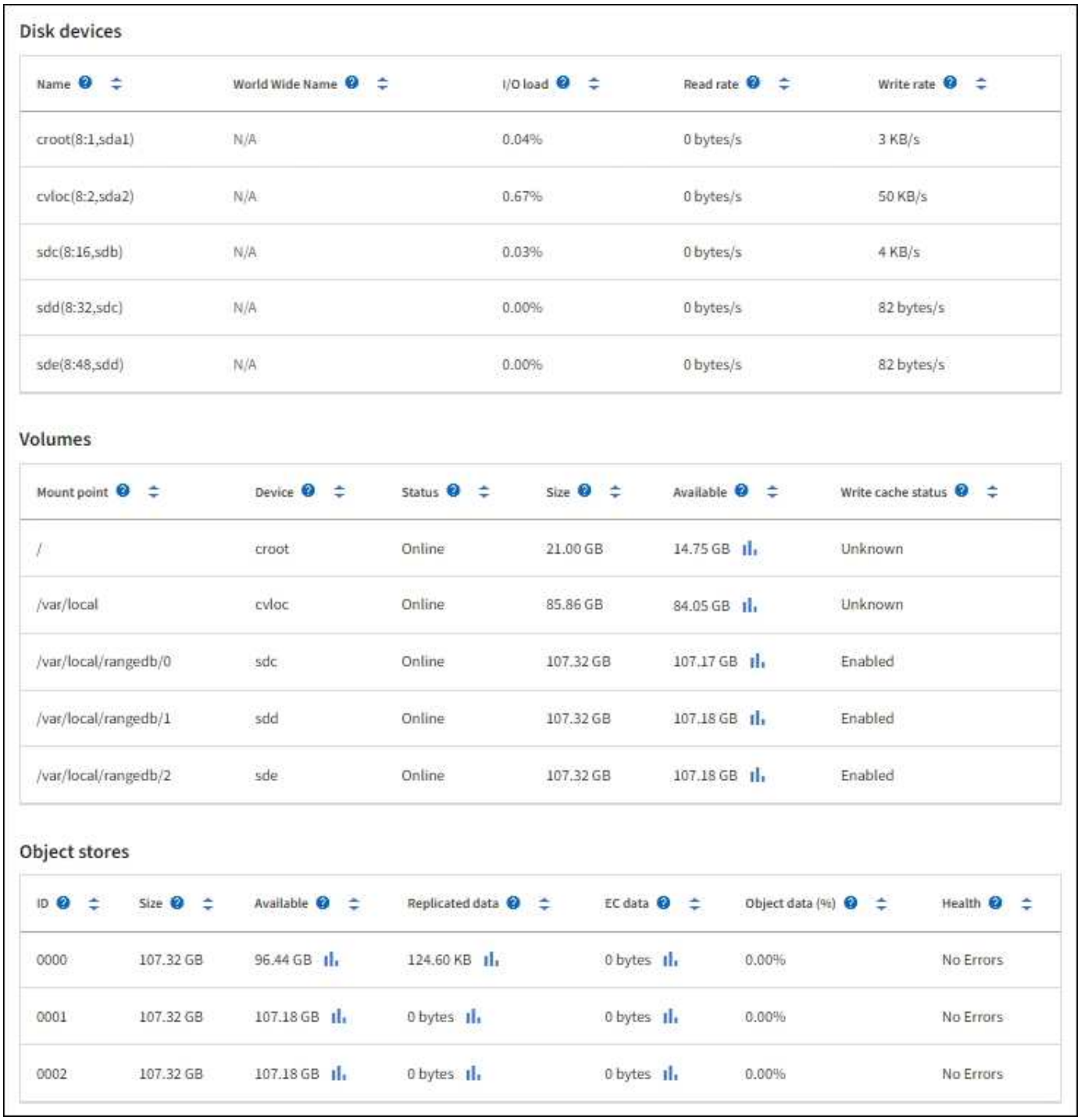


Tabelle dispositivi disco, volumi e archivi di oggetti

Per tutti i nodi, la scheda Archiviazione contiene i dettagli relativi ai dispositivi disco e ai volumi presenti sul nodo. Per i nodi di archiviazione, la tabella Archivi oggetti fornisce informazioni su ciascun volume di archiviazione.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

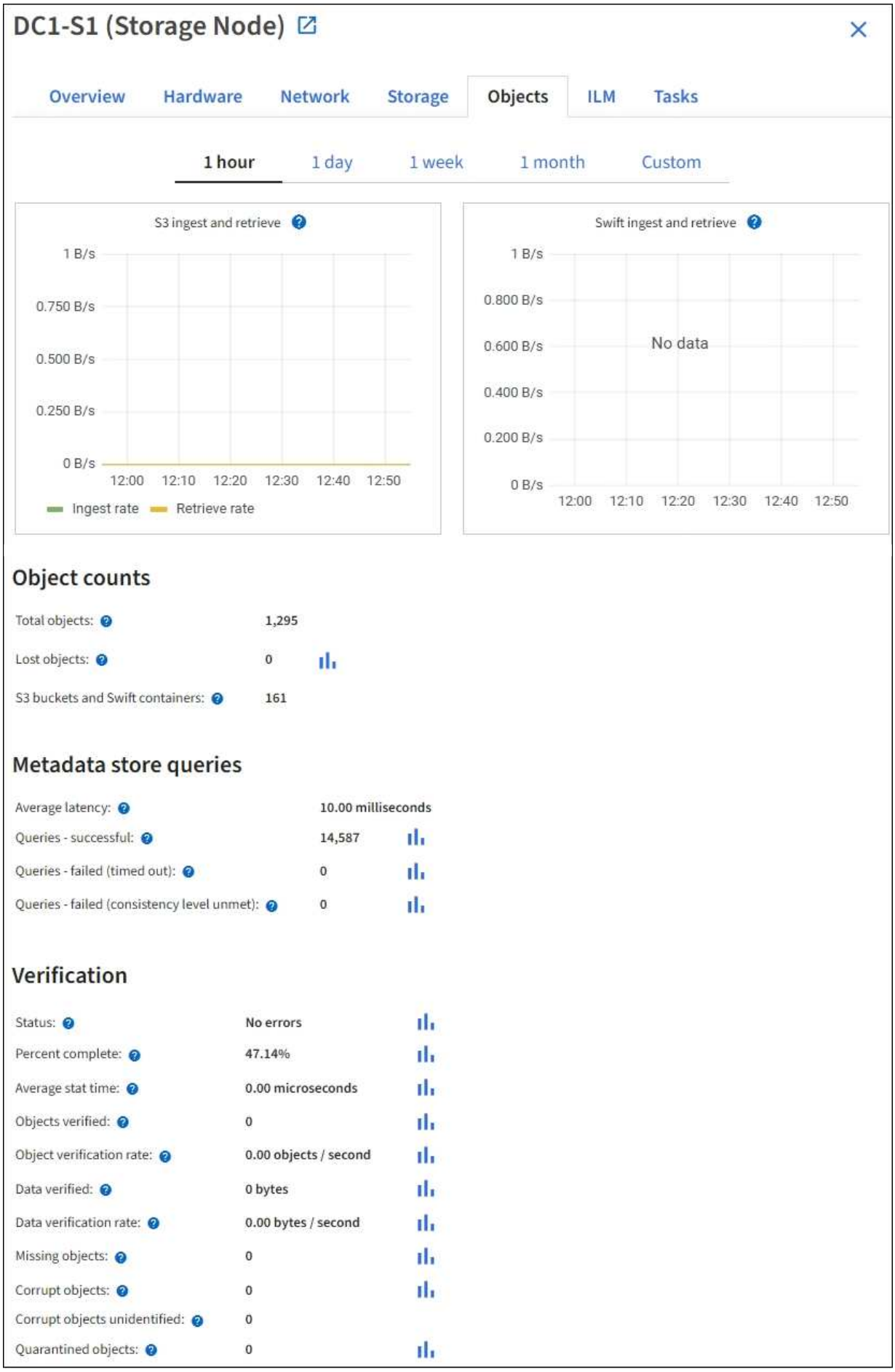
Informazioni correlate

"Monitora la capacità di archiviazione"

Visualizza la scheda Oggetti di StorageGRID

La scheda Oggetti fornisce informazioni su "Velocità di acquisizione e recupero S3".

La scheda Oggetti viene visualizzata per ogni Storage Node, per ogni sito e per l'intera griglia. Per i Storage Node, la scheda Oggetti fornisce anche il conteggio degli oggetti e informazioni sulle query dei metadati e sulla verifica in background.

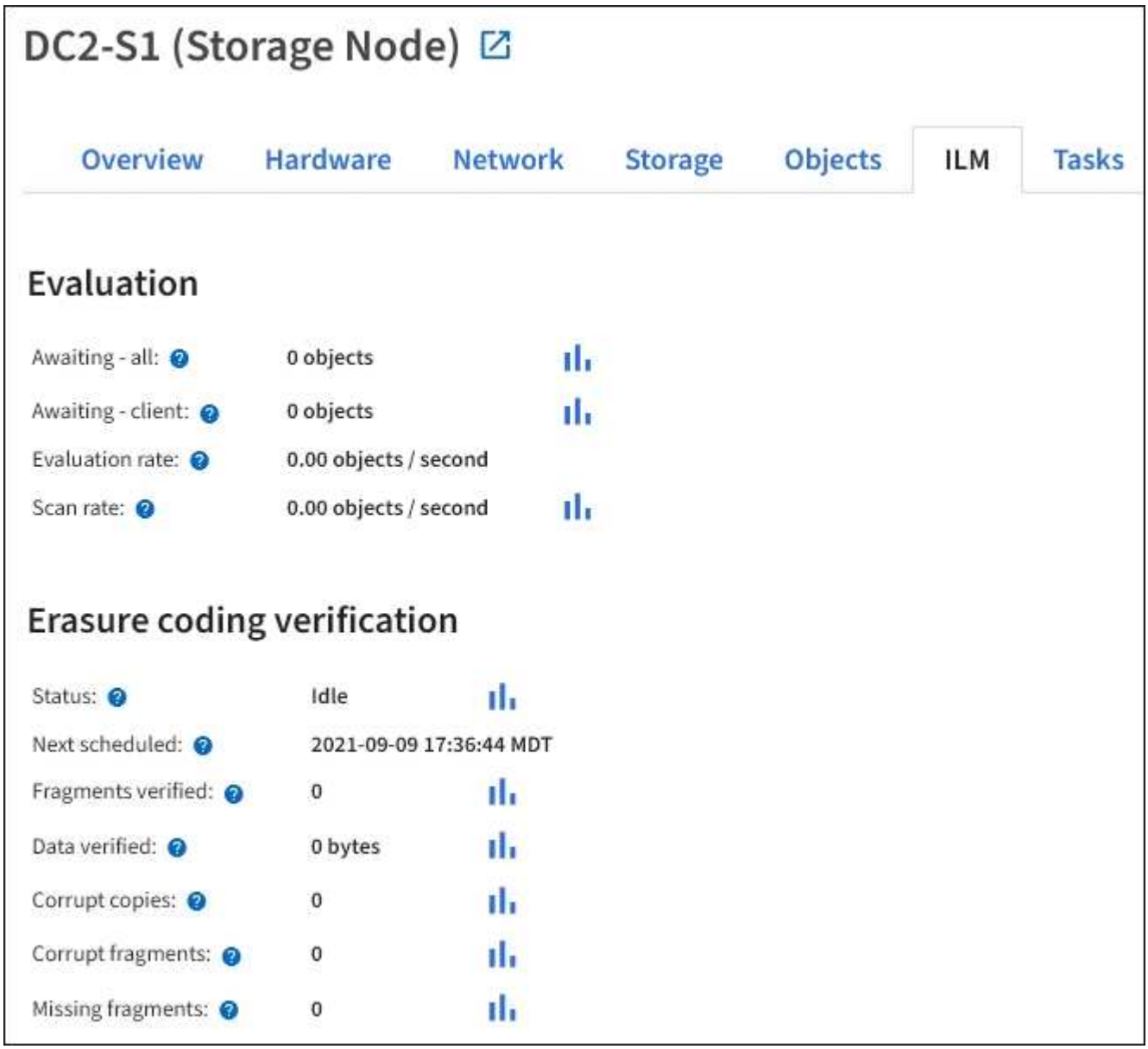

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

Visualizza la scheda StorageGRID ILM

La scheda ILM fornisce informazioni sulle operazioni di information lifecycle management (ILM).

La scheda ILM viene visualizzata per ogni Storage Node, ogni sito e l'intera grid. Per ogni sito e per la grid, la scheda ILM mostra un grafico della coda ILM nel tempo. Per la grid, questa scheda fornisce anche il tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

Per i nodi di archiviazione, la scheda ILM fornisce dettagli sulla valutazione ILM e sulla verifica in background per gli oggetti con codifica di cancellazione.



Informazioni correlate

- "Monitora il ciclo di vita delle informazioni"
- "${post_edited_translations.segment}"

Visualizza la scheda del bilanciatore del carico StorageGRID

La scheda Bilanciamento del carico include grafici di prestazioni e diagnostica relativi al funzionamento del servizio Load Balancer.

La scheda Bilanciamento del carico viene visualizzata per i nodi Admin e i nodi Gateway, per ogni sito e per l'intera grid. Per ogni sito, la scheda Bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i nodi di quel sito. Per l'intera grid, la scheda Bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i siti.

Se non viene eseguita alcuna operazione di I/O tramite il servizio Load Balancer, oppure se non è configurato alcun load balancer, i grafici visualizzano "Nessun dato".

Traffico di richiesta

Questo grafico fornisce una media mobile di 3 minuti del throughput dei dati trasmessi tra gli endpoint del bilanciatore di carico e i client che effettuano le richieste, in bit al secondo.

Questo valore viene aggiornato al termine di ogni richiesta. Di conseguenza, questo valore potrebbe differire dal throughput in real-time in caso di basse frequenze di richiesta o per richieste di lunga durata. Puoi consultare la scheda Network per ottenere una visione più realistica del comportamento attuale della rete.

Tasso di richieste in entrata

Questo grafico fornisce una media mobile di 3 minuti del numero di nuove richieste al secondo, suddivise per tipo di richiesta (GET, PUT, HEAD e DELETE). Questo valore viene aggiornato quando le intestazioni di una nuova richiesta sono state validate.

Durata media della richiesta (senza errori)

Questo grafico fornisce una media mobile di 3 minuti della durata delle richieste, suddivisa per tipo di richiesta (GET, PUT, HEAD e DELETE). La durata di ciascuna richiesta inizia quando l'intestazione della richiesta viene analizzata dal servizio Load Balancer e termina quando il corpo completo della risposta viene restituito al client.

Tasso di risposta agli errori

Questo grafico fornisce una media mobile di 3 minuti del numero di risposte di errore restituite ai client al secondo, suddiviso per codice di risposta di errore.

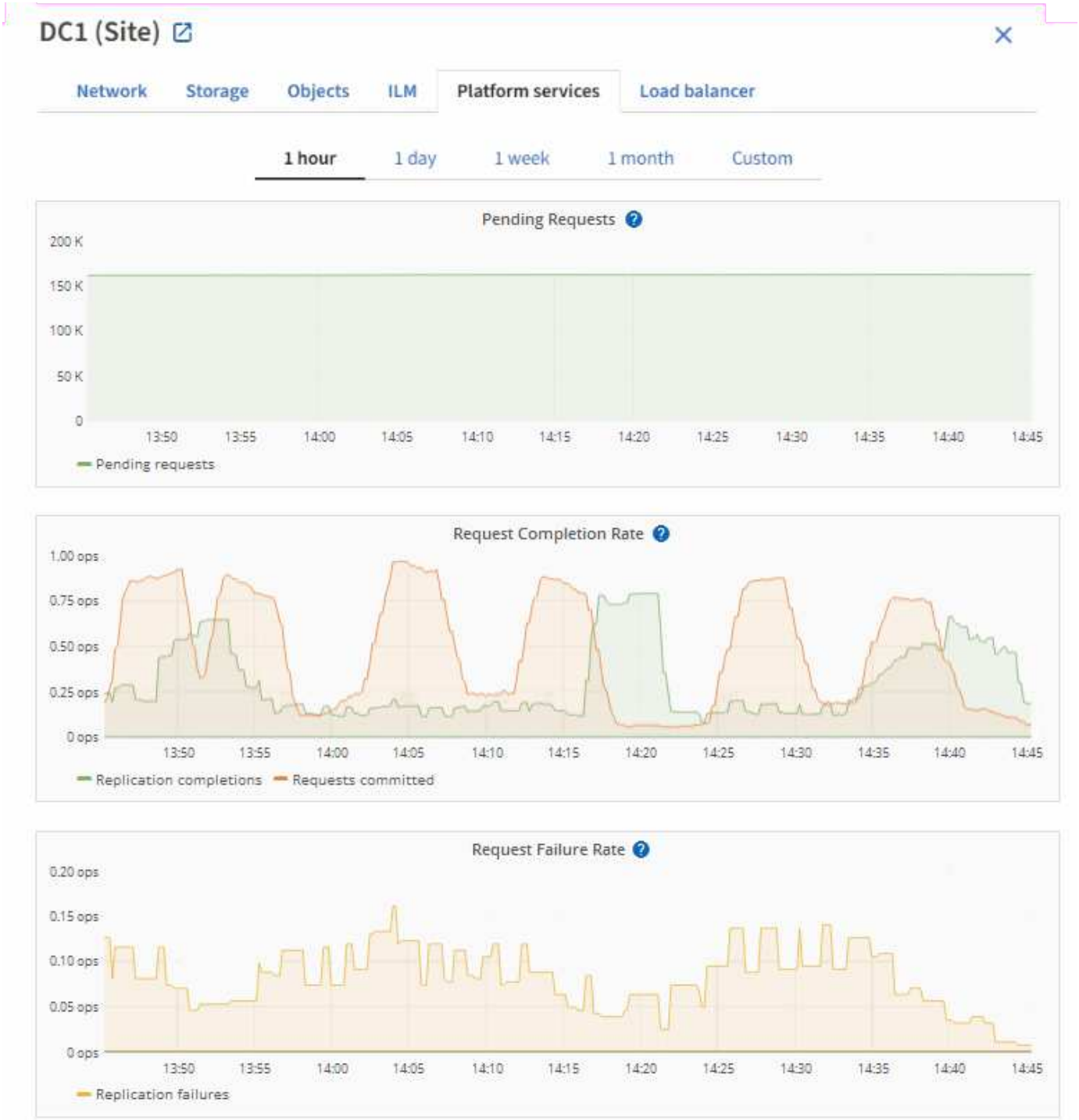
Informazioni correlate

- "Monitora le operazioni di bilanciamento del carico"
- "${post_edited_translations.segment}"

Visualizza la scheda Servizi della piattaforma StorageGRID

La scheda Servizi della piattaforma fornisce informazioni su qualsiasi operazione dei servizi della piattaforma S3 in un sito.

La scheda Servizi della piattaforma viene visualizzata per ogni sito. Questa scheda fornisce informazioni sui servizi della piattaforma S3, come la replica CloudMirror e il servizio di integrazione della ricerca. I grafici in questa scheda mostrano metriche come il numero di richieste in sospeso, il tasso di completamento delle richieste e il tasso di errori delle richieste.



Per ulteriori informazioni sui servizi della piattaforma S3, inclusi i dettagli sulla risoluzione dei problemi, consulta la "Istruzioni per l'amministrazione di StorageGRID".

Visualizza la scheda Gestisci unità di StorageGRID

La scheda Gestisci unità consente di accedere ai dettagli ed eseguire attività di risoluzione dei problemi e manutenzione sulle unità negli apparati che supportano questa funzionalità.

Tramite la scheda Gestisci unità, puoi eseguire le seguenti operazioni:

- Visualizza la disposizione delle unità di archiviazione dati nell'appliance
- Visualizza una tabella che elenca la posizione di ciascuna unità, il tipo, lo stato, la versione del firmware e il numero di serie
- Esegui le funzioni di risoluzione dei problemi e di manutenzione su ciascun drive

Per accedere alla scheda Gestisci unità, devi avere il "Autorizzazione di amministratore dell'appliance di storage o permesso di accesso root".

Per informazioni sull'utilizzo della scheda Gestisci unità, vedi "Usa la scheda Gestisci unità".

Visualizza la scheda SANtricity System Manager di StorageGRID

La scheda SANtricity System Manager ti permette di accedere a SANtricity System Manager senza dover configurare o collegare la porta di gestione dell'appliance di storage. Puoi usare questa scheda per visualizzare informazioni diagnostiche e ambientali sull'hardware, oltre a problemi relativi ai drive.

> L'accesso a SANtricity System Manager dal Grid Manager è generalmente pensato solo per monitorare l'hardware dell'appliance e configurare E-Series AutoSupport. Molte funzionalità e operazioni all'interno di SANtricity System Manager, come l'aggiornamento del firmware, non si applicano al monitoraggio della tua appliance StorageGRID. Per evitare problemi, segui sempre le istruzioni di manutenzione hardware per la tua appliance. Per aggiornare il firmware SANtricity, consulta la "Procedure di configurazione della manutenzione" per la tua appliance di storage.

> La scheda SANtricity System Manager viene visualizzata solo per i nodi degli appliance di storage che utilizzano hardware E-Series.

Utilizzando SANtricity System Manager, puoi fare quanto segue:

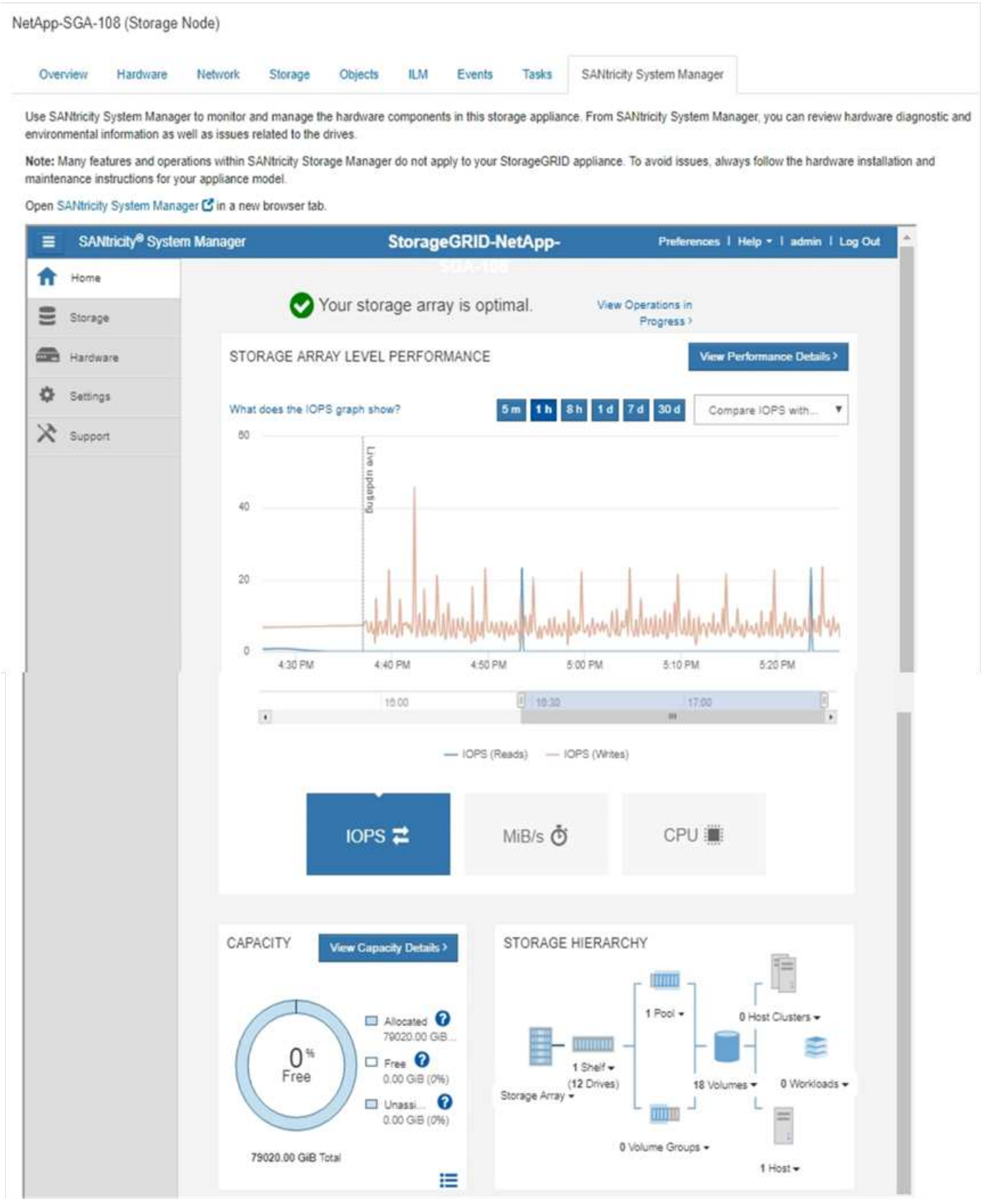
- Visualizza dati sulle prestazioni come le prestazioni a livello di array di storage, la latenza I/O, l'utilizzo della CPU dello storage controller e il throughput.
- Controlla lo stato dei componenti hardware.
- Esegui funzioni di supporto, tra cui la visualizzazione dei dati diagnostici e la configurazione di E-Series AutoSupport.

> Per utilizzare SANtricity System Manager per configurare un proxy per E-Series AutoSupport, vedi "Invia i pacchetti E-Series AutoSupport tramite StorageGRID".

Per accedere a SANtricity System Manager tramite Grid Manager, devi avere il "Autorizzazione di amministratore dell'appliance di storage o permesso di accesso root".

> Devi avere il firmware SANtricity 8.70 o superiore per accedere a SANtricity System Manager tramite Grid Manager.

La scheda visualizza la pagina iniziale di SANtricity System Manager.



Puoi usare il link SANtricity System Manager per aprire SANtricity System Manager in una nuova finestra del browser per una visualizzazione più semplice.

Per vedere i dettagli sulle prestazioni e sull'utilizzo della capacità a livello di array di storage, posiziona il

cursore su ciascun grafico.

Per ulteriori dettagli sulla visualizzazione delle informazioni accessibili dalla scheda SANtricity System Manager, vedi "NetApp E-Series e documentazione SANtricity".

Informazioni da monitorare regolarmente

Cosa e quando monitorare in StorageGRID

Anche se il sistema StorageGRID può continuare a funzionare in caso di errori o di indisponibilità di parti della grid, dovresti monitorare e risolvere i potenziali problemi prima che compromettano l'efficienza o la disponibilità della grid.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni sulle attività di monitoraggio

Un sistema complesso genera grandi quantità di informazioni. L'elenco seguente fornisce indicazioni sulle informazioni più importanti da monitorare costantemente.

Cosa monitorare	Frequenza
"stato di salute del sistema"	Quotidiano
Velocità con cui "Capacità degli oggetti e dei metadati del nodo di archiviazione" viene consumato	Settimanale
"Operazioni di gestione del ciclo di vita delle informazioni"	Settimanale
"Risorse di rete e di sistema"	Settimanale
"Attività tenant"	Settimanale
"operazioni client S3"	Settimanale
"Operazioni di bilanciamento del carico"	Dopo la configurazione iniziale e dopo qualsiasi modifica alla configurazione
"Connessioni di federazione di grid"	Settimanale

Monitorare lo stato di salute del sistema in StorageGRID

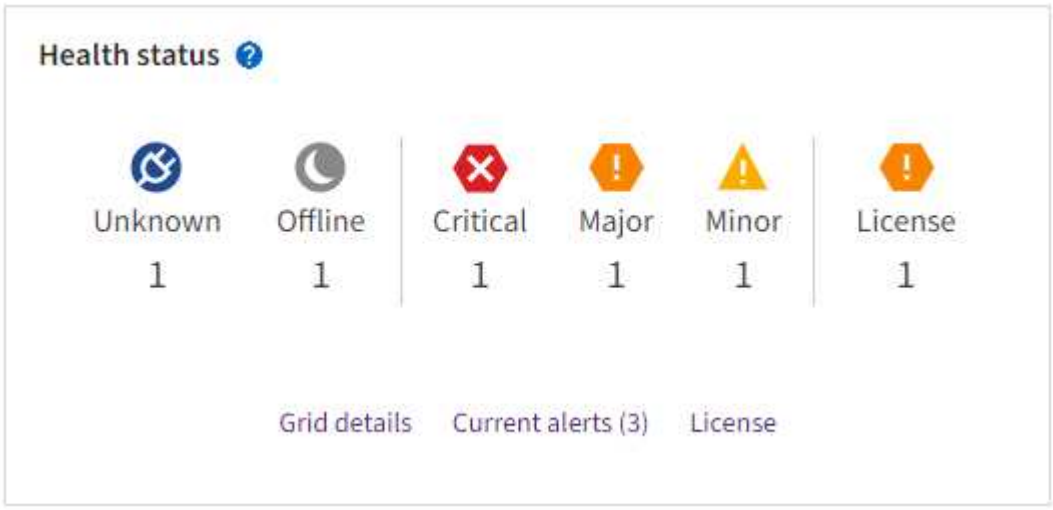
Monitora quotidianamente lo stato di salute generale del tuo sistema StorageGRID.

Informazioni su questa attività

Il sistema StorageGRID può continuare a funzionare quando alcune parti della grid non sono disponibili. I potenziali problemi indicati dagli avvisi non sono necessariamente problemi nelle operazioni del sistema.

Indaga sui problemi riassunti nella scheda Stato di salute della Dashboard di Grid Manager.

Per ricevere notifiche sugli avvisi non appena vengono attivati, puoi "Imposta le notifiche e-mail per gli avvisi" o "configurare le trap SNMP".



Quando ci sono problemi, compaiono dei link che ti permettono di vedere altri dettagli:

Collegamento	Appare quando…
Dettagli della griglia	Tutti i nodi sono disconnessi (stato della connessione Sconosciuto o Amministrativamente Down).
Allerte attuali (Critica, Maggiore, Minore)	Gli avvisi sono attualmente attivo.
Avvisi risolti di recente	Avvisi attivati nell'ultima settimana sono ora risolti.
Licenza	Si è verificato un problema con la licenza software per questo sistema StorageGRID. Puoi "aggiorna le informazioni sulla licenza secondo necessità".

Monitora lo stato di connessione dei nodi

Se uno o più nodi vengono disconnessi dalla grid, le operazioni critiche di StorageGRID potrebbero essere influenzate. Monitora lo stato di connessione dei nodi e risolvi subito eventuali problemi.

Icona	Descrizione	Azione richiesta
	Non connesso - Sconosciuto Per ragioni sconosciute, un nodo risulta disconnesso o i servizi sul nodo risultano inaspettatamente non disponibili. Ad esempio, un servizio sul nodo potrebbe essere stato interrotto oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un guasto imprevisto. Potrebbe anche essere attivato l'avviso **Impossibile comunicare con il nodo**. Potrebbero inoltre essere attivi altri avvisi.	Richiede attenzione immediata. Seleziona ogni avviso e segui le azioni consigliate. Ad esempio, potresti dover riavviare un servizio che si è arrestato o riavviare l'host per il nodo. **Nota**: Un nodo potrebbe apparire come Sconosciuto durante le operazioni di arresto gestito. Puoi ignorare lo stato Sconosciuto in questi casi.
	Non connesso - Amministrativamente inattivo Per un motivo prevedibile, il nodo non è connesso al grid. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando oppure il software viene aggiornato. Potrebbero anche essere attivi uno o più avvisi. In base al problema di fondo, questi nodi spesso tornano online senza intervento.	Verifica se ci sono avvisi che interessano questo nodo. Se uno o più avvisi sono attivi, seleziona ogni avviso e segui le azioni consigliate.
	Collegato Il nodo è connesso alla grid.	Non è richiesta alcuna azione.

Visualizza gli avvisi correnti e risolti

Avvisi correnti: Quando viene attivato un avviso, un'icona di avviso viene visualizzata nella dashboard. Un'icona di avviso viene visualizzata anche per il nodo nella pagina Nodi. Se "Le notifiche e-mail di avviso sono configurate", verrà inviata anche una notifica via e-mail, a meno che l'avviso non sia stato silenziato.

Avvisi risolti: Puoi cercare e visualizzare la cronologia degli avvisi risolti.

Facoltativamente, hai guardato il video:

Panoramica degli avvisi

La tabella seguente descrive le informazioni visualizzate in Grid Manager per gli avvisi correnti e risolti.

Intestazione di colonna	Descrizione
Nome o titolo	Il nome dell'allerta e la sua descrizione.
Gravità	La gravità dell'allerta. Per le allerte correnti, se più allerte sono raggruppate, la riga del titolo mostra quante istanze di quell'allerta si verificano per ogni livello di gravità. **Critico**: Si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. Devi risolvere immediatamente il problema alla radice. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati. **Grave**: Si è verificata una condizione anomala che sta influenzando le operazioni in corso o si sta avvicinando alla soglia per un avviso critico. Dovresti esaminare gli avvisi gravi e risolvere eventuali problemi sottostanti per assicurarti che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID. **Minore**: Il sistema funziona normalmente, ma è presente una condizione anomala che, se persiste, potrebbe compromettere la capacità del sistema di funzionare. Dovresti monitorare e risolvere gli avvisi minori che non si risolvono da soli per assicurarti che non causino un problema più serio.
Attivato a tempo	**Avvisi correnti**: La data e l'ora in cui l'avviso è stato attivato nel tuo fuso orario locale e in UTC. Se sono raggruppati più avvisi, la riga del titolo mostra gli orari per l'istanza più recente dell'avviso (*newest*) e per l'istanza più vecchia dell'avviso (*oldest*). **Avvisi risolti**: Da quanto tempo è stato attivato l'avviso.
Sito/Nodo	Il nome del sito e del nodo in cui si sta verificando o si è verificato l'avviso.
Stato	Indica se l'avviso è attivo, silenziato o risolto. Se sono raggruppati più avvisi e si seleziona **Tutti gli avvisi** nel menu a tendina, la riga del titolo mostra quante istanze di quell'avviso sono attive e quante sono state silenziate.
Tempo di risoluzione (solo avvisi risolti)	Quanto tempo fa hai risolto l'avviso.
Valori correnti o *valori dei dati*	Il valore della metrica che ha attivato l'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi per aiutarti a capire e a indagare sull'avviso. Ad esempio, i valori visualizzati per un avviso di **Low object data storage** includono la % di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzato. **Nota:** Se più avvisi correnti sono raggruppati, i valori correnti non vengono visualizzati nella riga del titolo.

Intestazione di colonna	Descrizione
Valori attivati (solo avvisi risolti)	Il valore della metrica che ha attivato l'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi per aiutarti a capire e a indagare sull'avviso. Ad esempio, i valori visualizzati per un avviso di **Low object data storage** includono la % di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzato.

Passaggi

1. Seleziona il collegamento **Avvisi correnti** o **Avvisi risolti** per visualizzare un elenco di avvisi in quelle categorie. Puoi anche visualizzare i dettagli di un avviso selezionando **Nodi** > ***nodo*** > **Panoramica** e poi selezionando l'avviso dalla tabella Avvisi.

   Per impostazione predefinita, gli avvisi correnti vengono visualizzati come segue:

   - Gli avvisi attivati più di recente sono mostrati per primi.
   - Più avvisi dello stesso tipo vengono mostrati come un gruppo.
   - Gli avvisi che hai silenziato non vengono visualizzati.
   - Per un avviso specifico su un nodo specifico, se vengono raggiunte le soglie per più di un livello di gravità, viene visualizzato solo l'avviso più grave. Cioè, se vengono raggiunte le soglie di allerta per i livelli di gravità minore, maggiore e critico, viene visualizzato solo l'avviso critico.

     La pagina degli avvisi correnti si aggiorna ogni due minuti.

2. Per espandere i gruppi di avvisi, seleziona la freccia in basso . Per comprimere i singoli avvisi di un gruppo, seleziona la freccia in alto o il nome del gruppo.
3. Per visualizzare avvisi singoli invece di gruppi di avvisi, deseleziona la casella di controllo **Raggruppa avvisi**.
4. Per ordinare gli avvisi correnti o i gruppi di avvisi, seleziona le frecce su/giù nell'intestazione di ciascuna colonna.
   - Quando selezioni **Avvisi di gruppo**, sia i gruppi di avvisi che i singoli avvisi all'interno di ciascun gruppo vengono ordinati. Ad esempio, potresti voler ordinare gli avvisi di un gruppo in base a **Ora di attivazione** per trovare l'istanza più recente di un avviso specifico.
   - Quando cancelli **Group alerts**, l'intero elenco di avvisi viene ordinato. Ad esempio, potresti voler ordinare tutti gli avvisi per **Node/Site** per vedere tutti gli avvisi che riguardano un nodo specifico.
5. Per filtrare gli avvisi correnti in base allo stato (**Tutti gli avvisi**, **Attivi** o **Silenziati**), usa il menu a discesa nella parte superiore della tabella.

   Vedi "Silenzia le notifiche di avviso".

6. Per ordinare gli avvisi risolti:
   - Seleziona un periodo di tempo dal menu a tendina **Quando viene attivato**.
   - Seleziona uno o più livelli di gravità dal menu a tendina **Gravità**.
   - Seleziona una o più regole di avviso predefinite o personalizzate dal menu a discesa **Regola di avviso** per filtrare gli avvisi risolti relativi a una specifica regola di avviso.
   - Seleziona uno o più nodi dal menu a tendina **Nodo** per filtrare gli avvisi risolti relativi a uno specifico nodo.

7. Per visualizzare i dettagli di un avviso specifico, seleziona l'avviso. Si apre una finestra di dialogo che fornisce dettagli e azioni consigliate per l'avviso che hai selezionato.
8. (Facoltativo) Per un avviso specifico, seleziona "Silenzia questo avviso" per silenziare la regola di avviso che ha causato l'attivazione di questo avviso.

   Devi avere la "Gestisci gli avvisi o i permessi di accesso root" per silenziare una regola di avviso.

   > Fai attenzione quando decidi di disattivare una regola di avviso. Se una regola di avviso è disattivata, potresti non rilevare un problema sottostante finché non impedisce il completamento di un'operazione critica.

9. Per visualizzare le condizioni attuali per la regola di avviso:
   a. Dai dettagli dell'avviso, seleziona **Visualizza condizioni**.

      Appare una finestra a comparsa che elenca l'espressione Prometheus per ogni livello di gravità definito.

   b. Per chiudere la finestra a comparsa, fai clic in un punto qualsiasi al di fuori della finestra.
10. Facoltativamente, seleziona **Modifica regola** per modificare la regola di avviso che ha causato l'attivazione di questo avviso.

    Devi avere i permessi "Gestisci gli avvisi o i permessi di accesso root" per modificare una regola di avviso.

    > Fai attenzione quando decidi di modificare una regola di avviso. Se cambi i valori di attivazione, potresti non rilevare un problema sottostante finché non impedisce il completamento di un'operazione critica.

11. Per chiudere i dettagli dell'avviso, seleziona **Chiudi**.

Monitora la capacità di archiviazione in StorageGRID

Monitora lo spazio totale utilizzabile disponibile per assicurarti che il sistema StorageGRID non esaurisca spazio di storage per gli oggetti o per i metadati.

StorageGRID memorizza i dati degli oggetti e i metadati degli oggetti separatamente, e riserva una quantità specifica di spazio per un database Cassandra distribuito che contiene i metadati degli oggetti. Monitora la quantità totale di spazio utilizzato per gli oggetti e per i metadati degli oggetti, così come le tendenze nella quantità di spazio utilizzato per ciascuno. Questo ti permetterà di pianificare in anticipo l'aggiunta di nodi ed evitare interruzioni del servizio.

Puoi "visualizza le informazioni sulla capacità di storage" per l'intera grid, per ogni sito e per ogni Storage Node nel tuo sistema StorageGRID.

Monitora la capacità di storage dell'intera grid

Monitora la capacità di storage complessiva della tua grid per assicurarti che rimanga spazio libero sufficiente per i dati degli oggetti e i metadati degli oggetti. Capire come cambia la capacità di storage nel tempo può aiutarti a pianificare l'aggiunta di Storage Node o volumi di storage prima che la capacità di storage utilizzabile della grid venga consumata.

La dashboard di Grid Manager ti permette di valutare rapidamente quanto spazio di storage è disponibile per l'intera grid e per ciascun data center. La pagina Nodes fornisce valori più dettagliati per i dati degli oggetti e i

metadati degli oggetti.

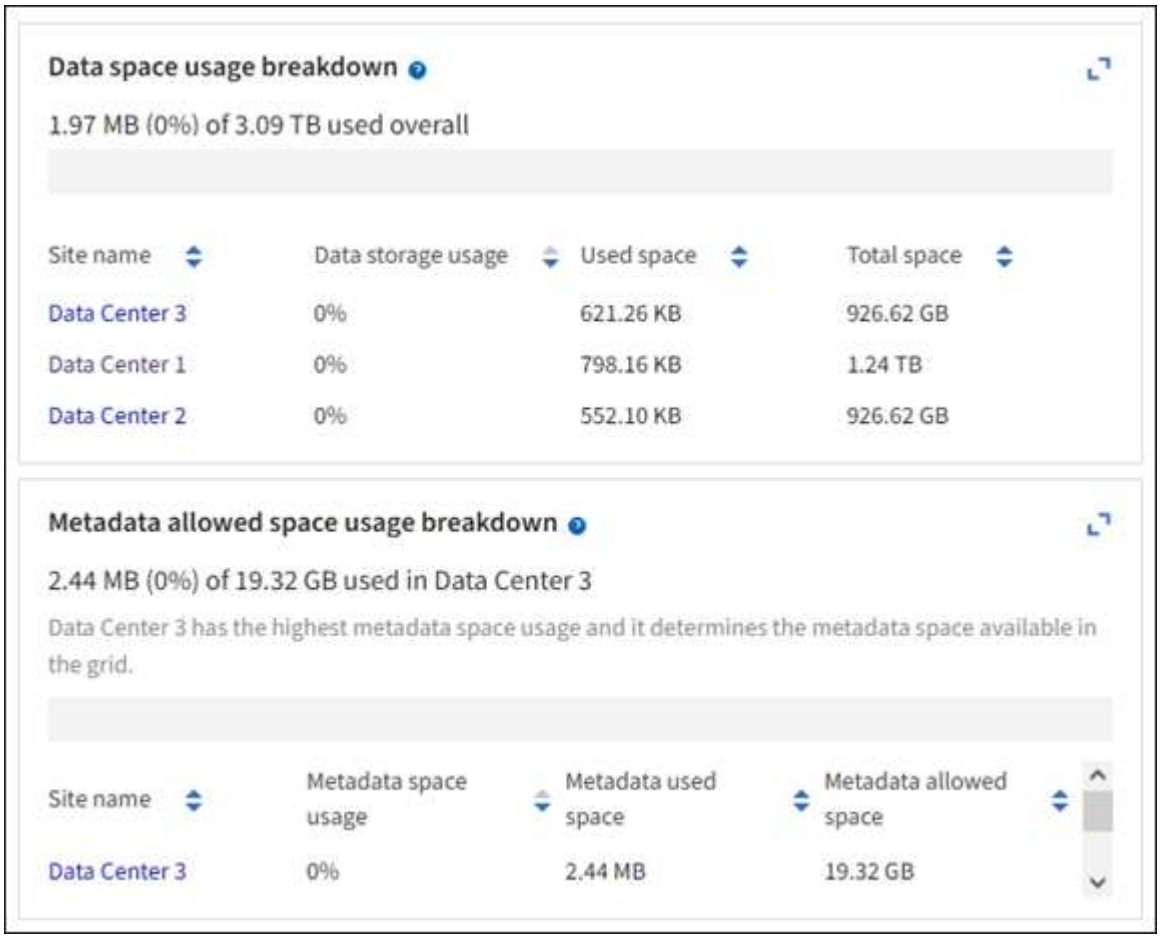
Passaggi

1. Valuta quanto spazio di storage è disponibile per l'intera grid e per ciascun data center.

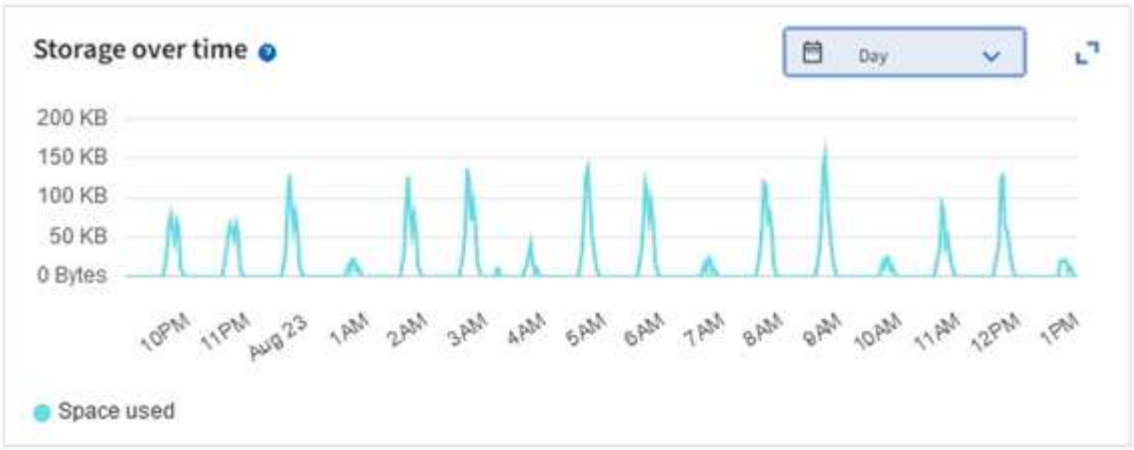
   a. Seleziona **Dashboard > Overview**.

   b. Nota i valori riportati nelle schede "Ripartizione dell'utilizzo dello spazio dati" e "Ripartizione dell'utilizzo dello spazio consentito per i metadati". Ogni scheda indica la % di utilizzo dello spazio di storage, la capacità dello spazio utilizzato e lo spazio totale disponibile o consentito per sito.

   > Il riepilogo non include i supporti di archiviazione.



   a. Nota il grafico nella scheda Storage over time. Usa il menu a discesa del periodo di tempo per capire quanto velocemente viene consumato lo storage.



2. Consulta la pagina Nodi per ulteriori dettagli su quanto spazio di storage è stato utilizzato e quanto spazio di storage rimane disponibile nella griglia per i dati a oggetti e i metadati degli oggetti.
   a. Selezionare **Nodi**.
   b. Seleziona ***grid*** > **Storage**.

   c. Posiziona il cursore sui grafici **Storage used - object data** e **Storage used - object metadata** per vedere quanta storage a oggetti e quanta storage a oggetti per i metadati è disponibile per l'intera griglia e quanto ne è stato utilizzato nel tempo.

> I valori totali per un sito o per la griglia non includono i nodi che non hanno segnalato metriche per almeno cinque minuti, come i nodi offline.

3. Pianifica di eseguire un'espansione per aggiungere Storage Node o volumi di storage prima che la capacità di storage utilizzabile del grid venga consumata.

   Quando pianifichi il momento di un'espansione, considera quanto tempo ci vorrà per procurare e installare storage aggiuntivo.

Se la policy ILM utilizza la codifica di cancellazione, potresti preferire espandere quando i nodi di storage esistenti sono pieni circa al 70%, per ridurre il numero di nodi da aggiungere.

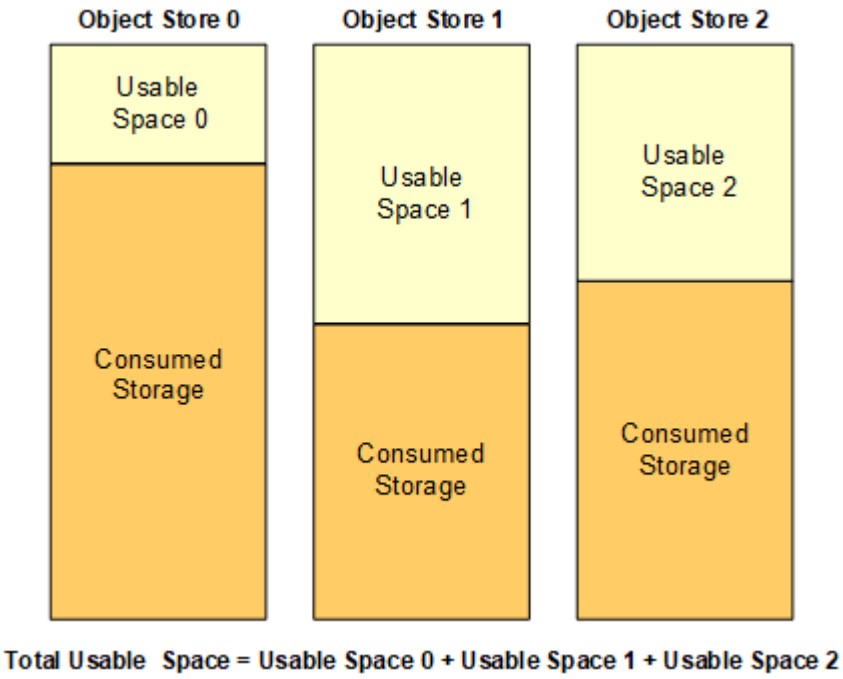
Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, consulta la "istruzioni per l'espansione di StorageGRID".

Monitora la capacità di storage per ciascun Storage Node

Monitora lo spazio totale utilizzabile per ciascun nodo di storage per assicurarti che il nodo abbia abbastanza spazio per i nuovi dati degli oggetti.

Informazioni su questa attività

Lo spazio utilizzabile è la quantità di spazio di storage disponibile per memorizzare gli oggetti. Lo spazio utilizzabile totale per un Storage Node è calcolato sommando lo spazio disponibile su tutti gli object store all'interno del nodo.



Passaggi

1. Seleziona **Nodes** > ***Storage Node*** > **Storage**.

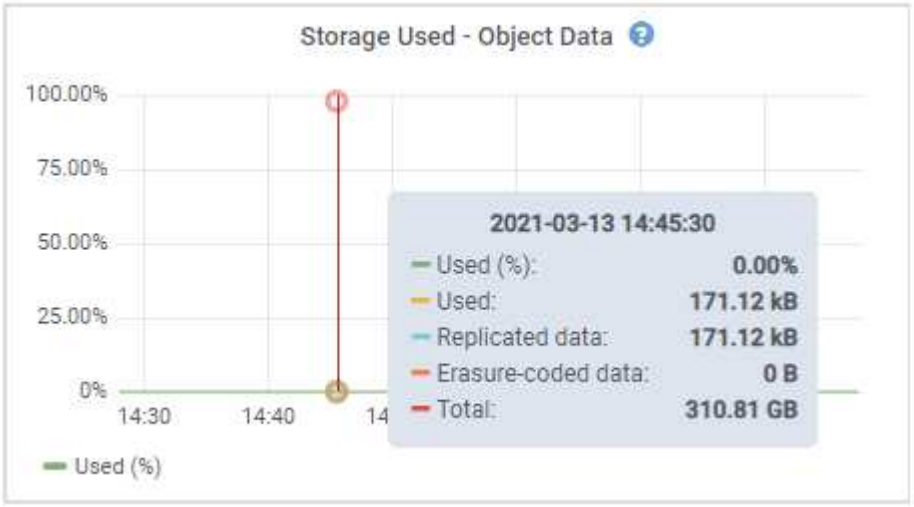
   Vengono visualizzati i grafici e le tabelle relativi al nodo.

2. Posiziona il cursore sul grafico "Storage used - object data".

   Vengono visualizzati i seguenti valori:

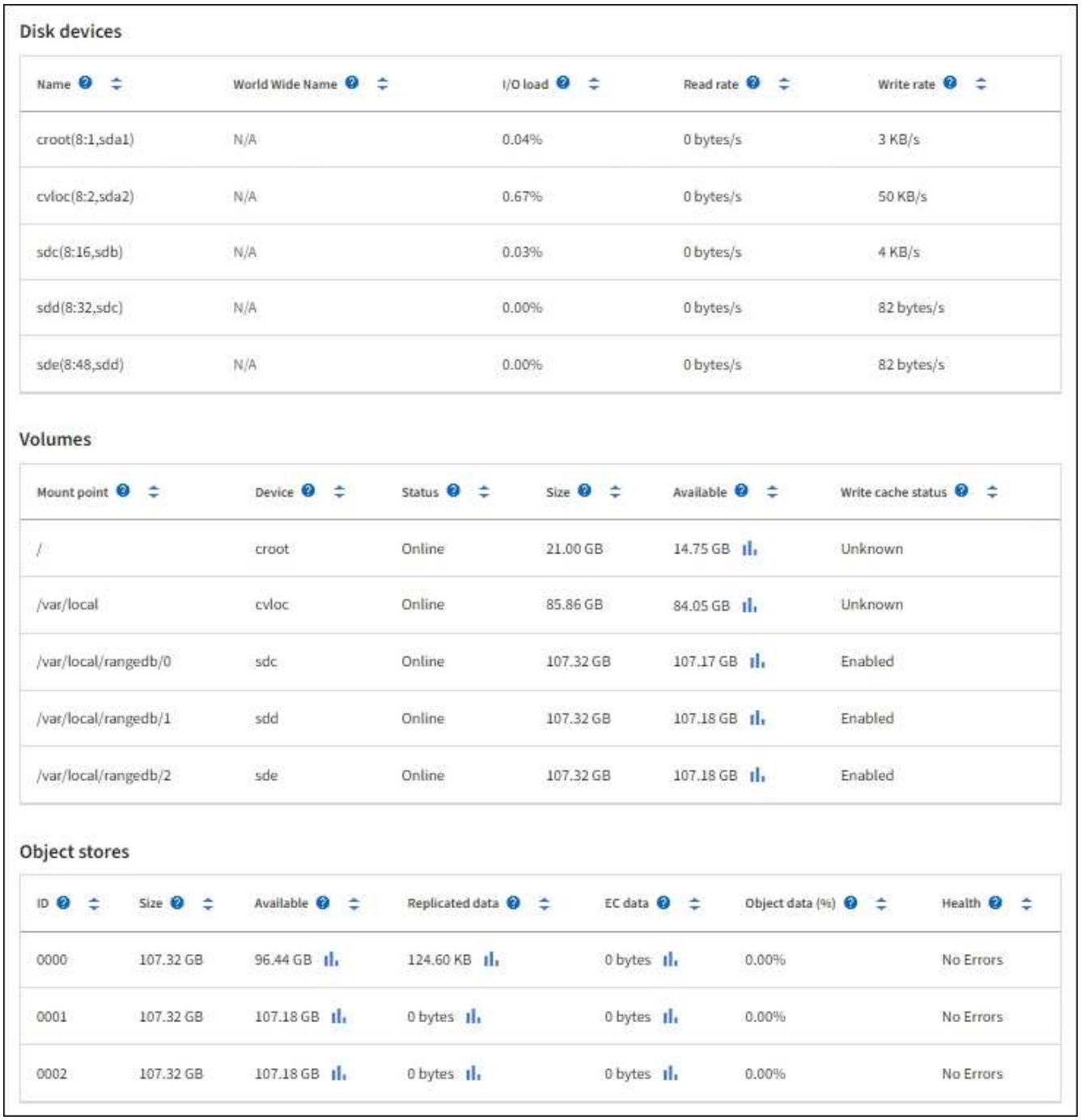
   - **Utilizzato (%)**: La percentuale dello spazio totale utilizzabile che hai usato per i dati degli oggetti.
   - **Utilizzato**: La quantità di spazio totale utilizzabile che hai usato per i dati degli oggetti.
   - **Dati replicati**: una stima della quantità di dati oggetto replicati su questo nodo, sito o grid.
   - **Dati codificati per la cancellazione**: una stima della quantità di dati oggetto codificati per la cancellazione su questo nodo, sito o grid.

- **Totale**: La quantità totale di spazio utilizzabile su questo nodo, sito o grid. Il valore utilizzato è la `storagegrid_storage_utilization_data_bytes` metrica.



3. Controlla i valori disponibili nelle tabelle Volumi e Archivi di oggetti, sotto i grafici.

> Per visualizzare i grafici di questi valori, clicca sulle icone dei grafici nelle colonne Disponibili.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. Monitora i valori nel tempo per stimare la velocità con cui lo spazio di storage utilizzabile viene consumato.
5. Per mantenere il normale funzionamento del sistema, aggiungi Storage Node, aggiungi volumi di storage o archivia i dati degli oggetti prima che lo spazio utilizzabile venga consumato.

   Quando pianifichi il momento di un'espansione, considera quanto tempo ci vorrà per procurare e installare storage aggiuntivo.

   > Se la policy ILM utilizza la codifica di cancellazione, potresti preferire espandere quando i nodi di storage esistenti sono pieni circa al 70%, per ridurre il numero di nodi da aggiungere.

   Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, consulta la "istruzioni per l'espansione di StorageGRID".

L'"Storage dati oggetto basso"avviso viene attivato quando lo spazio disponibile per memorizzare i dati degli oggetti su un nodo di Storage è insufficiente.

Monitora la capacità dei metadati degli oggetti per ciascun Storage Node

Monitora l'utilizzo dei metadati per ogni Storage Node per assicurarti che rimanga spazio sufficiente per le operazioni essenziali del database. Devi aggiungere nuovi Storage Node in ogni sito prima che i metadati degli oggetti superino il 100% dello spazio metadati consentito.

Informazioni su questa attività

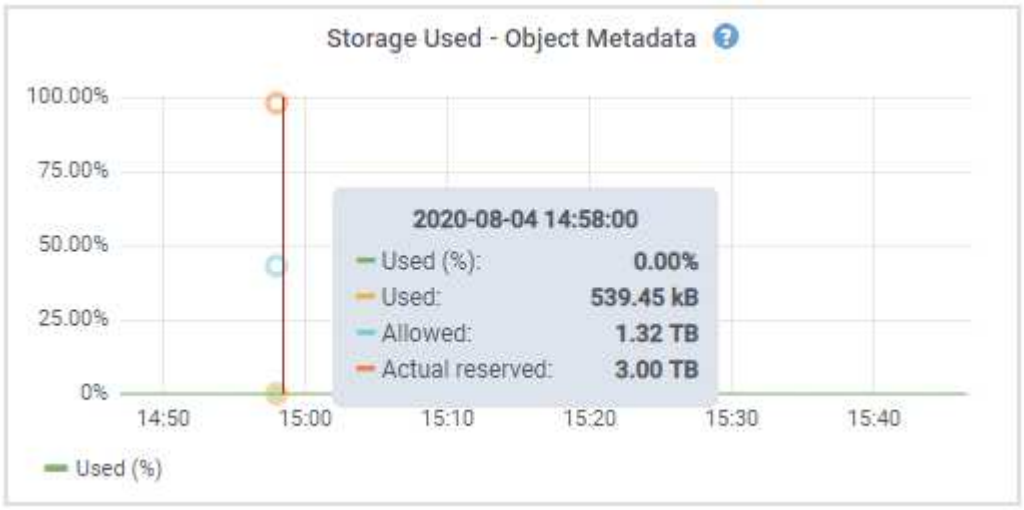
StorageGRID mantiene tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie sono distribuite uniformemente su tutti i nodi di storage di ciascun sito, utilizzando lo spazio riservato ai metadati sul volume di storage 0 di ciascun nodo di storage.

In alcuni casi, la capacità di metadati degli oggetti della griglia potrebbe essere consumata più rapidamente della sua capacità di storage a oggetti. Ad esempio, se normalmente acquisisci grandi quantità di oggetti di piccole dimensioni, potresti dover aggiungere Storage Node per aumentare la capacità di metadati anche se rimane sufficiente capacità di storage a oggetti.

Alcuni dei fattori che possono aumentare l'utilizzo dei metadati includono le dimensioni e la quantità dei metadati e dei tag utente, il numero totale di parti in un caricamento multiparte e la frequenza delle modifiche alle posizioni di storage di ILM.

Passaggi

1. Seleziona **Nodes** > ***Storage Node*** > **Storage**.
2. Posiziona il cursore sul grafico Storage used - object metadata per vedere i valori relativi a un momento specifico.



Usato (%)

La percentuale dello spazio metadati consentito che è stata utilizzata su questo Storage Node.

metriche Prometheus: `storagegrid_storage_utilization_metadata_bytes` e `storagegrid_storage_utilization_metadata_allowed_bytes`

Usato

I byte dello spazio metadati consentito che sono stati utilizzati su questo Storage Node.

Metrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Consentito

Lo spazio consentito per i metadati degli oggetti su questo Storage Node. Per sapere come viene determinato questo valore per ciascun Storage Node, consulta il "Descrizione completa dello spazio metadati consentito".

Metrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Riservato effettivo

Lo spazio effettivamente riservato per i metadati su questo Storage Node. Include lo spazio consentito e lo spazio richiesto per le operazioni essenziali sui metadati. Per sapere come viene calcolato questo valore per ciascun Storage Node, vedi la "Descrizione completa dello spazio riservato per i metadati".

La metrica Prometheus sarà aggiunta in una versione futura.

> I valori totali per un sito o per la griglia non includono i nodi che non hanno segnalato metriche per almeno cinque minuti, come i nodi offline.

3. Se il valore **Utilizzato (%)** è pari o superiore al 70%, espandi il tuo sistema StorageGRID aggiungendo Storage Nodes a ciascun sito.

> L'avviso **Spazio di archiviazione metadati insufficiente** viene attivato quando il valore **Utilizzato (%)** raggiunge determinate soglie. Possono verificarsi risultati indesiderati se i metadati utilizzano più del 100% dello spazio consentito.

Quando aggiungi i nuovi nodi, il sistema ribilancia automaticamente i metadati degli oggetti su tutti i nodi di storage all'interno del sito. Vedi "Istruzioni per l'espansione di un sistema StorageGRID".

Monitora le previsioni di utilizzo dello spazio

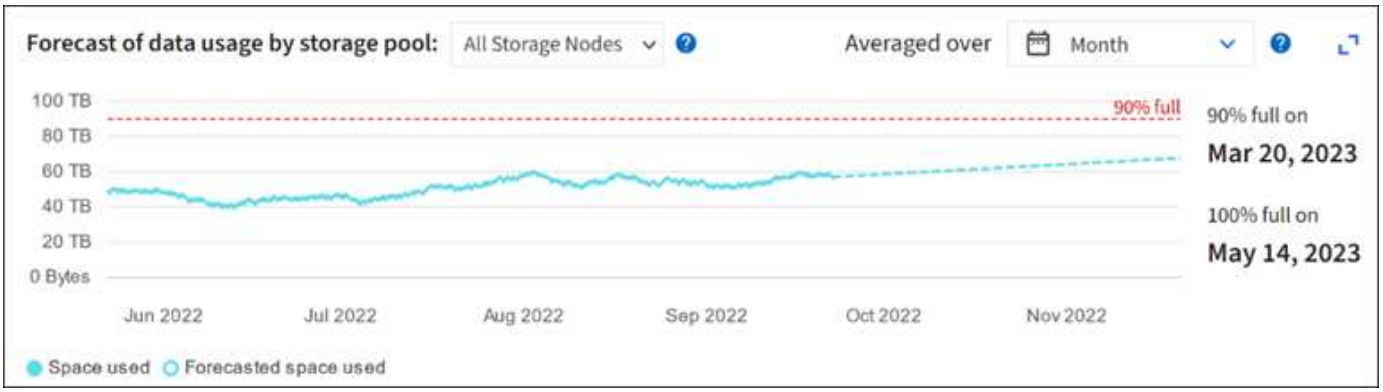
Monitora le previsioni di utilizzo dello spazio per i dati utente e metadati per stimare quando dovrai "espandi una griglia".

Se noti che il tasso di consumo varia nel tempo, seleziona un intervallo più breve dal menu a tendina **Media su** per riflettere solo i pattern di ingestione più recenti. Se noti pattern stagionali, seleziona un intervallo più lungo.

Se hai una nuova installazione di StorageGRID, lascia che dati e metadati si accumulino prima di valutare le previsioni sull'utilizzo dello spazio.

Passaggi

1. Nella dashboard, seleziona **Storage**.
2. Visualizza le schede del dashboard, Previsione dell'utilizzo dei dati per pool di storage e Previsione dell'utilizzo dei metadati per sito.
3. Utilizza questi valori per stimare quando dovrai aggiungere nuovi Storage Node per l'archiviazione dei dati e dei metadati.



Monitorare la gestione del ciclo di vita delle informazioni in StorageGRID

Il sistema di gestione del ciclo di vita delle informazioni (ILM) fornisce la gestione dei dati per tutti gli oggetti memorizzati nel grid. Devi monitorare le operazioni ILM per capire se il grid può gestire il carico attuale o se servono più risorse.

Informazioni su questa attività

Il sistema StorageGRID gestisce gli oggetti applicando le policy ILM attive. Le policy ILM e le relative regole ILM determinano quante copie vengono create, il tipo di copie che vengono create, dove vengono collocate le copie e per quanto tempo ciascuna copia viene conservata.

L'inserimento di oggetti e altre attività correlate agli oggetti possono superare la velocità con cui StorageGRID è in grado di valutare ILM, causando la messa in coda di oggetti le cui istruzioni di posizionamento ILM non possono essere soddisfatte in tempo quasi reale. Dovresti monitorare se StorageGRID riesce a tenere il passo con le azioni dei client.

Usa la scheda dashboard di Grid Manager

Passaggi

Utilizza la scheda ILM nella dashboard di Grid Manager per monitorare le operazioni ILM:

1. Accedi a Grid Manager.
2. Dalla dashboard, seleziona la scheda ILM e annota i valori sulla scheda Coda ILM (Oggetti) e sulla scheda Tasso di valutazione ILM.

   È normale che si verifichino picchi temporanei nella coda ILM (Oggetti) sulla dashboard. Tuttavia, se la coda continua ad aumentare senza mai diminuire, la grid necessita di più risorse per funzionare in modo efficiente: o più Storage Node, oppure, se la policy ILM posiziona gli oggetti in posizioni remote, maggiore larghezza di banda di rete.

Usa la pagina Nodi

Passaggi

Inoltre, esamina le code ILM utilizzando la pagina **Nodi**:

> I grafici presenti nella pagina **Nodi** verranno sostituiti con le corrispondenti schede del dashboard in una futura release di StorageGRID.

1. Selezionare **Nodi**.

2. Seleziona ***grid name*** > **ILM**.
3. Posiziona il cursore sul grafico della coda ILM per visualizzare il valore dei seguenti attributi in un dato momento:
   - **Oggetti in coda (da operazioni client)**: Il numero totale di oggetti in attesa di valutazione ILM a causa di operazioni client (ad esempio, ingest).
   - **Oggetti in coda (da tutte le operazioni)**: Il numero totale di oggetti in attesa di valutazione ILM.
   - **Frequenza di scansione (oggetti/sec)**: La velocità con cui gli oggetti nella grid vengono scansionati e messi in coda per ILM.
   - **Frequenza di valutazione (oggetti/sec)**: La frequenza attuale con cui gli oggetti vengono valutati rispetto alla policy ILM nel grid.

   La sezione relativa alla coda ILM è inclusa solo per il grid. Queste informazioni non vengono visualizzate nella scheda ILM per un sito o uno Storage Node.
4. Nella sezione Coda ILM, guarda i seguenti attributi.
   - **Periodo di scansione - stimato**: Tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

     Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti.
   - **Tentativi di riparazione**: Il numero totale di operazioni di riparazione degli oggetti per i dati replicati che sono state tentate. Questo conteggio aumenta ogni volta che un Storage Node tenta di riparare un oggetto ad alto rischio. Le riparazioni ILM ad alto rischio hanno la priorità se il grid diventa occupato.

     Lo stesso oggetto di riparazione potrebbe incrementare nuovamente se la replica non riesce dopo la riparazione. Questi attributi possono essere utili quando monitori l'avanzamento del ripristino del volume dello Storage Node. Se il numero di riparazioni tentate ha smesso di aumentare ed è stata completata una scansione completa, la riparazione probabilmente è terminata.
5. In alternativa, invia una query Prometheus per `storagegrid_ilm_scan_period_estimated_minutes` e `storagegrid_ilm_repairs_attempted`.

Monitora le risorse di rete e di sistema in StorageGRID

L'integrità e la larghezza di banda della rete tra nodi e siti, e l'utilizzo delle risorse da parte dei singoli nodi della griglia, sono fondamentali per un funzionamento efficiente.

Monitora le connessioni di rete e le prestazioni

La connettività di rete e la larghezza di banda sono particolarmente importanti se la tua policy di gestione del ciclo di vita delle informazioni (ILM) copia oggetti replicati tra siti o memorizza oggetti con codifica di cancellazione utilizzando uno schema che offre protezione in caso di perdita del sito. Se la rete tra i siti non è disponibile, la latenza di rete è troppo elevata o la larghezza di banda è insufficiente, alcune regole ILM potrebbero non essere in grado di posizionare gli oggetti dove previsto. Questo può causare errori di acquisizione (quando è selezionata l'opzione di acquisizione rigorosa per le regole ILM), oppure prestazioni di acquisizione scadenti e arretrati ILM.

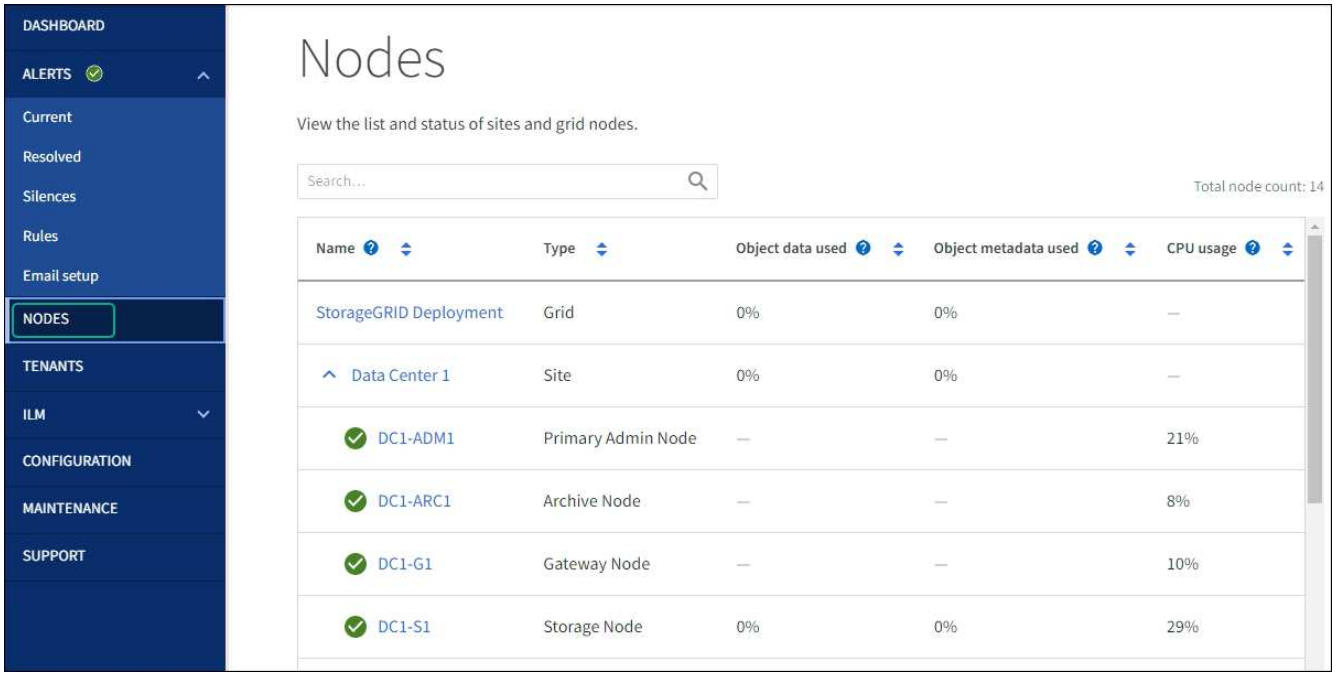
Utilizza Grid Manager per monitorare la connettività e le prestazioni della rete, così puoi risolvere subito eventuali problemi.

Inoltre, considera "creare policy di classificazione del traffico di rete" così puoi monitorare il traffico relativo a specifici tenant, bucket, subnet o endpoint del bilanciatore di carico. Puoi impostare criteri di limitazione del traffico secondo le tue esigenze.

Passaggi

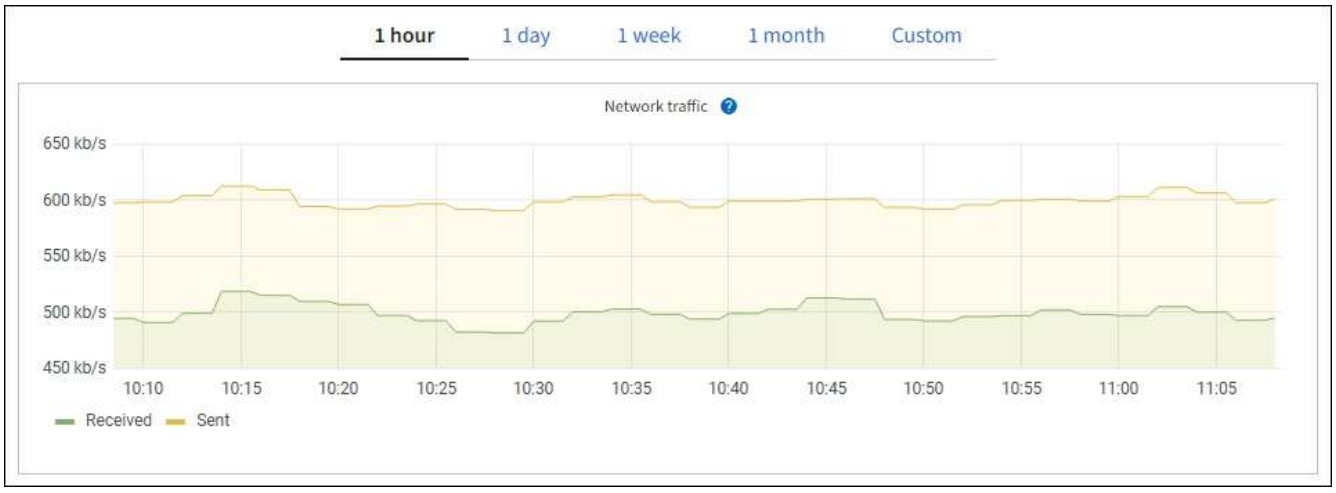
1. Selezionare **Nodi**.

   Viene visualizzata la pagina Nodi. Ogni nodo della griglia è elencato in formato tabellare.

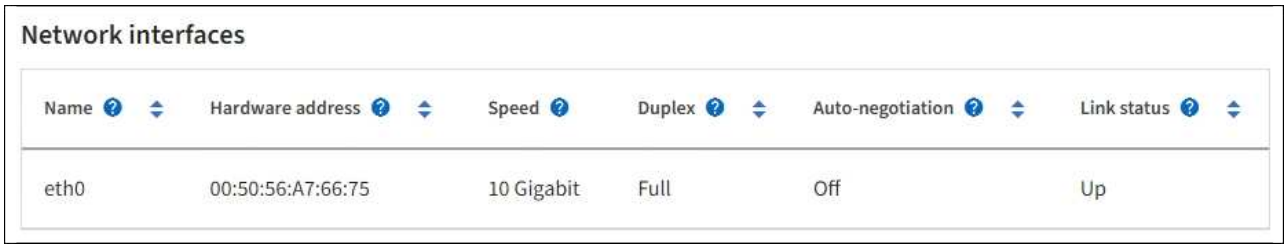


2. Seleziona il nome della griglia, un sito specifico del data center o un nodo della griglia, quindi seleziona la scheda **Network**.

   Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo per l'intera griglia, per il sito del data center o per il nodo.

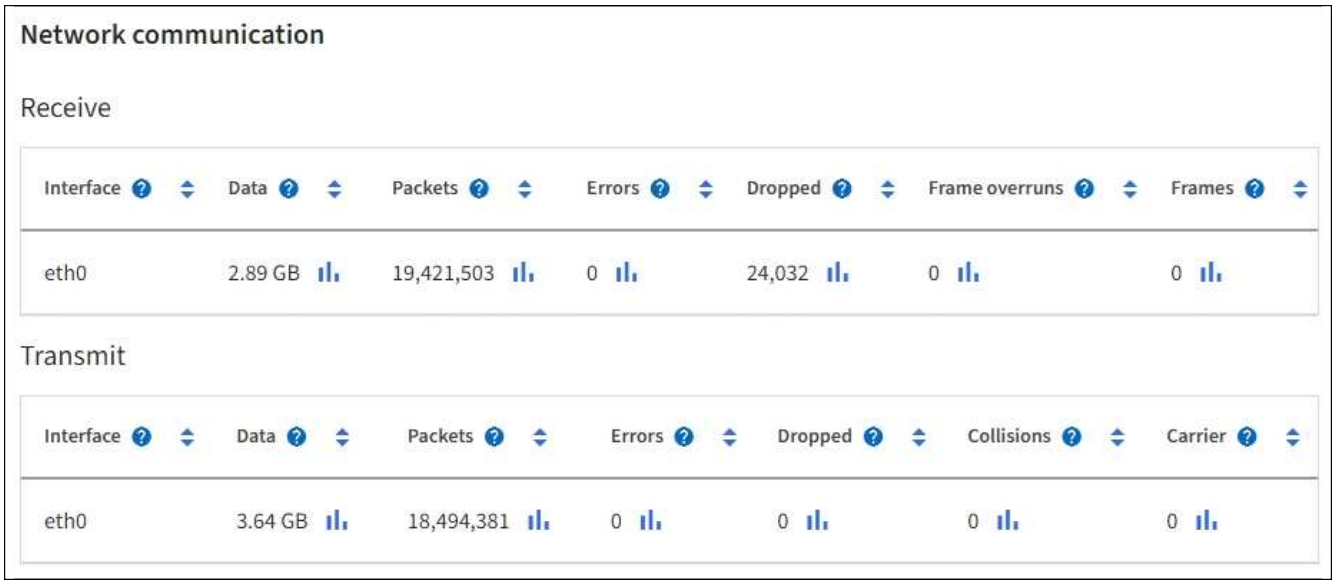


   a. Se hai selezionato un nodo della griglia, scorri verso il basso per visualizzare la sezione **Interfacce di rete** della pagina.



b. Per i nodi della griglia, scorri verso il basso per consultare la sezione **Network Communication** della pagina.

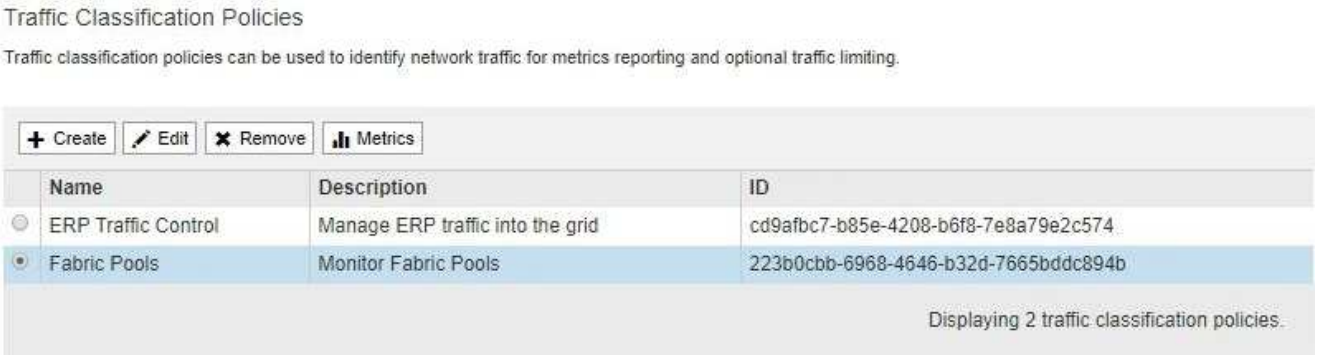
   Le tabelle Ricezione e Trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, oltre ad altre metriche di ricezione e trasmissione.



3. Utilizza le metriche associate alle tue politiche di classificazione del traffico per monitorare il traffico di rete.

   a. Seleziona **Configurazione** > **Rete** > **Classificazione del traffico**.

      Viene visualizzata la pagina "Politiche di classificazione del traffico" e le politiche esistenti sono elencate nella tabella.



   a. Per visualizzare i grafici che mostrano le metriche di rete associate a una policy, seleziona il pulsante di opzione a sinistra della policy e poi fai clic su **Metriche**.

   b. Esamina i grafici per comprendere il traffico di rete associato alla policy.

Se una politica di classificazione del traffico è progettata per limitare il traffico di rete, analizza con quale frequenza il traffico viene limitato e decidi se la politica continua a soddisfare le tue esigenze. Di tanto in tanto, "adatta ciascuna politica di classificazione del traffico secondo necessità".

Informazioni correlate

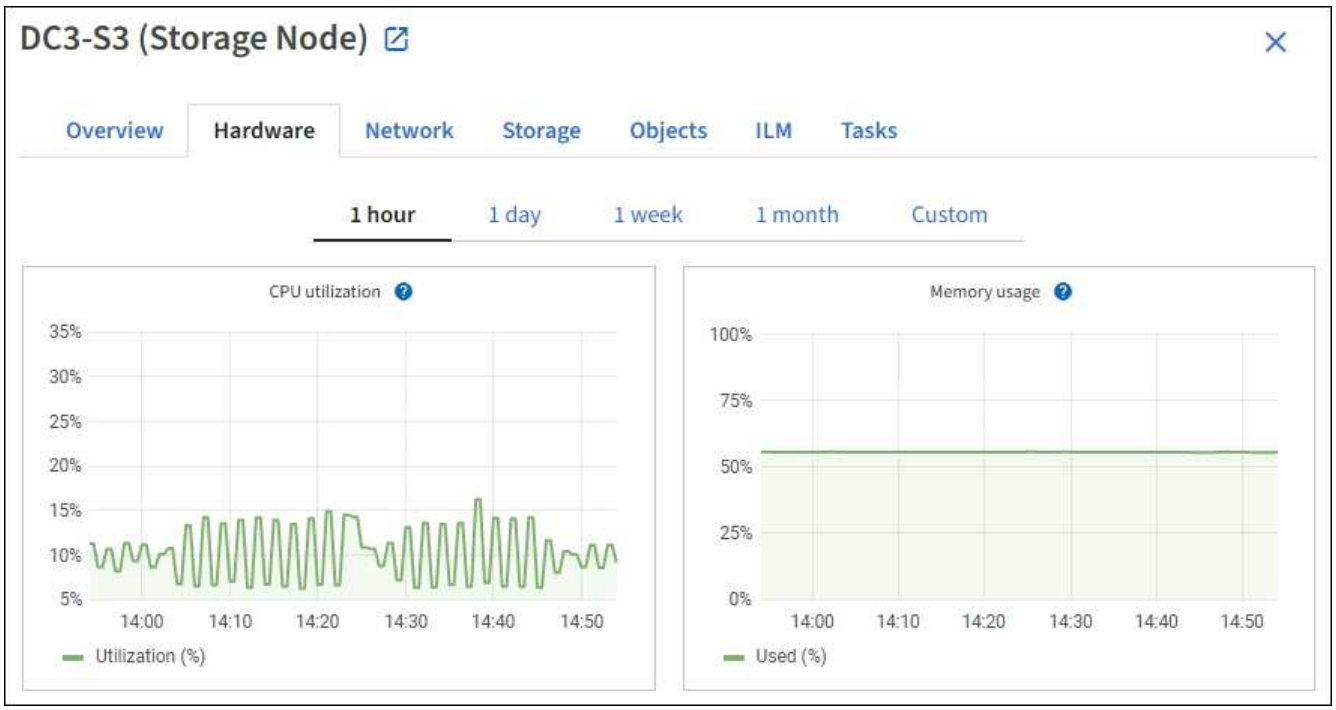
- "Visualizza la scheda Rete"
- "Monitora lo stato di connessione dei nodi"

Monitora le risorse a livello di nodo

Monitora i singoli nodi della griglia per verificarne i livelli di utilizzo delle risorse. Se i nodi sono costantemente sovraccarichi, potrebbero essere necessari più nodi per un funzionamento efficiente.

Passaggi

1. Dalla pagina **Nodi**, seleziona il nodo.
2. Seleziona la scheda **Hardware** per visualizzare i grafici relativi all'utilizzo della CPU e della memoria.



3. Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. Puoi visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. Puoi anche impostare un intervallo personalizzato, che ti permette di specificare intervalli di date e orari.
4. Se il nodo è ospitato su un'appliance di storage o un'appliance di servizi, scorri verso il basso per visualizzare le tabelle dei componenti. Lo stato di tutti i componenti dovrebbe essere "Nominale". Esamina i componenti che presentano uno stato diverso.

Informazioni correlate

- "Visualizza informazioni sui nodi di storage dell'appliance"
- "Visualizza le informazioni sui nodi Admin e sui nodi Gateway dell'appliance"

Monitorare l’attività dei tenant in StorageGRID

Tutte le attività dei client S3 sono associate agli account tenant di StorageGRID. Puoi usare Grid Manager per monitorare l’utilizzo dello storage o il traffico di rete per tutti i tenant o per un tenant specifico. Puoi usare il registro di audit o le dashboard di Grafana per raccogliere informazioni più dettagliate su come i tenant utilizzano StorageGRID.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Access root o autorizzazione account tenant".

Visualizza tutti i tenant

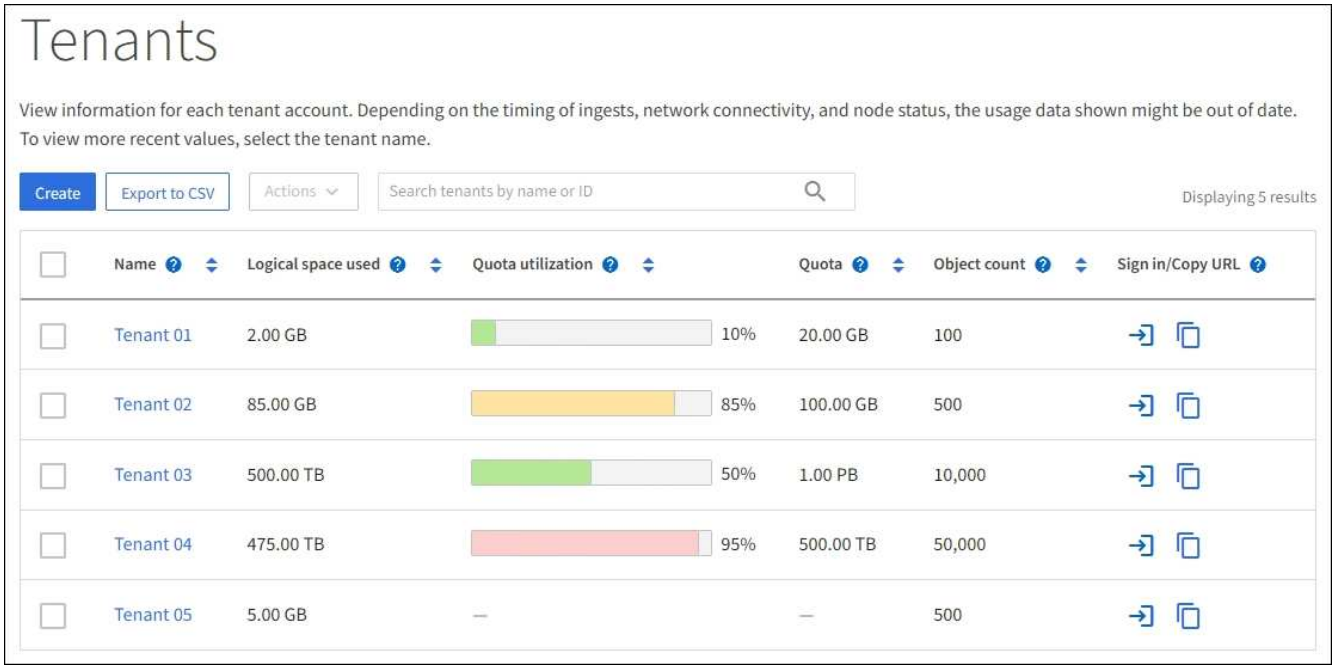
La pagina Tenant mostra le informazioni di base per tutti gli account tenant attivi.

Passaggi

1. Seleziona **tenant**.
2. Esamina le informazioni visualizzate nelle pagine Tenant.

   Lo spazio logico utilizzato, l’utilizzo della quota, la quota e il numero di oggetti sono elencati per ciascun tenant. Se non è stata impostata una quota per un tenant, i campi "Utilizzo della quota" e "Quota" contengono un trattino (—).

   > La dimensione logica di tutti gli oggetti appartenenti a questo tenant include i caricamenti multipart incompleti e in corso. La dimensione non include lo spazio fisico aggiuntivo utilizzato per le policy ILM. I valori relativi allo spazio utilizzato sono stime. Queste stime sono influenzate dal momento dell’ingestione, dalla connettività di rete e dallo stato dei nodi.



3. Facoltativamente, accedi a un tenant account selezionando il link di accesso nella colonna **Accedi/Copia URL**.
4. Facoltativamente, puoi copiare l’URL della pagina di accesso di un tenant selezionando il link "Copia URL"

nella colonna **Accedi/Copia URL**.

5. Facoltativamente, seleziona **Esporta in CSV** per visualizzare ed esportare un `.csv` file contenente i valori di utilizzo per tutti i tenant.

   Ti viene chiesto di aprire o salvare il `.csv` file.

   Il contenuto del file `.csv` si presenta come nell'esempio seguente:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

   Puoi aprire il `.csv` file in un'applicazione per fogli di calcolo o usarlo nell'automazione.

6. Se non vengono visualizzati oggetti, facoltativamente, seleziona **Azioni** > **Elimina** per rimuovere uno o più tenant. Vedi "Elimina account tenant".

   Non puoi rimuovere un tenant account se l'account include bucket o container.

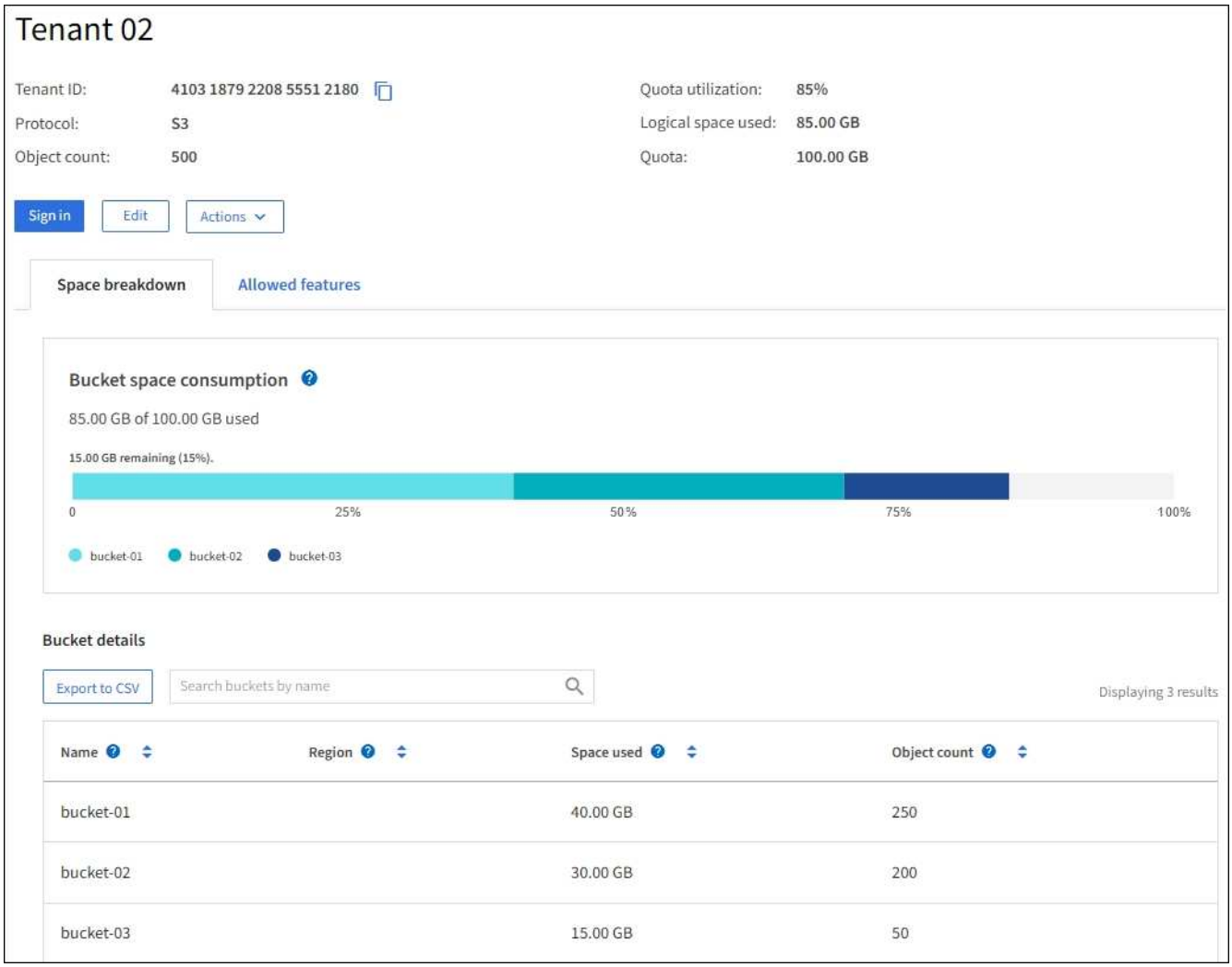
Visualizza un tenant specifico

Puoi visualizzare i dettagli di uno specifico tenant.

Passaggi

1. Seleziona il nome del tenant dalla pagina Tenant.

   Viene visualizzata la pagina dei dettagli del tenant.



2. Controlla la panoramica del tenant in cima alla pagina.

   Questa sezione della pagina dei dettagli fornisce informazioni di riepilogo per il tenant, inclusi il numero di oggetti del tenant, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

   > La dimensione logica di tutti gli oggetti appartenenti a questo tenant include i caricamenti multipart incompleti e in corso. La dimensione non include lo spazio fisico aggiuntivo utilizzato per le policy ILM. I valori relativi allo spazio utilizzato sono stime. Queste stime sono influenzate dal momento dell'ingestione, dalla connettività di rete e dallo stato dei nodi.

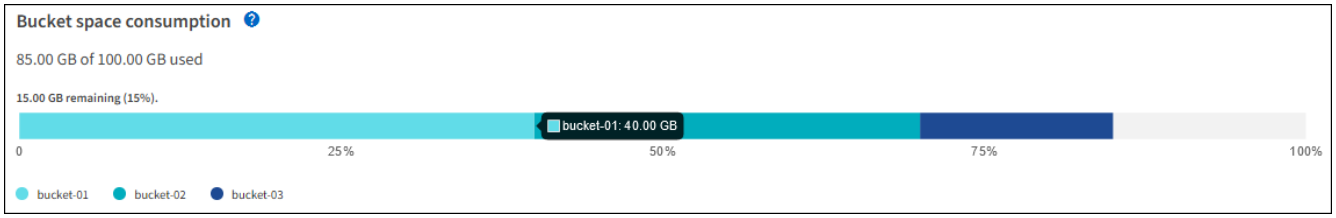
3. Dalla scheda **Ripartizione dello spazio**, controlla il grafico **Consumo di spazio**.

   Questo grafico mostra il consumo totale di spazio per tutti i bucket S3 del tenant.

   Se è stata impostata una quota per questo tenant, la quantità di quota utilizzata e quella rimanente vengono visualizzate in formato testuale (ad esempio, `85.00 GB of 100 GB used`). Se non è stata impostata alcuna quota, il tenant ha una quota illimitata e il testo include solo la quantità di spazio utilizzato (ad esempio, `85.00 GB used`). Il grafico a barre mostra la % di quota in ogni bucket o container. Se il tenant ha superato la quota di archiviazione di oltre l'1% e di almeno 1 GB, il grafico mostra la quota totale e la quantità in eccesso.

   Puoi posizionare il cursore sul grafico a barre per vedere lo spazio di archiviazione utilizzato da ciascun bucket o container. Puoi posizionare il cursore sul segmento di spazio libero per vedere la quantità di quota

di archiviazione rimanente.



L'utilizzo della quota si basa su stime interne e potrebbe essere superato in alcuni casi. Ad esempio, StorageGRID verifica la quota quando un tenant inizia a caricare oggetti e rifiuta i nuovi caricamenti se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente per determinare se la quota è stata superata. Se vengono eliminati oggetti, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino al ricalcolo dell'utilizzo della quota. Il calcolo dell'utilizzo della quota può richiedere 10 minuti o più.

L'utilizzo della quota di un tenant indica la quantità totale di dati oggetto che il tenant ha caricato su StorageGRID (dimensione logica). L'utilizzo della quota non rappresenta lo spazio utilizzato per archiviare copie di quegli oggetti e i loro metadati (dimensione fisica).

Puoi abilitare la regola di avviso **Elevato utilizzo della quota del tenant** per determinare se i tenant stanno consumando le proprie quote. Se abilitata, questa regola di avviso viene attivata quando un tenant ha utilizzato il 90% della propria quota. Per istruzioni, vedi "Modifica le regole di avviso".

4. Dalla scheda **Suddivisione dello spazio**, controlla i **Dettagli del bucket**.

   Questa tabella elenca i bucket S3 per il tenant. Lo spazio utilizzato corrisponde alla quantità totale di dati degli oggetti nel bucket o container. Questo valore non rappresenta lo spazio di storage necessario per le copie ILM e i metadati degli oggetti.

5. Facoltativamente, seleziona **Esporta in CSV** per visualizzare ed esportare un file .csv contenente i valori di utilizzo per ogni bucket o container.

   Il contenuto del file `.csv`di un singolo tenant S3 si presenta come nel seguente esempio:

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   Puoi aprire il `.csv` file in un'applicazione per fogli di calcolo o usarlo nell'automazione.

6. Facoltativamente, seleziona la scheda **Funzionalità consentite** per visualizzare un elenco delle autorizzazioni e delle funzionalità abilitate per il tenant. Vedi "Modifica account tenant" se hai bisogno di modificare una di queste impostazioni.
7. Se il tenant ha l'autorizzazione **Usa connessione di federazione a griglia**, puoi selezionare la scheda **Federazione a griglia** per saperne di più sulla connessione.

   Vedi "Che cos'è la federazione di griglie?" e "${post_edited_translations.segment}".

Visualizza traffico di rete

Se sono in atto delle policy di classificazione del traffico per un tenant, controlla il traffico di rete di quel tenant.

Passaggi

1. Seleziona **Configurazione** > **Rete** > **Classificazione del traffico**.

   Viene visualizzata la pagina "Politiche di classificazione del traffico" e le politiche esistenti sono elencate nella tabella.

2. Esamina l'elenco delle policy per identificare quelle che si applicano a uno specifico tenant.
3. Per visualizzare le metriche associate a una policy, seleziona il pulsante di opzione a sinistra della policy e seleziona **Metriche**.
4. Analizza i grafici per determinare con quale frequenza la policy limita il traffico e se devi modificarla.

Vedi "Gestisci le policy di classificazione del traffico" per maggiori informazioni.

Usa il registro di controllo

Facoltativamente, puoi utilizzare il registro di controllo per un monitoraggio più dettagliato delle attività di un tenant.

Ad esempio, puoi monitorare i seguenti tipi di informazioni:

- Operazioni specifiche del client, come PUT, GET o DELETE
- Dimensioni degli oggetti
- La regola ILM applicata agli oggetti
- L'indirizzo IP di origine delle richieste dei client

I log di controllo vengono scritti in file di testo che puoi analizzare utilizzando lo strumento di analisi dei log che preferisci. Questo ti permette di capire meglio le attività dei client o di implementare modelli di addebito e fatturazione più sofisticati.

Vedi "${post_edited_translations.segment}" per maggiori informazioni.

Usa le metriche Prometheus

Facoltativamente, puoi usare le metriche Prometheus per generare report sull'attività del tenant.

- In Grid Manager, seleziona **Support** > **Tools** > **Metrics**. Puoi utilizzare dashboard esistenti, come S3 Overview, per esaminare le attività dei client.

  > Gli strumenti disponibili nella pagina Metriche sono destinati principalmente all'utilizzo da parte del supporto tecnico. Alcune funzionalità e voci di menu all'interno di questi strumenti sono volutamente non funzionanti.

- Dalla parte superiore di Grid Manager, seleziona l'icona di aiuto e seleziona **API documentation**. Puoi utilizzare le metriche nella sezione Metrics dell'API di Grid Management per creare regole di avviso personalizzate e dashboard per l'attività dei tenant.

Vedi "Esamina le metriche di supporto" per maggiori informazioni.

Monitorare le operazioni del client S3 in StorageGRID

Puoi monitorare le velocità di acquisizione e recupero degli oggetti, così come le metriche relative al conteggio degli oggetti, alle query e alla verifica. Puoi visualizzare il numero di tentativi riusciti e non riusciti da parte delle applicazioni client di leggere, scrivere e modificare oggetti nel sistema StorageGRID.

Prima di iniziare

Sei connesso a Grid Manager utilizzando un "browser web supportato".

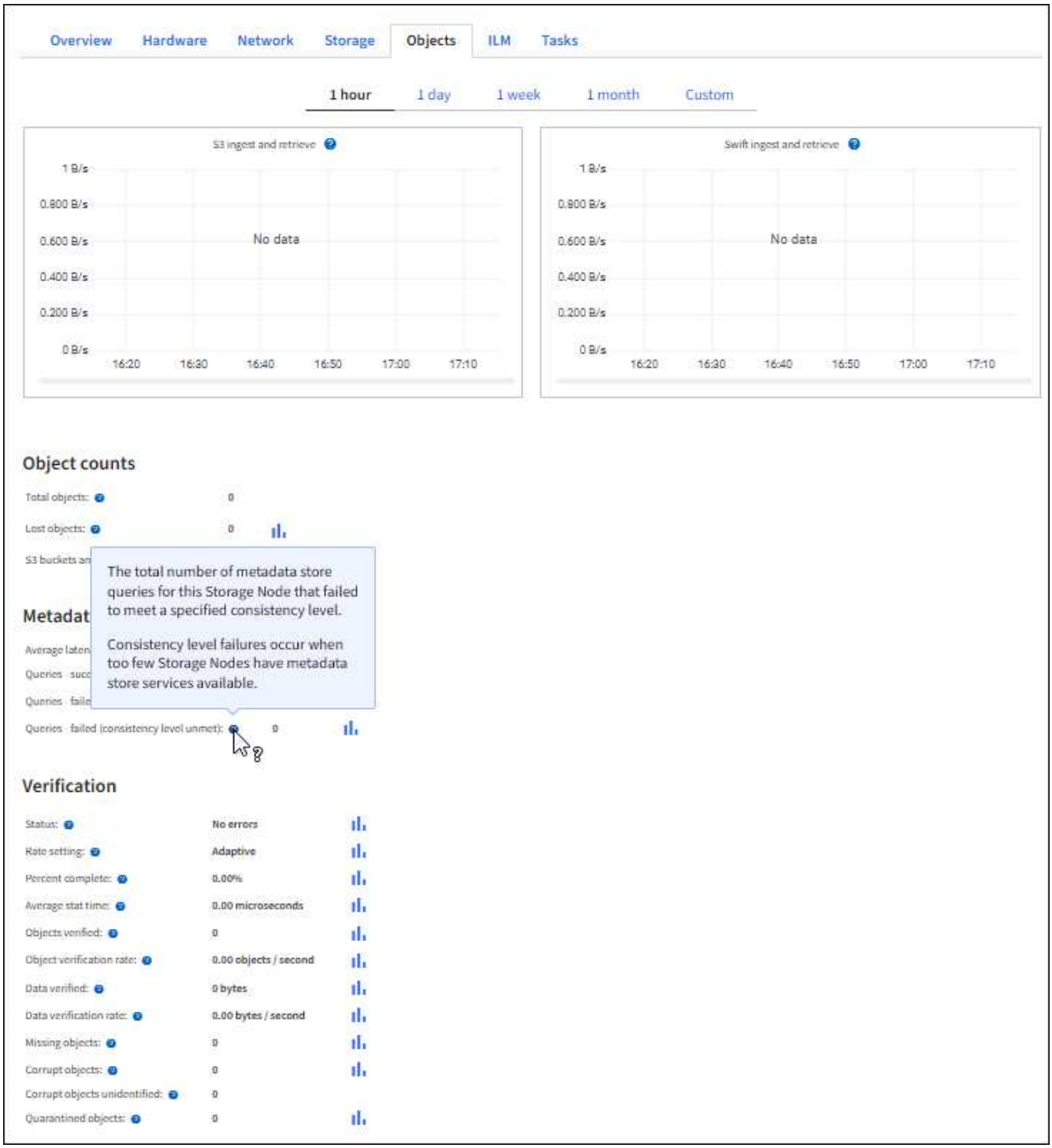
Passaggi

1. Dalla dashboard, seleziona la scheda **Performance**.
2. Consulta i grafici S3, che riepilogano il numero di operazioni client eseguite dai nodi di archiviazione e il numero di richieste API ricevute dai nodi di archiviazione durante il periodo di tempo selezionato.
3. Seleziona **Nodi** per accedere alla pagina dei nodi.
4. Dalla pagina iniziale dei nodi (livello griglia), seleziona la scheda **Oggetti**.

   Il grafico mostra le velocità di acquisizione e recupero S3 per l'intero sistema StorageGRID in byte al secondo e la quantità di dati acquisiti o recuperati. Puoi selezionare un intervallo di tempo o applicare un intervallo personalizzato.

5. Per visualizzare le informazioni relative a uno specifico Storage Node, seleziona il nodo dall'elenco a sinistra e seleziona la scheda **Oggetti**.

   Il grafico mostra le velocità di acquisizione e recupero per il nodo. La scheda include anche metriche per il conteggio degli oggetti, le query sui metadati e le operazioni di verifica.



Monitorare le operazioni di bilanciamento del carico in StorageGRID

Se usi un bilanciatore di carico per gestire le connessioni client a StorageGRID, dovresti monitorare le operazioni di bilanciamento del carico dopo aver configurato inizialmente il sistema e dopo aver apportato qualsiasi modifica alla configurazione o aver effettuato un'espansione.

Informazioni su questa attività

Puoi usare il servizio Load Balancer sui nodi di amministrazione, sui nodi gateway oppure un bilanciatore di carico esterno di terze parti per distribuire le richieste dei client su più nodi di Storage.

Dopo aver configurato il bilanciamento del carico, dovresti verificare che le operazioni di acquisizione e recupero degli oggetti siano distribuite uniformemente tra i nodi di storage. Le richieste distribuite uniformemente garantiscono che StorageGRID rimanga reattivo alle richieste dei client sotto carico e possono aiutare a mantenere le prestazioni dei client.

Se hai configurato un gruppo ad alta disponibilità (HA) di Gateway Nodes o Admin Nodes in modalità attivo-backup, solo un nodo del gruppo distribuisce attivamente le richieste dei client.

Per ulteriori informazioni, vedi "${post_edited_translations.segment}".

Passaggi

1. Se i client S3 si connettono utilizzando il servizio Load Balancer, verifica che i nodi Admin o i nodi Gateway distribuiscano attivamente il traffico come ti aspetti:
   a. Selezionare **Nodi**.
   b. Seleziona un nodo gateway o un nodo Admin.
   c. Nella scheda **Panoramica**, controlla se un'interfaccia del nodo è in un gruppo HA e se l'interfaccia del nodo ha il ruolo di Primaria.

      I nodi con il ruolo di Primary e i nodi che non fanno parte di un gruppo HA dovrebbero distribuire attivamente le richieste ai client.

   d. Per ogni nodo che deve distribuire attivamente le richieste dei client, seleziona il "Scheda Load Balancer".
   e. Esamina il grafico del traffico di richieste del Load Balancer dell'ultima settimana per assicurarti che il nodo abbia distribuito attivamente le richieste.

      In un gruppo HA attivo-backup, i nodi possono assumere il ruolo di backup di tanto in tanto. Durante quel periodo i nodi non distribuiscono le richieste dei client.

   f. Esamina il grafico del tasso di richieste in entrata del bilanciatore di carico per l'ultima settimana per verificare il throughput dell'oggetto del nodo.
   g. Ripeti questi passaggi per ogni Admin Node o Gateway Node nel sistema StorageGRID.
   h. Facoltativamente, puoi usare le policy di classificazione del traffico per visualizzare un'analisi più dettagliata del traffico gestito dal servizio Load Balancer.
2. Verifica che queste richieste vengano distribuite uniformemente ai Storage Node.
   a. Seleziona ***Storage Node*** > **LDR** > **HTTP**.
   b. Esamina il numero di **sessioni in entrata attualmente stabilite**.
   c. Ripeti l'operazione per ogni Storage Node nella grid.

      Il numero di sessioni dovrebbe essere approssimativamente uguale su tutti i nodi Storage.

Monitorare le connessioni della federazione della griglia StorageGRID

Puoi monitorare informazioni di base su tutte le "${post_edited_translations.segment}", informazioni dettagliate su una connessione specifica o metriche Prometheus sulle operazioni di replica tra griglie. Puoi monitorare una connessione da entrambe le griglie.

Prima di iniziare

- Hai effettuato l'accesso al Grid Manager su una delle due griglie utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root" per la griglia a cui hai effettuato l'accesso.

Visualizza tutte le connessioni

La pagina Federazione Grid mostra le informazioni di base su tutte le connessioni di federazione Grid e su tutti gli account tenant autorizzati a utilizzare le connessioni di federazione Grid.

Passaggi

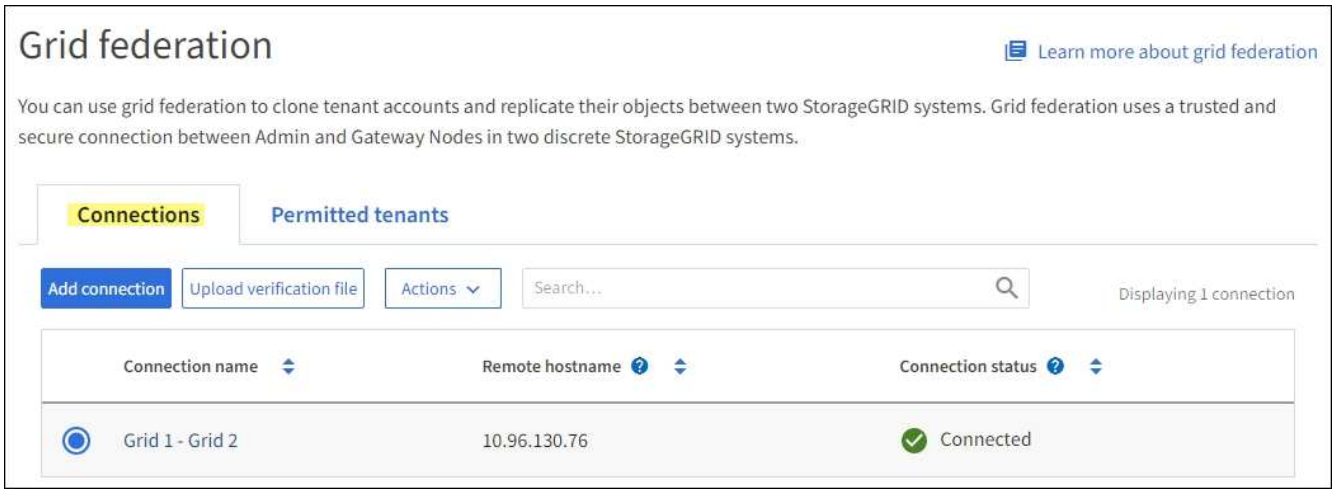
1. Seleziona **Configurazione** > **Sistema** > **Grid federation**.

   Viene visualizzata la pagina Grid federation.

2. Per vedere le informazioni di base su tutte le connessioni di questa griglia, seleziona la scheda **Connessioni**.

   Da questa scheda puoi:

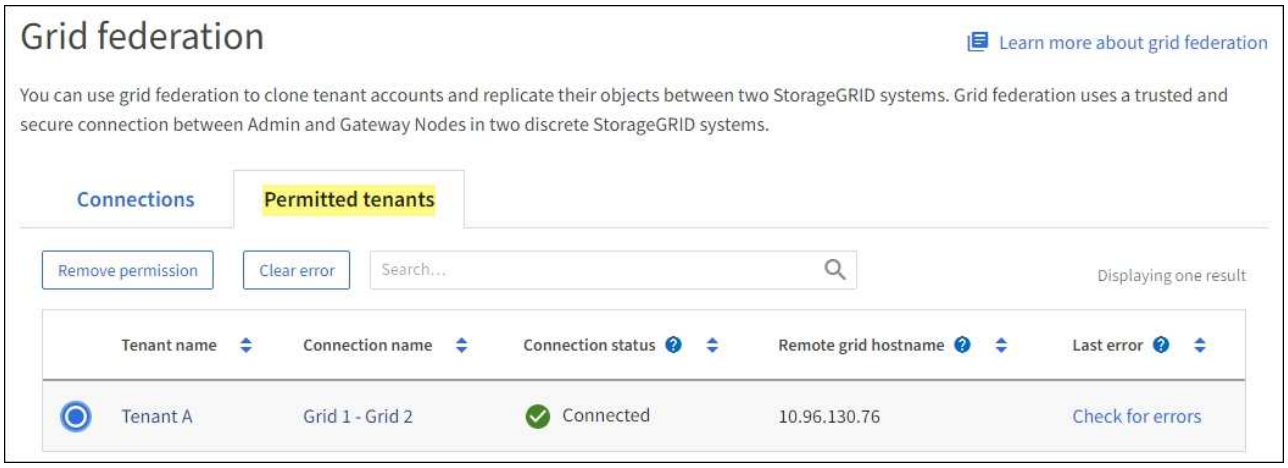
   - "Crea una nuova connessione".
   - Seleziona una connessione esistente a "modifica o prova".



3. Per vedere le informazioni di base di tutti gli account tenant su questa griglia che hanno il permesso **Usa la connessione di federazione della griglia**, seleziona la scheda **Tenant autorizzati**.

   Da questa scheda puoi:

   - "Visualizza la pagina dei dettagli per ogni tenant".
   - Visualizza la pagina dei dettagli per ogni connessione. Vedi Visualizza una connessione specifica.
   - Seleziona un tenant e "rimuovi l'autorizzazione".
   - Controlla la presenza di errori di replica tra griglie e cancella l'ultimo errore, se presente. Vedi "Risolvi i problemi relativi agli errori di federazione della griglia".



Visualizza una connessione specifica

Puoi visualizzare i dettagli di una specifica connessione di federazione di griglia.

Passaggi

1. Seleziona una delle schede dalla pagina Grid federation e poi seleziona il nome della connessione dalla tabella.

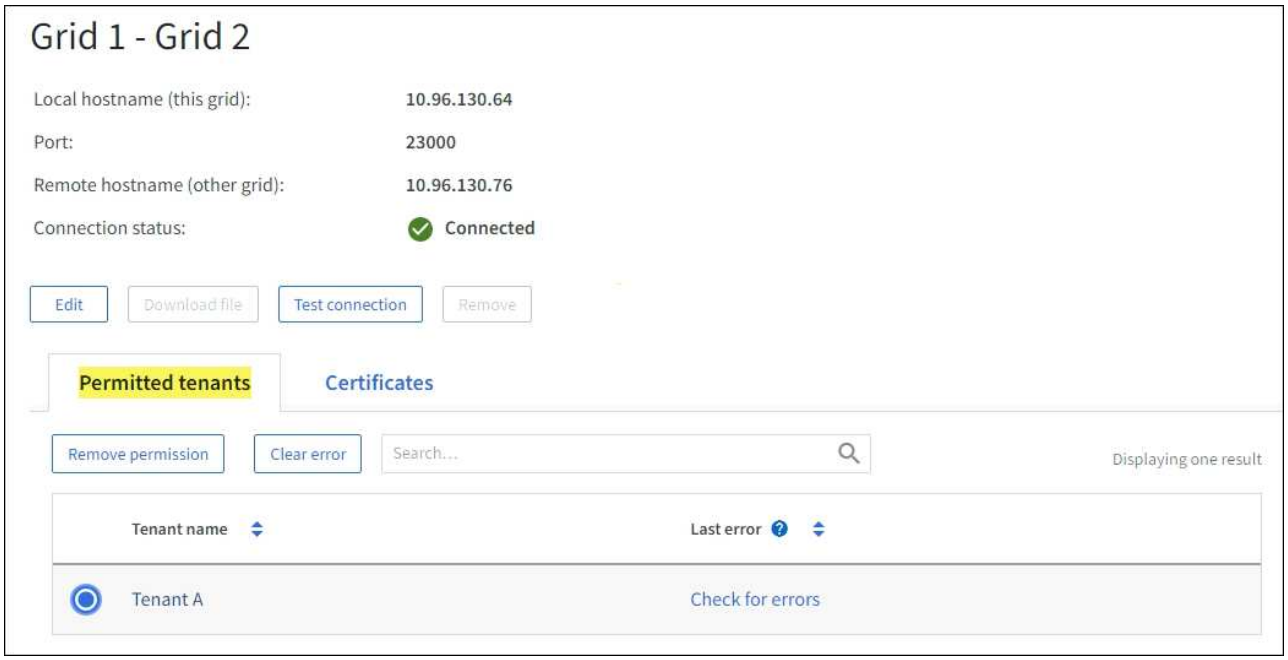
   Dalla pagina dei dettagli della connessione puoi:

   - Visualizza le informazioni di base sullo stato della connessione, inclusi i nomi host locali e remoti, la porta e lo stato della connessione.
   - Seleziona una connessione a "modifica, testa o rimuovi".

2. Quando visualizzi una connessione specifica, seleziona la scheda **Tenant autorizzati** per visualizzare i dettagli relativi ai tenant autorizzati per la connessione.

   Da questa scheda puoi:

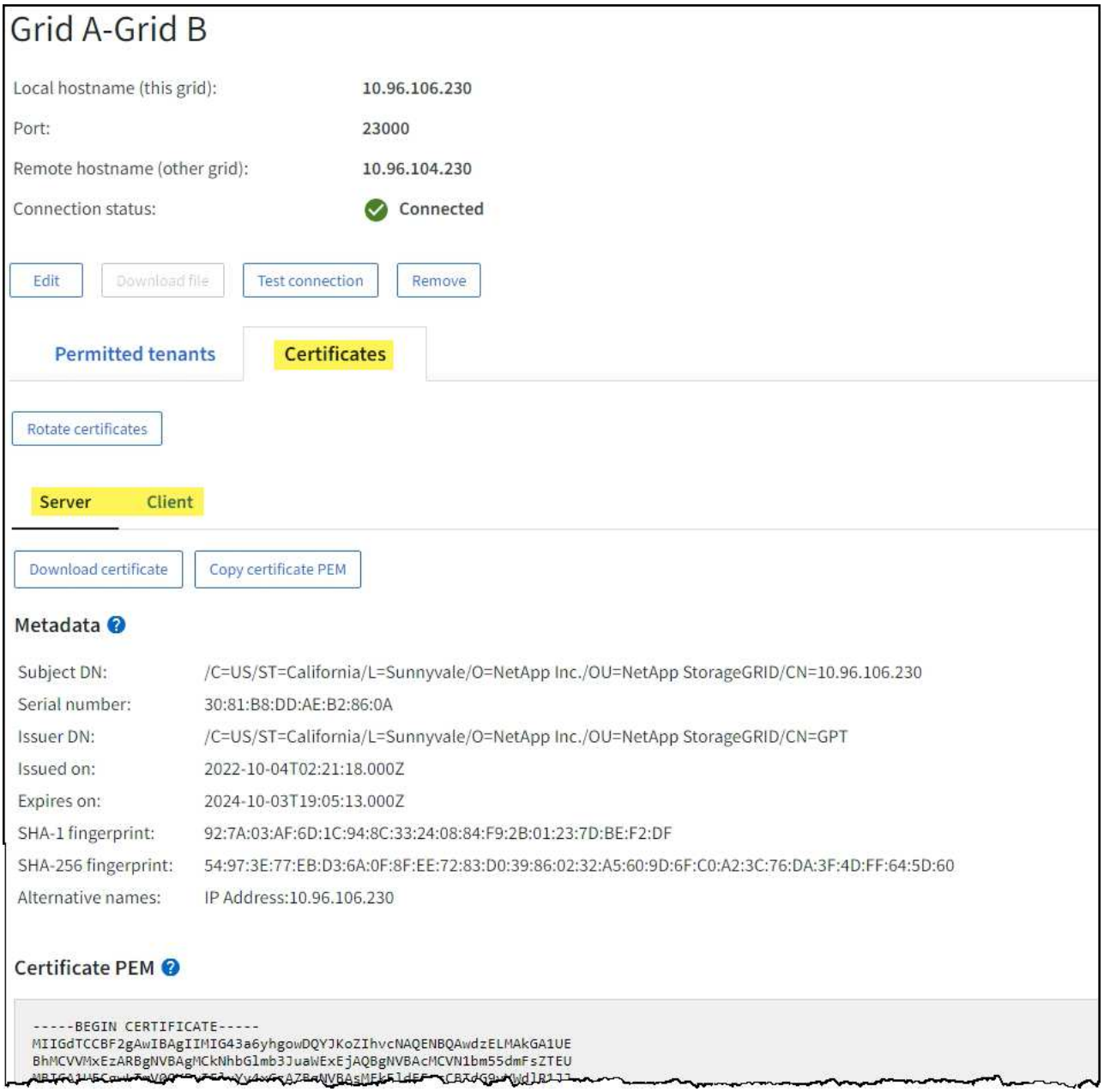
   - "Visualizza la pagina dei dettagli per ogni tenant".
   - "Rimuovi il permesso di un tenant" per utilizzare la connessione.
   - Verifica la presenza di errori di replica tra griglie e cancella l'ultimo errore. Vedi "Risolvi i problemi relativi agli errori di federazione della griglia".



3. Quando visualizzi una connessione specifica, seleziona la scheda **Certificati** per visualizzare i certificati server e client generati dal sistema per questa connessione.

   Da questa scheda puoi:

   - "Ruota i certificati di connessione".
   - Seleziona **Server** o **Client** per visualizzare o scaricare il certificato associato oppure copia il PEM del certificato.



Esamina le metriche di replica cross-grid

Puoi usare la dashboard Cross-Grid Replication in Grafana per visualizzare le metriche Prometheus sulle operazioni di replica cross-grid nella tua griglia.

Passaggi

1. Dal Grid Manager, seleziona **Support** > **Tools** > **Metrics**.

   Gli strumenti disponibili nella pagina Metriche sono destinati all'uso da parte del supporto tecnico. Alcune funzionalità e voci di menu all'interno di questi strumenti sono intenzionalmente non funzionanti e sono soggette a modifiche. Vedi l'elenco di "metriche Prometheus comunemente utilizzate".

2. Nella sezione Grafana della pagina, seleziona **Cross Grid Replication**.

   Per istruzioni dettagliate, vedere "Esamina le metriche di supporto".

3. Per riprovare la replica degli oggetti la cui replica non è riuscita, vedi "Identifica e riprova le operazioni di replica non riuscite".

Gestisci gli avvisi

Gestisci gli avvisi in StorageGRID

Il sistema di allerta fornisce un'interfaccia intuitiva per rilevare, valutare e risolvere i problemi che possono verificarsi durante il funzionamento di StorageGRID.

Gli avvisi vengono attivati a specifici livelli di gravità quando le condizioni della regola di avviso risultano vere. Quando viene attivato un avviso, si verificano le seguenti azioni:

- Un'icona che indica la gravità dell'avviso viene mostrata nella dashboard del Grid Manager e il conteggio degli avvisi correnti viene incrementato.
- L'avviso viene visualizzato nella pagina di riepilogo **Nodi** e nella scheda **Nodi** > ***nodo*** > **Panoramica**.
- Viene inviata una notifica via email, se hai configurato un server SMTP e fornito gli indirizzi email dei destinatari.
- Viene inviata una notifica Simple Network Management Protocol (SNMP), se hai configurato l'agente SNMP di StorageGRID.

Puoi creare avvisi personalizzati, modificare o disattivare gli avvisi e gestire le notifiche di avviso.

Per saperne di più:

- Guarda i video:

  Panoramica degli avvisi

  Avvisi personalizzati

- Fai riferimento a "Riferimento agli avvisi".

Visualizza le regole di avviso di StorageGRID

Le regole di avviso definiscono le condizioni che attivano "avvisi specifici". StorageGRID include una serie di regole di avviso predefinite, che puoi usare così come sono o modificare, oppure puoi creare regole di avviso personalizzate.

Puoi visualizzare l'elenco di tutte le regole di avviso predefinite e personalizzate per vedere quali condizioni attivano ciascun avviso e se ci sono avvisi disattivati.

Prima di iniziare

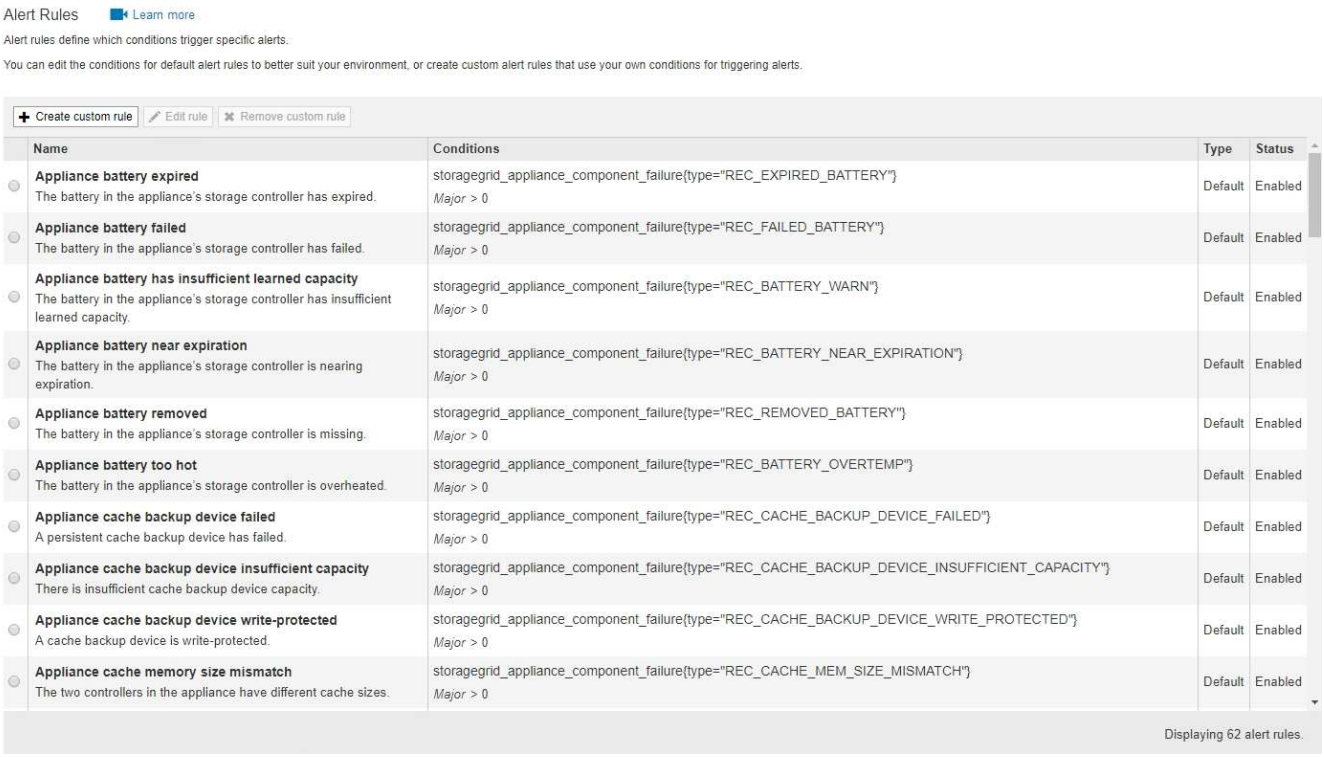
- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".
- Facoltativamente, hai guardato il video:

  Panoramica degli avvisi

Passaggi

1. Seleziona **Avvisi** > **Regole**.

   Viene visualizzata la pagina Regole di avviso.



2. Esamina le informazioni nella tabella delle regole di allerta:

Intestazione di colonna	Descrizione
Nome	Nome e descrizione univoci della regola di avviso. Le regole di avviso personalizzate sono elencate per prime, seguite da quelle predefinite. Il nome della regola di avviso è l'oggetto delle notifiche email.

Intestazione di colonna	Descrizione
Condizioni	Le espressioni Prometheus che determinano quando viene attivato questo avviso. Un avviso può essere attivato a uno o più dei seguenti livelli di gravità, ma non è richiesta una condizione per ciascun livello di gravità. • **Critico**: Esiste una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. Devi risolvere immediatamente il problema alla radice. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati. • **Grave**: Esiste una condizione anomala che sta influenzando le operazioni in corso o si sta avvicinando alla soglia per un avviso critico. Dovresti esaminare gli avvisi gravi e risolvere eventuali problemi sottostanti per assicurarti che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID. • **Minore**: Il sistema funziona normalmente, ma è presente una condizione anomala che potrebbe influire sulla capacità del sistema di funzionare se persiste. Dovresti monitorare e risolvere gli avvisi minori che non si risolvono da soli per assicurarti che non causino un problema più serio.
Tipo	Il tipo di regola di avviso: • **Predefinita**: Una regola di avviso fornita con il sistema. Puoi disabilitare una regola di avviso predefinita o modificarne le condizioni e la durata. Non puoi rimuovere una regola di avviso predefinita. • **Predefinito***: Una regola di avviso predefinita che include una condizione o una durata modificata. Se necessario, puoi facilmente ripristinare una condizione modificata al valore predefinito originale. • **Personalizzata**: Una regola di avviso che hai creato. Puoi disabilitare, modificare e rimuovere le regole di avviso personalizzate.
Stato	Indica se questa regola di avviso è attualmente abilitata o disabilitata. Le condizioni per le regole di avviso disabilitate non vengono valutate, quindi non vengono attivati avvisi.

Crea regole di avviso personalizzate in StorageGRID

Puoi creare regole di avviso personalizzate per definire le tue condizioni per l'attivazione degli avvisi.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".
- Hai familiarità con il "metriche Prometheus comunemente utilizzate".
- Capisci il "sintassi delle query di Prometheus".

- Facoltativamente, hai guardato il video:

  Avvisi personalizzati

Informazioni su questa attività

StorageGRID non convalida gli avvisi personalizzati. Se decidi di creare regole di avviso personalizzate, segui queste linee guida generali:

- Guarda le condizioni delle regole di avviso predefinite e usale come esempio per le tue regole di avviso personalizzate.
- Se definisci più condizioni per una regola di avviso, usa la stessa espressione per tutte le condizioni. Poi, cambia il valore di soglia per ciascuna condizione.
- Verifica attentamente ogni condizione per individuare eventuali errori di battitura o di logica.
- Usa solo le metriche elencate nell'API di gestione della griglia.
- Quando testi un'espressione utilizzando l'API di gestione della griglia, tieni presente che una risposta "positiva" potrebbe essere un corpo di risposta vuoto (nessun avviso attivato). Per vedere se l'avviso viene effettivamente attivato, puoi impostare temporaneamente una soglia su un valore che ti aspetti sia vero in questo momento.

  Ad esempio, per testare l'espressione `node_memory_MemTotal_bytes < 24000000000`, esegui prima `node_memory_MemTotal_bytes >= 0` e assicurati di ottenere i risultati attesi (tutti i nodi restituiscono un valore). Poi, cambia l'operatore e la soglia ai valori previsti ed esegui di nuovo. Nessun risultato indica che non ci sono avvisi correnti per questa espressione.

- Non dare per scontato che un avviso personalizzato funzioni a meno che tu non abbia verificato che venga attivato quando previsto.

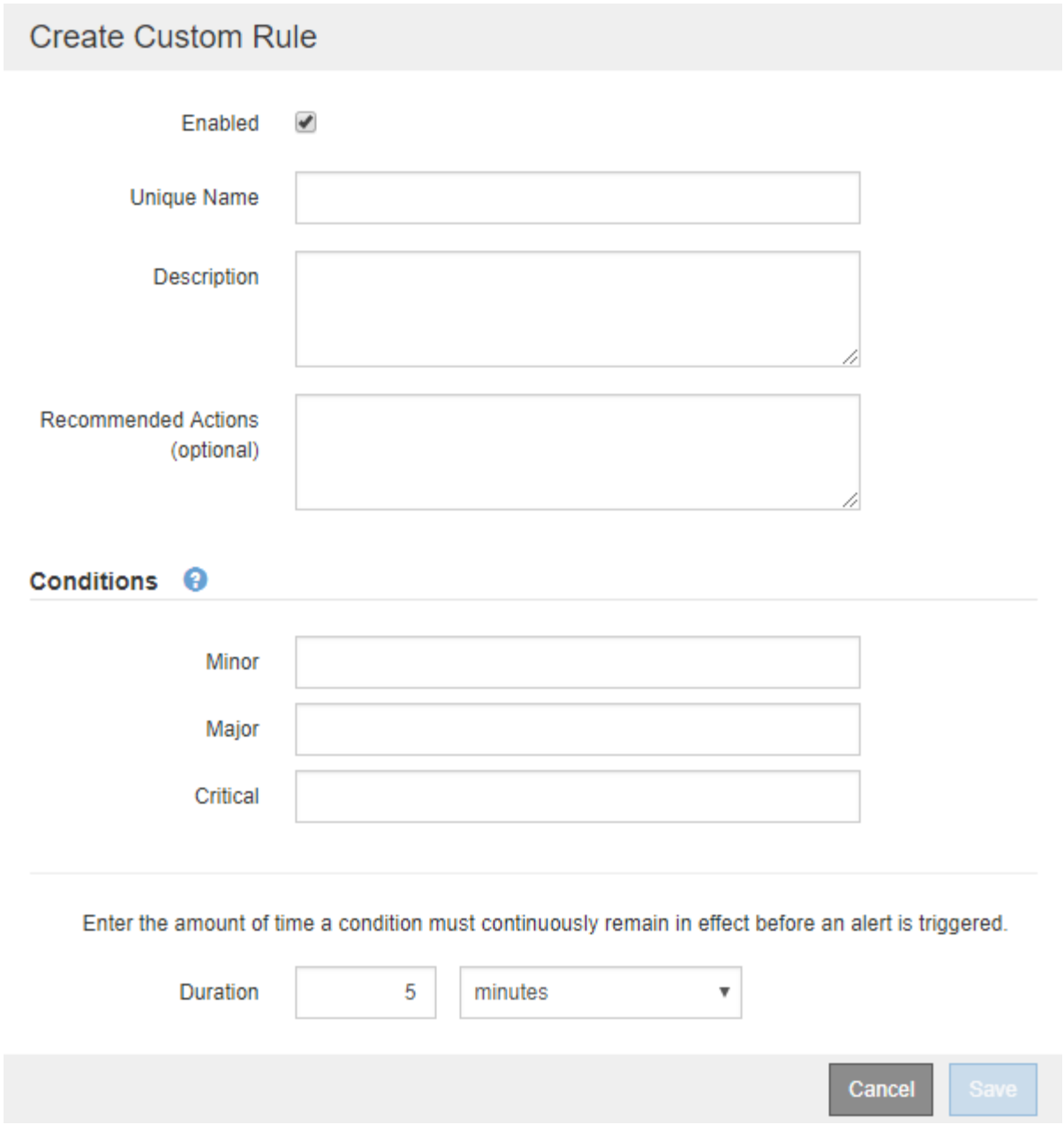
Passaggi

1. Seleziona **Avvisi** > **Regole**.

   Viene visualizzata la pagina Regole di avviso.

2. Seleziona **Crea regola personalizzata**.

   Viene visualizzata la finestra di dialogo Crea regola personalizzata.



3. Seleziona o deseleziona la casella di controllo **Abilitato** per decidere se questa regola di avviso è attualmente abilitata.

   Se una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non viene attivato alcun avviso.

4. Inserisci le seguenti informazioni:

Campo	Descrizione
Nome unico	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche email. I nomi delle regole di avviso possono essere composti da 1 a 64 caratteri.

Campo	Descrizione
Descrizione	Descrizione del problema riscontrato. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche email. Le descrizioni delle regole di avviso possono essere lunghe da 1 a 128 caratteri.
Azioni consigliate	Facoltativamente, puoi specificare le azioni consigliate da intraprendere quando viene attivato questo avviso. Inserisci le azioni consigliate come testo semplice (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1.024 caratteri.

5. Nella sezione Condizioni, inserisci un'espressione Prometheus per uno o più livelli di gravità dell'avviso.

   Un'espressione di base è solitamente della forma:

   ```
   [metric] [operator] [value]
   ```

   Le espressioni possono avere qualsiasi lunghezza, ma nell'interfaccia utente appaiono su un'unica riga. È richiesta almeno un'espressione.

   Questa espressione fa sì che venga attivato un avviso se la quantità di RAM installata per un nodo è inferiore a 24.000.000.000 di byte (24 GB).

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Per visualizzare le metriche disponibili e testare le espressioni Prometheus, seleziona l'icona di aiuto (?) e segui il collegamento alla sezione Metrics dell'API Grid Management.

6. Nel campo **Durata**, inserisci la quantità di tempo per cui una condizione deve rimanere in vigore in modo continuativo prima che venga attivato l'avviso e seleziona un'unità di tempo.

   Per attivare immediatamente un avviso quando una condizione diventa vera, inserisci **0**. Aumenta questo valore per evitare che condizioni temporanee attivino avvisi.

   Il valore predefinito è 5 minuti.

7. Seleziona **Salva**.

   La finestra di dialogo si chiude e la nuova regola di avviso personalizzata appare nella tabella Regole di avviso.

Modifica le regole di avviso in StorageGRID

Puoi modificare una regola di avviso per cambiare le condizioni di attivazione. Per una regola di avviso personalizzata, puoi anche aggiornare il nome della regola, la descrizione e le azioni consigliate.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".

- Hai il "Gestisci gli avvisi o i permessi di accesso root".

Informazioni su questa attività

Quando modifichi una regola di avviso predefinita, puoi cambiare le condizioni per gli avvisi di livello minore, maggiore e critico e la durata. Quando modifichi una regola di avviso personalizzata, puoi anche modificare il nome, la descrizione e le azioni consigliate della regola.

> Fai attenzione quando decidi di modificare una regola di avviso. Se cambi i valori di attivazione, potresti non rilevare un problema sottostante finché non impedisce il completamento di un'operazione critica.

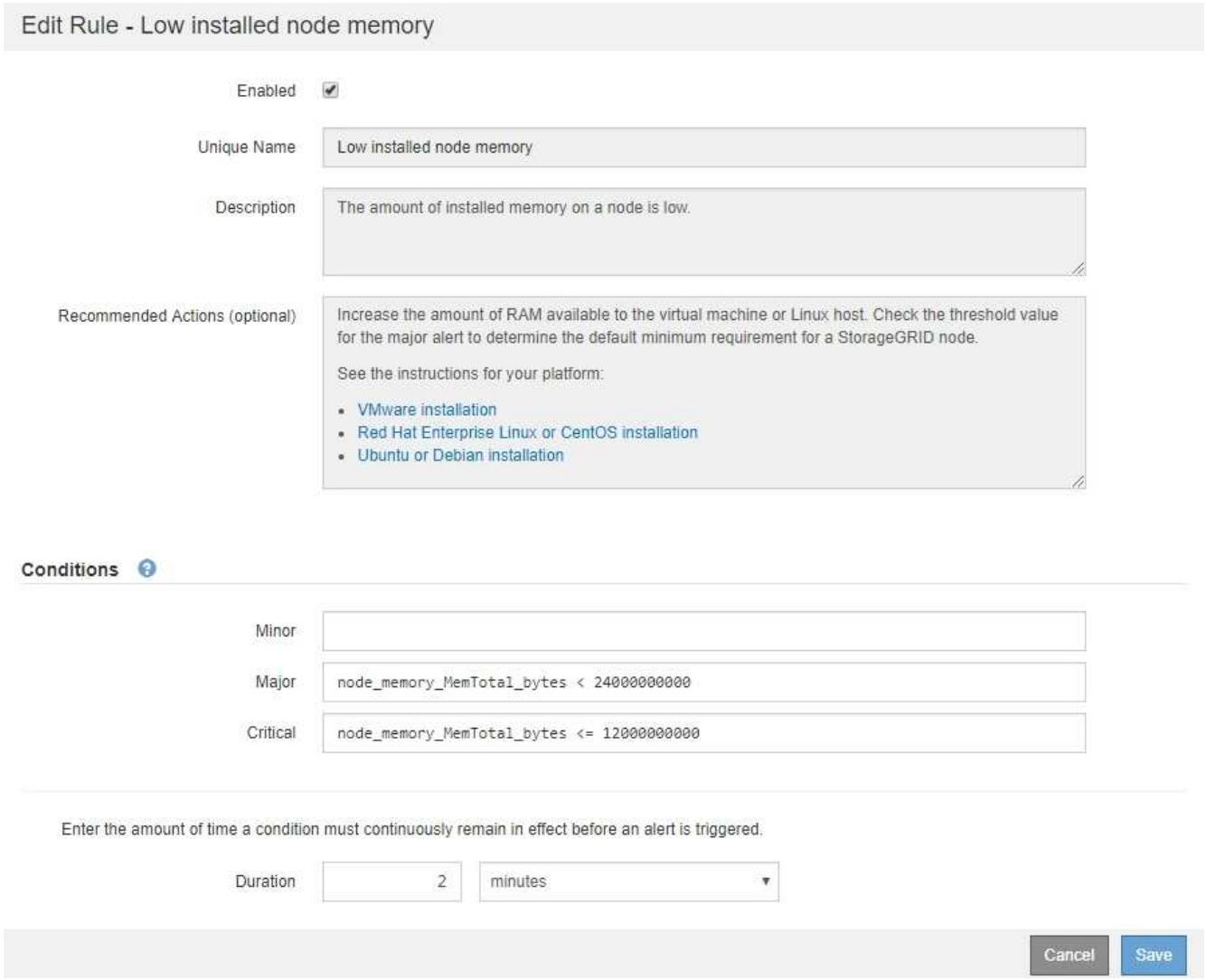
Passaggi

1. Seleziona **Avvisi** > **Regole**.

   Viene visualizzata la pagina Regole di avviso.

2. Seleziona il pulsante di opzione per la regola di avviso che vuoi modificare.
3. Seleziona **Modifica regola**.

   Viene visualizzata la finestra di dialogo Modifica regola. Questo esempio mostra una regola di avviso predefinita: i campi Unique Name, Description e Recommended Actions sono disabilitati e non possono essere modificati.



4. Seleziona o deseleziona la casella di controllo **Abilitato** per decidere se questa regola di avviso è attualmente abilitata.

   Se una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non viene attivato alcun avviso.

   > Se disattivi la regola di avviso per un avviso attivo, devi aspettare alcuni minuti prima che l'avviso non venga più visualizzato come attivo.

   > In generale, disabilitare una regola di avviso predefinita non è consigliabile. Se una regola di avviso è disabilitata, potresti non rilevare un problema sottostante finché non impedisce il completamento di un'operazione critica.

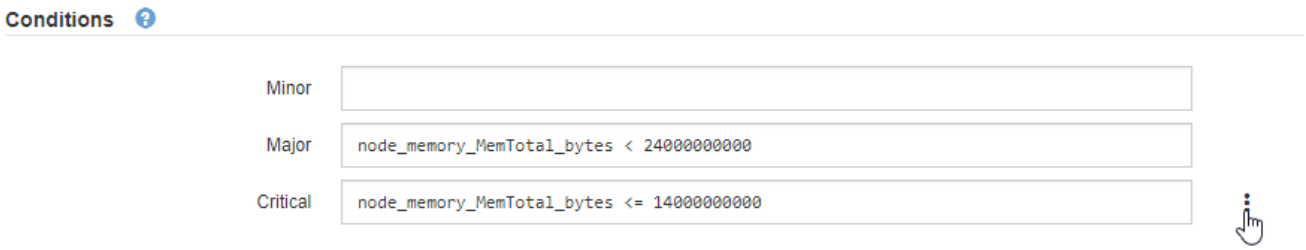
5. Per le regole di avviso personalizzate, aggiorna le seguenti informazioni secondo necessità.

   > Non puoi modificare queste informazioni per le regole di avviso predefinite.

Campo	Descrizione
Nome unico	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche email. I nomi delle regole di avviso possono essere composti da 1 a 64 caratteri.
Descrizione	Descrizione del problema riscontrato. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche email. Le descrizioni delle regole di avviso possono essere lunghe da 1 a 128 caratteri.
Azioni consigliate	Facoltativamente, puoi specificare le azioni consigliate da intraprendere quando viene attivato questo avviso. Inserisci le azioni consigliate come testo semplice (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1.024 caratteri.

6. Nella sezione Condizioni, inserisci o aggiorna l'espressione Prometheus per uno o più livelli di gravità dell'allerta.

> Se vuoi ripristinare il valore originale di una condizione per una regola di avviso predefinita modificata, seleziona i tre puntini a destra della condizione modificata.



> Se aggiorni le condizioni per un avviso corrente, le modifiche potrebbero non essere implementate finché la condizione precedente non viene risolta. La prossima volta che una delle condizioni per la regola viene soddisfatta, l'avviso rifletterà i valori aggiornati.

Un'espressione di base è solitamente della forma:

```
[metric] [operator] [value]
```

Le espressioni possono avere qualsiasi lunghezza, ma nell'interfaccia utente appaiono su un'unica riga. È richiesta almeno un'espressione.

Questa espressione fa sì che venga attivato un avviso se la quantità di RAM installata per un nodo è inferiore a 24.000.000.000 di byte (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

7. Nel campo **Durata**, inserisci la quantità di tempo per cui una condizione deve rimanere in vigore in modo continuativo prima che venga attivato l'avviso e seleziona l'unità di tempo.

Per attivare immediatamente un avviso quando una condizione diventa vera, inserisci **0**. Aumenta questo valore per evitare che condizioni temporanee attivino avvisi.

Il valore predefinito è 5 minuti.

8. Seleziona **Salva**.

   Se hai modificato una regola di avviso predefinita, nella colonna Tipo viene visualizzato **Default**. Se hai disabilitato una regola di avviso predefinita o personalizzata, nella colonna **Status** viene visualizzato **Disabled**.

Disabilita le regole di avviso in StorageGRID

Puoi modificare lo stato di attivazione/disattivazione per una regola di avviso predefinita o personalizzata.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".

Informazioni su questa attività

Quando una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non vengono attivati avvisi.

> In generale, disabilitare una regola di avviso predefinita non è consigliabile. Se una regola di avviso è disabilitata, potresti non rilevare un problema sottostante finché non impedisce il completamento di un'operazione critica.

Passaggi

1. Seleziona **Avvisi** > **Regole**.

   Viene visualizzata la pagina Regole di avviso.

2. Seleziona il pulsante di opzione per la regola di avviso che vuoi disabilitare o abilitare.
3. Seleziona **Modifica regola**.

   Viene visualizzata la finestra di dialogo Modifica regola.

4. Seleziona o deseleziona la casella di controllo **Abilitato** per decidere se questa regola di avviso è attualmente abilitata.

   Se una regola di avviso è disabilitata, le sue espressioni non vengono valutate e non viene attivato alcun avviso.

   > Se disattivi la regola di avviso per un avviso attivo, devi aspettare alcuni minuti prima che l'avviso non venga più visualizzato come attivo.

5. Seleziona **Salva**.

   Disabilitato compare nella colonna **Stato**.

Rimuovi le regole di avviso personalizzate in StorageGRID

Puoi rimuovere una regola di avviso personalizzata se non vuoi più usarla.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".

Passaggi

1. Seleziona **Avvisi** > **Regole**.

   Viene visualizzata la pagina Regole di avviso.

2. Seleziona il pulsante di opzione per la regola di avviso personalizzata che vuoi rimuovere.

   Non puoi rimuovere una regola di avviso predefinita.

3. Seleziona **Rimuovi regola personalizzata**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Seleziona **OK** per rimuovere la regola di avviso.

   Tutte le istanze attive dell'avviso verranno risolte entro 10 minuti.

Gestisci le notifiche di avviso

Imposta le notifiche SNMP per gli avvisi StorageGRID

Se vuoi che StorageGRID invii notifiche SNMP quando si verificano avvisi, devi abilitare l'agente SNMP di StorageGRID e configurare una o più destinazioni trap.

Puoi usare l'opzione **Configuration** > **Monitoring** > **SNMP agent** in Grid Manager oppure gli endpoint SNMP per la Grid Management API per abilitare e configurare l'agente SNMP di StorageGRID. L'agente SNMP supporta tutte e tre le versioni del protocollo SNMP.

Per sapere come configurare l'agente SNMP, vedi "Usa il monitoraggio SNMP".

Dopo che hai configurato l'agente SNMP di StorageGRID, possono essere inviati due tipi di notifiche basate su eventi:

- Le trap sono notifiche inviate dall'agente SNMP che non richiedono conferma da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che è successo qualcosa all'interno di StorageGRID, come ad esempio l'attivazione di un avviso. Le trap sono supportate in tutte e tre le versioni di SNMP.
- Gli inform sono simili ai trap, ma richiedono una conferma da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, reinvia l'inform finché non riceve una conferma o finché non viene raggiunto il valore massimo di tentativi. Gli inform sono supportati in SNMPv2c e SNMPv3.

Le notifiche di trap e inform vengono inviate quando viene attivato un avviso predefinito o personalizzato a qualsiasi livello di gravità. Per sopprimere le notifiche SNMP per un avviso, devi configurare un silenzio per l'avviso. Vedi "Silenzia le notifiche di avviso".

Se la tua distribuzione StorageGRID include più nodi di amministrazione, il nodo di amministrazione primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport e le trap e inform SNMP. Se il nodo di amministrazione primario diventa non disponibile, le notifiche vengono temporaneamente inviate dagli altri nodi di amministrazione. Vedi "Che cos'è un Admin Node?".

Configura le notifiche e-mail per gli avvisi di StorageGRID

Se vuoi che vengano inviate notifiche email quando si verificano avvisi, devi fornire le informazioni sul tuo server SMTP. Devi anche inserire gli indirizzi email dei destinatari delle notifiche di avviso.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".

Informazioni su questa attività

Le impostazioni email utilizzate per le notifiche di avviso non vengono utilizzate per i pacchetti AutoSupport. Tuttavia, puoi usare lo stesso server di posta elettronica per tutte le notifiche.

Se la tua distribuzione StorageGRID include più nodi di amministrazione, il nodo di amministrazione primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport e le trap e inform SNMP. Se il nodo di amministrazione primario diventa non disponibile, le notifiche vengono temporaneamente inviate dagli altri nodi di amministrazione. Vedi "Che cos'è un Admin Node?".

Passaggi

1. Seleziona **Avvisi** > **Configurazione email**.

   Viene visualizzata la pagina di configurazione della posta elettronica.

2. Seleziona la casella di controllo **Abilita notifiche e-mail** per indicare che vuoi che vengano inviate e-mail di notifica quando gli avvisi raggiungono le soglie configurate.

   Vengono visualizzate le sezioni Email (SMTP) Server, Transport Layer Security (TLS), Email Addresses e Filters.

3. Nella sezione Server di posta elettronica (SMTP), inserisci le informazioni necessarie a StorageGRID per accedere al tuo server SMTP.

   Se il server SMTP richiede l'autenticazione, devi fornire sia un nome utente che una password.

Campo	Inserisci
Server di posta	Il fully qualified domain name (FQDN) o l'indirizzo IP del server SMTP.
Porta	La porta utilizzata per accedere al server SMTP. Deve essere compresa tra 1 e 65535.
Nome utente (facoltativo)	Se il server SMTP richiede l'autenticazione, inserisci il nome utente con cui autenticarti.

Campo	Inserisci
Password (facoltativa)	Se il server SMTP richiede l'autenticazione, inserisci la password per autenticarti.

4. Nella sezione Indirizzi e-mail, inserisci gli indirizzi e-mail del mittente e di ciascun destinatario.
   a. Nel campo **Indirizzo email del mittente**, specifica un indirizzo email valido da usare come mittente per le notifiche di avviso.

      Ad esempio: `storagegrid-alerts@example.com`

   b. Nella sezione Destinatari, inserisci un indirizzo email per ogni lista email o persona che deve ricevere un'email quando si verifica un avviso.

      Seleziona l'icona più ➕ per aggiungere i destinatari.

5. Se per le comunicazioni con il server SMTP è necessario il protocollo Transport Layer Security (TLS), seleziona **Richiedi TLS** nella sezione Transport Layer Security (TLS).
   a. Nel campo **Certificato CA**, inserisci il certificato CA che verrà utilizzato per verificare l'identità del server SMTP.

      Puoi copiare e incollare il contenuto in questo campo oppure selezionare **Browse** e scegliere il file.

      Devi fornire un singolo file che contenga i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file deve contenere ciascun file di certificato CA codificato in formato PEM, concatenati nell'ordine della catena di certificati.

   b. Seleziona la casella di controllo **Invia certificato client** se il tuo server di posta SMTP richiede ai mittenti di fornire certificati client per l'autenticazione.
   c. Nel campo **Certificato client**, inserisci il certificato client codificato in formato PEM da inviare al server SMTP.

      Puoi copiare e incollare il contenuto in questo campo oppure selezionare **Browse** e scegliere il file.

   d. Nel campo **Chiave privata**, inserisci la chiave privata del certificato client in formato PEM non crittografato.

      Puoi copiare e incollare il contenuto in questo campo oppure selezionare **Browse** e scegliere il file.

   ⓘ Se devi modificare le impostazioni dell'email, seleziona l'icona della matita ✎ per aggiornare questo campo.

6. Nella sezione Filtri, seleziona quali livelli di gravità degli avvisi devono generare notifiche via e-mail, a meno che la regola per un avviso specifico non sia stata silenziata.

Gravità	Descrizione
Minore, maggiore, critico	Viene inviata una notifica via e-mail quando viene soddisfatta la condizione minore, maggiore o critica per una regola di avviso.

Gravità	Descrizione
Importante, critico	Ricevi una notifica via e-mail quando viene soddisfatta la condizione maggiore o critica per una regola di avviso. Le notifiche non vengono inviate per gli avvisi minori.
Solo critico	Ricevi una notifica via e-mail solo quando si verifica la condizione critica per una regola di avviso. Non ricevi notifiche per avvisi di minore o maggiore entità.

7. Quando sei pronto per testare le impostazioni della tua email, segui questi passaggi:
   a. Seleziona **Invia email di prova**.

      Viene visualizzato un messaggio di conferma che indica che è stata inviata un'email di prova.

   b. Controlla le caselle di posta di tutti i destinatari dell'email e verifica che sia stata ricevuta un'email di prova.

      Se non ricevi l'e-mail entro pochi minuti o se viene visualizzato l'avviso **Errore di notifica e-mail**, controlla le impostazioni e riprova.

   c. Accedi a qualsiasi altro Admin Node e invia un'email di prova per verificare la connettività da tutti i siti.

      Quando testi le notifiche di avviso, devi accedere a ogni Admin Node per verificare la connettività. Questo è diverso dal test dei pacchetti AutoSupport, in cui tutti gli Admin Node inviano l'email di prova.

8. Seleziona **Salva**.

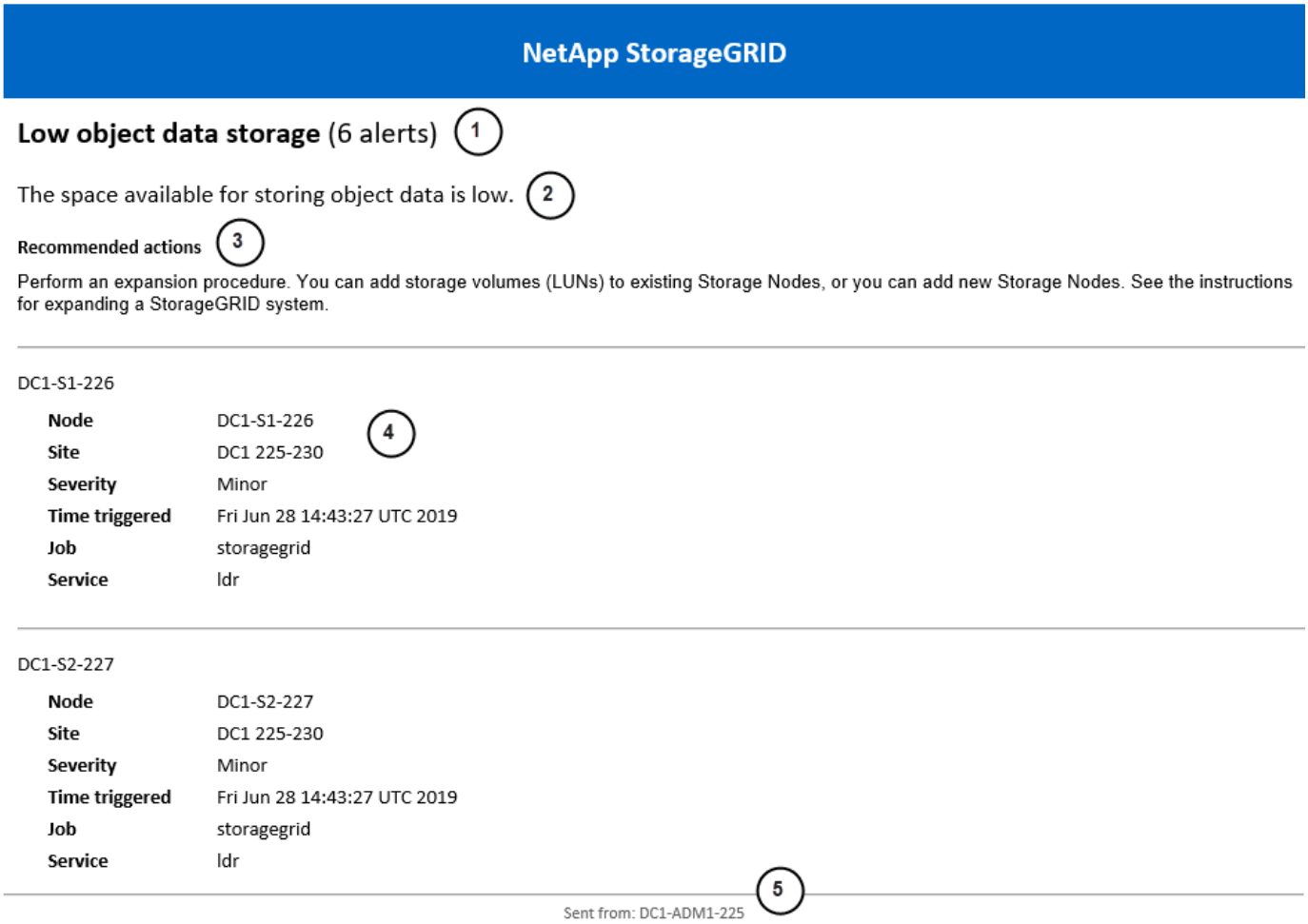
   L'invio di un'email di prova non salva le impostazioni. Devi selezionare **Salva**.

   Le impostazioni e-mail sono state salvate.

Informazioni incluse nelle notifiche e-mail di avviso

Dopo che hai configurato il server di posta SMTP, le notifiche email vengono inviate ai destinatari designati quando viene attivato un avviso, a meno che la regola di avviso non sia soppressa da un'opzione di silenzio. Vedi "Silenzia le notifiche di avviso".

Le notifiche via e-mail includono le seguenti informazioni:



Callout	Descrizione
1	Il nome dell'avviso, seguito dal numero di istanze attive di questo avviso.
2	La descrizione dell'allerta.
3	Eventuali azioni consigliate per l'avviso.
4	Dettagli relativi a ciascuna istanza attiva dell'avviso, inclusi il nodo e il sito interessati, la gravità dell'avviso, l'ora UTC in cui è stata attivata la regola di avviso e il nome del job e del servizio interessati.
5	Il nome host del nodo Admin che ha inviato la notifica.

Come vengono raggruppati gli avvisi

Per evitare che venga inviato un numero eccessivo di notifiche email quando vengono attivati degli avvisi, StorageGRID cerca di raggruppare più avvisi nella stessa notifica.

Consulta la tabella seguente per esempi di come StorageGRID raggruppa più avvisi nelle notifiche e-mail.

Comportamento	Esempio
Ogni notifica di avviso si applica solo agli avvisi che hanno lo stesso nome. Se due avvisi con nomi diversi vengono attivati contemporaneamente, vengono inviate due notifiche email.	• L'allarme A viene attivato contemporaneamente su due nodi. Viene inviata una sola notifica. • L'allarme A viene attivato sul nodo 1 e l'allarme B viene attivato contemporaneamente sul nodo 2. Vengono inviate due notifiche, una per ciascun allarme.
Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di un livello di gravità, viene inviata una notifica solo per l'avviso più grave.	• Viene attivato l'allarme A e vengono raggiunte le soglie di allarme minore, maggiore e critico. Per l'allarme critico viene inviata una sola notifica.
La prima volta che viene attivato un avviso, StorageGRID attende 2 minuti prima di inviare una notifica. Se durante questo lasso di tempo vengono attivati altri avvisi con lo stesso nome, StorageGRID li raggruppa tutti nella notifica iniziale.	1. L'allarme A viene attivato sul nodo 1 alle 08:00. Non viene inviata alcuna notifica. 2. L'allarme A viene attivato sul nodo 2 alle 08:01. Non viene inviata alcuna notifica. 3. Alle 08:02 viene inviata una notifica per segnalare entrambe le istanze dell'avviso.
Se viene attivato un altro avviso con lo stesso nome, StorageGRID attende 10 minuti prima di inviare una nuova notifica. La nuova notifica riporta tutti gli avvisi attivi (avvisi correnti che non sono stati silenziati), anche se sono già stati segnalati in precedenza.	1. L'allarme A viene attivato sul nodo 1 alle 08:00. Una notifica viene inviata alle 08:02. 2. L'allarme A viene attivato sul nodo 2 alle 08:05. Una seconda notifica viene inviata alle 08:15 (10 minuti dopo). Entrambi i nodi vengono segnalati.
Se sono presenti più avvisi attivi con lo stesso nome e uno di questi viene risolto, non viene inviata una nuova notifica se l'avviso si ripresenta sul nodo per il quale è stato risolto.	1. L'allarme A viene attivato per il nodo 1. Viene inviata una notifica. 2. L'allarme A viene attivato per il nodo 2. Viene inviata una seconda notifica. 3. L'avviso A è stato risolto per il nodo 2, ma rimane attivo per il nodo 1. 4. L'allerta A viene attivata nuovamente per il nodo 2. Non viene inviata alcuna nuova notifica perché l'allerta è ancora attiva per il nodo 1.
StorageGRID continua a inviare notifiche via e-mail ogni 7 giorni finché tutti i casi di avviso non vengono risolti o la regola di avviso non viene disattivata.	1. L'allerta A viene attivata per il nodo 1 l'8 marzo. Viene inviata una notifica. 2. L'avviso A non è risolto o silenziato. Ulteriori notifiche vengono inviate il 15 marzo, il 22 marzo, il 29 marzo e così via.

Risolvi i problemi delle notifiche email di avviso

Se viene visualizzato l'avviso **Errore di notifica e-mail** o non riesci a ricevere l'email di notifica di prova, segui questi passaggi per risolvere il problema.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".

Passaggi

1. Verifica le tue impostazioni.
   a. Seleziona **Avvisi** > **Configurazione email**.
   b. Verifica che le impostazioni del server email (SMTP) siano corrette.
   c. Verifica di aver specificato indirizzi email validi per i destinatari.
2. Controlla il filtro antispam e assicurati che l'email non sia stata inviata nella cartella della posta indesiderata.
3. Chiedi al tuo amministratore di posta elettronica di confermare che le email provenienti dall'indirizzo del mittente non vengano bloccate.
4. Raccogli un file di log per l'Admin Node e poi contatta il supporto tecnico.

   Il supporto tecnico può usare le informazioni nei file di log per aiutarti a capire cosa non ha funzionato. Ad esempio, il file prometheus.log potrebbe mostrare un errore durante la connessione al server che hai specificato.

   Vedi "Raccogli i file di log e i dati di sistema".

Silenzia le notifiche di alert in StorageGRID

Facoltativamente, puoi configurare i silenziamenti per sopprimere temporaneamente le notifiche di avviso.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".

Informazioni su questa attività

Puoi silenziare le regole di avviso sull'intera griglia, su un singolo sito o su un singolo nodo e per uno o più livelli di gravità. Ogni silenziamento sopprime tutte le notifiche per una singola regola di avviso o per tutte le regole di avviso.

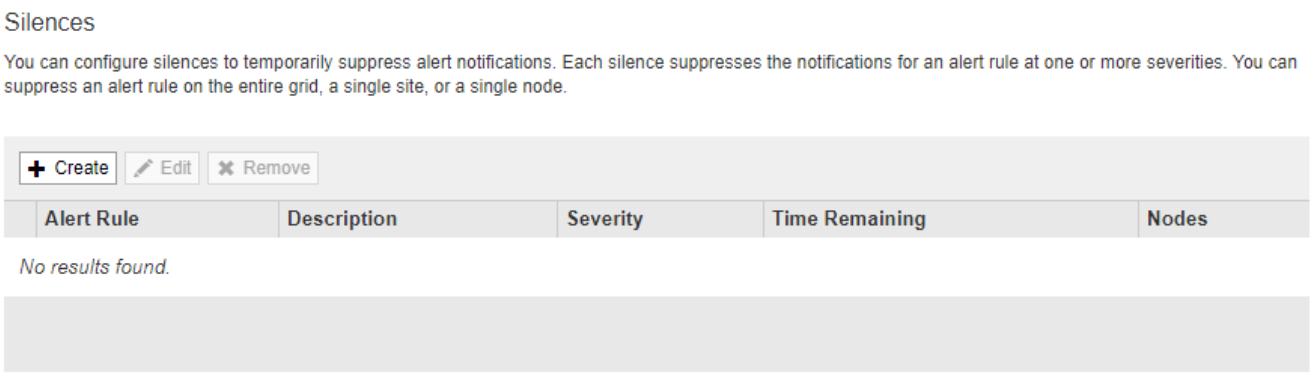
Se hai abilitato l'agente SNMP, le funzioni di silenziamento sopprimono anche le trap e le inform SNMP.

> Fai attenzione quando decidi di disattivare una regola di avviso. Se disattivi un avviso, potresti non rilevare un problema sottostante finché non impedisce il completamento di un'operazione critica.

Passaggi

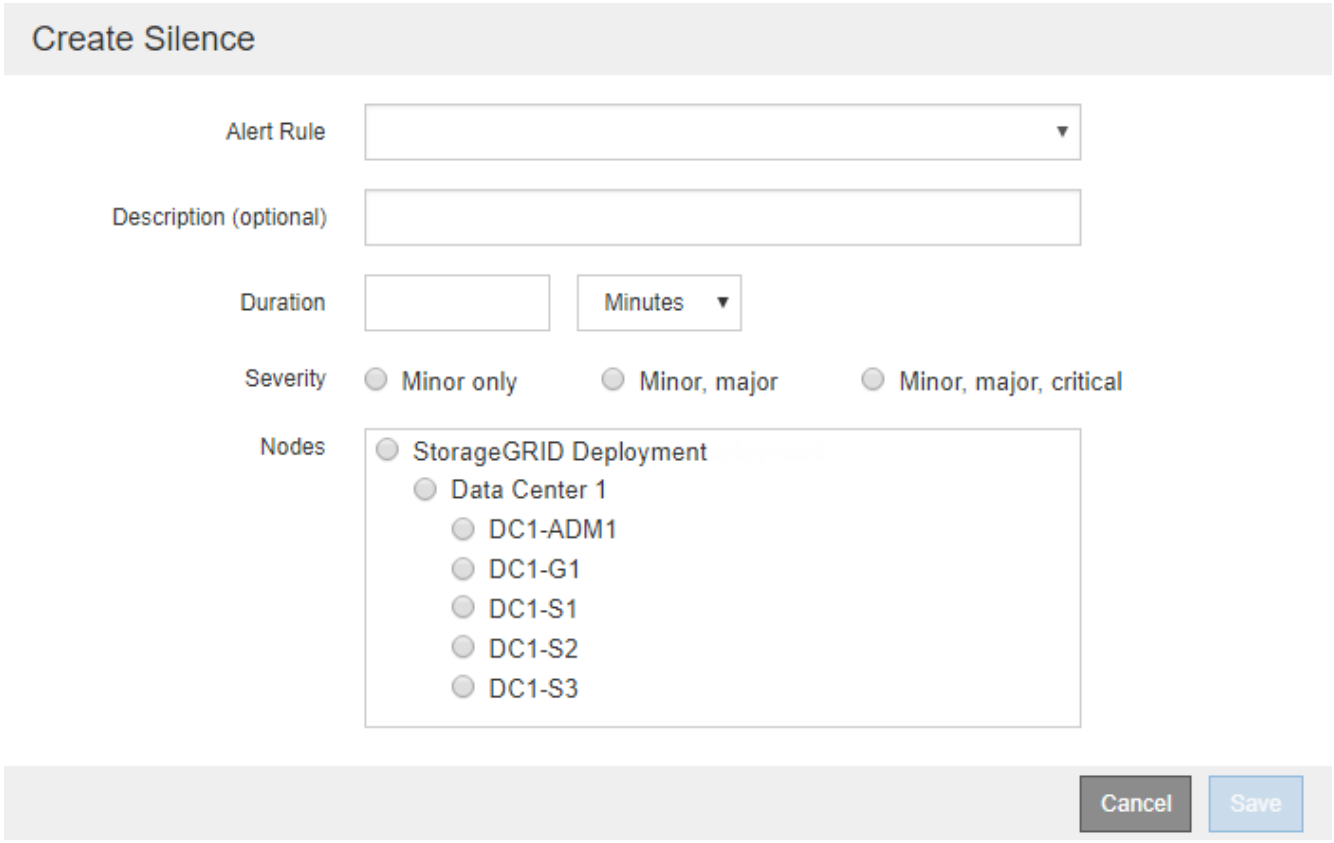
1. Seleziona **Avvisi** > **Silenzi**.

   Viene visualizzata la pagina Silences.



2. Seleziona **Create**.

   Viene visualizzata la finestra di dialogo Crea Silence.



3. Seleziona o inserisci le seguenti informazioni:

Campo	Descrizione
Regola di alert	Il nome della regola di avviso che vuoi silenziare. Puoi selezionare qualsiasi regola di avviso predefinita o personalizzata, anche se la regola di avviso è disabilitata. **Nota:** Seleziona **Tutte le regole** se vuoi silenziare tutte le regole di avviso usando i criteri specificati in questa finestra di dialogo.

Campo	Descrizione
Descrizione	Facoltativamente, una descrizione del silenzio. Ad esempio, descrivi lo scopo di questo silenzio.
Durata	Per quanto tempo desideri che questo silenzio rimanga in vigore, in minuti, ore o giorni. Un silenzio può essere in vigore da 5 minuti a 1.825 giorni (5 anni). **Nota:** Non dovresti silenziare una regola di avviso per un periodo di tempo prolungato. Se una regola di avviso viene silenziata, potresti non rilevare un problema sottostante finché non impedisce il completamento di un'operazione critica. Tuttavia, potresti dover usare un silenziamento prolungato se un avviso viene attivato da una configurazione specifica e intenzionale, come nel caso degli avvisi **Services appliance link down** e **Storage appliance link down**.
Gravità	Quale o quali livelli di gravità dell'avviso devono essere silenziati. Se l'avviso viene attivato a uno dei livelli di gravità selezionati, non vengono inviate notifiche.
Nodi	A quale nodo o nodi vuoi applicare questo silenziamento. Puoi sopprimere una regola di avviso o tutte le regole sull'intera griglia, su un singolo sito o su un singolo nodo. Se selezioni l'intera griglia, il silenziamento si applica a tutti i siti e a tutti i nodi. Se selezioni un sito, il silenziamento si applica solo ai nodi di quel sito. **Nota:** Non puoi selezionare più di un nodo o più di un sito per ogni silenziamento. Devi creare silenziamenti aggiuntivi se vuoi sopprimere la stessa regola di avviso su più di un nodo o più di un sito contemporaneamente.

4. Seleziona **Salva**.
5. Se vuoi modificare o interrompere un silenzio prima che scada, puoi modificarlo o rimuoverlo.

Opzione	Descrizione
Modifica un silenzio	a. Seleziona **Avvisi** > **Silenzi**. b. Dalla tabella, seleziona il pulsante di opzione per il silenzio che vuoi modificare. c. Seleziona **Modifica**. d. Modifica la descrizione, il tempo rimanente, le gravità selezionate o il nodo interessato. e. Seleziona **Salva**.

Opzione	Descrizione
Rimuovi un silenzio	a. Seleziona **Avvisi** > **Silenzi**. b. Dalla tabella, seleziona il pulsante di opzione per il silenzio che vuoi rimuovere. c. Seleziona **Rimuovi**. d. Seleziona **OK** per confermare che vuoi rimuovere questo silenzio. **Nota**: Le notifiche verranno ora inviate quando questo avviso viene attivato (a meno che non siano soppresse da un altro silenzio). Se questo avviso è attualmente attivato, potrebbero essere necessari alcuni minuti prima che le notifiche email o SNMP vengano inviate e che la pagina degli avvisi venga aggiornata.

Informazioni correlate

"Configura l'agente SNMP"

Avvisi in StorageGRID

Questo documento elenca gli avvisi predefiniti visualizzati in Grid Manager. Le azioni consigliate sono nel messaggio di avviso che ricevi.

Se necessario, puoi creare regole di avviso personalizzate per adattarle al tuo approccio di gestione del sistema.

Alcuni degli avvisi predefiniti utilizzano "metriche Prometheus".

Avvisi sull'appliance

Nome dell'allerta	Descrizione
Batteria dell'appliance scaduta	La batteria dello storage controller dell'appliance è scarica.
La batteria dell'appliance si è guastata	La batteria dello storage controller si è guastata.
La batteria dell'appliance ha una capacità appresa insufficiente	La batteria dello storage controller dell'appliance ha una capacità appresa insufficiente.
Batteria dell'appliance in fase di esaurimento	La batteria dello storage controller dell'appliance sta per esaurirsi.
Batteria dell'appliance rimossa	La batteria dello storage controller è mancante.
La batteria dell'appliance è troppo calda	La batteria dello storage controller è surriscaldata.

Nome dell'allerta	Descrizione
Errore di comunicazione BMC dell'appliance	La comunicazione con il controller di gestione della scheda di base (BMC) è stata persa.
Rilevato guasto al dispositivo di avvio dell'appliance	È stato rilevato un problema con il dispositivo di avvio nell'appliance.
Il dispositivo di backup della cache dell'appliance non è riuscito	Si è verificato un errore nel dispositivo di backup della cache persistente.
Capacità insufficiente del dispositivo di backup della cache dell'appliance	La capacità del dispositivo di backup della cache è insufficiente.
Dispositivo di backup della cache dell'appliance protetto da scrittura	Un dispositivo di backup della cache è protetto da scrittura.
Dimensione della memoria cache dell'appliance non corrispondente	I due controller presenti nell'apparecchio hanno dimensioni di cache diverse.
Guasto della batteria CMOS dell'appliance	È stato rilevato un problema con la batteria CMOS nell'apparecchio.
Temperatura dello chassis del controller di elaborazione dell'appliance troppo elevata	La temperatura del compute controller in un'appliance StorageGRID ha superato una soglia nominale.
Temperatura della CPU del controller di elaborazione dell'appliance troppo alta	La temperatura della CPU nel compute controller in un'appliance StorageGRID ha superato una soglia nominale.
Il controller di elaborazione dell'appliance necessita di attenzione	È stato rilevato un guasto hardware nel compute controller di un appliance StorageGRID.
L'alimentatore del compute controller dell'appliance A ha un problema	L'alimentatore A del controller di calcolo presenta un problema.
L'alimentatore del controller di elaborazione dell'appliance B ha un problema	L'alimentatore B del controller di calcolo ha un problema.
Il servizio di monitoraggio dell'hardware di elaborazione dell'appliance è bloccato	Il servizio che monitora lo stato dell'hardware di archiviazione si è bloccato.

Nome dell'allerta	Descrizione
L'unità DAS dell'appliance supera il limite di dati scritti al giorno	Ogni giorno viene scritta una quantità eccessiva di dati sull'unità, il che potrebbe invalidarne la garanzia.
Rilevato guasto all'unità DAS dell'appliance	È stato rilevato un problema con un'unità di archiviazione ad accesso diretto (DAS) nell'appliance.
L'unità DAS dell'appliance si trova nello slot o nel nodo sbagliato	Un'unità di archiviazione ad accesso diretto (DAS) si trova nello slot o nel nodo sbagliato
Spia di localizzazione dell'unità DAS dell'appliance accesa	La spia di localizzazione dell'unità per una o più unità di archiviazione collegate direttamente (DAS) in un Storage Node dell'appliance è accesa.
Ricostruzione dell'unità DAS dell'appliance	Un'unità di archiviazione ad accesso diretto (DAS) è in fase di ricostruzione. Questo è previsto se è stata recentemente sostituita o rimossa/reinserita.
Rilevato guasto alla ventola dell'appliance	È stato rilevato un problema con un'unità di ventilazione nell'appliance.
Rilevato guasto Fibre Channel dell'appliance	È stato rilevato un problema di collegamento Fibre Channel tra lo storage controller dell'appliance e il compute controller.
Guasto alla porta HBA Fibre Channel dell'appliance	Una porta HBA Fibre Channel sta fallendo o ha già fallito.
Unità di cache flash dell'appliance non ottimali	Le unità utilizzate per la cache SSD non sono ottimali.
Interconnessione appliance/contenitore della batteria rimosso	Il canister interconnect/batteria è mancante.
Porta LACP dell'appliance mancante	Una porta su un'appliance StorageGRID non partecipa al bond LACP.
Rilevato guasto alla scheda di interfaccia di rete dell'apparecchio	È stato rilevato un problema con una scheda di interfaccia di rete (NIC) nell'appliance.
Alimentazione elettrica complessiva dell'appliance degradata	La potenza di un'appliance StorageGRID si è discostata dalla tensione di funzionamento raccomandata.
È necessario aggiornare il software SANtricity OS dell'appliance	La versione del software SANtricity è inferiore al minimo consigliato per questa release di StorageGRID.

Nome dell’allerta	Descrizione
Avviso critico sull’SSD del dispositivo	Un’unità SSD di un appliance sta segnalando un avviso critico.
Guasto allo storage controller dell’appliance A	Lo storage controller A in un’appliance StorageGRID ha smesso di funzionare.
Guasto dello storage controller B dell’appliance	Lo storage controller B in un’appliance StorageGRID ha smesso di funzionare.
Guasto dell’unità del controller di storage dell’appliance	Uno o più dischi in un’appliance StorageGRID hanno smesso di funzionare o non sono ottimali.
Problema hardware dello storage controller dell’appliance	Il software SANtricity segnala "Necessita di attenzione" per un componente in un’appliance StorageGRID.
Guasto all’alimentatore dello storage controller dell’appliance	L’alimentatore A in un’appliance StorageGRID ha deviato dalla tensione di esercizio raccomandata.
Guasto all’alimentatore B dello storage controller dell’appliance	L’alimentatore B in un’appliance StorageGRID si è discostato dalla tensione di esercizio raccomandata.
Il servizio di monitoraggio dell’hardware di storage dell’appliance è bloccato	Il servizio che monitora lo stato dell’hardware di archiviazione si è bloccato.
Ripiani di storage dell’appliance degradati	Lo stato di uno dei componenti dello shelf di storage di un storage appliance è degradato.
Temperatura dell’appliance superata	La temperatura nominale o massima dello storage controller è stata superata.
Sensore di temperatura dell’appliance rimosso	È stato rimosso un sensore di temperatura.
Errore di avvio protetto UEFI dell’appliance	Un dispositivo non è stato avviato in modo sicuro.
L’I/O del disco è molto lento	Le operazioni di I/O del disco molto lente potrebbero influire sulle prestazioni del grid.
Rilevato guasto alla ventola dell’appliance di storage	È stato rilevato un problema con un’unità ventola nello storage controller di un appliance.
Connettività di storage dell’appliance degradata	C’è un problema con una o più connessioni tra il compute controller e lo storage controller.

Nome dell'allerta	Descrizione
Dispositivo di storage inaccessibile	Impossibile accedere al dispositivo di storage.

Avvisi di audit e syslog

Nome dell'allerta	Descrizione
I log di controllo vengono aggiunti alla coda in memoria	Node non riesce a inviare i log al syslog server locale e la coda in memoria si sta riempiendo.
Errore di inoltro del server syslog esterno	Node non può inoltrare i log al server syslog esterno.
Lunga coda di audit	La coda su disco per i messaggi di audit è piena. Se questo problema non viene risolto, le operazioni S3 potrebbero non riuscire.
I log vengono aggiunti alla coda su disco	Node non riesce a inoltrare i log al server syslog esterno e la coda su disco si sta riempiendo.

Avvisi bucket

Nome dell'allerta	Descrizione
FabricPool bucket ha un'impostazione di coerenza del bucket non supportata	Un bucket FabricPool utilizza il livello di coerenza Available o Strong-site, che non è supportato.
FabricPool bucket ha un'impostazione di versioning non supportata	Un bucket FabricPool ha la gestione delle versioni o il blocco degli oggetti S3 abilitati, che non sono supportati.

Avvisi Cassandra

Nome dell'allerta	Descrizione
Errore del compattatore automatico di Cassandra	Il compattatore automatico di Cassandra ha riscontrato un errore.
Le metriche di auto-compactor di Cassandra non sono aggiornate	Le metriche che descrivono l'auto-compactor di Cassandra sono obsolete.
Errore di comunicazione Cassandra	I nodi che eseguono il servizio Cassandra stanno avendo problemi a comunicare tra loro.
Compaction di Cassandra sovraccariche	Il processo di compaction di Cassandra è sovraccarico.

Nome dell'allerta	Descrizione
Errore di scrittura sovradimensionata in Cassandra	Un processo interno di StorageGRID ha inviato a Cassandra una richiesta di scrittura troppo grande.
Le metriche di repair di Cassandra non sono aggiornate	Le metriche che descrivono i job di riparazione di Cassandra sono obsolete.
Avanzamento della riparazione di Cassandra lento	L'avanzamento delle riparazioni del database Cassandra è lento.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione di Cassandra non è disponibile.
Corruzione della tabella Cassandra	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva un danneggiamento della tabella.

Avvisi relativi ai Cloud Storage Pool

Nome dell'allerta	Descrizione
Errore di connettività del pool di storage cloud	Il controllo di integrità dei Cloud Storage Pools ha rilevato uno o più nuovi errori.
Scadenza della certificazione dell'entità finale IAM Roles Anywhere	Il certificato dell'entità finale di IAM Roles Anywhere sta per scadere.

Avvisi di replica cross-grid

Nome dell'allerta	Descrizione
Guasto permanente della replica cross-grid	Si è verificato un errore di replica tra griglie che richiede l'intervento dell'utente per essere risolto.
Risorse di replica cross-grid non disponibili	Le richieste di replica tra griglie sono in sospeso perché una risorsa non è disponibile.

Avvisi DHCP

Nome dell'allerta	Descrizione
Lease DHCP scaduto	Il lease DHCP su una scheda di interfaccia di rete è scaduto.
Il lease DHCP sta per scadere	Il lease DHCP su un'interfaccia di rete sta per scadere.
Server DHCP non disponibile	Il server DHCP non è disponibile.

Avvisi di debug e tracciamento

Nome dell'allerta	Descrizione
Impatto sulle prestazioni del debug	Quando la modalità di debug è abilitata, le prestazioni del sistema potrebbero essere influenzate negativamente.
Configurazione di tracciamento abilitata	Quando la configurazione di traccia è abilitata, le prestazioni del sistema potrebbero essere influenzate negativamente.

Email e avvisi AutoSupport

Nome dell'allerta	Descrizione
AutoSupport messaggio non inviato	L'ultimo messaggio AutoSupport non è stato inviato.
Errore nella risoluzione del nome di dominio	Il nodo StorageGRID non è stato in grado di risolvere i nomi di dominio.
Notifica e-mail non riuscita	Impossibile inviare la notifica e-mail relativa all'avviso.
Bucket di destinazione per l'archiviazione dei log non trovato	Il bucket di destinazione per l'archiviazione dei log non è presente, il che impedisce l'archiviazione dei log nel bucket di destinazione.
errori inform SNMP	Errori durante l'invio delle notifiche SNMP inform a una destinazione trap.
Accesso esterno SSH abilitato	L'accesso SSH esterno è abilitato da più di 24 ore.
Rilevato accesso SSH o console	Nelle ultime 24 ore, un utente ha effettuato l'accesso tramite Web Console o SSH.

Avvisi di erasure coding (EC)

Nome dell'allerta	Descrizione
Errore di ribilanciamento EC	La procedura di ribilanciamento EC non è riuscita o è stata interrotta.
guasto alla riparazione EC	Un'operazione di riparazione dei dati EC non è riuscita o è stata interrotta.
Riparazione EC bloccata	Un intervento di riparazione dei dati EC si è bloccato.
Errore di verifica del frammento con codifica di cancellazione	I frammenti codificati con il metodo di cancellazione non possono più essere verificati. I frammenti corrotti potrebbero non essere riparati.

Avvisi di scadenza dei certificati

Nome dell'allerta	Descrizione
Scadenza del certificato CA del proxy admin	Uno o più certificati nel bundle CA del proxy server amministrativo stanno per scadere.
Scadenza del certificato client	Uno o più certificati client stanno per scadere.
Scadenza del certificato server globale per S3	Il certificato server globale per S3 sta per scadere.
Scadenza del certificato dell'endpoint del bilanciatore di carico	Uno o più certificati degli endpoint del load balancer stanno per scadere.
Scadenza del certificato del server per l'interfaccia di gestione	Il certificato del server utilizzato per l'interfaccia di gestione sta per scadere.
Scadenza del certificato CA syslog esterno	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server syslog esterno sta per scadere.
Scadenza del certificato del client syslog esterno	Il certificato client per un syslog server esterno sta per scadere.
Scadenza del certificato del server syslog esterno	Il certificato del server presentato dal server syslog esterno sta per scadere.

Avvisi della Grid Network

Nome dell'allerta	Descrizione
Mancata corrispondenza dell'MTU nella rete di griglia	L'impostazione MTU per l'interfaccia Grid Network (eth0) varia significativamente tra i nodi della griglia.

Avvisi di federazione della grid

Nome dell'allerta	Descrizione
Scadenza del certificato di federazione della grid	Uno o più certificati di federazione della grid stanno per scadere.
Errore di connessione alla federazione di grid	La connessione di federazione tra la grid locale e quella remota non funziona.

Avvisi di utilizzo elevato o latenza elevata

Nome dell'allerta	Descrizione
Elevato utilizzo della Java heap	Stai usando una percentuale elevata di spazio heap Java.
Latenza elevata per le query sui metadati	Il tempo medio delle query sui metadati di Cassandra è troppo lungo.

Avvisi di federazione delle identità

Nome dell'allerta	Descrizione
Errore di sincronizzazione della federazione delle identità	Impossibile sincronizzare gruppi e utenti federati dall'origine dell'identità.
Errore di sincronizzazione della federazione delle identità per un tenant	Impossibile sincronizzare gruppi e utenti federati dall'origine di identità configurata da un tenant.

Avvisi di gestione del ciclo di vita delle informazioni (ILM)

Nome dell'allerta	Descrizione
Posizionamento ILM irraggiungibile	Non è possibile eseguire un'istruzione di posizionamento in una regola ILM per determinati oggetti.
frequenza di scansione ILM bassa	La frequenza di scansione dell'ILM è impostata a meno di 100 oggetti/secondo.

Avvisi del server di gestione delle chiavi (KMS)

Nome dell'allerta	Descrizione
Scadenza del certificato KMS CA	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del key management server (KMS) sta per scadere.
Scadenza del certificato client KMS	Il certificato client per un server di gestione delle chiavi sta per scadere
Impossibile caricare la configurazione KMS	La configurazione per il server di gestione delle chiavi esiste ma non è stato possibile caricarla.
${post_edited_translations.segment}	Un nodo dell'appliance non riesce a connettersi al key management server per il suo sito.
${post_edited_translations.segment}	Il server di gestione delle chiavi configurato non dispone di una chiave di crittografia che corrisponde al nome fornito.
${post_edited_translations.segment}	Tutti i volumi dell'appliance sono stati decrittografati correttamente, ma uno o più volumi non sono riusciti a ruotare alla chiave più recente.

Nome dell’allerta	Descrizione
${post_edited_translations.segment}	Non esiste un server di gestione delle chiavi per questo sito.
La chiave KMS non è riuscita a decrittografare un volume dell’appliance	Uno o più volumi su un appliance con crittografia del nodo abilitata non possono essere decrittografati con la chiave KMS corrente.
Scadenza del certificato del server KMS	Il certificato del server utilizzato dal server di gestione delle chiavi (KMS) sta per scadere.
Errore di connettività del server KMS	Un nodo dell’appliance non è riuscito a connettersi a uno o più server nel cluster del key management server per il suo sito.

Avvisi del load balancer

Nome dell’allerta	Descrizione
Connessioni di bilanciamento del carico zero-request elevate	Un’elevata percentuale di connessioni agli endpoint del bilanciatore di carico si è disconnessa senza eseguire richieste.

Avvisi di scostamento dell’orologio locale

Nome dell’allerta	Descrizione
Grande scostamento orario dell’orologio locale	Lo scostamento tra l’orologio locale e l’ora del Network Time Protocol (NTP) è troppo grande.

Avvisi di memoria insufficiente o spazio insufficiente

Nome dell’allerta	Descrizione
Capacità disco dei log di controllo insufficiente	Lo spazio disponibile per i log di controllo è insufficiente. Se questo problema non viene risolto, le operazioni S3 potrebbero non riuscire.
Memoria disponibile del nodo insufficiente	La quantità di RAM disponibile su un nodo è bassa.
Poco spazio libero per pool di storage	Lo spazio disponibile per l’archiviazione dei dati degli oggetti nello Storage Node è basso.
Memoria installata del nodo insufficiente	La quantità di memoria installata su un nodo è bassa.
Archiviazione di metadati ridotta	Lo spazio disponibile per l’archiviazione dei metadati è basso.

Nome dell'allerta	Descrizione
Bassa capacità del disco delle metriche	Lo spazio disponibile per il database delle metriche è basso.
Storage dati oggetto basso	Lo spazio disponibile per l'archiviazione dei dati degli oggetti è basso.
Sovrascrittura della soglia di sola lettura a basso livello	La soglia di override della watermark di sola lettura del volume di storage è inferiore alla soglia minima ottimizzata per un Storage Node.
Bassa capacità del disco di root	Lo spazio disponibile sul disco di root è basso.
Capacità di dati di sistema ridotta	Lo spazio disponibile per /var/local è insufficiente. Se questo problema non viene risolto, le operazioni S3 potrebbero non riuscire.
Spazio libero della directory tmp basso	Lo spazio disponibile nella directory /tmp è insufficiente.

Avvisi relativi al nodo o alla rete di nodi

Nome dell'allerta	Descrizione
Quorum ADC non raggiunto	Il nodo di archiviazione con servizio ADC è offline. Le operazioni di espansione e decommissionare sono bloccate fino al ripristino del quorum ADC.
Utilizzo della rete Admin	L'utilizzo della ricezione sulla rete di amministrazione è elevato.
Utilizzo della trasmissione della rete Admin	L'utilizzo della banda di trasmissione sulla rete amministrativa è elevato.
Errore di configurazione del firewall	Impossibile applicare la configurazione del firewall.
Endpoint dell'interfaccia di gestione in modalità fallback	Tutti gli endpoint dell'interfaccia di gestione stanno tornando alle porte predefinite da troppo tempo.
Errore di connettività di rete del nodo	Si sono verificati errori durante il trasferimento dei dati tra i nodi.
Errore di ricezione del frame nella rete del nodo	Un'alta percentuale dei frame di rete ricevuti da un nodo aveva errori.
Nodo non sincronizzato con server NTP	Il nodo non è sincronizzato con il server NTP.
Nodo non bloccato con server NTP	Il nodo non è vincolato a un server NTP.

Nome dell'allerta	Descrizione
Rete dei nodi non-appliance inattiva	Uno o più dispositivi di rete sono offline o disconnessi.
Collegamento del dispositivo di servizio non funzionante sulla rete amministrativa	L'interfaccia del dispositivo verso la rete di amministrazione (eth1) è disattivata o disconnessa.
Collegamento del dispositivo di servizio interrotto sulla porta 1 della Admin Network	La porta di rete Admin 1 sull'appliance è offline o disconnessa.
Collegamento del dispositivo di servizio interrotto sulla rete client	L'interfaccia del dispositivo verso la Client Network (eth2) è inattiva o disconnessa.
Collegamento del dispositivo di servizio interrotto sulla porta di rete 1	La porta di rete 1 sull'appliance è offline o disconnessa.
Collegamento del dispositivo di servizio interrotto sulla porta di rete 2	La porta di rete 2 sull'appliance è offline o disconnessa.
Collegamento del services appliance interrotto sulla porta di rete 3	La porta di rete 3 sull'appliance è offline o disconnessa.
Collegamento del dispositivo di servizio interrotto sulla porta di rete 4	La porta di rete 4 sull'appliance è down o disconnessa.
Collegamento del dispositivo di storage non funzionante sulla rete Admin	L'interfaccia del dispositivo verso la rete di amministrazione (eth1) è disattivata o disconnessa.
Collegamento del dispositivo di storage interrotto sulla porta 1 della Admin Network	La porta di rete Admin 1 sull'appliance è offline o disconnessa.
Collegamento del dispositivo di storage interrotto sulla rete client	L'interfaccia del dispositivo verso la Client Network (eth2) è inattiva o disconnessa.
Collegamento storage appliance interrotto sulla porta di rete 1	La porta di rete 1 sull'appliance è offline o disconnessa.
Collegamento del dispositivo di storage interrotto sulla porta di rete 2	La porta di rete 2 sull'appliance è offline o disconnessa.

Nome dell'allerta	Descrizione
Collegamento storage appliance interrotto sulla porta di rete 3	La porta di rete 3 sull'appliance è offline o disconnessa.
Collegamento del dispositivo di storage interrotto sulla porta di rete 4	La porta di rete 4 sull'appliance è down o disconnessa.
Il nodo di storage non è nello stato di storage desiderato	Il servizio LDR su un nodo di archiviazione non può passare allo stato desiderato a causa di un errore interno o di un problema relativo al volume
utilizzo della connessione TCP	Il numero di connessioni TCP su questo nodo si sta avvicinando al numero massimo che può essere tracciato.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono oppure il nodo non è raggiungibile.
Riavvio imprevisto del nodo	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore.

Avvisi sugli oggetti

Nome dell'allerta	Descrizione
Verifica dell'esistenza dell'oggetto fallita	Il processo di verifica dell'esistenza dell'oggetto non è riuscito.
Verifica dell'esistenza dell'oggetto bloccata	Il processo di verifica dell'esistenza dell'oggetto si è bloccato.
Oggetti potenzialmente persi	Uno o più oggetti potenzialmente persi dalla griglia.
Oggetti orfani rilevati	Sono stati rilevati oggetti orfani.
Dimensione oggetto S3 PUT troppo grande	Un client sta tentando un'operazione PUT Object che supera i limiti di dimensione di S3.
Rilevato oggetto corrotto non identificato	È stato trovato un file nello storage a oggetti replicato che non è stato possibile identificare come oggetto replicato.

Avvisi di danneggiamento degli oggetti

Nome dell'allerta	Descrizione
Discrepanza nelle dimensioni dell'oggetto	Dimensione oggetto inattesa rilevata durante la procedura di verifica dell'esistenza dell'oggetto.

Avvisi dei servizi della piattaforma

Nome dell'allerta	Descrizione
Capacità delle richieste in sospeso dei Platform Services bassa	Il numero di richieste in sospeso per i Platform Services si sta avvicinando alla capacità.
Servizi della piattaforma non disponibili	Sono in esecuzione o disponibili troppo pochi Storage Node con il servizio RSM in un sito.

Avvisi relativi al volume di storage

Nome dell'allerta	Descrizione
Il volume di storage necessita di attenzione	Un volume di archiviazione è offline e richiede attenzione.
È necessario ripristinare il volume di storage	È stato recuperato un volume di storage che deve essere ripristinato.
volume di storage offline	Un volume di storage è offline da più di 5 minuti.
Tentativo di rimontaggio del volume di archiviazione	Un volume di archiviazione era offline e ha attivato un rimontaggio automatico. Questo potrebbe indicare un problema con l'unità o errori del filesystem.
Il ripristino del volume non è riuscito ad avviare la riparazione dei dati replicati	Non è stato possibile avviare automaticamente la riparazione dei dati replicati per un volume riparato.

Avvisi dei servizi StorageGRID

Nome dell'allerta	Descrizione
Servizio nginx che utilizza la configurazione del backup	La configurazione del servizio nginx non è valida. Ora viene utilizzata la configurazione precedente.
Servizio nginx-gw che utilizza la configurazione del backup	La configurazione del servizio nginx-gw non è valida. Ora viene utilizzata la configurazione precedente.
Riavvio necessario per disabilitare FIPS	La politica di sicurezza non richiede la modalità FIPS, ma i moduli FIPS sono in uso.
Riavvia per abilitare FIPS	La politica di sicurezza richiede la modalità FIPS, ma i moduli FIPS non sono in uso.
Servizio SSH che utilizza la configurazione del backup	La configurazione del servizio SSH non è valida. Ora viene utilizzata la configurazione precedente.

Avvisi tenant

Nome dell'allerta	Descrizione
Elevato utilizzo della quota del tenant	Viene utilizzata un'elevata percentuale dello spazio di quota. Questa regola è disabilitata per impostazione predefinita perché potrebbe generare troppe notifiche.

Metriche Prometheus comunemente utilizzate in StorageGRID

Consulta questo elenco di metriche Prometheus comunemente utilizzate per comprendere meglio le condizioni delle regole di avviso predefinite o per definire le condizioni delle regole di avviso personalizzate.

Puoi anche ottenere un elenco completo di tutte le metriche.

Per i dettagli sulla sintassi delle query di Prometheus, vedi "Interrogare Prometheus".

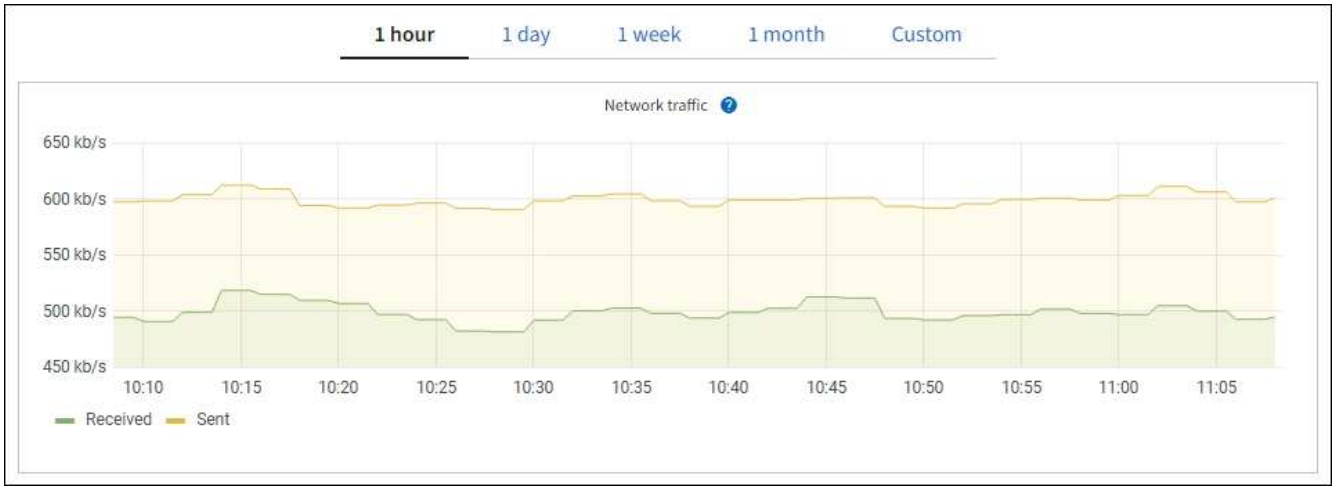
Che cosa sono le metriche di Prometheus?

Le metriche Prometheus sono misurazioni di serie temporali. Il servizio Prometheus sui nodi di amministrazione raccoglie queste metriche dai servizi su tutti i nodi. Le metriche vengono memorizzate su ciascun nodo di amministrazione fino a quando lo spazio riservato ai dati di Prometheus è pieno. Quando il `/var/local/mysql_ibdata/` volume raggiunge la capacità, le metriche più vecchie vengono eliminate per prime.

Dove vengono utilizzate le metriche di Prometheus?

Le metriche raccolte da Prometheus vengono utilizzate in diversi punti del Grid Manager:

- **Pagina Nodi**: I grafici e i diagrammi presenti nelle schede disponibili nella pagina Nodi utilizzano lo strumento di visualizzazione Grafana per mostrare le metriche delle serie temporali raccolte da Prometheus. Grafana visualizza i dati delle serie temporali in formato grafico e diagrammatico, mentre Prometheus funge da origine dati backend.



- **Avvisi**: Gli avvisi vengono attivati a specifici livelli di gravità quando le condizioni delle regole di avviso che utilizzano metriche Prometheus risultano vere.
- **Grid Management API**: Puoi usare le metriche Prometheus nelle regole di avviso personalizzate o con

strumenti di automazione esterni per monitorare il tuo sistema StorageGRID. Un elenco completo delle metriche Prometheus è disponibile tramite la Grid Management API. (Dalla parte superiore di Grid Manager, seleziona l'icona di aiuto e scegli **API documentation** > **metrics**.) Anche se sono disponibili oltre mille metriche, solo un numero relativamente piccolo è necessario per monitorare le operazioni StorageGRID più critiche.

> Le metriche che includono *private* nel loro nome sono destinate esclusivamente all'uso interno e sono soggette a modifiche tra le versioni di StorageGRID senza preavviso.

- Le pagine **Supporto** > **Strumenti** > **Diagnostica** e **Supporto** > **Strumenti** > **Metriche**: queste pagine, destinate principalmente all'utilizzo da parte del supporto tecnico, forniscono diversi strumenti e grafici che utilizzano i valori delle metriche Prometheus.

> Alcune funzionalità e voci di menu all'interno della pagina Metriche sono intenzionalmente non funzionanti e sono soggette a modifiche.

Elenco delle metriche più comuni

Il seguente elenco contiene le metriche Prometheus più comunemente utilizzate.

> Le metriche che includono *private* nel loro nome sono destinate esclusivamente all'uso interno e sono soggette a modifiche senza preavviso tra una versione e l'altra di StorageGRID.

alertmanager_notifications_failed_total
Il numero totale di notifiche di avviso non riuscite.

node_filesystem_avail_bytes
Quantità di spazio file system disponibile per gli utenti non root, in byte.

node_memory_MemAvailable_bytes
Campo delle informazioni sulla memoria MemAvailable_bytes.

node_network_carrier
Valore del vettore `/sys/class/net/iface`.

node_network_receive_errs_total
Statistiche del dispositivo di rete `receive_errs`.

node_network_transmit_errs_total
Statistiche del dispositivo di rete `transmit_errs`.

storagegrid_amministrativamente_disattivato
Il nodo non è connesso alla grid per un motivo previsto. Ad esempio, il nodo, o i servizi sul nodo, sono stati arrestati correttamente, il nodo è in fase di riavvio oppure il software è in fase di aggiornamento.

stato hardware del controller di calcolo dell'appliance StorageGRID
Lo stato dell'hardware del compute controller in un appliance.

dischi guasti dell'appliance StorageGRID
Per lo storage controller in un appliance, il numero di drive che non sono ottimali.

storagegrid_appliance_storage_controller_hardware_status

Lo stato generale dell'hardware dello storage controller in un appliance.

bucket e container di StorageGRID

Il numero totale di bucket S3 noti a questo Storage Node.

storagegrid_content_objects

Il numero totale di oggetti dati S3 noti a questo Storage Node. Il conteggio è valido solo per gli oggetti dati creati dalle applicazioni client che interagiscono con il sistema tramite S3.

storagegrid_content_objects_lost

Il numero totale di oggetti che questo servizio rileva come mancanti dal sistema StorageGRID. Dovresti intervenire per determinare la causa della perdita e se è possibile recuperarli.

"Risolvi i problemi relativi ai dati degli oggetti persi o mancanti"

storagegrid_http_sessions_incoming_attempted

Il numero totale di sessioni HTTP che sono state tentate verso uno Storage Node.

storagegrid_http_sessions_incoming_currently_established

Il numero di sessioni HTTP attualmente attive (aperte) sullo Storage Node.

storagegrid_http_sessions_incoming_failed

Il numero totale di sessioni HTTP che non sono state completate con successo, a causa di una richiesta HTTP non valida o di un errore durante l'elaborazione di un'operazione.

storagegrid_http_sessions_incoming_successful

Il numero totale di sessioni HTTP completate con successo.

storagegrid_ilm_awaiting_background_objects

Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalla scansione.

storagegrid_ilm_awaiting_client_evaluation_objects_per_second

La frequenza attuale con cui gli oggetti vengono valutati rispetto alla policy ILM su questo nodo.

storagegrid_ilm_awaiting_client_objects

Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalle operazioni del client (ad esempio, ingest).

storagegrid_ilm_awaiting_total_objects

Il numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_objects_per_second

La frequenza con cui gli oggetti di proprietà di questo nodo vengono scansionati e messi in coda per ILM.

minuti stimati del periodo di scansione ILM di StorageGRID

Tempo stimato per completare una scansione ILM completa su questo nodo.

Nota: Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti di proprietà di questo nodo.

tempo di scadenza del certificato dell'endpoint del load balancer di StorageGRID

Il tempo di scadenza del certificato dell'endpoint del load balancer in secondi dall'epoca.

latenza media delle query sui metadati di StorageGRID in millisecondi

Il tempo medio necessario per eseguire una query sullo store dei metadati tramite questo servizio.

byte ricevuti dalla rete StorageGRID

Quantità totale di dati ricevuti dall'installazione.

byte trasmessi dalla rete StorageGRID

Quantità totale di dati inviati dall'installazione.

percentuale di utilizzo della CPU del nodo StorageGRID

La percentuale di tempo CPU disponibile attualmente utilizzata da questo servizio. Indica quanto il servizio sia occupato. La quantità di tempo CPU disponibile dipende dal numero di CPU del server.

storagegrid_ntp_chosen_time_source_offset_milliseconds

Offset sistematico dell'ora fornito da una sorgente oraria selezionata. L'offset viene introdotto quando il ritardo per raggiungere una sorgente oraria non è uguale al tempo necessario affinché la sorgente oraria raggiunga il client NTP.

storagegrid_ntp_locked

Il nodo non è vincolato a un server Network Time Protocol (NTP).

storagegrid_s3_data_transfers_bytes_ingested

La quantità totale di dati acquisiti dai client S3 in questo Storage Node dall'ultimo ripristino dell'attributo.

storagegrid_s3_data_transfers_bytes_retrieved

La quantità totale di dati recuperati dai client S3 da questo Storage Node dall'ultimo ripristino dell'attributo.

storagegrid_s3_operations_failed

Numero totale di operazioni S3 non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da errori di autorizzazione S3.

storagegrid_s3_operations_successful

Numero totale di operazioni S3 riuscite (codice di stato HTTP 2xx).

storagegrid_s3_operations_unauthorized

Il numero totale di operazioni S3 non riuscite a causa di un errore di autorizzazione.

storagegrid_servercertificate_management_interface_cert_expiry_days

Il numero di giorni prima che il certificato dell'interfaccia di gestione scada.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

Il numero di giorni prima che il certificato dell'API Object Storage scada.

storagegrid_service_cpu_seconds

Il tempo complessivo in cui la CPU è stata utilizzata da questo servizio dall'installazione.

storagegrid_service_memory_usage_bytes

La quantità di memoria (RAM) attualmente utilizzata da questo servizio. Questo valore è identico a quello visualizzato dall'utility top di Linux come RES.

byte ricevuti dalla rete di servizi di StorageGRID

La quantità totale di dati ricevuti da questo servizio dall'installazione.

byte trasmessi dalla rete del servizio StorageGRID

Quantità totale di dati inviati da questo servizio.

riavvii del servizio StorageGRID

Il numero totale di volte in cui il servizio è stato riavviato.

storagegrid_service_runtime_seconds

Il tempo totale in cui il servizio è stato in esecuzione dall'installazione.

storagegrid_service_uptime_seconds

Il tempo totale in cui il servizio è stato in esecuzione dall'ultimo riavvio.

storagegrid_storage_state_current

Stato attuale dei servizi di storage. I valori degli attributi sono:

- 10 = Offline
- 15 = Manutenzione
- 20 = Sola lettura
- 30 = Online

storagegrid_storage_status

Stato attuale dei servizi di storage. I valori degli attributi sono:

- 0 = Nessun errore
- 10 = In transizione
- 20 = Spazio libero insufficiente
- 30 = Volume(i) non disponibili
- 40 = Errore

storagegrid_storage_utilization_data_bytes

Una stima della dimensione totale dei dati degli oggetti replicati e codificati con cancellazione sul Storage Node.

storagegrid_storage_utilization_metadata_allowed_bytes

Lo spazio totale sul volume 0 di ciascun Storage Node che è consentito per i metadati degli oggetti. Questo valore è sempre inferiore allo spazio effettivamente riservato per i metadati su un nodo, perché una parte dello spazio riservato è necessaria per operazioni essenziali del database (come compaction e riparazione) e per futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati degli oggetti controlla la capacità complessiva degli oggetti.

utilizzo dei metadati di StorageGRID

Quantità di metadati degli oggetti sul volume di storage 0, in byte.

storagegrid_storage_utilization_total_space_bytes

La quantità totale di spazio di storage allocato a tutti gli object store.

storagegrid_storage_utilization_usable_space_bytes

La quantità totale di spazio di storage a oggetti rimanente. Calcolata sommando la quantità di spazio disponibile per tutti gli object store sullo Storage Node.

storagegrid_tenant_usage_data_bytes

La dimensione logica di tutti gli oggetti per il tenant.

conteggio degli oggetti utilizzati dal tenant in StorageGRID

Il numero di oggetti per il tenant.

storagegrid_tenant_usage_quota_bytes

La quantità massima di spazio logico disponibile per gli oggetti del tenant. Se non viene fornita una metrica di quota, è disponibile una quantità illimitata di spazio.

Ottieni un elenco di tutte le metriche

Per ottenere l'elenco completo delle metriche, usa l'API Grid Management.

Passaggi

1. Dalla parte superiore di Grid Manager, seleziona l'icona di aiuto e seleziona **API documentation**.
2. Individua le operazioni **metriche**.
3. Esegui l' `GET /grid/metric-names`operazione.
4. Scarica i risultati.

Riferimento ai file di registro

File di log di StorageGRID

StorageGRID fornisce log che vengono utilizzati per registrare eventi, messaggi diagnostici e condizioni di errore. Potrebbe esserti chiesto di raccogliere i file di log e inviarli al supporto tecnico per aiutare nella risoluzione dei problemi.

I log sono classificati come segue:

- "Registri software StorageGRID"
- "Registri di implementazione e manutenzione"
- "Informazioni sul file bycast.log"

> I dettagli forniti per ciascun tipo di log sono solo a scopo di riferimento. I log sono destinati alla risoluzione avanzata dei problemi da parte del supporto tecnico. Le tecniche avanzate che prevedono la ricostruzione della cronologia del problema utilizzando i log di audit e i file di log dell'applicazione sono al di fuori dell'ambito di queste istruzioni.

Accedi ai registri

Per accedere ai log, puoi "raccogli file di log e dati di sistema" da uno o più nodi come un unico archivio di file di log. Oppure puoi accedere ai singoli file di log per ciascun nodo della griglia come segue:

Passaggi

1. Inserisci il seguente comando: `ssh admin@grid_node_IP`
2. Inserisci la password indicata nel file `Passwords.txt`.
3. Inserisci il seguente comando per passare all'utente root: `su -`
4. Inserisci la password indicata nel file `Passwords.txt`.

Esporta i log sul server syslog

L'esportazione dei log al server syslog offre queste funzionalità:

- Ricevi un elenco di tutte le richieste Grid Manager e Tenant Manager, oltre alle richieste S3.
- Maggiore visibilità sulle richieste S3 che restituiscono errori, senza l'impatto sulle prestazioni causato dai metodi di audit logging.
- Accesso alle richieste a livello HTTP e ai codici di errore facili da analizzare.
- Maggiore visibilità sulle richieste bloccate dai classificatori di traffico sul bilanciatore di carico.

Per esportare i log, fai riferimento a "Configura la gestione dei log e il server syslog esterno".

Categorie dei file di log

L'archivio dei file di log di StorageGRID contiene i log descritti per ciascuna categoria e file aggiuntivi che contengono metriche e output dei comandi di debug.

Posizione archivio	Descrizione
audit	Messaggi di audit generati durante il normale funzionamento del sistema.
log del sistema operativo di base	Informazioni di base sul sistema operativo, incluse le versioni dell'immagine StorageGRID.
bundle	Informazioni di configurazione globali (bundle).
cache-svc	Log del servizio cache (solo sui nodi gateway).
cassandra	Informazioni sul database Cassandra e file di log di riparazione di Reaper.
ec	Informazioni VCS sul nodo corrente e informazioni sul gruppo EC tramite ID profilo.
griglia	Registri generali della griglia, inclusi i log di debug (`bycast.log`) e `servermanager` log.
grid.json	File di configurazione della grid condiviso tra tutti i nodi. Inoltre, `node.json` è specifico per il nodo corrente.
hagroups	Metriche e log dei gruppi ad alta disponibilità.

Posizione archivio	Descrizione
installare	`Gdu-server` e i log di installazione.
Lambda-arbitrator	Registri relativi alla richiesta proxy S3 Select.
leakd	Log dal servizio leakd.
lumberjack.log	Messaggi di debug relativi alla raccolta dei log.
Metriche	Log di servizio per Grafana, Jaeger, node exporter e Prometheus.
miscd	Registri di accesso ed errore di Miscd.
mysql	La configurazione del database mariaDB e i relativi log.
net	Log generati dagli script relativi alla rete e dal servizio Dynip.
nginx	File di configurazione e log del bilanciatore di carico e della federazione della grid. Include anche i log del traffico di Grid Manager e Tenant Manager.
nginx-gw	• `access.log`: Messaggi di log delle richieste di Grid Manager e Tenant manager. ◦ Questi messaggi sono preceduti da `mgmt:` quando vengono esportati tramite syslog. ◦ Il formato di questi messaggi di registro è `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: Richieste di replica cross-grid in entrata. ◦ Questi messaggi sono preceduti da `cgr:` quando vengono esportati tramite syslog. ◦ Il formato di questi messaggi di registro è `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`Richieste S3 agli endpoint del bilanciatore di carico. ◦ Questi messaggi sono preceduti da `endpoint:` quando vengono esportati tramite syslog. ◦ Il formato di questi messaggi di registro è `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Relativo al nuovo avviso di controllo DNS.

Posizione archivio	Descrizione
ntp	File di configurazione NTP e log.
Oggetti orfani	Registri relativi agli oggetti orfani.
sistema operativo	File di stato dei nodi e della griglia, inclusi i servizi `pid`.
altro	File di registro sotto `/var/local/log` che non vengono raccolti in altre cartelle.
perf	Informazioni sulle prestazioni di CPU, rete e I/O del disco.
prometheus-data	Metriche Prometheus correnti, se la raccolta dei log include dati Prometheus.
provisioning	Registri relativi al processo di provisioning del grid.
raft	Log dal cluster Raft utilizzati nei servizi della piattaforma.
ssh	Registri relativi alla configurazione e al servizio SSH.
snmp	Configurazione dell'agente SNMP utilizzata per l'invio di notifiche SNMP.
dati dei socket	Dati dei socket per il debug di rete.
system-commands.txt	Output dei comandi del container StorageGRID. Contiene informazioni di sistema, come networking e utilizzo del disco.
sincronizza-pacchetto-di-ripristino	Relativo al mantenimento della coerenza del pacchetto di ripristino più recente su tutti i nodi di amministrazione e Storage Nodes che ospitano il servizio ADC.

Registri software StorageGRID

Puoi usare i log di StorageGRID per risolvere i problemi.

> Se vuoi inviare i tuoi log a un server syslog esterno o cambiare la destinazione delle informazioni di audit come la `bycast.log` e `nms.log`, consulta "Configura la gestione dei log".

Registri generali di StorageGRID

Nome file	Note	Trovato su
/var/local/log/bycast.log	Il file principale di StorageGRID per la risoluzione dei problemi.	Tutti i nodi

Nome file	Note	Trovato su
/var/local/log/bycast-err.log	Contiene un sottoinsieme di `bycast.log` (messaggi con gravità ERROR e CRITICAL). I messaggi CRITICAL vengono visualizzati anche nel sistema.	Tutti i nodi
/var/local/core/	Contiene eventuali file di core dump creati se il programma termina in modo anomalo. Le possibili cause includono errori di asserzione, violazioni o timeout dei thread. **Nota**: Il file `` `/var/local/core/kexec_cmd `` di solito è presente sui nodi dell'appliance e non indica un errore.	Tutti i nodi

Registri relativi alla cifratura

Nome file	Note	Trovato su
/var/local/log/ssh-config-generation.log	Contiene i log relativi alla generazione delle configurazioni SSH e al ricaricamento dei servizi SSH.	Tutti i nodi
/var/local/log/nginx/config-generation.log	Contiene i log relativi alla generazione delle configurazioni di nginx e al ricaricamento dei servizi di nginx.	Tutti i nodi
/var/local/log/nginx-gw/config-generation.log	Contiene i log relativi alla generazione delle configurazioni di nginx-gw (e al ricaricamento dei servizi di nginx-gw).	Nodi di amministrazione e gateway
/var/local/log/update-cipher-configurations.log	Contiene i log relativi alla configurazione delle policy TLS e SSH.	Tutti i nodi

Log della federazione di grid

Nome file	Note	Trovato su
/var/local/log/update_grid_federation_config.log	Contiene i log relativi alla generazione delle configurazioni di nginx e nginx-gw per le connessioni di federazione della grid.	Tutti i nodi

Registri NMS

Nome file	Note	Trovato su
/var/local/log/nms.log	• Acquisisce le notifiche dal Grid Manager e dal Tenant Manager. • Cattura gli eventi relativi al funzionamento del servizio NMS. Ad esempio, notifiche email e modifiche alla configurazione. • Contiene aggiornamenti del bundle XML derivanti da modifiche di configurazione effettuate nel sistema. • Contiene messaggi di errore relativi al downsampling dell'attributo, eseguito una volta al giorno. • Contiene messaggi di errore del server web Java, ad esempio errori di generazione della pagina ed errori HTTP Status 500. • Contiene i log relativi a AutoSupport.	Nodi di amministrazione
/var/local/log/nms.errlog	Contiene messaggi di errore relativi agli aggiornamenti del database MySQL. Contiene il flusso di errore standard (stderr) dei servizi corrispondenti. C'è un file di log per ogni servizio. Questi file sono generalmente vuoti, a meno che non ci siano problemi con il servizio.	Nodi di amministrazione
/var/local/log/nms.requestlog	Contiene informazioni sulle connessioni in uscita dall'API di gestione verso i servizi interni di StorageGRID.	Nodi di amministrazione

Log di Server Manager

Nome file	Note	Trovato su
/var/local/log/servermanager.log	File di log dell'applicazione Server Manager in esecuzione sul server.	Tutti i nodi
/var/local/log/GridstatBackend.errlog	File di log per l'applicazione backend GUI di Server Manager.	Tutti i nodi
/var/local/log/gridstat.errlog	File di log per l'interfaccia grafica di Server Manager.	Tutti i nodi

Registri dei servizi StorageGRID

Nome file	Note	Trovato su
/var/local/log/acct.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/adc.errlog	Contiene il flusso di errore standard (stderr) dei servizi corrispondenti. C'è un file di log per ogni servizio. Questi file sono generalmente vuoti, a meno che non ci siano problemi con il servizio.	Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/ams.errlog		Nodi di amministrazione
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	Registri del servizio cache.	${post_edited_translations.segment}
/var/local/log/cassandra/system.log	Informazioni per l'archivio dei metadati (database Cassandra) che puoi usare se si verificano problemi durante l'aggiunta di nuovi Storage Node o se l'attività di riparazione di nodetool si blocca.	Nodi di storage
/var/local/log/cassandra-reaper.log	Informazioni sul servizio Cassandra Reaper, che si occupa della riparazione dei dati nel database Cassandra.	Nodi di storage
/var/local/log/cassandra-reaper.errlog	Informazioni di errore per il servizio Cassandra Reaper.	Nodi di storage
/var/local/log/chunk.errlog		Nodi di storage
/var/local/log/cmn.errlog		Nodi di amministrazione
/var/local/log/cms.errlog	Questo file di log potrebbe essere presente sui sistemi che sono stati aggiornati da una versione precedente di StorageGRID. Contiene informazioni obsolete.	Nodi di storage
/var/local/log/dds.errlog		Nodi di storage
/var/local/log/dmv.errlog		Nodi di storage

Nome file	Note	Trovato su
/var/local/log/dynip*	Contiene i log relativi al servizio dynip, che monitora la grid per rilevare modifiche dinamiche degli indirizzi IP e aggiorna la configurazione locale.	Tutti i nodi
/var/local/log/grafana.log	Il file di log associato al servizio Grafana, utilizzato per la visualizzazione delle metriche nel Grid Manager.	Nodi di amministrazione
/var/local/log/hagroups.log	Il log associato ai gruppi ad alta disponibilità.	Nodi di amministrazione e nodi gateway
/var/local/log/hagroups_events.log	Tiene traccia dei cambiamenti di stato, come la transizione da BACKUP a MASTER o FAULT.	Nodi di amministrazione e nodi gateway
/var/local/log/idnt.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/jaeger.log	Il log associato al servizio jaeger, che viene utilizzato per la raccolta delle tracce.	Tutti i nodi
/var/local/log/kstn.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/lambda*	Contiene i log del servizio S3 Select.	Nodi di amministrazione e gateway Solo alcuni nodi Admin e Gateway contengono questo registro. Vedi il "Requisiti e limitazioni di S3 Select per i nodi Admin e Gateway".
/var/local/log/ldr.errlog		Nodi di storage
/var/local/log/miscd/*.log	Contiene i log del servizio MISCd (Information Service Control Daemon), che fornisce un'interfaccia per interrogare e gestire i servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, come interrogare lo stato dei servizi in esecuzione su altri nodi.	Tutti i nodi

Nome file	Note	Trovato su
/var/local/log/nginx/*.log	Contiene i log del servizio nginx, che funge da meccanismo di autenticazione e comunicazione sicura per consentire a vari servizi di grid (come Prometheus e Dynip) di comunicare con i servizi su altri nodi tramite API HTTPS.	Tutti i nodi
/var/local/log/nginx-gw/*.log	Contiene i log generali relativi al servizio nginx-gw, inclusi i log degli errori e i log per le porte admin con accesso limitato sugli Admin Nodes.	Nodi di amministrazione e nodi gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene i registri di accesso relativi al traffico di replica cross-grid.	Nodi amministratori, nodi gateway o entrambi, a seconda della configurazione della federazione della griglia. Presenti solo sulla grid di destinazione per la replica tra grid.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene i log di accesso per il servizio Load Balancer, che fornisce il bilanciamento del carico del traffico S3 dai client ai Storage Node.	Nodi di amministrazione e nodi gateway
/var/local/log/persistence*	Contiene i log del servizio Persistence, che gestisce i file sul disco di root che devono persistere anche dopo un riavvio.	Tutti i nodi
/var/local/log/prometheus.log	Per tutti i nodi, contiene il registro del servizio node exporter e il registro del servizio metriche ade-exporter. Per i nodi amministratori, contiene anche i log dei servizi Prometheus e Alert Manager.	Tutti i nodi
/var/local/log/raft.log	Contiene l'output della libreria utilizzata dal servizio RSM per il protocollo Raft.	Nodi di archiviazione con servizio RSM
/var/local/log/rms.errlog	Contiene i log del servizio Replicated State Machine Service (RSM), utilizzato per i servizi della piattaforma S3.	Nodi di archiviazione con servizio RSM
/var/local/log/ssm.errlog		Tutti i nodi

Nome file	Note	Trovato su
/var/local/log/update-s3vs-domains.log	Contiene i log relativi all'elaborazione degli aggiornamenti per la configurazione dei nomi di dominio virtuali ospitati su S3. Consulta le istruzioni per implementare le applicazioni client S3.	Nodi di amministrazione e gateway
/var/local/log/update-snmp-firewall.*	Contengono log relativi alle porte del firewall gestite per SNMP.	Tutti i nodi
/var/local/log/update-sysl.log	Contiene log relativi alle modifiche apportate alla configurazione del syslog di sistema.	Tutti i nodi
/var/local/log/update-traffic-classes.log	Contiene i log relativi alle modifiche apportate alla configurazione dei classificatori di traffico.	Nodi di amministrazione e gateway
/var/local/log/update-utcn.log	Contiene i log relativi alla modalità Untrusted Client Network su questo nodo.	Tutti i nodi

Informazioni correlate

- "Informazioni sul file bycast.log"
- "${post_edited_translations.segment}"

Registri di distribuzione e manutenzione in StorageGRID

Puoi usare i registri di distribuzione e manutenzione per risolvere i problemi.

Nome file	Note	Trovato su
/var/local/log/install.log	Creato durante l'installazione del software. Contiene una registrazione degli eventi di installazione.	Tutti i nodi
/var/local/log/expansion-progress.log	Creato durante le operazioni di espansione. Contiene una registrazione degli eventi di espansione.	Nodi di storage
/var/local/log/pa-move.log	Creato durante l'esecuzione dello `pa-move.sh` script.	Nodo amministrativo primario
/var/local/log/pa-move-new_pa.log	Creato durante l'esecuzione dello `pa-move.sh` script.	Nodo amministrativo primario
/var/local/log/pa-move-old_pa.log	Creato durante l'esecuzione dello `pa-move.sh` script.	Nodo amministrativo primario

Nome file	Note	Trovato su
/var/local/log/gdu-server.log	Creato dal servizio GDU. Contiene eventi relativi alle procedure di provisioning e manutenzione gestite dal nodo amministratore primario.	Nodi di amministrazione
/var/local/log/send_admin_hw.log	Creato durante l'installazione. Contiene informazioni di debug relative alle comunicazioni di un nodo con il nodo amministratore primario.	Tutti i nodi
/var/local/log/upgrade.log	Creato durante l'aggiornamento del software. Contiene una registrazione degli eventi di aggiornamento del software.	Tutti i nodi

Scopri il file bycast.log di StorageGRID

Il file `/var/local/log/bycast.log` è il file principale per la risoluzione dei problemi del software StorageGRID. Esiste un `bycast.log` file per ogni nodo della griglia. Il file contiene messaggi specifici per quel nodo della griglia.

Il file `/var/local/log/bycast-err.log` è un sottoinsieme di `bycast.log`. Contiene messaggi di gravità ERROR e CRITICAL.

Facoltativamente, puoi modificare la destinazione dei log di audit e inviare le informazioni di audit a un server syslog esterno. I log locali dei record di audit continuano a essere generati e archiviati quando è configurato un server syslog esterno. Vedi "Configura la gestione dei log e il server syslog esterno".

Rotazione dei file per bycast.log

Quando il `bycast.log` file raggiunge 1 GB, il file esistente viene salvato e viene avviato un nuovo file di log.

Il file salvato viene rinominato `bycast.log.1`, e il nuovo file viene chiamato `bycast.log`. Quando il nuovo `bycast.log` raggiunge 1 GB, `bycast.log.1` viene rinominato e compresso per diventare `bycast.log.2.gz`, e `bycast.log` viene rinominato `bycast.log.1`.

Il limite di rotazione per `bycast.log` è di 21 file. Quando viene creata la 22a versione del file `bycast.log`, il file più vecchio viene eliminato.

Il limite di rotazione per `bycast-err.log` è di sette file.

> Se un file di log è stato compresso, non devi decomprimerlo nella stessa posizione in cui è stato scritto. Decomprimere il file nella stessa posizione può interferire con gli script di rotazione dei log.

Facoltativamente, puoi modificare la destinazione dei log di audit e inviare le informazioni di audit a un server syslog esterno. I log locali dei record di audit continuano a essere generati e archiviati quando è configurato un server syslog esterno. Vedi "Configura la gestione dei log e il server syslog esterno".

Informazioni correlate

"Raccogli i file di log e i dati di sistema"

Messaggi in bycast.log

I messaggi in `bycast.log` sono scritti dall'ADE (Asynchronous Distributed Environment). ADE è l'ambiente di runtime utilizzato dai servizi di ciascun nodo della griglia.

Esempio di messaggio ADE:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

I messaggi ADE contengono le seguenti informazioni:

Messaggio segmento	Valore nell'esempio
ID nodo	12455685
ID del processo ADE	0357819531
Nome modulo	SVMR
Identificatore del messaggio	EVHR
ora di sistema UTC	2019-05-05T27T17:10:29.784677 (YYYY-MM-DDTHH:MM:SS.uuuuuu)
Livello di gravità	ERRORE
Numero di tracciamento interno	0906
Messaggio	SVMR: Il controllo di integrità sul volume 3 non è riuscito con il motivo "TOUT"

Gravità dei messaggi nel file bycast.log

I messaggi in `bycast.log` vengono assegnati a livelli di gravità.

Ad esempio:

- **AVVISO** — Si è verificato un evento che deve essere registrato. La maggior parte dei messaggi di registro si trova a questo livello.
- **ATTENZIONE** — Si è verificata una condizione imprevista.
- **ERRORE** — Si è verificato un errore grave che avrà un impatto sulle operazioni.
- **CRITICO** — Si è verificata una condizione anomala che ha interrotto le normali operazioni. Dovresti risolvere subito la causa del problema.

Codici di errore in `bycast.log`

La maggior parte dei messaggi di errore in `bycast.log` contiene codici di errore.

La tabella seguente elenca i codici non numerici più comuni in `bycast.log`. Il significato esatto di un codice non numerico dipende dal contesto in cui viene riportato.

Codice di errore	Significato
SUCS	Nessun errore
GERR	Sconosciuto
CANC	Annullato
ABRT	Interrotto
TUTTO	Timeout
INVL	Non valido
NFND	Non trovato
VERS	Versione
CONF	Configurazione
ERRORE	Fallito
ICPL	Incompleto
FATTO	Fatto
SUNV	Servizio non disponibile

La tabella seguente elenca i codici di errore numerici in `bycast.log`.

Numero di errore	Codice di errore	Significato
001	EPERM	Operazione non consentita
002	ENOENT	Nessun file o directory
003	ESRCH	Nessun processo di questo tipo
004	EINTR	Chiamata di sistema interrotta

Numero di errore	Codice di errore	Significato
005	EIO	Errore di I/O
006	ENXIO	Nessun dispositivo o indirizzo di questo tipo
007	E2BIG	L'elenco degli argomenti è troppo lungo
008	ENOEXEC	Errore di formato eseguibile
009	EBADF	Numero di file errato
010	ECHILD	Nessun processo figlio
011	EAGAIN	Riprova
012	ENOMEM	Memoria esaurita
013	EACCES	Autorizzazione negata
014	EFAULT	Indirizzo errato
015	ENOTBLK	Dispositivo di blocco necessario
016	EBUSY	Dispositivo o risorsa occupata
017	EEXIST	Il file esiste
018	EXDEV	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo di questo tipo
020	ENOTDIR	Non è una directory
021	EISDIR	È una directory
022	EINVAL	Argomento non valido
023	ENFILE	Overflow della tabella dei file
024	EMFILE	Troppi file aperti
025	ENOTTY	Non è una macchina da scrivere

Numero di errore	Codice di errore	Significato
026	ETXTBSY	File di testo occupato
027	EFBIG	File troppo grande
028	ENOSPC	Spazio insufficiente sul dispositivo
029	ESPIPE	Ricerca illegale
030	EROFS	file system di sola lettura
031	EMLINK	Troppi link
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dal dominio della funzione
034	ERANGE	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un deadlock delle risorse
036	ENAMETOOLONG	Nome file troppo lungo
037	ENOLCK	Nessun blocco record disponibile
038	ENOSYS	Funzione non implementata
039	ENOTEMPTY	Directory non vuota
040	ELOOP	Sono stati rilevati troppi collegamenti simbolici
041		
042	ENOMSG	Nessun messaggio del tipo desiderato
043	EIDRM	Identificativo rimosso
044	ECHRNG	Numero di canale fuori intervallo
045	EL2NSYNC	Livello 2 non sincronizzato
046	EL3HLT	Livello 3 sospeso

Numero di errore	Codice di errore	Significato
047	EL3RST	Ripristino del livello 3
048	ELNRNG	Numero di collegamento fuori intervallo
049	EUNATCH	Driver di protocollo non collegato
050	ENOCSI	Nessuna struttura CSI disponibile
051	EL2HLT	Livello 2 sospeso
052	EBADE	Scambio non valido
053	EBADR	Descrizione richiesta non valida
054	EXFULL	Exchange completo
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato del file del font errato
060	ENOSTR	Dispositivo non è uno stream
061	ENODATA	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse di stream esaurite
064	ENONET	La macchina non è sulla rete
065	ENOPKG	Pacchetto non installato
066	EREMOTE	L'oggetto è remoto
067	ENOLINK	Il collegamento è stato interrotto

Numero di errore	Codice di errore	Significato
068	EADV	Errore di pubblicità
069	ESRMNT	Errore Srmount
070	ECOMM	Errore di comunicazione durante l'invio
071	EPROTO	Errore di protocollo
072	EMULTIHOP	Tentativo di multihop
073	EDOTDOT	errore specifico RFS
074	EBADMSG	Non è un messaggio di dati
075	TRABOCCO	Valore troppo grande per il tipo di dati definito
076	ENOTUNIQ	Nome non univoco sulla rete
077	EBADFD	Descrittore del file in stato non corretto
078	EREMCHG	Indirizzo remoto modificato
079	ELIBACC	Impossibile accedere a una libreria condivisa necessaria
080	ELIBBAD	Accesso a una libreria condivisa danneggiata
081	ELIBSCN	
082	ELIBMAX	Tentativo di collegare troppe librerie condivise
083	ELIBEXEC	Non puoi eseguire direttamente una libreria condivisa
084	EILSEQ	Sequenza di byte illegale
085	ERESTART	La chiamata di sistema interrotta dovrebbe essere riavviata
086	ESTRPIPE	Errore pipe dei flussi
087	EUSERS	Troppi utenti

Numero di errore	Codice di errore	Significato
088	ENOTSOCK	Operazione di socket su un non-socket
089	EDESTADDRREQ	Indirizzo di destinazione richiesto
090	EMSGSIZE	Messaggio troppo lungo
091	EPROTOTYPE	Protocollo di tipo errato per il socket
092	ENOPROTOOPT	Protocollo non disponibile
093	EPROTONOSUPPORT	Protocollo non supportato
094	ESOCKTNOSUPPORT	Tipo di socket non supportato
095	EOPNOTSUPP	Operazione non supportata sull'endpoint di trasporto
096	EPFNOSUPPORT	Famiglia di protocolli non supportata
097	EAFNOSUPPORT	Famiglia di indirizzi non supportata dal protocollo
098	EADDRINUSE	Indirizzo già in uso
099	EADDRNOTAVAIL	Impossibile assegnare l'indirizzo richiesto
100	ENETDOWN	La rete non funziona
101	ENETUNREACH	Rete irraggiungibile
102	ENETRESET	Connessione di rete interrotta a causa del reset
103	ECONNABORTED	Il software ha causato la chiusura della connessione
104	ECONNRESET	Connessione reimpostata dal peer
105	ENOBUFS	Spazio buffer non disponibile
106	EISCONN	L'endpoint di trasporto è già connesso
107	ENOTCONN	L'endpoint di trasporto non è connesso
108	ESHUTDOWN	Impossibile inviare dopo la chiusura dell'endpoint di trasporto

Numero di errore	Codice di errore	Significato
109	ETOOMANYREFS	Troppi riferimenti: impossibile unire
110	ETIMEDOUT	Connessione scaduta
111	ECONNREFUSED	Connessione rifiutata
112	EHOSTDOWN	Host non è attivo
113	EHOSTUNREACH	Nessun percorso verso l'host
114	GIÀ	Operazione già in corso
115	IN PROGRESSO	Operazione in corso
116		
117	EUCLEAN	La struttura necessita di pulizia
118	ENOTNAM	Non è un file di tipo denominato XENIX
119	DISPONIBILE	Nessun semaforo XENIX disponibile
120	EISNAM	È un file di tipo denominato
121	EREMOTEIO	Errore di I/O remoto
122	EDQUOT	Quota superata
123	ENOMEDIUM	Nessun supporto trovato
124	EMEDIUMTYPE	Tipo di supporto errato
125	CANCELLATO	Operazione annullata
126	ENOKEY	Chiave richiesta non disponibile
127	CHIAVE ELETTRONICA SCADUTA	La chiave è scaduta
128	CHIAVE REVOCATA	La chiave è stata revocata
129	EKEYREJECTED	La chiave è stata rifiutata dal servizio

Numero di errore	Codice di errore	Significato
130	EOWNERDEAD	Per mutex robusti: proprietario morto
131	ENOTRECOVERABLE	Per i mutex robusti: stato non recuperabile

Configura la gestione dei log e il server syslog esterno

Server syslog esterni in StorageGRID

Un server syslog esterno è un server esterno a StorageGRID che puoi usare per raccogliere le informazioni di audit del sistema in un'unica posizione. Usare un server syslog esterno ti permette di ridurre il traffico di rete sui nodi di amministrazione e di gestire le informazioni in modo più efficiente. Per StorageGRID, il formato dei pacchetti dei messaggi syslog outbound è conforme alla RFC 3164.

Le tipologie di informazioni di controllo che puoi inviare al syslog server esterno includono:

- Registri di controllo contenenti i messaggi di controllo generati durante il normale funzionamento del sistema
- Eventi relativi alla sicurezza come accessi ed escalation a root
- I log dell'applicazione potrebbero essere richiesti se è necessario aprire una richiesta di supporto per risolvere un problema che hai riscontrato

Quando utilizzare un syslog server esterno

Un syslog server esterno è particolarmente utile se hai una griglia di grandi dimensioni, usi diversi tipi di applicazioni S3 o vuoi conservare tutti i dati di audit. Inviare le informazioni di audit a un syslog server esterno ti permette di:

- Raccogli e gestisci informazioni di audit, come messaggi di audit, log delle applicazioni ed eventi di sicurezza, in modo più efficiente.
- Riduci il traffico di rete sui tuoi Admin Node perché le informazioni di audit vengono trasferite direttamente dai vari Storage Node al server syslog esterno, senza dover passare attraverso un Admin Node.

> Quando i log vengono inviati a un syslog server esterno, i singoli log di dimensioni superiori a 8.192 byte vengono troncati alla fine del messaggio per conformarsi alle limitazioni comuni nelle implementazioni dei syslog server esterni.

> Per massimizzare le opzioni di recovery di dati in caso di guasto del syslog server esterno, fino a 20 GB di log locali dei record di audit (`localaudit.log` vengono mantenuti su ciascun nodo.

Come configurare un server syslog esterno

Per sapere come configurare un server syslog esterno, vedi "Configura la gestione dei log e il server syslog esterno".

Se vuoi configurare e utilizzare il protocollo TLS o RELP/TLS, devi avere i seguenti certificati:

- **Certificati CA del server**: uno o più certificati CA attendibili per la verifica del syslog server esterno in codifica PEM. Se omesso, verrà utilizzato il certificato CA predefinito di Grid.
- **Certificato client**: Il certificato client per l'autenticazione al server syslog esterno in codifica PEM.
- **Chiave privata del client**: Chiave privata per il certificato client in codifica PEM.

> Se usi un certificato client, devi usare anche una chiave privata client. Se fornisci una chiave privata crittografata, devi fornire anche la passphrase. Non ci sono vantaggi significativi in termini di sicurezza nell'usare una chiave privata crittografata, perché sia la chiave che la passphrase devono essere memorizzate; per semplicità, è consigliato usare una chiave privata non crittografata, se disponibile.

Come stimare le dimensioni del syslog server esterno

Normalmente, la tua grid viene dimensionata per raggiungere un throughput, definito in termini di operazioni S3 al secondo o byte al secondo. Ad esempio, potresti avere la necessità che la tua grid gestisca 1.000 operazioni S3 al secondo, o 2.000 MB al secondo, di ingest e retrieval di oggetti. Dovresti dimensionare il tuo server syslog esterno in base ai requisiti di dati della tua grid.

Questa sezione fornisce alcune formule euristiche che ti aiutano a stimare la frequenza e la dimensione media dei messaggi di log di vario tipo che il server syslog esterno deve essere in grado di gestire, espresse in termini di caratteristiche prestazionali note o desiderate della grid (operazioni S3 al secondo).

Usa le operazioni S3 al secondo nelle formule di stima

Se la tua grid è stata dimensionata per un throughput espresso in byte al secondo, devi convertire questo dimensionamento in operazioni S3 al secondo per poter utilizzare le formule di stima. Per convertire il throughput della grid, devi prima determinare la dimensione media degli oggetti, cosa che puoi fare utilizzando le informazioni presenti nei log di audit e nelle metriche (se disponibili), oppure basandoti sulla tua conoscenza delle applicazioni che utilizzeranno StorageGRID. Ad esempio, se la tua grid è stata dimensionata per raggiungere un throughput di 2.000 MB/secondo e la dimensione media degli oggetti è di 2 MB, allora la tua grid è stata dimensionata per gestire 1.000 operazioni S3 al secondo (2.000 MB / 2 MB).

> Le formule per il dimensionamento del server syslog esterno presentate nelle sezioni seguenti forniscono stime basate sul caso più comune (anziché sul caso peggiore). A seconda della configurazione e del carico di lavoro, potresti vedere un numero di messaggi syslog o un volume di dati syslog superiore o inferiore rispetto a quanto previsto dalle formule. Le formule sono da intendersi esclusivamente come linee guida.

Formule di stima per i registri di controllo

Se non hai altre informazioni sul carico di lavoro S3 oltre al numero di operazioni S3 al secondo che la tua grid dovrebbe supportare, puoi stimare il volume dei log di audit che il syslog server esterno dovrà gestire usando le seguenti formule, supponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie impostate su Normal, tranne Storage, che è impostata su Error):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Ad esempio, se la tua grid è dimensionata per 1.000 operazioni S3 al secondo, il tuo syslog server esterno dovrebbe essere dimensionato per supportare 2.000 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e di solito memorizzare) dati di audit log a una velocità di 1,6 MB al secondo.

Conoscendo meglio il carico di lavoro, puoi ottenere stime più accurate. Per i log di audit, le variabili aggiuntive più importanti sono la % di operazioni S3 che sono PUT (rispetto a GET) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni di 4 caratteri usate nella tabella sono i nomi dei campi del log di audit):

Codice	Campo	Descrizione
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Utilizziamo P per rappresentare la percentuale di operazioni S3 che sono PUT, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT al 100%, P = 1, e per un carico di lavoro GET al 100%, P = 0).

Usa K per rappresentare la dimensione media della somma dei nomi degli account S3, dei bucket S3 e delle chiavi S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi il valore di K è 90 (13+13+28+36).

Se puoi determinare i valori di P e K, puoi stimare il volume dei log di audit che il server syslog esterno dovrà gestire utilizzando le seguenti formule, supponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie impostate su Normale, tranne Storage, che è impostata su Errore):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Ad esempio, se la tua grid è dimensionata per 1.000 operazioni S3 al secondo, il tuo carico di lavoro è composto per il 50% da PUT, e i nomi degli account S3, dei bucket e degli oggetti hanno una media di 90 byte, il tuo syslog server esterno dovrebbe essere dimensionato per supportare 1.500 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e di solito memorizzare) i dati del log di audit a una velocità di circa 1 MB al secondo.

Formule di stima per i livelli di audit non predefiniti

Le formule fornite per i log di controllo presuppongono l'utilizzo delle impostazioni predefinite del livello di controllo (tutte le categorie impostate su Normale, tranne Storage, che è impostata su Errore). Non sono disponibili formule dettagliate per stimare la frequenza e la dimensione media dei messaggi di controllo per impostazioni del livello di controllo diverse da quelle predefinite. Tuttavia, la tabella seguente può essere usata per fare una stima approssimativa della frequenza; puoi usare la formula per la dimensione media fornita per i log di controllo, ma tieni presente che probabilmente otterrai una sovrastima perché i messaggi di controllo "extra" sono, in media, più piccoli dei messaggi di controllo predefiniti.

Condizione	Formula
Replica: tutti i livelli di audit sono impostati su Debug o Normale	Frequenza dei log di controllo = 8 x Frequenza delle operazioni S3
Codifica di cancellazione: tutti i livelli di audit sono impostati su Debug o Normale	Usa la stessa formula delle impostazioni predefinite

Formule di stima per eventi di sicurezza

Gli eventi di sicurezza non sono correlati alle operazioni S3 e in genere producono un volume trascurabile di log e dati. Per questi motivi, non vengono fornite formule di stima.

Formule di stima per i log delle applicazioni

Se non hai altre informazioni sul carico di lavoro S3 oltre al numero di operazioni S3 al secondo che la tua grid dovrebbe supportare, puoi stimare il volume dei log delle applicazioni che il tuo syslog server esterno dovrà gestire usando le seguenti formule:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Quindi, ad esempio, se la tua grid è dimensionata per 1.000 operazioni S3 al secondo, il tuo syslog server esterno dovrebbe essere dimensionato per supportare 3.300 log applicativi al secondo ed essere in grado di ricevere (e memorizzare) dati di log applicativi a una velocità di circa 1,2 MB al secondo.

Conoscendo meglio il carico di lavoro, è possibile ottenere stime più accurate. Per i log delle applicazioni, le variabili aggiuntive più importanti sono la strategia di protezione dei dati (replica o codifica di cancellazione), la % di operazioni S3 di tipo PUT (rispetto a GET/altro) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni di 4 caratteri utilizzate nella tabella sono i nomi dei campi del log di audit):

Codice	Campo	Descrizione
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.

Codice	Campo	Descrizione
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Esempi di stime dimensionali

Questa sezione illustra casi di esempio su come utilizzare le formule di stima per le griglie con i seguenti metodi di protezione dei dati:

- Replica
- Erasure coding

Se usi la replica per la protezione dei dati

Sia P la percentuale di operazioni S3 che sono PUT, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT al 100%, P = 1, e per un carico di lavoro GET al 100%, P = 0).

Sia K la dimensione media della somma dei nomi degli account S3, dei bucket S3 e delle chiavi S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Allora K ha un valore di 90 (13+13+28+36).

Se puoi determinare i valori di P e K, puoi stimare il volume dei log delle applicazioni che il syslog server esterno dovrà essere in grado di gestire usando le seguenti formule.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Ad esempio, se la tua grid è dimensionata per 1.000 operazioni S3 al secondo, il tuo carico di lavoro è composto per il 50% da PUT, e i nomi degli account S3, dei bucket e degli oggetti hanno una media di 90 byte, il tuo syslog server esterno dovrebbe essere dimensionato per supportare 1800 log applicativi al secondo e riceverà (e di solito memorizzerà) dati applicativi a una velocità di 0.5 MB al secondo.

Se usi la codifica di cancellazione per la protezione dei dati

Sia P la percentuale di operazioni S3 che sono PUT, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT al 100%, P = 1, e per un carico di lavoro GET al 100%, P = 0).

Sia K la dimensione media della somma dei nomi degli account S3, dei bucket S3 e delle chiavi S3.

Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Allora K ha un valore di 90 (13+13+28+36).

Se puoi determinare i valori di P e K, puoi stimare il volume dei log delle applicazioni che il syslog server esterno dovrà essere in grado di gestire usando le seguenti formule.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Ad esempio, se la tua grid è dimensionata per 1.000 operazioni S3 al secondo, il tuo carico di lavoro è composto per il 50% da PUT, e i nomi degli account S3, dei bucket e degli oggetti hanno una media di 90 byte, il tuo syslog server esterno dovrebbe essere dimensionato per supportare 2.250 log applicativi al secondo e dovrebbe essere in grado di ricevere (e di solito memorizzare) dati applicativi a una velocità di 0,6 MB al secondo.

Configura la gestione dei log in StorageGRID

Se necessario, configura i livelli di audit, le intestazioni del protocollo e la posizione dei messaggi e dei log di audit.

Tutti i nodi StorageGRID generano messaggi di audit e log per tracciare l'attività e gli eventi del sistema. I messaggi di audit e i log sono strumenti essenziali per il monitoraggio e la risoluzione dei problemi.

Facoltativamente, puoi "configura un server syslog esterno" per salvare le informazioni di audit in remoto. Usare un server esterno riduce al minimo l'impatto sulle prestazioni della registrazione dei messaggi di audit senza ridurre la completezza dei dati di audit. Un server syslog esterno è particolarmente utile se hai una griglia di grandi dimensioni, usi diversi tipi di applicazioni S3 o vuoi conservare tutti i dati di audit.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di manutenzione o di accesso root".
- Se hai intenzione di configurare un syslog server esterno, hai già esaminato e seguito le "Considerazioni sull'utilizzo di un server syslog esterno".
- Se vuoi configurare un syslog server esterno utilizzando il protocollo TLS o RELP/TLS, hai i certificati CA del server e del client richiesti e la chiave privata del client.

Modifica i livelli dei messaggi di audit

Puoi impostare un livello di audit diverso per ciascuna delle seguenti categorie di messaggi nel registro di audit:

Categoria di audit	Impostazione predefinita	Ulteriori informazioni
Sistema	Normale	"Messaggi di audit di sistema"
Storage	Errore	"Messaggi di audit dello storage a oggetti"

Categoria di audit	Impostazione predefinita	Ulteriori informazioni
Gestione	Normale	"Messaggio di audit gestionale"
Letture client	Normale	"Lettura dei messaggi di audit dal client"
Il client scrive	Normale	"Il client scrive messaggi di audit"
ILM	Normale	"Messaggi di audit ILM"
Replicazione cross-grid	Errore	"CGRR: Richiesta di replica cross-grid"

Durante gli upgrade, le configurazioni del livello di audit non saranno immediatamente effettive.

Passaggi

1. Seleziona **Configurazione** > **Monitoraggio** > **Gestione dei log**.
2. Per ogni categoria di messaggio di controllo, seleziona un livello di controllo dal menu a discesa:

Livello di audit	Descrizione
Spento	Nessun messaggio di controllo di questa categoria viene registrato.
Errore	Vengono registrati solo i messaggi di errore, ovvero i messaggi di audit per i quali il codice di risultato non era "successful" (SUCS).
Normale	Vengono registrati i messaggi transazionali standard: i messaggi elencati in queste istruzioni per la categoria.
Debug	Obsoleto. Questo livello si comporta allo stesso modo del livello di controllo normale.

I messaggi inclusi per un determinato livello comprendono quelli che verrebbero registrati ai livelli superiori. Ad esempio, il livello Normale include tutti i messaggi di errore.

Se non hai bisogno di una registrazione dettagliata delle operazioni di lettura del client per le tue applicazioni S3, puoi facoltativamente modificare l'impostazione **Letture client** in **Errore** per ridurre il numero di messaggi di audit registrati nel registro di audit.

3. Seleziona **Salva**.

Definisci le intestazioni della richiesta HTTP

Puoi opzionalmente definire qualsiasi intestazione di richiesta HTTP che vuoi includere nei messaggi di audit di lettura e scrittura del client.

Passaggi

1. Nella sezione **Intestazioni del protocollo di audit**, definisci le intestazioni della richiesta HTTP che vuoi includere nei messaggi di audit di lettura e scrittura del client.

   Usa l'asterisco (*) come carattere jolly per trovare zero o più caratteri. Usa la sequenza di escape (*) per trovare un asterisco letterale.

2. Seleziona **Aggiungi un'altra intestazione** per creare ulteriori intestazioni, se necessario.

   Quando vengono rilevate intestazioni HTTP in una richiesta, sono incluse nel messaggio di audit nel campo HTRH.

   > Le intestazioni delle richieste del protocollo di audit vengono registrate solo se il livello di audit per **Client Reads** o **Client Writes** non è **Off**.

3. Seleziona **Save**

Configura la posizione del registro

Per impostazione predefinita, i messaggi di audit e i log vengono salvati sui nodi in cui vengono generati. Vengono periodicamente ruotati e infine eliminati per evitare che consumino troppo spazio su disco. Se vuoi salvare i messaggi di audit e un sottoinsieme di log esternamente, usa un server syslog esterno.

Se vuoi salvare i file di log internamente, scegli un tenant e un bucket per lo storage dei log e abilita l'archiviazione dei log.

Utilizza un server syslog esterno

Puoi configurare facoltativamente un syslog server esterno per salvare i log di audit, i log delle applicazioni e i log degli eventi di sicurezza in una posizione esterna alla tua grid.

> Se non vuoi usare un syslog server esterno, salta questo passaggio e vai a ${post_edited_translations.segment}.

> Se le opzioni di configurazione disponibili in questa procedura non sono abbastanza flessibili per soddisfare le tue esigenze, puoi applicare opzioni di configurazione aggiuntive usando gli endpoint `audit-destinations`, che si trovano nella sezione API privata del "API di gestione della griglia". Ad esempio, puoi usare l'API se vuoi utilizzare server syslog diversi per gruppi di nodi diversi.

Inserisci le informazioni di syslog

Accedi alla procedura guidata Configura server syslog esterno e fornisci le informazioni di cui StorageGRID ha bisogno per accedere al server syslog esterno.

Passaggi

1. Dalla scheda Nodo locale e server esterno, seleziona **Configura syslog server esterno**. Oppure, se hai già configurato un syslog server esterno, seleziona **Modifica syslog server esterno**.

   Viene visualizzata la procedura guidata Configura server syslog esterno.

2. Per il passaggio **Inserisci informazioni syslog** della procedura guidata, inserisci un fully qualified domain name valido oppure un indirizzo IPv4 o IPv6 per il server syslog esterno nel campo **Host**.

3. Inserisci la porta di destinazione sul server NTP syslog esterno (deve essere un numero intero compreso tra 1 e 65535). La porta predefinita è 514.
4. Seleziona il protocollo utilizzato per inviare le informazioni di audit al server syslog esterno.

   Si consiglia di utilizzare **TLS** o **RELP/TLS**. Devi caricare un certificato server per usare una di queste opzioni. L'uso dei certificati aiuta a proteggere le connessioni tra la tua grid e il server syslog esterno. Per maggiori informazioni, vedi "Gestisci i certificati di sicurezza".

   Tutte le opzioni del protocollo richiedono il supporto e la configurazione del server syslog esterno. Devi scegliere un'opzione compatibile con il server syslog esterno.

   > Il Reliable Event Logging Protocol (RELP) estende la funzionalità del protocollo syslog per garantire la consegna affidabile dei messaggi di evento. Usare RELP può aiutarti a prevenire la perdita di informazioni di audit se il tuo server syslog esterno deve essere riavviato.

5. Seleziona **Continue**.
6. Se hai selezionato **TLS** o **RELP/TLS**, carica i certificati CA del server, il certificato client e la chiave privata del client.
   a. Seleziona **Sfoglia** per il certificato o la chiave che vuoi usare.
   b. Seleziona il file del certificato o della chiave.
   c. Seleziona **Apri** per caricare il file.

      Accanto al nome del certificato o del file chiave compare un segno di spunta verde, che ti informa che è stato caricato correttamente.
7. Seleziona **Continue**.

Gestisci il contenuto di syslog

Puoi selezionare quali informazioni inviare al server syslog esterno.

Passaggi

1. Per la fase **Gestisci il contenuto syslog** della procedura guidata, seleziona ogni tipo di informazione di audit che vuoi inviare al server syslog esterno.
   - **Invia registri di controllo**: Invia eventi StorageGRID e attività di sistema
   - **Invia eventi di sicurezza**: Invia eventi di sicurezza come quando un utente non autorizzato tenta di accedere o un utente accede come root
   - **Invia i log dell'applicazione**: Invia "File di log del software StorageGRID" utili per la risoluzione dei problemi, tra cui:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Solo per nodi amministratori)
     - `prometheus.log`
     - `raft.log`

- `hagroups.log`

- **Invio dei log di accesso**: Invia i log di accesso HTTP per le richieste esterne a Grid Manager, Tenant Manager, endpoint del bilanciatore di carico configurati e richieste di federazione della griglia da sistemi remoti.

2. Utilizza i menu a tendina per selezionare il livello di gravità e la facility (tipo di messaggio) per ciascuna categoria di informazioni di audit che desideri inviare.

   Impostare i valori di gravità e di facility può aiutarti ad aggregare i log in modi personalizzabili per un'analisi più semplice.

   a. Per **Gravità**, seleziona **Passthrough** oppure seleziona un valore di gravità compreso tra 0 e 7.

      Se selezioni un valore, il valore selezionato verrà applicato a tutti i messaggi di questo tipo. Le informazioni sui diversi livelli di gravità andranno perse se sovrascrivi la gravità con un valore fisso.

Gravità	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno deve avere lo stesso valore di gravità di quando è stato registrato localmente sul nodo: • Per i registri di controllo, il livello di gravità è "info". • Per gli eventi di sicurezza, i valori di gravità vengono generati dalla distribuzione Linux sui nodi. • Nei log delle applicazioni, il livello di gravità varia tra "info" e "notice", a seconda del problema. Ad esempio, aggiungere un server NTP e configurare un gruppo HA dà un valore "info", mentre arrestare intenzionalmente il servizio SSM o RSM dà un valore "notice". • Per i registri di accesso, il livello di gravità è "info".
0	Emergenza: il sistema non è utilizzabile
1	Attenzione: devi intervenire immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore
4	Attenzione: condizioni di warning
5	Avviso: condizione normale ma significativa
6	Informativo: Messaggi informativi
7	Debug: messaggi di livello debug

   b. Per **Struttura**, seleziona **Passthrough** oppure seleziona un valore di struttura compreso tra 0 e 23.

      Se selezioni un valore, verrà applicato a tutti i messaggi di questo tipo. Le informazioni sulle diverse

facility andranno perse se sovrascrivi la facility con un valore fisso.

Struttura	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno deve avere lo stesso valore di facility di quando è stato registrato localmente sul nodo: • Per i log di controllo, la facility inviata al server syslog esterno è "local7". • Per gli eventi di sicurezza, i valori delle facility vengono generati dalla distribuzione Linux sui nodi. • Per i log delle applicazioni, i log delle applicazioni inviati al server syslog esterno hanno i seguenti valori di facility: ◦ `bycast.log`: utente o demone ◦ `bycast-err.log`: utente, demone, local3 o local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Per i log di accesso, la facility inviata al server syslog esterno è "local0".
0	kern (messaggi del kernel)
1	utente (messaggi a livello utente)
2	mail
3	demone (demoni di sistema)
4	auth (messaggi di sicurezza/autorizzazione)
5	syslog (messaggi generati internamente da syslogd)
6	lpr (sottosistema stampante di linea)
7	news (sottosistema di news di rete)
8	UUCP
9	cron (demone dell'orologio)
10	sicurezza (messaggi di sicurezza/autorizzazione)

Struttura	Descrizione
11	FTP
12	NTP
13	logaudit (log di audit)
14	logalert (avviso di registro)
15	orologio (demone clock)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Seleziona **Continue**.

Invia messaggi di prova

Prima di iniziare a utilizzare un server NTP esterno, dovresti chiedere a tutti i nodi della tua grid di inviare messaggi di prova al server NTP esterno. Dovresti usare questi messaggi di prova per aiutarti a convalidare l'intera infrastruttura di raccolta dei log prima di iniziare a inviare dati al server NTP esterno.

> Non utilizzare la configurazione del server syslog esterno finché non hai verificato che il server syslog esterno abbia ricevuto un messaggio di prova da ciascun nodo della tua griglia e che il messaggio sia stato elaborato come previsto.

Passaggi

1. Se non vuoi inviare messaggi di prova perché sei certo che il server syslog esterno sia configurato correttamente e possa ricevere informazioni di audit da tutti i nodi della tua grid, seleziona **Salta e termina**.

   Un banner verde indica che la configurazione è stata salvata.

2. In alternativa, seleziona **Invia messaggi di prova** (consigliato).

I risultati del test vengono visualizzati continuamente sulla pagina finché non interrompi il test. Durante l'esecuzione del test, i messaggi di audit continuano a essere inviati alle destinazioni configurate in precedenza.

3. Se ricevi errori durante la configurazione del server syslog o in fase di esecuzione, correggili e seleziona di nuovo **Invia messaggi di prova**.

   Vedi "Risolvi i problemi di un server syslog esterno" per aiutarti a risolvere eventuali errori.

4. Attendi finché non vedi un banner verde che indica che tutti i nodi hanno superato i test.
5. Controlla il tuo server syslog per verificare se i messaggi di test vengono ricevuti ed elaborati come previsto.

   Se usi UDP, controlla tutta la tua infrastruttura di raccolta dei log. Il protocollo UDP non permette un rilevamento degli errori rigoroso come gli altri protocolli.

6. Seleziona **Interrompi e termina**.

   Verrai reindirizzato alla pagina **Audit e syslog server**. Un banner verde indica che la configurazione del server syslog è stata salvata.

   Le informazioni di audit di StorageGRID non vengono inviate al server syslog esterno finché non selezioni una destinazione che includa il server syslog esterno.

${post_edited_translations.segment}

Puoi specificare dove vengono inviati i log di controllo, i log degli eventi di sicurezza, "Registri delle applicazioni StorageGRID" e i log di accesso.

StorageGRID utilizza per impostazione predefinita le destinazioni di audit dei nodi locali e memorizza le informazioni di audit in `/var/local/log/localaudit.log`.

Quando usi `/var/local/log/localaudit.log`, le voci del registro di audit di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo Storage. Puoi trovare quale nodo ha le voci più recenti usando il comando `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`.

Alcune destinazioni sono disponibili solo se hai configurato un server syslog esterno.

Passaggi

1. Seleziona **Posizione log** > **Nodo locale e server esterno**.
2. Per modificare la posizione dei file di log per i diversi tipi di log, seleziona un'opzione diversa.

   Solo nodi locali e **server syslog esterno** offrono in genere prestazioni migliori.

Opzione	Descrizione
Solo nodi locali (impostazione predefinita)	I messaggi di audit, i registri degli eventi di sicurezza e i registri delle applicazioni non vengono inviati ai nodi di amministrazione. Vengono invece salvati solo sui nodi che li hanno generati ("il nodo locale"). Le informazioni di audit generate su ogni nodo locale vengono memorizzate in `/var/local/log/localaudit.log`. **Nota**: StorageGRID rimuove periodicamente i log locali a rotazione per liberare spazio. Quando il file di log per un nodo raggiunge 1 GB, il file esistente viene salvato e viene avviato un nuovo file di log. Il limite di rotazione per il log è 21 file. Quando viene creata la 22a versione del file di log, il file di log più vecchio viene eliminato. In media, su ogni nodo vengono memorizzati circa 20 GB di dati di log. Per memorizzare i log per un periodo di tempo prolungato, usa un tenant e un bucket per l'archiviazione dei log.
${post_edited_translations.segment}	I messaggi di audit vengono inviati al file di log di audit sugli Admin Node, mentre i log degli eventi di sicurezza e i log delle applicazioni vengono memorizzati sui nodi che li hanno generati. Le informazioni di audit vengono memorizzate nei seguenti file: • Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante. Potrebbe contenere informazioni secondarie, come una copia aggiuntiva di alcuni messaggi.
${post_edited_translations.segment}	Le informazioni di audit vengono inviate a un server syslog esterno e salvate sui nodi locali (`/var/local/log/localaudit.log`). Il tipo di informazioni inviate dipende da come hai configurato il server syslog esterno. Questa opzione è abilitata solo dopo che hai configurato un server syslog esterno.
Nodi di amministrazione e server syslog esterno	I messaggi di audit vengono inviati al registro di audit (`/var/local/audit/export/audit.log`) sui nodi di amministrazione, e le informazioni di audit vengono inviate al server syslog esterno e salvate sul nodo locale (`/var/local/log/localaudit.log`). Il tipo di informazioni inviate dipende da come hai configurato il server syslog esterno. Questa opzione è abilitata solo dopo che hai configurato un server syslog esterno.

3. Seleziona **Salva**.

   Viene visualizzato un messaggio di avviso.

4. Seleziona **OK** per confermare che vuoi cambiare la destinazione delle informazioni di audit.

   I nuovi file di log vengono inviati alle destinazioni che hai selezionato. I file di log esistenti rimangono nella loro posizione attuale.

Usa un bucket

I log vengono ruotati periodicamente. Utilizza un bucket S3 nella stessa grid per archiviare i log per un periodo di tempo prolungato.

1. Seleziona **Log location** > **Usa un bucket**.
2. Seleziona la casella di controllo **Abilita archive logs**.
3. Se il tenant e il bucket elencati non sono quelli che vuoi usare, seleziona **Cambia tenant e bucket** e poi seleziona **Crea tenant e bucket** oppure **Seleziona tenant e bucket**.

   Crea tenant e bucket

   a. Inserisci un nuovo nome tenant.
   b. Inserisci e conferma una password per il nuovo tenant.
   c. Inserisci un nuovo nome per il bucket.
   d. Seleziona **Crea e abilita**.

   Seleziona tenant e bucket

   a. Seleziona un nome tenant dal menu a tendina.
   b. Seleziona un bucket dal menu a tendina.
   c. Seleziona **Seleziona e abilita**.

4. Seleziona **Salva**.

   I log verranno archiviati nel tenant e nel bucket che hai specificato. Il nome della chiave oggetto per i log ha questo formato:

   ```
   system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
   {last_modified_time}.gz
   ```

   Ad esempio:

   ```
   system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
   ```

Usa il monitoraggio SNMP

Utilizza il monitoraggio SNMP in StorageGRID

Se vuoi monitorare StorageGRID utilizzando il Simple Network Management Protocol (SNMP), devi configurare l'agente SNMP incluso in StorageGRID.

- "Configura l'agente SNMP"
- "Aggiorna l'agente SNMP"

Capacità

Ogni nodo StorageGRID esegue un agente SNMP, o demone, che fornisce una MIB. La MIB di StorageGRID contiene le definizioni di tabelle e notifiche per gli avvisi. La MIB contiene anche informazioni di descrizione del sistema, come la piattaforma e il numero di modello per ciascun nodo. Ogni nodo StorageGRID supporta inoltre un sottoinsieme di oggetti MIB-II.

Vedi "Accedi ai file MIB" se vuoi scaricare i file MIB sui nodi della tua griglia.

Inizialmente, SNMP è disabilitato su tutti i nodi. Quando configuri l'agente SNMP, tutti i nodi StorageGRID ricevono la stessa configurazione.

L'agente SNMP di StorageGRID supporta tutte e tre le versioni del protocollo SNMP. Fornisce accesso MIB in sola lettura per le query e può inviare due tipi di notifiche basate su eventi a un sistema di gestione:

Trappole

Le trap sono notifiche inviate dall'agente SNMP che non richiedono una conferma da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che è successo qualcosa all'interno di StorageGRID, come ad esempio l'attivazione di un avviso.

Le trap sono supportate in tutte e tre le versioni di SNMP.

Informa

Gli inform sono simili ai trap, ma richiedono una conferma da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, reinvia l'inform finché non riceve una conferma o viene raggiunto il valore massimo di tentativi.

Gli inform sono supportati in SNMPv2c e SNMPv3.

Le notifiche di intercettazione e informazione vengono inviate nei seguenti casi:

- Un avviso predefinito o personalizzato viene attivato a qualsiasi livello di gravità. Per sopprimere le notifiche SNMP per un avviso, devi "configura un silenzio" per l'avviso. Le notifiche di avviso vengono inviate dal "Nodo amministratore mittente preferito".

  Ogni avviso è mappato a uno dei tre tipi di trap in base al livello di gravità dell'avviso: activeMinorAlert, activeMajorAlert e activeCriticalAlert. Per un elenco degli avvisi che possono attivare queste trap, vedi il "Riferimento agli avvisi".

Supporto versioni SNMP

La tabella fornisce un riepilogo high-level di ciò che è supportato per ciascuna versione di SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Query (GET e GETNEXT)	Query MIB di sola lettura	Query MIB di sola lettura	Query MIB di sola lettura
Autenticazione della query	Stringa community	Stringa community	Utente del modello di sicurezza basato sull'utente (USM)

	SNMPv1	SNMPv2c	SNMPv3
Notifiche (TRAP e INFORM)	Solo trap	Trappole e informa	Trappole e informa
Autenticazione della notifica	Comunità di trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Comunità di trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Utente USM per ogni destinazione trap

Limitazioni

- StorageGRID supporta l'accesso MIB in sola lettura. L'accesso in lettura e scrittura non è supportato.
- Tutti i nodi della grid ricevono la stessa configurazione.
- SNMPv3: StorageGRID non supporta il Transport Support Mode (TSM).
- SNMPv3: L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).
- SNMPv3: L'unico protocollo di privacy supportato è AES.

Configura l'agente SNMP in StorageGRID

Puoi configurare l'agente SNMP di StorageGRID per utilizzare un sistema di gestione SNMP di terze parti per l'accesso MIB in sola lettura e le notifiche.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "Permesso di accesso root".

Informazioni su questa attività

L'agente SNMP di StorageGRID supporta SNMPv1, SNMPv2c e SNMPv3. Puoi configurare l'agente per una o più versioni. Per SNMPv3, è supportata solo l'autenticazione User Security Model (USM).

Tutti i nodi della griglia utilizzano la stessa configurazione SNMP.

Specifica la configurazione di base

Come primo passo, abilita l'agente SMNP di StorageGRID e fornisci le informazioni di base.

Passaggi

1. Seleziona **Configurazione** > **Monitoraggio** > **Agente SNMP**.

   Viene visualizzata la pagina dell'agente SNMP.

2. Per abilitare l'agente SNMP su tutti i nodi della griglia, seleziona la casella di controllo **Abilita SNMP**.
3. Inserisci le seguenti informazioni nella sezione Configurazione di base.

Campo	Descrizione
Contatto di sistema	Opzionale. Il contatto principale per il sistema StorageGRID, che viene restituito nei messaggi SNMP come sysContact. Il contatto di sistema è in genere un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID. **System contact** può contenere un massimo di 255 caratteri.
Posizione del sistema	Opzionale. La posizione del sistema StorageGRID, che viene restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere qualsiasi informazione utile per identificare dove si trova il tuo sistema StorageGRID. Ad esempio, puoi usare l'indirizzo della struttura. Questo valore si applica a tutti i nodi del sistema StorageGRID. **System location** può essere lungo al massimo 255 caratteri.
Abilita le notifiche dell'agente SNMP	• Se selezionato, l'agente SNMP di StorageGRID invia notifiche trap e inform. • Se non selezionato, l'agente SNMP supporta l'accesso MIB in sola lettura, ma non invia alcuna notifica SNMP.
Abilita le trap di autenticazione	Se selezioni questa opzione, l'agente SNMP di StorageGRID invia trap di autenticazione se riceve messaggi di protocollo non autenticati correttamente.

Inserisci le stringhe della community

Se usi SNMPv1 o SNMPv2c, completa la sezione delle stringhe della community.

Quando il sistema di gestione interroga la MIB di StorageGRID, invia una stringa di comunità. Se la stringa di comunità corrisponde a uno dei valori specificati qui, l'agente SNMP invia una risposta al sistema di gestione.

Passaggi

1. Per la **community di sola lettura**, puoi inserire facoltativamente una stringa di community per consentire l'accesso MIB in sola lettura agli indirizzi agente IPv4 e IPv6.

   Per garantire la sicurezza del tuo sistema StorageGRID, non usare "public" come stringa di comunità. Se lasci questo campo vuoto, l'agente SNMP usa l'ID grid del tuo sistema StorageGRID come stringa di comunità.

   Ogni stringa di comunità può contenere un massimo di 32 caratteri e non può contenere caratteri di spazio.

2. Seleziona **Aggiungi un'altra stringa della community** per aggiungere altre stringhe.

   Sono consentite fino a cinque stringhe.

Crea destinazioni trap

Utilizza la scheda Destinazioni trap nella sezione Altre configurazioni per definire una o più destinazioni per le notifiche trap o inform di StorageGRID. Quando abiliti l'agente SNMP e selezioni **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inviate anche notifiche standard per le entità MIB-II supportate (ad esempio, ifDown e coldStart).

Passaggi

1. Per il campo **Community trap predefinita**, inserisci facoltativamente la stringa community predefinita che vuoi usare per le destinazioni trap SNMPv1 o SNMPv2.

   Se necessario, puoi fornire una stringa di comunità diversa ("personalizzata") quando definisci una destinazione trap specifica.

   La **trap community predefinita** può essere lunga al massimo 32 caratteri e non può contenere spazi.

2. Per aggiungere una destinazione trap, seleziona **Crea**.
3. Seleziona quale versione SNMP verrà utilizzata per questa destinazione trap.
4. Completa il modulo Crea destinazione trap per la versione che hai selezionato.

SNMPv1

Se hai selezionato SNMPv1 come versione, compila questi campi.

Campo	Descrizione
Tipo	Deve essere Trap per SNMPv1.
Host	Un indirizzo IPv4 o IPv6 oppure un domain name (FQDN) per ricevere la trap.
Porta	Utilizza 162, che è la porta standard per le trap SNMP, a meno che tu non debba utilizzare un valore diverso.
Protocollo	Utilizza UDP, che è il protocollo standard SNMP trap, a meno che tu non debba utilizzare TCP.
Stringa community	Utilizza la community di trap predefinita, se ne è stata specificata una, oppure inserisci una stringa di community personalizzata per questa destinazione di trap. La stringa della community personalizzata può essere lunga al massimo 32 caratteri e non può contenere spazi.

SNMPv2c

Se hai selezionato SNMPv2c come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o inform.
Host	Un indirizzo IPv4 o IPv6 oppure un FQDN per ricevere la trap.
Porta	Utilizza la 162, che è la porta standard per le trap SNMP, a meno che tu non debba usare un altro valore.
Protocollo	Utilizza UDP, che è il protocollo standard SNMP trap, a meno che tu non debba utilizzare TCP.
Stringa community	Utilizza la community di trap predefinita, se ne è stata specificata una, oppure inserisci una stringa di community personalizzata per questa destinazione di trap. La stringa della community personalizzata può essere lunga al massimo 32 caratteri e non può contenere spazi.

SNMPv3

Se hai selezionato SNMPv3 come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o inform.
Host	Un indirizzo IPv4 o IPv6 oppure un FQDN per ricevere la trap.
Porta	Utilizza la 162, che è la porta standard per le trap SNMP, a meno che tu non debba usare un altro valore.
Protocollo	Utilizza UDP, che è il protocollo standard SNMP trap, a meno che tu non debba utilizzare TCP.
utente USM	L'utente USM che userai per l'autenticazione. • Se hai selezionato **Trap**, vengono mostrati solo gli utenti USM senza ID motore autorevoli. • Se hai selezionato **Inform**, vengono mostrati solo gli utenti USM con engine ID autorevoli. • Se non vengono visualizzati utenti: i. Crea e salva la destinazione trap. ii. Vai su Crea utenti USM e crea l'utente. iii. Torna alla scheda Destinazioni Trap, seleziona la destinazione salvata dalla tabella e seleziona **Modifica**. iv. Seleziona l'utente.

5. Seleziona **Create**.

   La destinazione trap viene creata e aggiunta alla tabella.

Crea indirizzi agente

Facoltativamente, usa la scheda Indirizzi agente nella sezione Altre configurazioni per specificare uno o più "indirizzi di ascolto". Questi sono gli indirizzi StorageGRID su cui l'agente SNMP può ricevere le query.

Se non configuri un indirizzo agente, l'indirizzo di ascolto predefinito è la porta UDP 161 su tutte le reti StorageGRID.

Passaggi

1. Seleziona **Create**.
2. Inserisci le seguenti informazioni.

Campo	Descrizione
Protocollo Internet	Indica se questo indirizzo utilizzerà IPv4 o IPv6. Per impostazione predefinita, SNMP utilizza IPv4.

Campo	Descrizione
Protocollo di trasporto	Se questo indirizzo utilizzerà UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
rete StorageGRID	Su quale rete StorageGRID l'agente rimarrà in ascolto. • Reti Grid, Admin e Client: l'agente SNMP ascolterà le query su tutte e tre le reti. • ${post_edited_translations.segment} • Rete di amministrazione • ${post_edited_translations.segment} **Nota**: Se usi la rete client per dati non protetti e crei un indirizzo agente per la rete client, sappi che anche il traffico SNMP sarà non protetto.
Porta	Facoltativamente, il numero di porta su cui l'agente SNMP deve ascoltare. La porta UDP predefinita per un agente SNMP è 161, ma puoi inserire qualsiasi numero di porta non utilizzato. **Nota**: Quando salvi l'agente SNMP, StorageGRID apre automaticamente le porte dell'indirizzo dell'agente sul firewall interno. Devi assicurarti che eventuali firewall esterni consentano l'accesso a queste porte.

3. Seleziona **Create**.

   L'indirizzo dell'agente viene creato e aggiunto alla tabella.

Crea utenti USM

Se usi SNMPv3, usa la scheda Utenti USM nella sezione Altre configurazioni per definire gli utenti USM autorizzati a interrogare la MIB o a ricevere trap e inform.

> Per le destinazioni SNMPv3 *trap*, si consiglia di creare un utente USM per ogni Admin Node. Se ogni Admin Node non dispone di un utente USM, il sistema di gestione potrebbe smettere di ricevere notifiche se il primary Admin Node va giù.

> Le destinazioni SNMPv3 *inform* devono avere utenti con ID motore. Le destinazioni SNMPv3 *trap* non possono avere utenti con ID motore.

Questi passaggi non si applicano se usi solo SNMPv1 o SNMPv2c.

Passaggi

1. Seleziona **Create**.

2. Inserisci le seguenti informazioni.

Campo	Descrizione
Nome utente	Un nome univoco per questo utente USM. I nomi utente possono avere una lunghezza massima di 32 caratteri e non possono contenere spazi. Il nome utente non può essere modificato dopo la creazione dell'utente.
Accesso MIB in sola lettura	Se selezionato, questo utente dovrebbe avere accesso in sola lettura alla MIB.
ID motore autorevole	Se userai questo utente in una destinazione inform, l'ID del motore autorevole per questo utente. Inserisci da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è obbligatorio per gli utenti USM che verranno selezionati come destinazione delle trap per gli inform. Questo valore non è consentito per gli utenti USM che verranno selezionati come destinazione delle trap per le trap. **Nota**: Questo campo non viene visualizzato se hai selezionato **Accesso MIB in sola lettura** perché gli utenti USM con accesso MIB in sola lettura non possono avere engine ID.
Livello di sicurezza	Livello di sicurezza per l'utente USM: • **authPriv**: Questo utente comunica tramite autenticazione e privacy (crittografia). Devi specificare un protocollo di autenticazione e una password e un protocollo di privacy e una password. • **authNoPriv**: Questo utente comunica con autenticazione e senza riservatezza (nessuna crittografia). Devi specificare un protocollo di autenticazione e una password.
Protocollo di autenticazione	Imposta sempre su SHA, che è l'unico protocollo supportato (HMAC-SHA-96).
Password	La password che questo utente userà per l'autenticazione.
Protocollo sulla privacy	Mostrato solo se hai selezionato **authPriv** e sempre impostato su AES, che è l'unico protocollo di privacy supportato.
Password	Mostrato solo se hai selezionato **authPriv**. La password che questo utente utilizzerà per la privacy.

3. Seleziona **Create**.

   L'utente USM viene creato e aggiunto alla tabella.

4. Quando hai completato la configurazione dell'agente SNMP, seleziona **Salva**.

   La nuova configurazione dell'agente SNMP diventa attiva.

Aggiorna l'agente SNMP di StorageGRID

Puoi disabilitare le notifiche SNMP, aggiornare le stringhe di comunità o aggiungere o rimuovere indirizzi agente, utenti USM e destinazioni trap.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "Permesso di accesso root".

Informazioni su questa attività

Vedi "Configura l'agente SNMP" per i dettagli su ciascun campo nella pagina dell'agente SNMP. Devi selezionare **Salva** in fondo alla pagina per confermare qualsiasi modifica apportata in ciascuna scheda.

Passaggi

1. Seleziona **Configurazione** > **Monitoraggio** > **Agente SNMP**.

   Viene visualizzata la pagina dell'agente SNMP.

2. Per disabilitare l'agente SNMP su tutti i nodi della griglia, deseleziona la casella di controllo **Abilita SNMP** e seleziona **Salva**.

   Se riattivi l'agente SNMP, le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Facoltativamente, aggiorna le informazioni nella sezione Configurazione di base:
   a. Se necessario, aggiorna il **contatto di sistema** e la **posizione del sistema**.
   b. Facoltativamente, seleziona o deseleziona la casella di controllo **Abilita notifiche agente SNMP** per controllare se l'agente SNMP di StorageGRID invia notifiche trap e inform.

      Quando questa casella di controllo non è selezionata, l'agente SNMP supporta l'accesso MIB in sola lettura, ma non invia notifiche SNMP.

   c. Facoltativamente, seleziona o deseleziona la casella di controllo **Abilita trap di autenticazione** per controllare se l'agente SNMP di StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo non autenticati correttamente.
4. Se usi SNMPv1 o SNMPv2c, puoi aggiornare o aggiungere una **community di sola lettura** nella sezione Stringhe della community.
5. Per aggiornare le destinazioni trap, seleziona la scheda Destinazioni trap nella sezione Altre configurazioni.

   Utilizza questa scheda per definire una o più destinazioni per le notifiche trap o inform di StorageGRID. Quando abiliti l'agente SNMP e selezioni **Salva**, StorageGRID invia notifiche a ciascuna destinazione quando vengono attivati gli avvisi. Vengono inviate anche notifiche standard per le entità MIB-II supportate (ad esempio, ifDown e coldStart).

   Per i dettagli su cosa inserire, vedi "Crea destinazioni trap".

   - Facoltativamente, aggiorna o rimuovi la trap community predefinita.

Se rimuovi la community predefinita per le trap, devi prima assicurarti che tutte le destinazioni delle trap esistenti utilizzino una stringa di community personalizzata.

- Per aggiungere una destinazione trap, seleziona **Crea**.
- Per modificare una destinazione trap, seleziona il pulsante di opzione e seleziona **Modifica**.
- Per rimuovere una destinazione trap, seleziona il pulsante di opzione e seleziona **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

6. Per aggiornare gli indirizzi degli agenti, seleziona la scheda Indirizzi degli agenti nella sezione Altre configurazioni.

   Utilizza questa scheda per specificare uno o più "indirizzi di ascolto". Questi sono gli indirizzi StorageGRID sui quali l'agente SNMP può ricevere query.

   Per i dettagli su cosa inserire, vedi "Crea indirizzi agente".

   - Per aggiungere un indirizzo agente, seleziona **Crea**.
   - Per modificare l'indirizzo di un agente, seleziona il pulsante di opzione e seleziona **Modifica**.
   - Per rimuovere un indirizzo agente, seleziona il pulsante di opzione e seleziona **Rimuovi**.
   - Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

7. Per aggiornare gli utenti USM, seleziona la scheda Utenti USM nella sezione Altre configurazioni.

   Usa questa scheda per definire gli utenti USM autorizzati a interrogare la MIB o a ricevere trap e inform.

   Per i dettagli su cosa inserire, vedi "Crea utenti USM".

   - Per aggiungere un utente USM, seleziona **Crea**.
   - Per modificare un utente USM, seleziona il pulsante di opzione e seleziona **Modifica**.

     Il nome utente di un utente USM esistente non può essere cambiato. Se devi cambiare un nome utente, devi rimuovere l'utente e crearne uno nuovo.

     > Se aggiungi o rimuovi l'ID motore autorevole di un utente e quell'utente è attualmente selezionato per una destinazione, devi modificare o rimuovere la destinazione. Altrimenti, si verifica un errore di convalida quando salvi la configurazione dell'agente SNMP.

   - Per rimuovere un utente USM, seleziona il pulsante di opzione e seleziona **Rimuovi**.

     > Se l'utente che hai rimosso è attualmente selezionato per una destinazione trap, devi modificare o rimuovere la destinazione. Altrimenti, si verifica un errore di convalida quando salvi la configurazione dell'agente SNMP.

   - Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

8. Quando hai aggiornato la configurazione dell'agente SNMP, seleziona **Salva**.

Accedere ai file MIB di StorageGRID

I file MIB contengono definizioni e informazioni sulle proprietà delle risorse e dei servizi gestiti per i nodi della tua griglia. Puoi accedere ai file MIB che definiscono gli oggetti e le notifiche per StorageGRID. Questi file possono essere utili per monitorare la tua griglia.

Vedi "Usa il monitoraggio SNMP" per ulteriori informazioni su SNMP e sui file MIB.

Accedi ai file MIB

Segui questi passaggi per accedere ai file MIB.

Passaggi

1. Seleziona **Configurazione** > **Monitoraggio** > **Agente SNMP**.
2. Nella pagina dell'agente SNMP, seleziona il file che vuoi scaricare:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definisce la tabella degli avvisi e le notifiche (trap) accessibili su tutti i nodi di amministrazione.
   - **ES-NETAPP-06-MIB.mib**: Definisce oggetti e notifiche per appliance basati su E-Series.
   - **MIB_1_10.zip**: Definisce oggetti e notifiche per dispositivi con interfaccia BMC.

   Puoi anche accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID di StorageGRID dal file MIB:
   a. Ottieni l'OID della radice della MIB di StorageGRID:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Risultato: `.1.3.6.1.4.1.789.28669` (`28669` è sempre l'OID per StorageGRID)

   b. Cerca l'OID di StorageGRID nell'intero albero (utilizzando `paste` per unire le righe):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

   Il comando `snmptranslate` offre molte opzioni utili per esplorare la MIB. Questo comando è disponibile su qualsiasi nodo StorageGRID.

Contenuto del file MIB

Tutti gli oggetti sono sotto l'OID di StorageGRID.

Nome oggetto	ID oggetto (OID)	Descrizione
		Il modulo MIB per le entità NetApp StorageGRID.

oggetti MIB

Nome oggetto	ID oggetto (OID)	Tipo	Accesso	Modulo MIB	Descrizione
activeAlertCount		Integer32	Sola lettura	NETAPP-STORAGEGRID-MIB	Il numero di avvisi attivi nella activeAlertTable.

Nome oggetto	ID oggetto (OID)	Tipo	Accesso	Modulo MIB	Descrizione
activeAlertTable		Sequenza di ActiveAlertEntry	Non accessibile	NETAPP-STORAGEGRID-MIB	Una tabella degli avvisi attivi in StorageGRID.
activeAlertEntry		Sequenza	Non accessibile	NETAPP-STORAGEGRID-MIB	Un singolo avviso StorageGRID, indicizzato tramite ID avviso.
activeAlertId		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	L'ID dell'avviso. Univoco solo nell'insieme corrente di avvisi attivi.
activeAlertName		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	Il nome dell'allerta.
activeAlertInstance		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
activeAlertSeverity		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	La gravità dell'allerta.
activeAlertStartTime		Data e ora	Sola lettura	NETAPP-STORAGEGRID-MIB	L'ora in cui è scattato l'allarme.

Raccogli ulteriori dati StorageGRID

Monitorare le prestazioni PUT e GET in StorageGRID

Puoi monitorare le prestazioni di alcune operazioni, come archivio di oggetti e recupero, per aiutarti a identificare cambiamenti che potrebbero richiedere ulteriori indagini.

Informazioni su questa attività

Per monitorare le prestazioni delle operazioni PUT e GET, puoi eseguire i comandi S3 direttamente da una workstation oppure utilizzando l'applicazione open source S3tester. Usando questi metodi puoi valutare le prestazioni indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o con una rete esterna.

Quando esegui test delle operazioni PUT e GET, segui queste linee guida:

- Utilizza dimensioni degli oggetti paragonabili a quelle degli oggetti che solitamente inserisci nella tua grid.
- Esegui operazioni sia su siti locali che remoti.

I messaggi "registro di controllo" indicano il tempo totale necessario per eseguire determinate operazioni. Ad

esempio, per determinare il tempo totale di elaborazione per una richiesta S3 GET, puoi esaminare il valore dell'attributo TIME nel messaggio di audit SGET. Puoi anche trovare l'attributo TIME nei messaggi di audit per le seguenti operazioni S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Quando analizzi i risultati, guarda il tempo medio necessario per soddisfare una richiesta, così come il throughput complessivo che puoi ottenere. Ripeti regolarmente gli stessi test e registra i risultati, così puoi individuare tendenze che potrebbero richiedere un'indagine.

- È possibile "Scarica S3tester da GitHub".

Monitorare le operazioni di verifica degli oggetti in StorageGRID

Il sistema StorageGRID può verificare l'integrità dei dati degli oggetti sui nodi di archiviazione, controllando sia gli oggetti danneggiati che quelli mancanti.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di manutenzione o di accesso root".

Informazioni su questa attività

Due "processi di verifica" lavorano insieme per garantire l'integrità dei dati:

- **La verifica in background** viene eseguita automaticamente, controllando continuamente la correttezza dei dati degli oggetti.

  La verifica in background controlla automaticamente e continuamente tutti i nodi di Storage per determinare se sono presenti copie danneggiate dei dati degli oggetti replicati e codificati per la cancellazione. Se vengono rilevati problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati degli oggetti danneggiati con copie archiviate altrove nel sistema. La verifica in background non viene eseguita sugli oggetti in un Cloud Storage Pool.

  > ⓘ L'avviso **Rilevato oggetto danneggiato non identificato** viene attivato se il sistema rileva un oggetto danneggiato che non può essere corretto automaticamente.

- La funzione **Controllo esistenza oggetto** può essere attivata da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) dei dati oggetto.

  Il controllo di esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti codificati per la cancellazione esistono su un Storage Node. Il controllo di esistenza degli oggetti offre un modo per verificare l'integrità dei dispositivi di storage, soprattutto se un recente problema hardware potrebbe aver influenzato l'integrità dei dati.

Dovresti esaminare regolarmente i risultati delle verifiche in background e dei controlli di esistenza degli oggetti. Indaga subito su eventuali casi di dati degli oggetti corrotti o mancanti per determinarne la causa principale.

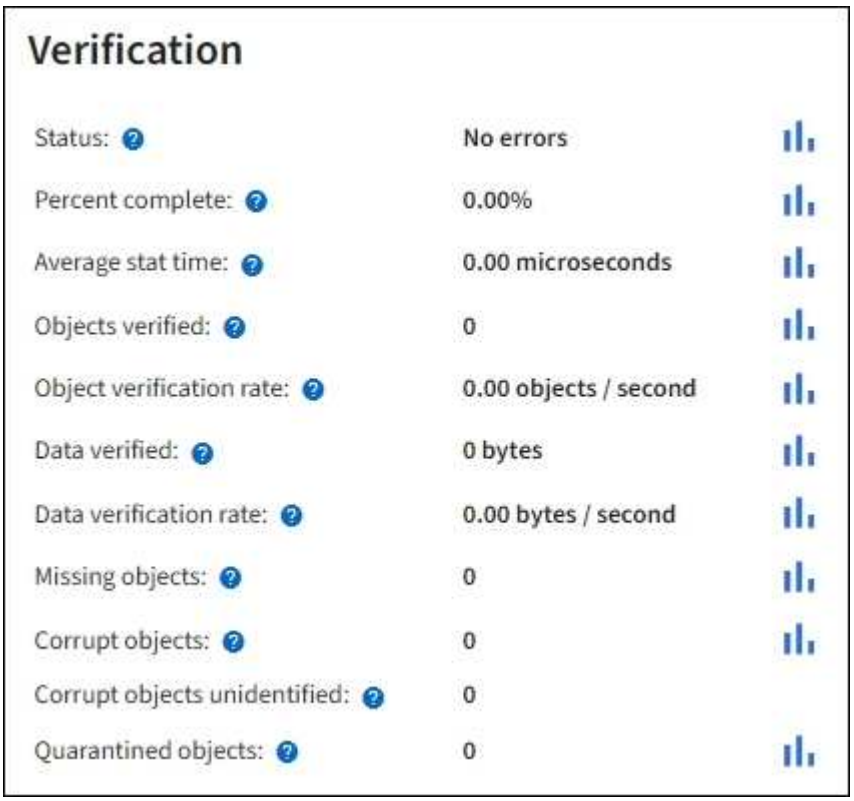
Passaggi

1. Esamina i risultati delle verifiche dei precedenti:

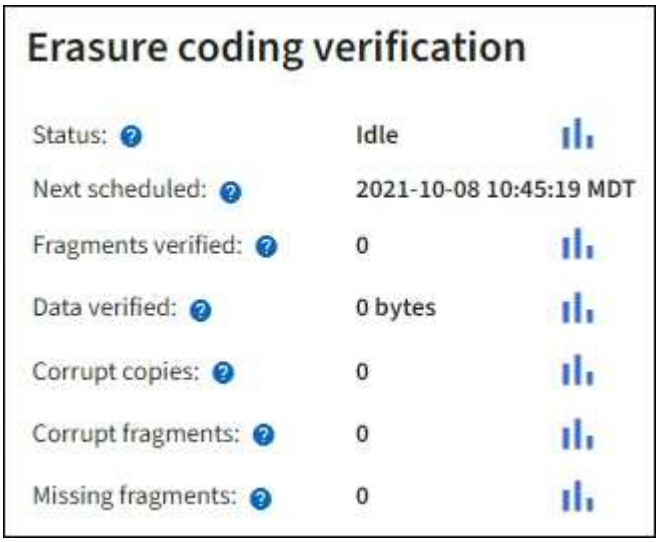
   a. Seleziona **Nodes** > ***Storage Node*** > **Objects**.

   b. Controlla i risultati della verifica:

- Per verificare la validità dei dati degli oggetti replicati, guarda gli attributi nella sezione Verifica.

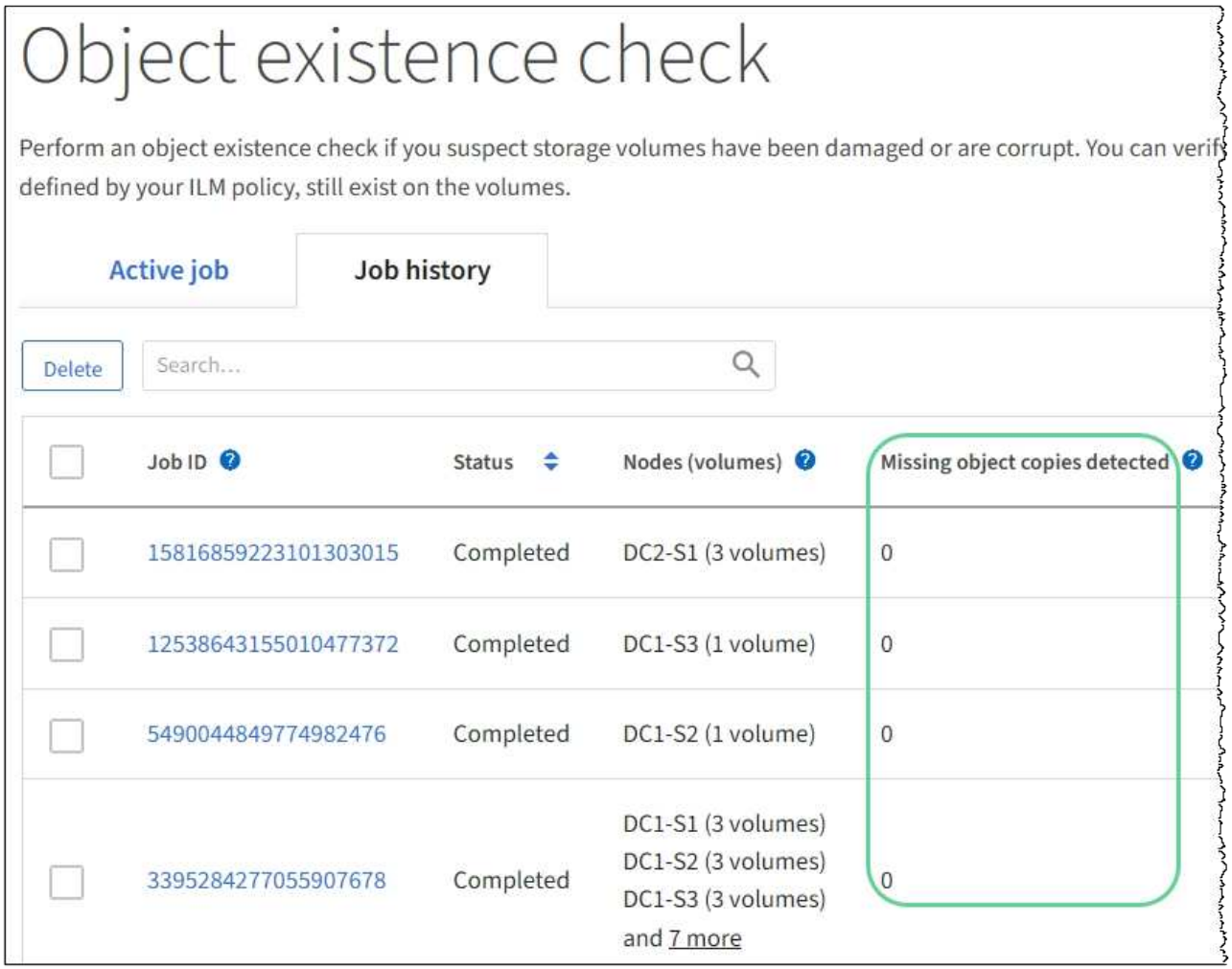


- Per controllare la verifica dei frammenti con codifica di cancellazione, seleziona ***Storage Node*** > **ILM** e consulta gli attributi nella sezione Verifica della codifica di cancellazione.



Seleziona il punto interrogativo (?) accanto al nome di un attributo per visualizzare il testo di aiuto.

2. Esamina i risultati delle operazioni di verifica dell'esistenza degli oggetti:
   a. Seleziona **Manutenzione** > **Verifica esistenza oggetto** > **Cronologia interventi**.
   b. Esamina la colonna "Copie di oggetti mancanti rilevate". Se uno qualsiasi dei processi ha generato 100 o più copie di oggetti mancanti e l'avviso **Oggetti potenzialmente persi** è stato attivato, contatta il supporto tecnico.



Esaminare i messaggi di audit di StorageGRID

I messaggi di audit possono aiutarti a comprendere meglio il funzionamento dettagliato del tuo sistema StorageGRID. Puoi utilizzare i log di audit per risolvere i problemi e valutare le prestazioni.

Durante il normale funzionamento del sistema, tutti i servizi di StorageGRID generano messaggi di audit, come segue:

- I messaggi di audit del sistema sono correlati al sistema di auditing stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema e alle operazioni di backup dei servizi.
- I messaggi di controllo dello storage a oggetti sono correlati allo storage e alla gestione degli oggetti all'interno di StorageGRID, inclusi lo storage a oggetti e i recuperi, i trasferimenti da nodo della griglia a nodo della griglia e le verifiche.
- I messaggi di audit di lettura e scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare, modificare o recuperare un oggetto.
- I messaggi di audit della gestione registrano le richieste degli utenti all'API di Management.

Ogni nodo amministratore memorizza i messaggi di audit in file di testo. La cartella condivisa di audit contiene il file attivo (audit.log) e i log di audit compressi dei giorni precedenti. Ogni nodo della griglia memorizza inoltre una copia delle informazioni di audit generate sul nodo stesso.

Puoi accedere ai file di log di audit direttamente dalla riga di comando dell'Admin Node.

StorageGRID può inviare le informazioni di audit per impostazione predefinita, oppure puoi cambiarne la destinazione:

- StorageGRID utilizza come destinazione predefinita per l'audit le destinazioni dei nodi locali.
- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di storage.
- Facoltativamente, puoi modificare la destinazione dei log di audit e inviare le informazioni di audit a un server syslog esterno. I log locali dei record di audit continuano a essere generati e archiviati quando è configurato un server syslog esterno.
- "Scopri come configurare la gestione dei log".

Per dettagli sul file di log di audit, sul formato dei messaggi di audit, sui tipi di messaggi di audit e sugli strumenti disponibili per analizzare i messaggi di audit, vedi "${post_edited_translations.segment}".

Raccogli i file di registro StorageGRID e i dati di sistema

Puoi recuperare i file di log di StorageGRID e i dati di sistema, inclusi i dati di configurazione, e inviarli al supporto tecnico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su qualsiasi nodo Admin utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- ${post_edited_translations.segment}

Informazioni su questa attività

Utilizza Grid Manager per raccogliere "file di log", dati di sistema e dati di configurazione da qualsiasi nodo della griglia per il periodo di tempo che selezioni. I dati vengono raccolti e archiviati in un `.tar.gz` file che puoi quindi scaricare sul tuo computer locale o inviare al supporto tecnico.

Facoltativamente, puoi modificare la destinazione dei log di audit e inviare le informazioni di audit a un server syslog esterno. I log locali dei record di audit continuano a essere generati e archiviati quando è configurato un server syslog esterno. Vedi "Configura la gestione dei log e il server syslog esterno".

Passaggi

1. Seleziona **Support** > **Tools** > **Log collection**. Viene visualizzata una tabella di nodi.
2. Seleziona i nodi della griglia per i quali vuoi raccogliere i file di log.

   Puoi ordinare per nome del nodo, sito e tipo di nodo. Le colonne Sito e Tipo di nodo contengono filtri per selezionare singoli siti e tipi di nodo.

3. Seleziona **Continue**.
4. Seleziona l'intervallo di date e orari dei dati da includere nei file di log.

   Se selezioni un periodo di tempo molto lungo o raccogli i log da tutti i nodi di una griglia di grandi dimensioni, l'archivio dei log potrebbe diventare troppo grande per essere memorizzato su un nodo o troppo grande per essere raccolto da un Admin Node per il download. Se si verifica uno di questi scenari, riavvia la raccolta dei log con un set di dati più piccolo.

5. Seleziona i tipi di log che desideri raccogliere.
   - **Log delle applicazioni**: Log specifici delle applicazioni che il supporto tecnico utilizza più frequentemente per la risoluzione dei problemi. I log raccolti rappresentano un sottoinsieme dei log delle applicazioni disponibili.
   - **Registri di controllo**: Registri contenenti i messaggi di controllo generati durante il normale funzionamento del sistema.
   - **Traccia di rete**: Log utilizzati per il debug della rete.
   - **Database Prometheus**: metriche delle serie temporali dai servizi su tutti i nodi.
6. Facoltativamente, utilizza la casella di testo **Note** per inserire note sui file di log che stai raccogliendo.

   Puoi usare queste note per fornire informazioni di supporto tecnico sul problema che ti ha spinto a raccogliere i file di log. Le tue note vengono aggiunte a un file chiamato `info.txt`, insieme ad altre informazioni sulla raccolta dei file di log. Il file `info.txt` viene salvato nel pacchetto di archivio dei file di log.

7. Nella casella di testo **Passphrase di provisioning**, inserisci la passphrase di provisioning per il tuo sistema StorageGRID.
8. Seleziona **Raccogli log**.

   Puoi usare la pagina di raccolta dei log per monitorare l'avanzamento della raccolta dei file di log per ogni nodo della griglia.

   Se ricevi un messaggio di errore relativo alle dimensioni del file di log, prova a raccogliere i log per un periodo di tempo più breve o per un numero inferiore di nodi.

9. Se la raccolta dei log non riesce:
   - Se viene visualizzato il messaggio "Raccolta dei log non riuscita", puoi riprovare la raccolta dei log oppure terminare la sessione senza riprovare.
   - Se viene visualizzato il messaggio "Raccolta dei log parzialmente non riuscita", puoi riprovare la raccolta dei log, terminare la sessione, scaricare il file di log o inviare il file di log a AutoSupport.
10. Quando la raccolta dei file di log è completa:
    - Seleziona **Scarica** per scaricare il `.tar.gz` file.
    - Seleziona **Invia a AutoSupport** per inviare il file `.tar.gz` al supporto tecnico.

      Il `.tar.gz`file contiene tutti i file di log di tutti i nodi della griglia in cui la raccolta dei log è andata a buon fine. Il `.tar.gz`file combinato contiene un archivio di file di log per ciascun nodo della griglia.

    L'oggetto del pacchetto AutoSupport è `USER_TRIGGERED_SUPPORT_BUNDLE`.

11. Seleziona **Fine**.

    Il `.tar.gz`file viene eliminato quando selezioni **Fine**. Assicurati di scaricare o inviare prima il file.

Attivare manualmente un pacchetto StorageGRID AutoSupport

Per aiutare il supporto tecnico a risolvere i problemi del tuo sistema StorageGRID, puoi

inviare manualmente un pacchetto AutoSupport.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai l'accesso Root o l'autorizzazione per altre configurazioni della grid.

Passaggi

1. Seleziona **Support** > **Tools** > **AutoSupport**.
2. Nella scheda **Azioni**, seleziona **Invia AutoSupport attivato dall'utente**.

   StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp. Se il tentativo ha esito positivo, i valori **Risultato più recente** e **Ultimo momento in cui l'operazione è andata a buon fine** nella scheda **Risultati** vengono aggiornati. Se c'è un problema, il valore **Risultato più recente** viene aggiornato a "Non riuscito" e StorageGRID non prova a inviare di nuovo il pacchetto AutoSupport.

3. Dopo 1 minuto, aggiorna la pagina AutoSupport nel tuo browser per accedere ai risultati più recenti.

Inoltre, puoi "raccogli file di registro e dati di sistema più completi" e inviarli al NetApp Support Site.

Esaminare le metriche di StorageGRID

Quando risolvi un problema, puoi collaborare con il supporto tecnico per esaminare metriche e grafici dettagliati del tuo sistema StorageGRID.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

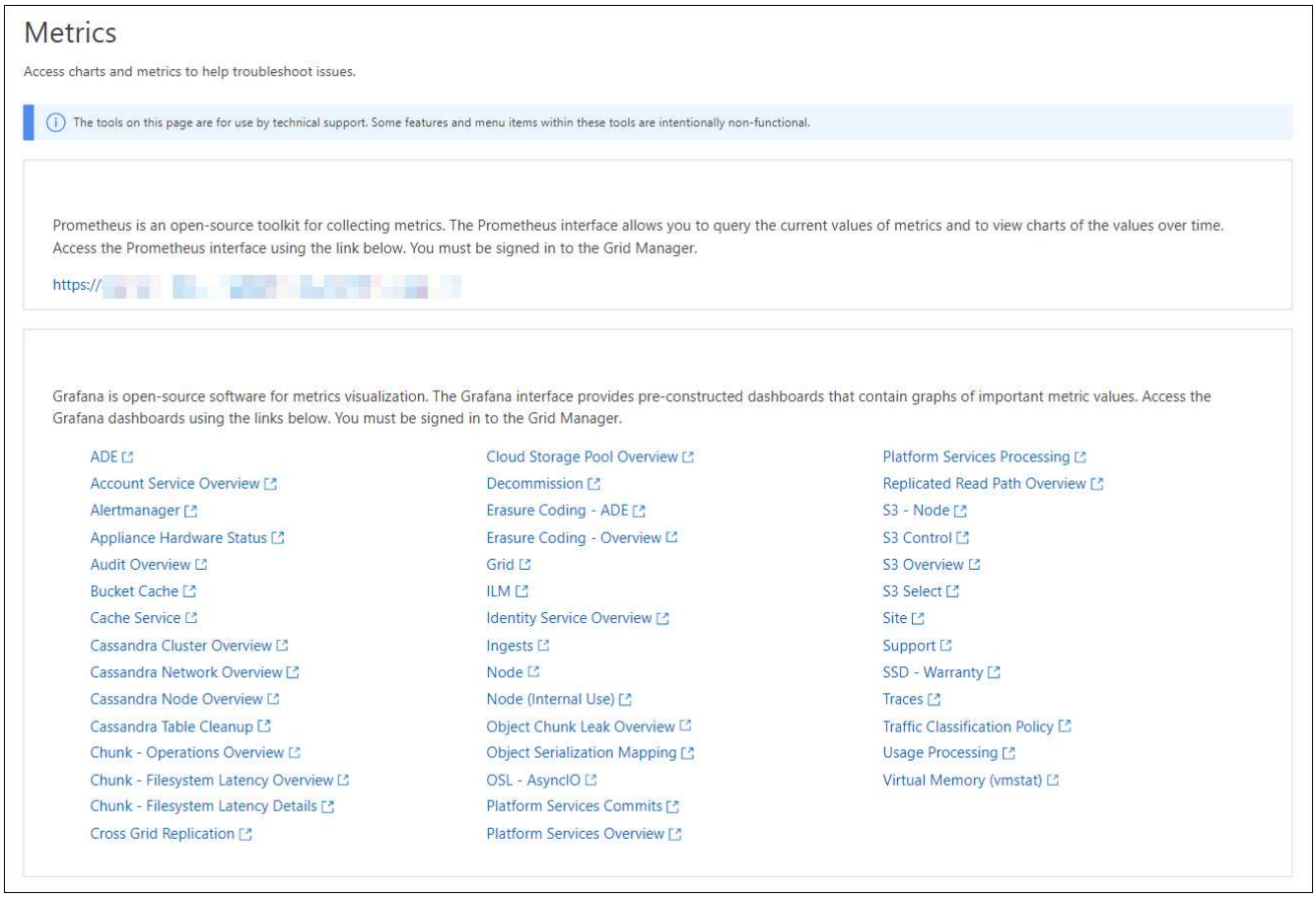
La pagina Metriche consente di accedere alle interfacce utente di Prometheus e Grafana. Prometheus è un software open source per la raccolta delle metriche. Grafana è un software open source per la visualizzazione delle metriche.

Gli strumenti disponibili nella pagina Metriche sono pensati per l'uso da parte del supporto tecnico. Alcune funzionalità e voci di menu all'interno di questi strumenti sono intenzionalmente non funzionanti e sono soggette a modifiche. Vedi l'elenco di "metriche Prometheus comunemente utilizzate".

Passaggi

1. Come indicato dal supporto tecnico, seleziona **Support** > **Tools** > **Metrics**.

   Ecco un esempio della pagina delle metriche:



2. Per interrogare i valori correnti delle metriche di StorageGRID e per visualizzare i grafici dei valori nel tempo, fai clic sul link nella sezione Prometheus.

   Viene visualizzata l'interfaccia di Prometheus. Puoi utilizzare questa interfaccia per eseguire query sulle metriche di StorageGRID e per visualizzare graficamente le metriche di StorageGRID nel tempo.

   > Le metriche che includono *private* nel loro nome sono destinate esclusivamente all'uso interno e sono soggette a modifiche tra le versioni di StorageGRID senza preavviso.

3. Per accedere a dashboard predefinite contenenti grafici delle metriche di StorageGRID nel tempo, fai clic sui collegamenti nella sezione Grafana.

   Viene visualizzata l'interfaccia di Grafana per il link che hai selezionato.

Modifica la priorità di I/O in StorageGRID

La prioritizzazione di input/output (I/O) ti permette di modificare le priorità relative delle operazioni di I/O sul grid.

Per impostazione predefinita, al traffico I/O PUT e GET dei client viene assegnata la massima priorità rispetto alle attività in background come la cancellazione dei dati erasure-coded (EC) e la riparazione EC. Aumentando la priorità delle attività di cancellazione dei dati erasure-coded (EC) e di riparazione EC, queste attività possono essere completate più rapidamente. L'efficacia delle modifiche alla priorità I/O è influenzata dalla frequenza delle richieste dei client, dalle fluttuazioni del traffico di rete e da altre attività di rete in corso.

Prima di iniziare

- Esamina la pagina di prioritizzazione I/O per determinare quali opzioni potrebbero influire sul tuo grid.
- Valuta se il traffico di client in corso può gestire in sicurezza tempi di attesa più lunghi o timeout dei client.
- Preparati a monitorare l'effetto della modifica delle priorità e ad apportare le modifiche necessarie. Queste modifiche vengono implementate rapidamente, ma potrebbero essere necessarie alcune ore prima che il loro effetto diventi visibile.

Passaggi

1. Seleziona **Support** > **I/O prioritization**.
2. (Facoltativo) Cambia la priorità di eliminazione e riparazione EC, per le operazioni in background che eliminano i dati EC, rispetto ai valori predefiniti.

> Usa la priorità predefinita bassa di eliminazione e riparazione EC per le griglie che hanno nodi basati su RAID.

3. Seleziona **Salva**.
4. Monitora "metriche" per valutare l'effetto delle modifiche di priorità.

Esegui la diagnostica in StorageGRID

Quando risolvi un problema, puoi collaborare con il supporto tecnico per eseguire la diagnostica sul tuo sistema StorageGRID e analizzarne i risultati.

- "Esamina le metriche di supporto"
- "Metriche Prometheus comunemente utilizzate"

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

La pagina Diagnostica esegue una serie di controlli diagnostici sullo stato attuale della griglia. Ogni controllo diagnostico può avere uno dei tre stati seguenti:

- **Normale**: Tutti i valori rientrano nell'intervallo normale.
- **Attenzione**: uno o più valori sono al di fuori dell'intervallo normale.
- **Attenzione**: uno o più valori sono significativamente al di fuori dell'intervallo normale.

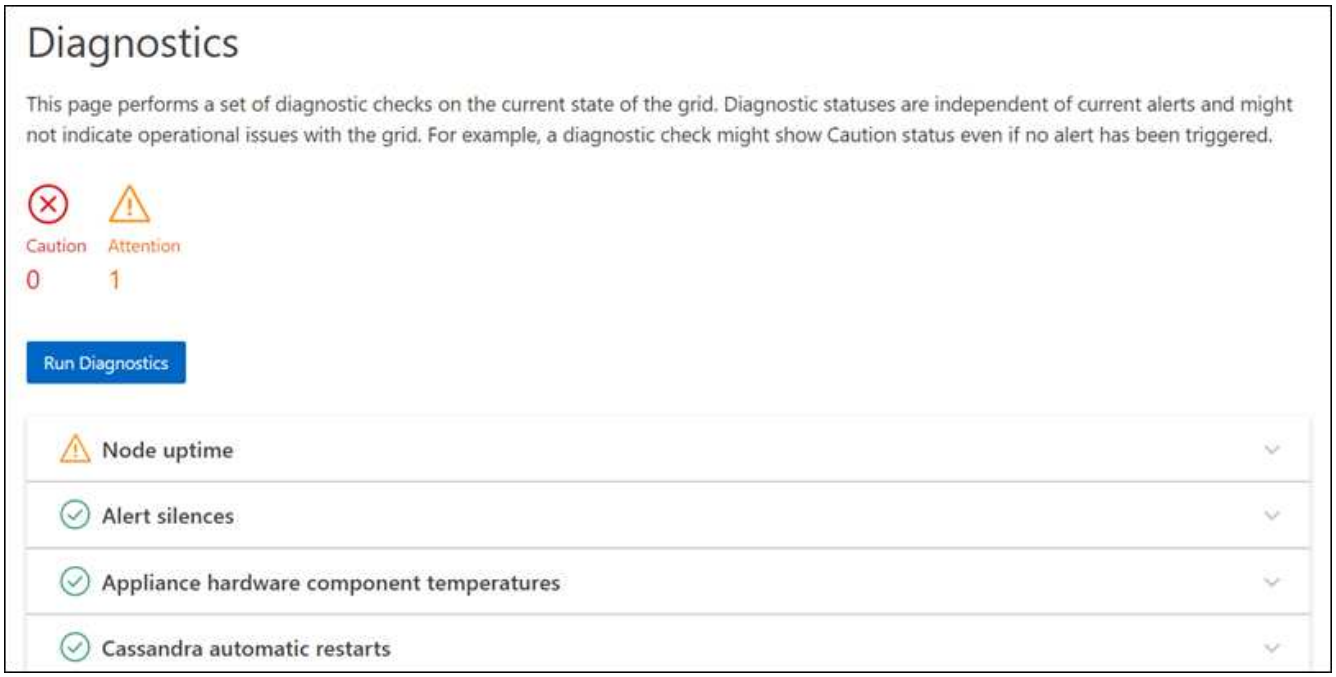
Gli stati diagnostici sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con il grid. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato Caution anche se non è stato attivato alcun avviso.

Passaggi

1. Seleziona **Support** > **Tools** > **Diagnostics**.

   Viene visualizzata la pagina Diagnostica, che elenca i risultati di ogni controllo diagnostico. I risultati sono ordinati per gravità (Caution, Attention e poi Normale). All'interno di ciascun livello di gravità, i risultati sono ordinati alfabeticamente.

   In questo esempio, una diagnosi ha lo stato Attenzione e tre diagnosi hanno lo stato Normale.



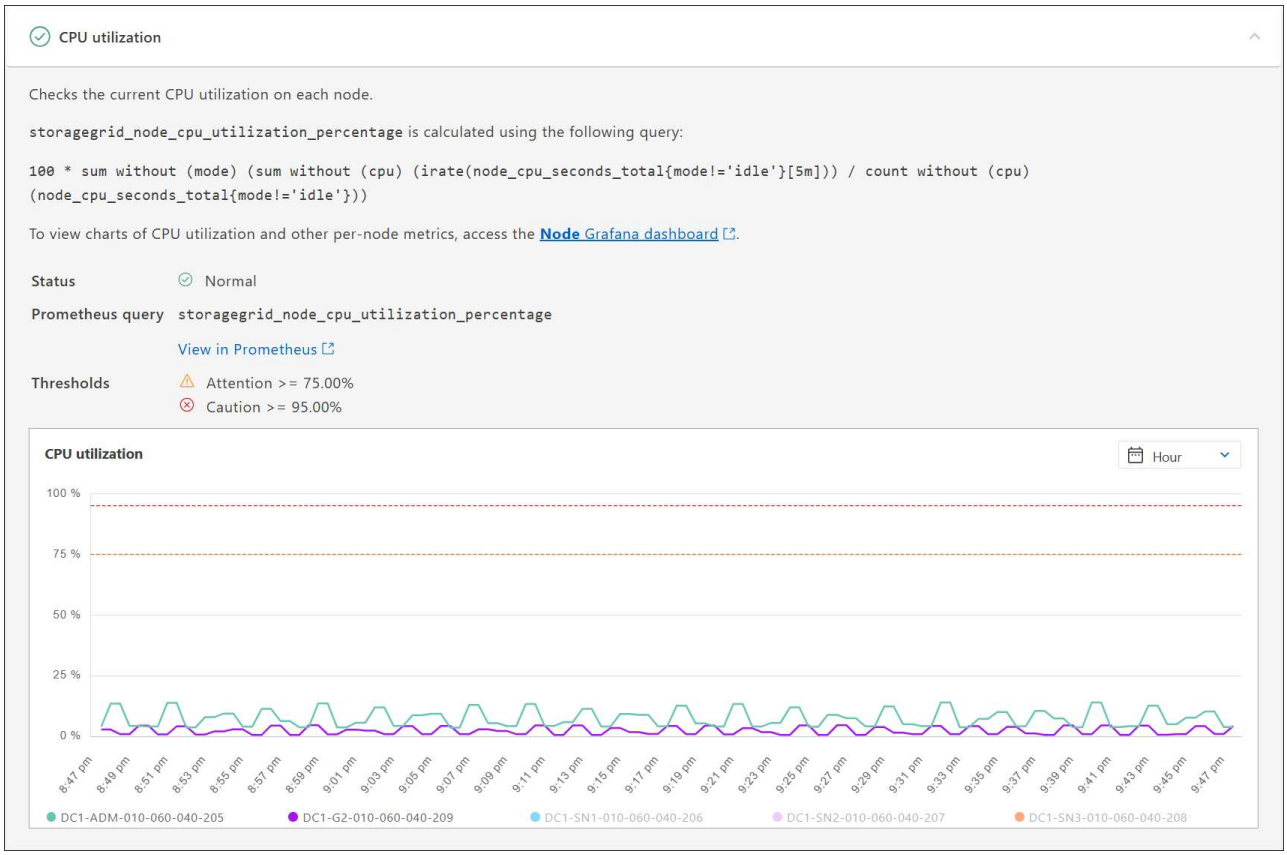
2. Per saperne di più su una diagnosi specifica, fai clic in un punto qualsiasi della riga.

   Vengono visualizzati i dettagli relativi alla diagnosi e i relativi risultati attuali. Di seguito sono elencati i dettagli:

   - **Stato**: Lo stato attuale di questa diagnosi: Normale, Attenzione o Cautela.
   - **Query Prometheus**: Se usata per la diagnostica, l'espressione Prometheus che è stata utilizzata per generare i valori di stato. (Non tutte le diagnostiche usano un'espressione Prometheus.)
   - **Soglie**: Se disponibili per la diagnostica, le soglie definite dal sistema per ogni stato diagnostico anomalo. (I valori di soglia non vengono utilizzati per tutte le diagnostiche.)

     Non puoi modificare queste soglie.

   - **Valori di stato**: Un grafico e una tabella (tabella non mostrata nello screenshot) che mostrano lo stato e il valore della diagnostica in tutto il sistema StorageGRID. In questo esempio, viene mostrato l'utilizzo corrente della CPU per ogni nodo in un sistema StorageGRID. Tutti i valori dei nodi sono al di sotto delle soglie di Attenzione e Cautela, quindi lo stato generale della diagnostica è Normale.



3. **Facoltativo**: Per vedere i grafici di Grafana relativi a questa diagnostica, seleziona **Grafana dashboard**.

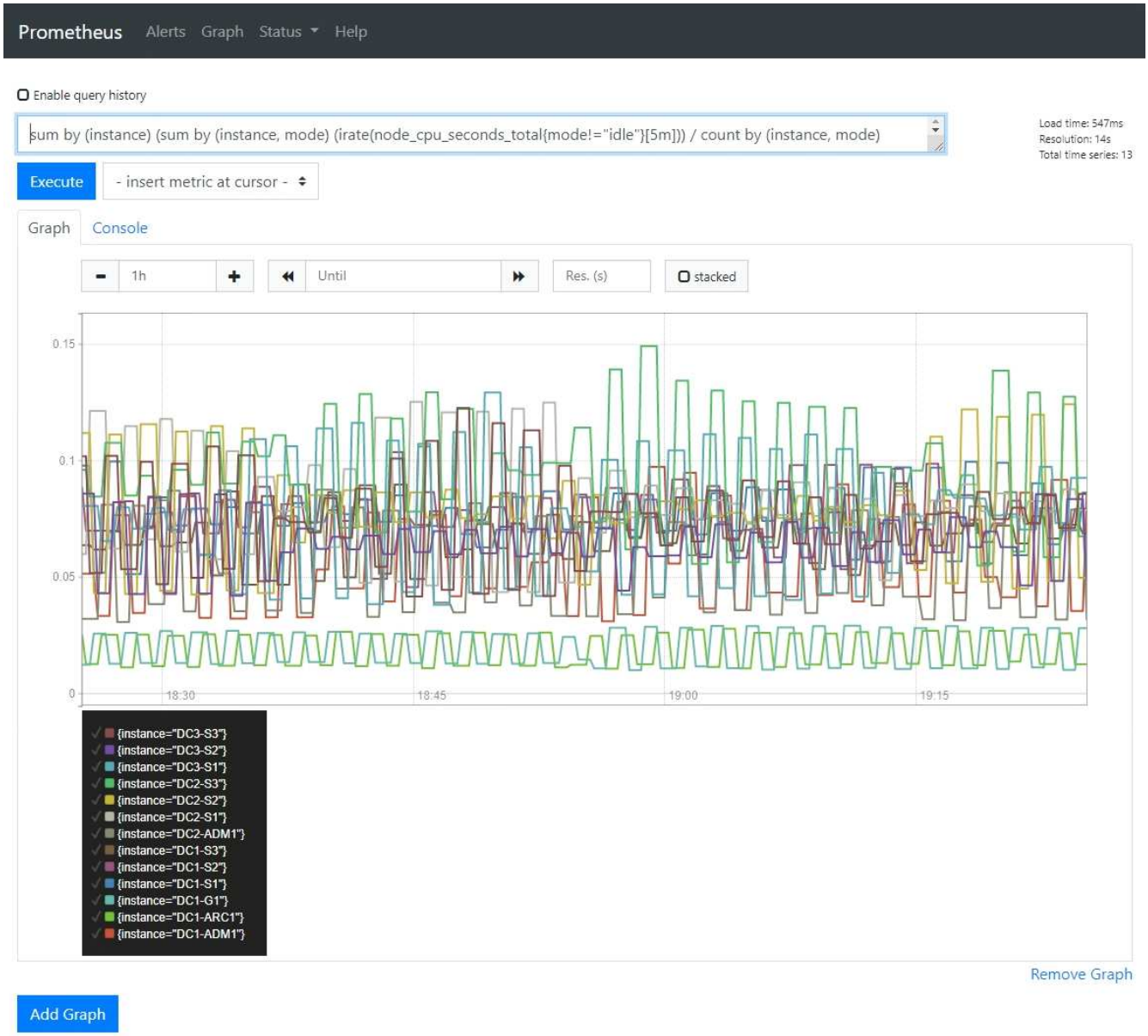
   Questo collegamento non viene visualizzato per tutte le diagnostiche.

   Viene visualizzata la dashboard di Grafana corrispondente. In questo esempio, viene visualizzata la dashboard del nodo che mostra l'utilizzo della CPU nel tempo per questo nodo, oltre ad altri grafici di Grafana relativi al nodo.

   > Puoi anche accedere alle dashboard Grafana predefinite dalla sezione Grafana della pagina **Supporto** > **Strumenti** > **Metriche**.

4. **Opzionale**: Per vedere un grafico dell'espressione Prometheus nel tempo, fai clic su **Visualizza in Prometheus**.

   Viene visualizzato un grafico Prometheus dell'espressione utilizzata nella diagnostica.



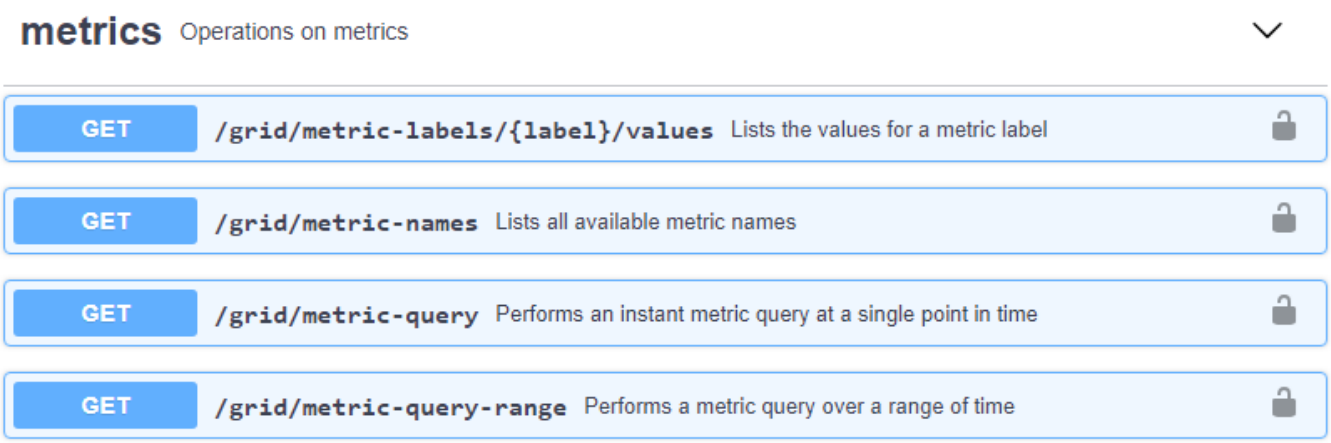
Crea applicazioni di monitoraggio personalizzate per StorageGRID

Puoi creare applicazioni di monitoraggio e dashboard personalizzate utilizzando le metriche StorageGRID disponibili tramite l'API di gestione della griglia.

Se vuoi monitorare metriche che non sono visualizzate in una pagina esistente del Grid Manager, o se vuoi creare dashboard personalizzate per StorageGRID, puoi usare l'API di Grid Management per interrogare le metriche di StorageGRID.

Puoi anche accedere alle metriche Prometheus direttamente con uno strumento di monitoraggio esterno, come Grafana. L'uso di uno strumento esterno richiede che tu carichi o generi un certificato client amministrativo per permettere a StorageGRID di autenticare lo strumento per la sicurezza. Vedi la "Istruzioni per l'amministrazione di StorageGRID".

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, vai su Grid Manager. Dalla parte superiore della pagina, seleziona l'icona di aiuto e seleziona **API documentation** > **metrics**.



I dettagli relativi all'implementazione di un'applicazione di monitoraggio personalizzata esulano dall'ambito di questa documentazione.

Risoluzione dei problemi del sistema StorageGRID

Risolvi i problemi di un sistema StorageGRID

Se riscontri un problema durante l'utilizzo di un sistema StorageGRID, consulta i suggerimenti e le linee guida in questa sezione per ricevere assistenza nell'individuazione e nella risoluzione del problema.

Spesso puoi risolvere i problemi da solo; tuttavia, potresti dover segnalare alcuni problemi al supporto tecnico.

Definisci il problema

Il primo passo per risolvere un problema è definirlo chiaramente.

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

Domanda	Risposta tipo
Cosa sta facendo o non facendo il sistema StorageGRID? Quali sono i suoi sintomi?	Le applicazioni client segnalano che non è possibile importare oggetti in StorageGRID.
Quando è iniziato il problema?	L'inserimento dell'oggetto è stato negato per la prima volta intorno alle 14:50 dell'8 gennaio 2020.
Come hai notato per la prima volta il problema?	Notificato dall'applicazione client. Ricevute anche notifiche di avviso via email.
Il problema si verifica sempre o solo a volte?	Il problema è ancora in corso.
Se il problema si verifica regolarmente, quali passaggi lo causano	Il problema si verifica ogni volta che un client tenta di ingerire un oggetto.

Domanda	Risposta tipo
Se il problema si verifica in modo intermittente, quando si manifesta? Annota gli orari di ogni episodio di cui sei a conoscenza.	Il problema non è intermittente.
Hai già riscontrato questo problema? Quante volte hai avuto questo problema in passato?	È la prima volta che vedo questo problema.

Valuta il rischio e l'impatto sul sistema

Dopo aver definito il problema, valuta il rischio e l'impatto sul sistema StorageGRID. Ad esempio, la presenza di avvisi critici non significa necessariamente che il sistema non stia erogando i servizi essenziali.

Questa tabella riassume l'impatto che il problema in questione sta avendo sul funzionamento del sistema:

Domanda	Risposta tipo
Il sistema StorageGRID può acquisire contenuti?	No.
Le applicazioni client possono recuperare contenuti?	Alcuni oggetti possono essere recuperati e altri no.
I dati sono a rischio?	No.
La capacità di svolgere l'attività commerciale 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.

Raccogli dati

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

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Crea una cronologia delle modifiche recenti	Le modifiche al tuo sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	• Crea una cronologia delle modifiche recenti

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Rivedi gli avvisi	Gli avvisi possono aiutarti a individuare rapidamente la causa principale di un problema fornendo indizi importanti sui problemi sottostanti che potrebbero esserne all'origine. Esamina l'elenco degli avvisi correnti per vedere se StorageGRID ha identificato la causa principale di un problema per te. Esamina gli avvisi attivati in passato per ulteriori informazioni.	• "Visualizza gli avvisi correnti e risolti"
Stabilisci i parametri di riferimento	Raccogli informazioni sui livelli normali di vari valori operativi. Questi valori di riferimento, e le deviazioni da essi, possono fornire indizi preziosi.	• Stabilisci i parametri di riferimento
Esegui test di ingestione e recupero	Per risolvere i problemi di prestazioni relativi all'acquisizione e al recupero, usa una workstation per archiviare e recuperare gli oggetti. Confronta i risultati con quelli ottenuti usando l'applicazione client.	• "Monitora le prestazioni PUT e GET"
Esamina i messaggi di audit	Esamina i messaggi di audit per seguire nel dettaglio le operazioni di StorageGRID. Le informazioni contenute nei messaggi di audit possono essere utili per risolvere molti tipi di problemi, inclusi quelli relativi alle prestazioni.	• "Esamina i messaggi di audit"
Controlla la posizione degli oggetti e l'integrità dello storage	Se riscontri problemi di archiviazione, verifica che gli oggetti vengano posizionati dove ti aspetti. Controlla l'integrità dei dati degli oggetti su un Storage Node.	• "Monitora le operazioni di verifica degli oggetti" • "Conferma la posizione dei dati degli oggetti" • "Verifica l'integrità dell'oggetto"
Raccogli dati per il supporto tecnico	Il supporto tecnico potrebbe chiederti di raccogliere dati o di esaminare informazioni specifiche per facilitare la risoluzione dei problemi.	• "Raccogli i file di log e i dati di sistema" • "Avvia manualmente un pacchetto AutoSupport" • "Esamina le metriche di supporto"

Crea una cronologia delle modifiche recenti

Quando si verifica un problema, dovresti considerare cosa è cambiato di recente e quando sono avvenuti questi cambiamenti.

- Le modifiche al tuo sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.
- Una cronologia delle modifiche può aiutarti a identificare quali modifiche potrebbero essere responsabili di un problema e come ciascuna modifica potrebbe averne influenzato lo sviluppo.

Crea una tabella delle modifiche recenti apportate al tuo sistema che includa informazioni su quando si è verificata ciascuna modifica e tutti i dettagli rilevanti, come ad esempio cosa stava succedendo mentre la modifica era in corso:

Tempo di cambiamento	Tipo di modifica	Dettagli
Ad esempio: • Quando hai avviato il ripristino del nodo? • Quando hai completato l'aggiornamento del software? • Hai interrotto il processo?	Cos'è successo? Cosa hai fatto?	Documenta tutti i dettagli rilevanti relativi alla modifica. Ad esempio: • Dettagli delle modifiche alla rete. • Quale hotfix hai installato. • Come sono cambiati i carichi di lavoro dei client. Assicurati di annotare se più modifiche sono state apportate contemporaneamente. Ad esempio, questa modifica è stata effettuata mentre era in corso un aggiornamento?

Esempi di cambiamenti recenti significativi

Ecco alcuni esempi di cambiamenti potenzialmente significativi:

- Il sistema StorageGRID è stato installato, ampliato o ripristinato di recente?
- Il sistema è stato aggiornato di recente? È stato applicato un hotfix?
- Hai riparato o sostituito di recente qualche componente hardware?
- 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 hai aggiunto o rimosso un gruppo ad alta disponibilità di Admin Node o Gateway Node?
- Hai avviato delle attività che potrebbero richiedere molto tempo per essere completate? Esempi includono:
  - Ripristino di un nodo di archiviazione guasto
  - Dismissione del nodo di archiviazione
- Hai apportato modifiche all'autenticazione degli utenti, come l'aggiunta di un tenant o la modifica della configurazione LDAP?
- La migrazione dei dati è in corso?
- Hai abilitato o modificato di recente i servizi della piattaforma?

- Hai attivato la conformità di recente?
- Hai aggiunto o rimosso dei Cloud Storage Pools?
- Hai apportato modifiche alla compressione o alla crittografia dello storage?
- Ci sono state modifiche all'infrastruttura di rete? Ad esempio, VLAN, router o DNS.
- Hai apportato modifiche alle fonti NTP?
- Hai apportato modifiche alle interfacce Grid, Admin o Client Network?
- Hai apportato altre modifiche al sistema StorageGRID o al suo ambiente?

Stabilisci i parametri di riferimento

Puoi stabilire dei valori di riferimento per il tuo sistema registrando i livelli normali di diversi parametri operativi. In futuro, puoi confrontare i valori attuali con questi valori di riferimento per aiutarti a individuare e risolvere valori anomali.

Proprietà	Valore	Come ottenere
Consumo medio di storage	GB consumati/giorno % consumato/giorno	Vai al Grid Manager. Nella pagina Nodi, seleziona l'intera griglia o un sito e vai alla scheda Storage. Nel grafico "Spazio di archiviazione utilizzato - Dati oggetto", individua un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare quanto spazio di archiviazione consumi ogni giorno. Puoi raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Consumo medio di metadati	GB consumati/giorno % consumato/giorno	Vai al Grid Manager. Nella pagina Nodi, seleziona l'intera griglia o un sito e vai alla scheda Storage. Nel grafico "Spazio di archiviazione utilizzato - Metadati degli oggetti", individua un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare quanta memoria di archiviazione per i metadati viene consumata ogni giorno. Puoi raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Frequenza delle operazioni S3	Operazioni/secondo	Nella dashboard di Grid Manager, seleziona **Prestazioni** > **Operazioni S3 per i nodi di archiviazione**. Per visualizzare i tassi e i conteggi di ingest e retrieval per un sito o un nodo specifico, seleziona **Nodes** > ***site or Storage Node*** > **Objects**. Posiziona il cursore sul grafico di ingest e retrieval S3.

Proprietà	Valore	Come ottenere
Tasso di valutazione ILM	Oggetti/secondo	Dalla pagina Nodi, seleziona ***grid*** > **ILM**. Sul grafico della coda ILM, individua un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di riferimento per **Evaluation rate** del tuo sistema.
Frequenza di scansione ILM	Oggetti/secondo	Seleziona **Nodes** > ***grid*** > **ILM**. Sul grafico della coda ILM, individua un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di riferimento per **Scan rate** del tuo sistema.
Oggetti accodati dalle operazioni del client	Oggetti/secondo	Seleziona **Nodes** > ***grid*** > **ILM**. Sul grafico della coda ILM, individua un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di riferimento per **Oggetti in coda (provenienti da operazioni client)** per il tuo sistema.
Latenza media delle query	Millisecondi	Seleziona **Nodi** > ***Nodo di storage*** > **Oggetti**. Nella tabella Query, visualizza il valore della Latenza media.

${post_edited_translations.segment}

${post_edited_translations.segment}

L'analisi dipende dal problema specifico, ma in generale:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Se non riesci a risolvere il problema autonomamente, contatta il supporto tecnico. Prima di contattare il supporto tecnico, raccogli le informazioni elencate nella tabella seguente per facilitare la risoluzione del problema.

✔	Articolo	Note
	Dichiarazione del problema	Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo costante o intermittente? Se intermittente, in quali momenti si è verificato? Definisci il problema
	${post_edited_translations.segment}	Qual è la gravità del problema? Qual è l'impatto sull'applicazione client? • ${post_edited_translations.segment} • ${post_edited_translations.segment}
	${post_edited_translations.segment}	Seleziona **Manutenzione** > **Sistema** > **Licenza**. L'ID sistema StorageGRID viene visualizzato come parte della licenza corrente.
	Versione software	${post_edited_translations.segment}
	Personalizzazione	Riassumi come è configurato il tuo sistema StorageGRID. Ad esempio, elenca quanto segue: • La griglia utilizza la compressione dello storage, la crittografia dello storage o la conformità? • ILM crea oggetti replicati o con codifica di cancellazione? ILM garantisce la ridondanza del sito? Le regole di ILM utilizzano i comportamenti di acquisizione Balanced, Strict o Dual Commit?
	File di registro e dati di sistema	Raccogli i file di log e i dati di sistema per il tuo sistema. Seleziona **Supporto** > **Strumenti** > **Raccolta log**. ${post_edited_translations.segment} Se stai raccogliendo i log solo per i nodi selezionati, assicurati di includere almeno un Storage Node che disponga del servizio ADC. I primi tre Storage Node installati in un sito includono il servizio ADC.
	Informazioni di base	Raccogli informazioni di base sulle operazioni di acquisizione, sulle operazioni di recupero e sul consumo di storage. Stabilisci i parametri di riferimento
	Cronologia delle modifiche recenti	${post_edited_translations.segment} Crea una cronologia delle modifiche recenti

✔	Articolo	Note
	Storia degli sforzi per diagnosticare il problema	${post_edited_translations.segment}

Risolvi i problemi relativi a oggetti e storage

Conferma le posizioni dei dati degli oggetti in StorageGRID

A seconda del problema, potresti voler "conferma dove vengono memorizzati i dati dell'oggetto". Ad esempio, potresti voler verificare che la policy ILM funzioni come previsto e che i dati degli oggetti vengano archiviati nella posizione prevista.

Prima di iniziare

- Devi avere un identificatore di oggetto, che può essere uno dei seguenti:
  - **UUID**: Identificatore univoco universale dell'oggetto. Inserisci l'UUID tutto in maiuscolo.
  - **CBID**: Identificativo univoco dell'oggetto all'interno di StorageGRID. Puoi ottenere il CBID di un oggetto dal registro di audit. Inserisci il CBID tutto in maiuscolo.
  - **Bucket S3 e chiave oggetto**: Quando un oggetto viene acquisito tramite "Interfaccia S3", l'applicazione client utilizza una combinazione di bucket e chiave oggetto per archiviare e identificare l'oggetto.

Passaggi

1. Seleziona **ILM** > **Object metadata lookup**.
2. Digita l'identificativo dell'oggetto nel campo **Identificativo**.

   Puoi inserire un UUID, un CBID o un bucket/oggetto S3.

3. Se vuoi cercare una versione specifica dell'oggetto, inserisci l'ID della versione (opzionale).

4. Seleziona **Look Up**.

   Appaiono "risultati della ricerca dei metadati dell'oggetto". Questa pagina elenca i seguenti tipi di informazioni:

   - Metadati di sistema, inclusi l'ID dell'oggetto (UUID), l'ID della versione (opzionale), il nome dell'oggetto, il nome del container, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora

in cui l'oggetto è stato creato per la prima volta e la data e l'ora dell'ultima modifica dell'oggetto.

- ${post_edited_translations.segment}
- Per gli oggetti S3, tutte le coppie chiave-valore dei tag associate all'oggetto.
- ${post_edited_translations.segment}
- Per le copie di oggetti con codifica di cancellazione, la posizione di archiviazione 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'identificativo univoco dell'oggetto.
- Per gli oggetti segmentati e gli oggetti composti da più parti, viene visualizzato un elenco dei segmenti dell'oggetto, inclusi gli identificatori dei segmenti e le dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono mostrati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati di sistema interni che non è garantito persistano da una release all'altra.

Il seguente esempio mostra i risultati della ricerca dei metadati di un oggetto di test S3 archiviato come due copie replicate.

System Metadata

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

Replicated Copies

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

Raw Metadata


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

Scopri i guasti dell'archivio di oggetti per i volumi di storage in StorageGRID

Lo storage sottostante su un Storage Node è suddiviso in archivi di oggetti. Gli archivi di oggetti sono noti anche come volumi di storage.

Puoi visualizzare le informazioni sull'archivio di oggetti per ciascun Storage Node. Seleziona **Nodes** > ***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

A seconda della natura del guasto, i problemi relativi a un volume di archiviazione potrebbero riflettersi in "avvisi relativi al volume di storage". Se un volume di archiviazione si guasta, dovresti riparare il volume di archiviazione guasto per ripristinare la piena funzionalità del nodo di storage il prima possibile. Se necessario, puoi andare alla scheda **Configuration** e "imposta il nodo di archiviazione in modalità di sola lettura" così che il sistema StorageGRID possa utilizzarlo per il recupero dei dati mentre ti prepari per un ripristino completo del server.

Verificare l'integrità dei dati degli oggetti in StorageGRID

Il sistema StorageGRID verifica l'integrità dei dati degli oggetti sui nodi di archiviazione, controllando la presenza di oggetti danneggiati o mancanti.

Esistono due processi di verifica: la verifica in background e il controllo dell'esistenza degli oggetti (precedentemente chiamato verifica in primo piano). Questi processi lavorano insieme per garantire l'integrità dei dati. La verifica in background viene eseguita automaticamente e controlla continuamente la correttezza dei dati degli oggetti. Il controllo dell'esistenza degli oggetti può essere attivato da un utente per verificare più rapidamente l'esistenza (ma non la correttezza) degli oggetti.

Che cos'è la verifica dei precedenti?

Il processo di verifica in background controlla automaticamente e continuamente i nodi di archiviazione Storage Nodes alla ricerca di copie corrotte dei dati degli oggetti e tenta automaticamente di riparare eventuali problemi rilevati.

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

- **Oggetti replicati**: Se il processo di verifica in background rileva un oggetto replicato danneggiato, la copia danneggiata viene rimossa dalla sua posizione e messa in quarantena altrove sul Storage Node. Poi, viene generata una nuova copia non danneggiata e posizionata per soddisfare le policy ILM attive. La nuova copia potrebbe non essere posizionata sullo Storage Node utilizzato per la copia originale.

  > I dati degli oggetti danneggiati vengono messi in quarantena anziché eliminati dal sistema, così puoi ancora accedervi. Per ulteriori informazioni su come accedere ai dati degli oggetti in quarantena, contatta 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 danneggiato, StorageGRID tenta automaticamente di ricostruire il frammento mancante sul posto, sullo stesso Storage Node, utilizzando i frammenti di dati e di parità rimanenti. Se il frammento danneggiato non può essere ricostruito, si tenta di recuperare un'altra copia dell'oggetto. Se il recupero ha successo, viene eseguita una valutazione ILM per creare una copia sostitutiva dell'oggetto con codifica 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 per poter essere sottoposti a verifica in background.

La verifica in background viene eseguita a una velocità continua, progettata per non interferire con le normali attività di sistema. La verifica in background non può essere interrotta. Tuttavia, puoi aumentare la velocità della verifica in background per verificare più rapidamente il contenuto di uno Storage Node se sospetti un problema.

Avvisi relativi alla verifica in background

Se il sistema rileva un oggetto danneggiato che non può correggere automaticamente (perché il danneggiamento impedisce l'identificazione dell'oggetto), viene attivato l'avviso **Unidentified corrupt object detected**.

Se la verifica in background non riesce a sostituire un oggetto danneggiato perché non riesce a trovarne un'altra copia, viene attivato l'avviso **Oggetti potenzialmente persi**.

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

Il controllo di esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti codificati per la cancellazione esistono su un Storage Node. Il controllo di esistenza degli oggetti non verifica i dati degli oggetti stessi (questo lo fa la verifica in background); invece, offre un modo per verificare l'integrità dei dispositivi di archiviazione, soprattutto se un recente problema hardware potrebbe aver influenzato l'integrità dei dati.

A differenza della verifica in background, che avviene automaticamente, devi avviare manualmente un processo di verifica dell'esistenza di un oggetto.

Il controllo di esistenza dell'oggetto legge i metadati di ogni oggetto memorizzato in StorageGRID e verifica l'esistenza sia delle copie replicate dell'oggetto sia dei frammenti di oggetto codificati con cancellazione. Eventuali dati mancanti vengono gestiti come segue:

- **Copie replicate**: Se manca una copia dei dati di un oggetto replicato, StorageGRID tenta automaticamente di sostituirla con una copia memorizzata altrove nel sistema. Il nodo di storage esegue una valutazione ILM su una copia esistente, che determinerà che la policy ILM corrente non è più soddisfatta per questo oggetto perché manca un'altra copia. Viene generata una nuova copia e posizionata per soddisfare le policy ILM attive del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa posizione in cui era memorizzata la copia mancante.
- **Frammenti codificati per la cancellazione**: Se manca un frammento di un oggetto codificato per la cancellazione, StorageGRID tenta automaticamente di ricostruire il frammento mancante sul posto, sullo stesso Storage Node, utilizzando i frammenti rimanenti. Se il frammento mancante non può essere ricostruito (perché sono andati persi troppi frammenti), ILM tenta di trovare un'altra copia dell'oggetto, che può utilizzare per generare un nuovo frammento codificato per la cancellazione.

Esegui il controllo di esistenza dell'oggetto

Crei ed esegui un solo job di verifica dell'esistenza di un oggetto alla volta. Quando crei un job, selezioni gli Storage Node e i volumi che vuoi verificare. Selezioni anche la consistenza per il job.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di manutenzione o di accesso root".
- Hai verificato che i Storage Node che vuoi controllare siano online. Seleziona **Nodes** per visualizzare la tabella dei nodi. Assicurati che non compaiano icone di avviso accanto al nome del nodo per i nodi che vuoi controllare.
- Hai verificato che le seguenti procedure **non** sono in esecuzione sui nodi che vuoi controllare:
  - Espansione della griglia per aggiungere un nodo di storage
  - Decommission del nodo di storage
  - Ripristino di un volume di storage guasto

- Ripristino di un nodo di storage con un'unità di sistema guasta
- ribilanciamento EC
- Clonazione del nodo appliance

Il controllo dell'esistenza dell'oggetto non fornisce informazioni utili mentre queste procedure sono in corso.

Informazioni su questa attività

Un'operazione di verifica dell'esistenza di un oggetto può richiedere giorni o settimane per essere completata, a seconda del numero di oggetti nella grid, dei Storage Node e dei volumi selezionati e della coerenza selezionata. Puoi eseguire solo un'operazione alla volta, ma puoi selezionare più Storage Node e volumi contemporaneamente.

Passaggi

1. Seleziona **Manutenzione** > **Attività** > **Verifica esistenza oggetto**.
2. Seleziona **Crea processo**. Viene visualizzata la procedura guidata Crea un processo di verifica dell'esistenza dell'oggetto.
3. Seleziona i nodi contenenti i volumi che desideri verificare. Per selezionare tutti i nodi online, seleziona la casella di controllo **Nome del nodo** nell'intestazione della colonna.

   Puoi cercare per nome del nodo o per sito.

   Non puoi selezionare nodi che non sono collegati alla griglia.

4. Seleziona **Continue**.
5. Seleziona uno o più volumi per ciascun nodo nell'elenco. Puoi cercare i volumi utilizzando il numero del volume di archiviazione o il nome del nodo.

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

6. Seleziona **Continue**.
7. Seleziona la consistenza per il job.

   La coerenza determina quante copie dei metadati dell'oggetto vengono utilizzate per la verifica dell'esistenza dell'oggetto.

   - **Sito forte**: Due copie dei metadati in un unico sito.
   - **Strong-global**: Due copie dei metadati in ogni sito.
   - **Tutti** (impostazione predefinita): Tutte e tre le copie dei metadati in ciascun sito.

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

8. Seleziona **Continue**.
9. Rivedi e verifica le tue selezioni. Puoi selezionare **Precedente** per tornare a una fase precedente della procedura guidata e aggiornare le tue selezioni.

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

   - Il lavoro è completato.

- Puoi mettere in pausa o annullare un'attività. Puoi riprendere un'attività che hai messo in pausa, ma non puoi riprendere un'attività che hai annullato.
- Il processo si blocca. Viene attivato l'avviso **Verifica esistenza oggetto bloccata**. Segui le azioni correttive specificate per l'avviso.
- L'operazione non riesce. Viene attivato l'avviso **Verifica dell'esistenza dell'oggetto non riuscita**. Segui le azioni correttive specificate per l'avviso.
- Viene visualizzato un messaggio "Servizio non disponibile" o "Errore interno del server". Dopo un minuto, aggiorna la pagina per continuare a monitorare il job.

> Se necessario, puoi uscire dalla pagina di verifica dell'esistenza dell'oggetto e ritornarvi per continuare a monitorare il job.

10. Durante l'esecuzione del job, visualizza la scheda **Active job** e prendi nota del valore di Missing object copies detected.

    Questo valore rappresenta il numero totale di copie mancanti di oggetti replicati e oggetti codificati con 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 archiviazione.

11. Una volta completato il lavoro, esegui tutte le azioni aggiuntive necessarie:
    - Se il numero di copie di oggetti mancanti rilevate è zero, non sono stati riscontrati problemi. Non è richiesta alcuna azione.
    - Se il numero di copie di oggetti mancanti rilevate è maggiore di zero e l'avviso **Oggetti potenzialmente persi** non è stato attivato, significa che tutte le copie mancanti sono state riparate dal sistema. Verifica che eventuali problemi hardware siano stati risolti per evitare danni futuri alle copie degli oggetti.
    - Se il numero di copie di oggetti mancanti rilevate è maggiore di zero e l'avviso **Oggetti potenzialmente persi** è stato attivato, l'integrità dei dati potrebbe essere compromessa. Contatta il supporto tecnico.
    - Puoi esaminare le copie di oggetti potenzialmente perse utilizzando grep per estrarre i messaggi di audit LLST: `grep LLST audit_file_name`.

      Questa procedura è simile a quella per "analisi di oggetti potenzialmente persi", anche se per le copie degli oggetti cerchi `LLST` invece di `OLST`.

12. Se hai selezionato la coerenza strong-site o strong-global per il job, aspetta circa tre settimane per la coerenza dei metadati e poi esegui di nuovo il job sugli stessi volumi.

    Quando StorageGRID ha avuto il tempo di raggiungere la coerenza dei metadati per i nodi e i volumi inclusi nel job, la riesecuzione del job potrebbe eliminare copie di oggetti mancanti segnalate erroneamente o far sì che vengano controllate copie di oggetti aggiuntive se erano state omesse.

    a. Seleziona **Manutenzione** > **Verifica esistenza oggetto** > **Cronologia interventi**.
    b. Determina quali processi sono pronti per essere rieseguiti:
        i. Guarda la colonna **Ora di fine** per vedere quali processi sono stati eseguiti più di tre settimane fa.
        ii. Per questi lavori, esamina la colonna Controllo coerenza per strong-site o strong-global.
    c. Seleziona la casella di controllo per ogni processo che vuoi rieseguire, poi seleziona **Riesegui**.

d. Nella procedura guidata di riesecuzione dei processi, controlla i nodi e i volumi selezionati e la coerenza.

e. Quando sei pronto a rieseguire i processi, seleziona **Riesegui**.

Viene visualizzata la scheda Lavori attivi. Tutti i lavori che hai selezionato vengono rieseguiti come un unico lavoro con coerenza strong-site. Un campo **Lavori correlati** nella sezione Dettagli elenca gli ID dei lavori originali.

Risolvi l'avviso S3 PUT object size too large in StorageGRID

L'avviso "Dimensioni dell'oggetto S3 PUT troppo grandi" viene attivato se un tenant tenta un'operazione PutObject non multipart che supera il limite di dimensione di S3 pari a 5 GiB.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Individua quali tenant utilizzano oggetti più grandi di 5 GiB, così puoi avvisarli.

Passaggi

1. Vai su **Configurazione** > **Monitoraggio** > **Audit and syslog server**.
2. Se le scritture del client sono normali, accedi al registro di controllo:

   a. Inserisci `ssh admin@primary_Admin_Node_IP`

   b. Inserisci la password indicata nel file `Passwords.txt`.

   c. Inserisci il seguente comando per passare all'utente root: `su -`

   d. Inserisci la password indicata nel file `Passwords.txt`.

   Quando sei connesso come root, il prompt cambia da `$` a `#`.

   e. ${post_edited_translations.segment}

   La directory dei log di controllo e i nodi applicabili dipendono dalle impostazioni di destinazione dei log di controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	`/var/local/log/localaudit.log`
${post_edited_translations.segment}	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
${post_edited_translations.segment}	`/var/local/log/localaudit.log`

In base alle tue impostazioni di destinazione dell'audit, inserisci: `cd /var/local/log` o `/var/local/audit/export/`

Per saperne di più, consulta "${post_edited_translations.segment}".

f. Identifica quali tenant stanno utilizzando oggetti più grandi di 5 GiB.

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

ii. Per ogni messaggio di audit nei risultati, guarda il campo `S3AI` per determinare l'ID account tenant. Usa gli altri campi del messaggio per determinare quale indirizzo IP è stato utilizzato dal client, il bucket e l'oggetto:

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

Esempio di risultati del registro di controllo

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

3. Se le scritture del client non sono normali, usa il tenant ID dall'avviso per identificare il tenant:

a. Vai a **Support** > **Tools** > **Log collection**. Raccogli i log dell'applicazione per lo Storage Node nell'avviso. Specifica 15 minuti prima e dopo l'avviso. Fai riferimento a "Raccogli i file di log e i dati di sistema".

b. Estrai il file e vai a `bycast.log`:

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

c. Cerca nel registro per `method=PUT` e identifica il client nel campo `clientIP`.

Esempio bycast.log

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

4. Informa i tenant che la dimensione massima di PutObject è 5 GiB e che devono usare i caricamenti multipart per oggetti superiori a 5 GiB.
5. Ignora l'avviso per una settimana se l'applicazione è stata modificata.

Risolvi i problemi relativi ai dati degli oggetti persi o mancanti

Scopri i dati degli oggetti persi e mancanti in StorageGRID

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

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

Se il recupero ha esito positivo, il sistema StorageGRID sostituisce la copia mancante dell'oggetto. In caso contrario, viene attivato l'avviso **Oggetti potenzialmente persi**, come segue:

- Nel caso di copie replicate, se non è possibile recuperare un'altra copia, l'oggetto viene considerato perso e viene attivato l'avviso.
- Nel caso di copie con codifica di cancellazione, se non è possibile recuperare una copia dalla posizione prevista, l'attributo Corrupt Copies Detected (ECOR) viene incrementato di uno prima di tentare di recuperare una copia da un'altra posizione. Se non viene trovata alcuna altra copia, viene attivato l'avviso.

Dovresti indagare immediatamente su tutti gli avvisi di **Oggetti potenzialmente persi** per determinare la causa principale della perdita e per capire se l'oggetto potrebbe ancora esistere in un nodo di storage offline o comunque attualmente non disponibile. Vedi "Indaga su eventuali oggetti smarriti". Gli avvisi di oggetti persi potrebbero essere attivati erroneamente per precauzione.

Nel caso in cui i dati di un oggetto senza copie vengano persi, non esiste una soluzione di recupero. Tuttavia, devi "reimposta il contatore degli oggetti potenzialmente persi" impedire che gli oggetti persi noti mascherino eventuali nuovi oggetti persi.

Risolvi l'avviso degli oggetti potenzialmente persi in StorageGRID

Quando viene attivato l'avviso **Oggetti potenzialmente persi**, devi indagare immediatamente. Raccogli informazioni sugli oggetti interessati e contatta il supporto tecnico.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

- Hai "autorizzazioni di accesso specifiche".
- Devi avere il file `Passwords.txt`.

Informazioni su questa attività

L'avviso **Oggetti potenzialmente persi** indica che, in base alle informazioni disponibili in StorageGRID, non sono presenti copie di un oggetto nella griglia. I dati potrebbero essere andati persi in modo permanente.

Esamina immediatamente gli avvisi di oggetti smarriti. Potresti dover intervenire per prevenire ulteriori perdite di dati. In alcuni casi, potresti riuscire a ripristinare un oggetto smarrito se agisci tempestivamente.

> Se vengono segnalati più di 10 oggetti smarriti, contatta il supporto tecnico. Non seguire questa procedura da solo.

Passaggi

1. Selezionare **Nodi**.
2. Seleziona ***Storage Node*** > **Objects**.
3. Esamina il numero di oggetti smarriti visualizzato nella tabella Conteggi oggetti.

   Questo numero indica il numero totale di oggetti che questo nodo della griglia rileva come mancanti nell'intero sistema StorageGRID. Il valore è la somma dei contatori degli oggetti persi del componente Data store all'interno dei servizi LDR e DDS.

4. Da un Admin Node, "${post_edited_translations.segment}" per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **Oggetti potenzialmente persi**:
   a. Accedi al nodo della griglia:
      i. Inserisci il seguente comando: `ssh admin@grid_node_IP`
      ii. Inserisci la password indicata nel file `Passwords.txt`.
      iii. Inserisci il seguente comando per passare all'utente root: `su -`
      iv. Inserisci la password indicata nel `Passwords.txt` file. Quando effettui l'accesso come root, il prompt cambia da `$` a `#`.
   b. ${post_edited_translations.segment}

      La directory dei log di controllo e i nodi applicabili dipendono dalle impostazioni di destinazione dei log di controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	`/var/local/log/localaudit.log`
${post_edited_translations.segment}	• Nodi amministrativi (primario e non primario): `/var/local/audit/export/audit.log` • Tutti i nodi: Il `/var/local/log/localaudit.log` file è in genere vuoto o mancante in questa modalità.
${post_edited_translations.segment}	`/var/local/log/localaudit.log`

In base alle tue impostazioni di destinazione dell'audit, inserisci: `cd /var/local/log` o `/var/local/audit/export/`

Per saperne di più, consulta "${post_edited_translations.segment}".

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

d. ${post_edited_translations.segment}

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

5. Cerca i metadati dell'oggetto smarrito usando l'UUID:

a. Seleziona **ILM** > **Object metadata lookup**.

b. ${post_edited_translations.segment}

c. ${post_edited_translations.segment}

${post_edited_translations.segment}	**Conclusione**
Oggetto <object_identifier> non trovato	${post_edited_translations.segment} Se l'oggetto non viene trovato, reimposta il contatore degli oggetti potenzialmente persi per cancellare l'allarme. L'assenza di un oggetto indica che l'oggetto è stato eliminato intenzionalmente.
Località > 0	${post_edited_translations.segment} Verifica che gli oggetti esistano. Usa il Node ID e il percorso del file indicati nell'output per confermare che il file oggetto si trovi nella posizione indicata. Se gli oggetti esistono, reimposta il contatore degli oggetti potenzialmente persi cancella l'avviso.
${post_edited_translations.segment}	Se nell'output non sono elencate posizioni, l'oggetto potrebbe essere mancante. Contatta il supporto tecnico. L'assistenza tecnica potrebbe chiederti di verificare se è in corso una procedura di ripristino dello storage. Consulta le informazioni su "${post_edited_translations.segment}" e "${post_edited_translations.segment}".

6. Dopo aver risolto i problemi relativi agli oggetti persi, reimposta il contatore degli oggetti potenzialmente persi per assicurarti che gli avvisi non siano falsi positivi:
   a. Selezionare **Nodi**.
   b. Seleziona ***Storage Node*** > **Attività**.
   c. Nella sezione Reimposta contatore oggetti potenzialmente persi, seleziona **Reimposta**.

Risolvi l'avviso di archiviazione dati oggetto insufficiente in StorageGRID

L'avviso **Spazio di archiviazione dati oggetto insufficiente** monitora la quantità di spazio disponibile per l'archiviazione dei dati oggetto su ciascun Storage Node.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

L'avviso **Spazio di archiviazione dati oggetto insufficiente** viene attivato quando la quantità totale di dati oggetto replicati e codificati per la cancellazione su un Storage Node soddisfa una delle condizioni configurate nella regola di avviso.

Di default, viene attivato un avviso importante quando questa condizione risulta vera:

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

In questa condizione:

- `storagegrid_storage_utilization_data_bytes` è una stima della dimensione totale dei dati degli oggetti replicati e codificati con erasure coding per un Storage Node.
- `storagegrid_storage_utilization_usable_space_bytes` è la quantità totale di storage a oggetti rimanente per un nodo di archiviazione.

Se viene attivato un avviso di **Low object data storage**, sia esso di grave o lieve entità, dovresti eseguire una procedura di espansione il prima possibile.

Passaggi

1. Seleziona **Avvisi** > **Attuali**.

   Viene visualizzata la pagina Avvisi.

2. Dalla tabella degli avvisi, espandi il gruppo di avvisi **Low object data storage**, se necessario, e seleziona l'avviso che vuoi visualizzare.

   Seleziona l'avviso, non l'intestazione per un gruppo di avvisi.

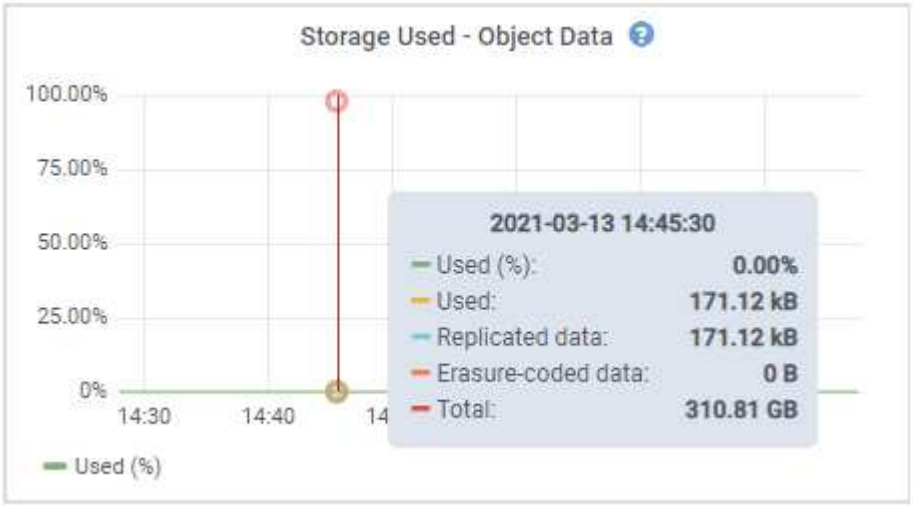
3. Esamina i dettagli nella finestra di dialogo e prendi nota di quanto segue:
   - Attivato a tempo

- Il nome del sito e del nodo
- I valori attuali delle metriche per questo alert

4. Seleziona **Nodes** > ***Storage Node or Site*** > **Storage**.
5. Posiziona il cursore sul grafico "Storage Used - Object Data".

   Vengono visualizzati i seguenti valori:

   - **Utilizzato (%)**: La percentuale dello spazio totale utilizzabile che hai usato per i dati degli oggetti.
   - **Utilizzato**: La quantità di spazio totale utilizzabile che hai usato per i dati degli oggetti.
   - **Dati replicati**: una stima della quantità di dati oggetto replicati su questo nodo, sito o grid.
   - **Dati codificati per la cancellazione**: una stima della quantità di dati oggetto codificati per la cancellazione su questo nodo, sito o grid.
   - **Totale**: La quantità totale di spazio utilizzabile su questo nodo, sito o grid. Il valore utilizzato è la `storagegrid_storage_utilization_data_bytes` metrica.



6. Seleziona i controlli temporali sopra il grafico per visualizzare l'utilizzo dello storage in diversi periodi di tempo.

   Analizzare l'utilizzo dello storage nel tempo può aiutarti a capire quanto storage è stato usato prima e dopo che l'avviso è stato attivato e può aiutarti a stimare quanto tempo potrebbe volerci prima che lo spazio rimanente del nodo si riempia.

7. Il prima possibile, "aggiungere capacità di storage" sulla tua griglia.

   Puoi aggiungere volumi di storage (LUN) ai nodi di storage esistenti oppure puoi aggiungere nuovi nodi di storage.

   Per ulteriori informazioni, vedi "Gestisci nodi di storage completi".

Risolvi l'override della filigrana in StorageGRID

Se usi valori personalizzati per le filigrane del volume di storage, potresti dover risolvere l'avviso **Low read-only watermark override**. Se possibile, dovresti aggiornare il sistema per iniziare a usare i valori ottimizzati.

Nelle versioni precedenti, i tre "watermark del volume di storage" erano impostazioni globali — gli stessi valori si applicavano a ogni volume di storage su ciascun Storage Node. A partire da StorageGRID 11.6, il software può ottimizzare questi watermark per ciascun volume di storage, in base alle dimensioni dello Storage Node e alla capacità relativa del volume.

${post_edited_translations.segment}

- Il sistema è quasi saturo e non sarebbe in grado di accettare nuovi dati se venissero applicati watermark ottimizzati. In questo caso, StorageGRID non modificherà le impostazioni del watermark.
- In precedenza hai impostato uno dei watermark del volume di storage su un valore personalizzato. StorageGRID non sovrascriverà le impostazioni personalizzate del watermark con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso **Low read-only watermark override** se il valore personalizzato per il watermark soft di sola lettura del volume di storage è troppo basso.

${post_edited_translations.segment}

Se usi valori personalizzati per le filigrane del volume di storage, l'avviso **Low read-only watermark override** potrebbe essere attivato per uno o più Storage Nodes.

Ogni avviso indica che il valore personalizzato del watermark di sola lettura del volume di archiviazione è inferiore al valore minimo ottimizzato per quel Storage Node. Se continui a usare l'impostazione personalizzata, il nodo di archiviazione potrebbe rimanere con spazio critico prima di poter passare in sicurezza allo stato di sola lettura. Alcuni volumi di archiviazione potrebbero diventare inaccessibili (smontati automaticamente) quando il nodo raggiunge la capacità.

Ad esempio, supponi di aver impostato in precedenza la soglia soft di sola lettura del volume di storage a 5 GB. Ora supponi 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
${post_edited_translations.segment}	11 GB
${post_edited_translations.segment}	15 GB

L'avviso **Override del watermark di sola lettura basso** viene attivato per lo Storage Node A perché il watermark personalizzato (5 GB) è inferiore al valore minimo ottimizzato per tutti i volumi in quel nodo (11 GB). Se continui a utilizzare l'impostazione personalizzata, lo spazio sul nodo potrebbe ridursi a livelli critici prima che possa passare in modo sicuro allo stato di sola lettura.

Risolvi l'avviso

Segui questi passaggi se sono stati attivati uno o più avvisi **Low read-only watermark override**. Puoi usare queste istruzioni anche se attualmente usi impostazioni filigrana personalizzate e vuoi iniziare a usare impostazioni ottimizzate anche se non sono stati attivati avvisi.

Prima di iniziare

- Hai completato l'aggiornamento a StorageGRID 11.6 o superiore.
- Sei connesso a Grid Manager utilizzando un "browser web supportato".

- Hai "Permesso di accesso root".

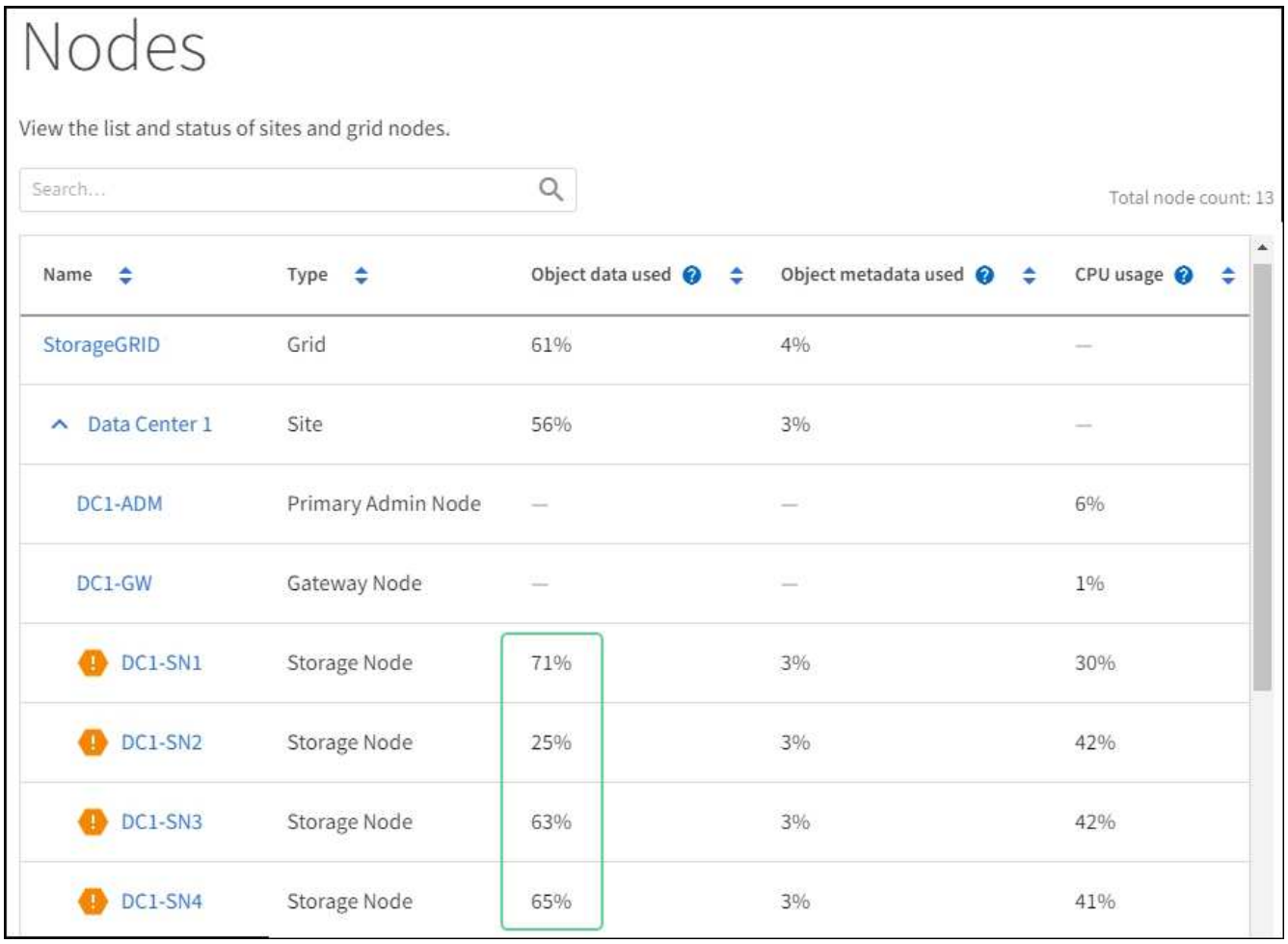
Informazioni su questa attività

Puoi risolvere l'avviso **Low read-only watermark override** aggiornando le impostazioni personalizzate della filigrana ai nuovi override della filigrana. Tuttavia, se uno o più Storage Node sono quasi pieni o se hai requisiti ILM speciali, devi prima visualizzare le filigrane di storage ottimizzate e determinare se è sicuro utilizzarle.

Valuta l'utilizzo dei dati degli oggetti per l'intera griglia

Passaggi

1. Selezionare **Nodi**.
2. Per ogni sito nella griglia, espandi l'elenco dei nodi.
3. Esamina i valori percentuali indicati nella colonna **Dati oggetto utilizzati** per ciascun Storage Node in ogni sito.



4. Segui il passaggio appropriato:
   a. Se nessuno dei nodi di archiviazione è quasi pieno (ad esempio, tutti i valori **Dati oggetto utilizzati** sono inferiori all'80%), puoi iniziare a usare le impostazioni di override. Vai a Usa filigrane ottimizzate.
   b. Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se specifici pool di archiviazione sono quasi pieni, esegui i passaggi in Visualizza le watermarks di storage ottimizzate e Verifica se puoi utilizzare filigrane ottimizzate.

Visualizza le filigrane di archiviazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati che ha calcolato per il watermark soft di sola lettura del volume di storage. Puoi visualizzare i valori minimi e massimi ottimizzati per ciascun Storage Node nella tua grid.

Passaggi

1. ${post_edited_translations.segment}
2. Nella sezione Prometheus, seleziona il collegamento per accedere all'interfaccia utente di Prometheus.
3. ${post_edited_translations.segment}

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore minimo ottimizzato del watermark soft di sola lettura per tutti i volumi di archiviazione su ciascun Storage Node. Se questo valore è superiore all'impostazione personalizzata per il watermark soft di sola lettura del volume di archiviazione, viene attivato l'avviso **Low read-only watermark override** per lo Storage Node.

4. Per vedere il valore massimo consigliato per la filigrana soft read-only, inserisci la seguente metrica Prometheus e seleziona **Esegui**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   ${post_edited_translations.segment}

5. Nota il valore massimo ottimizzato per ciascun Storage Node.

Determina se puoi utilizzare filigrane ottimizzate

Passaggi

1. Selezionare **Nodi**.
2. Ripeti questi passaggi per ogni nodo di archiviazione online:
   a. Seleziona ***Storage Node*** > **Storage**.
   b. Scorri verso il basso fino alla tabella Archivi oggetti.
   c. Confronta il valore **Disponibile** per ogni archivio di oggetti (volume) con il massimo watermark ottimizzato che hai annotato per quel Storage Node.
3. Se almeno un volume su ogni nodo di archiviazione online ha più spazio disponibile rispetto al limite massimo ottimizzato per quel nodo, vai a Usa filigrane ottimizzate per iniziare a utilizzare i limiti ottimizzati.

   Altrimenti, espandi la griglia il prima possibile. O "aggiungi volumi di archiviazione" su un nodo esistente o "aggiungi nuovi Storage Node". Quindi, vai a Usa filigrane ottimizzate per aggiornare le impostazioni della watermark.

4. Se devi continuare a usare valori personalizzati per le filigrane del volume di archiviazione, "silenzio" oppure "disabilitare" l'avviso **Low read-only watermark override**.

> Gli stessi valori di watermark personalizzati vengono applicati a ogni volume di archiviazione su ogni Storage Node. L'utilizzo di valori inferiori a quelli consigliati per i watermark dei volumi di archiviazione potrebbe rendere alcuni volumi di archiviazione inaccessibili (smontati automaticamente) quando il nodo raggiunge la capacità.

Utilizza filigrane ottimizzate

Passaggi

1. Vai su **Support** > **Other** > **Storage watermarks**.
2. Seleziona la casella di controllo **Usa valori ottimizzati**.
3. Seleziona **Salva**.

Le impostazioni ottimizzate della filigrana per il volume di archiviazione sono ora attive per ciascun volume di archiviazione, in base alle dimensioni del Storage Node e alla capacità relativa del volume.

Risolvere i problemi relativi ai metadati in StorageGRID

Se si verificano problemi con i metadati, gli avvisi ti informeranno sulla causa dei problemi e sulle azioni consigliate da intraprendere. In particolare, devi aggiungere nuovi Storage Node se viene attivato l'avviso Low metadata storage.

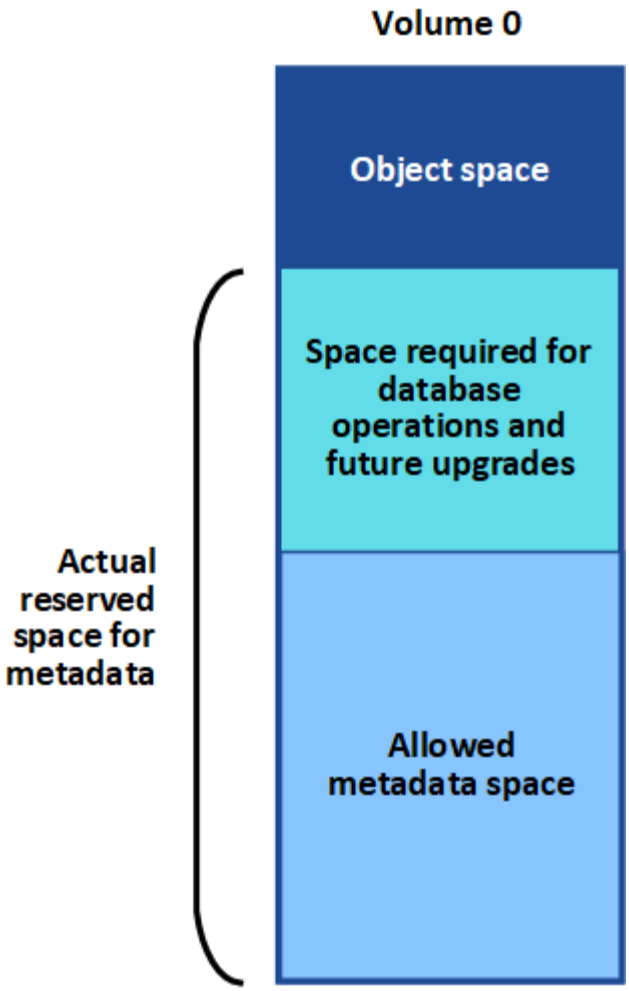
Prima di iniziare

Sei connesso a Grid Manager utilizzando un "browser web supportato".

Informazioni su questa attività

Segui le azioni consigliate per ogni avviso relativo ai metadati che viene attivato. Se viene attivato l'avviso **Low metadata storage**, devi aggiungere nuovi Storage Nodes.

StorageGRID riserva una certa quantità di spazio sul volume 0 di ciascun Storage Node per i metadati degli oggetti. Questo spazio, noto come *spazio riservato effettivo*, è suddiviso nello spazio consentito per i metadati degli oggetti (lo spazio metadati consentito) e nello spazio necessario per le operazioni essenziali del database, come compaction e riparazione. Lo spazio metadati consentito determina la capacità complessiva degli oggetti.



Se i metadati degli oggetti occupano 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 Storage Node" aiutarti ad anticipare gli errori e correggerli prima che si verifichino.

StorageGRID utilizza la seguente metrica di Prometheus per misurare quanto è pieno lo spazio consentito per i metadati:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

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

- **Problema minore**: i metadati degli oggetti stanno utilizzando il 70% o più dello spazio metadati consentito. Dovresti aggiungere nuovi Storage Node il prima possibile.
- **Problema grave**: i metadati degli oggetti stanno utilizzando il 90% o più dello spazio metadati consentito. Devi aggiungere subito nuovi Storage Node.

Quando i metadati degli oggetti utilizzano il 90% o più dello spazio metadati consentito, viene visualizzato un avviso nella dashboard. Se viene visualizzato questo avviso, devi aggiungere subito nuovi Storage Node. Non devi mai permettere che i metadati degli oggetti utilizzino più del 100% dello spazio consentito.

- **Critico**: i metadati degli oggetti stanno utilizzando il 100% o più dello spazio metadati consentito e stanno iniziando a consumare lo spazio necessario per le operazioni essenziali del database. Devi interrompere l'ingest di nuovi oggetti e aggiungere immediatamente nuovi Storage Node.

Se la dimensione del volume 0 è inferiore all'opzione di storage Spazio riservato ai metadati (ad esempio, in un ambiente non di produzione), il calcolo per l'alert **Low metadata storage** potrebbe essere inaccurato.

Passaggi

1. Seleziona **Avvisi** > **Attuali**.
2. Dalla tabella degli avvisi, espandi il gruppo di avvisi **Low metadata storage**, se necessario, e seleziona l'avviso specifico che vuoi visualizzare.
3. Esamina i dettagli nella finestra di dialogo di avviso.
4. Se è stato attivato un avviso importante o critico di **Low metadata storage**, esegui immediatamente un'espansione per aggiungere Storage Nodes.

Poiché StorageGRID conserva copie complete di tutti i metadati in ogni sito, la capacità di metadati dell'intera griglia è limitata dalla capacità di metadati del sito più piccolo. Se hai bisogno di aggiungere capacità di metadati a un sito, dovresti anche "espandi altri siti" aggiungere lo stesso numero di Storage Node.

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

Risolvere gli errori dei certificati in StorageGRID

Se riscontri un problema di sicurezza o relativo al certificato quando tenti di connetterti a StorageGRID tramite un browser web, un client S3 o uno strumento di monitoraggio esterno, dovresti controllare il certificato.

Informazioni su questa attività

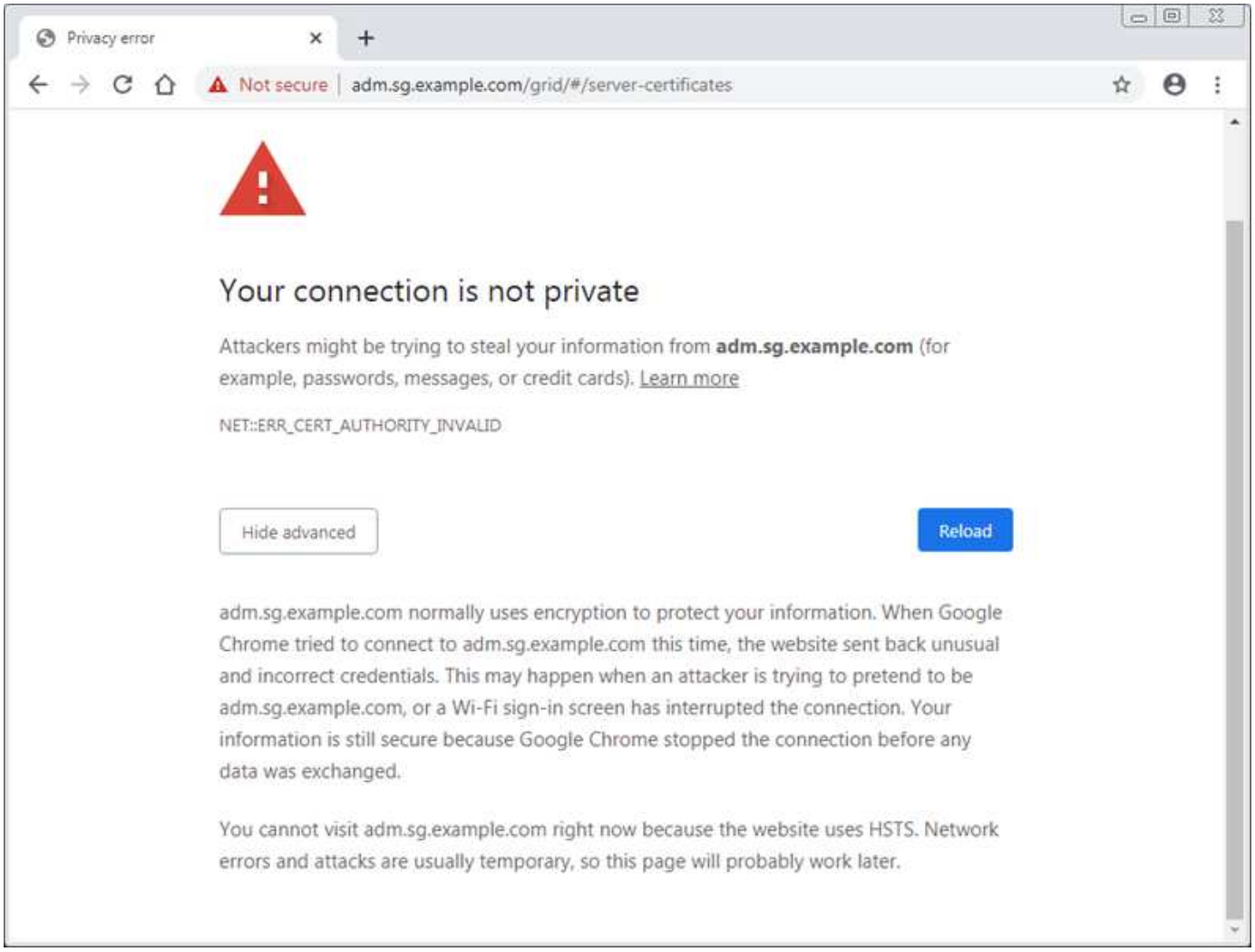
Gli errori relativi ai certificati possono causare problemi quando provi a connetterti a StorageGRID utilizzando Grid Manager, Grid Management API, Tenant Manager o Tenant Management API. Gli errori relativi ai certificati possono verificarsi anche quando provi a connetterti con un client S3 o uno strumento di monitoraggio esterno.

Se accedi a Grid Manager o Tenant Manager utilizzando un domain name invece di un indirizzo IP, il browser mostra un errore relativo al certificato senza possibilità di ignorarlo se si verifica una delle seguenti situazioni:

- Il certificato della tua interfaccia di gestione personalizzata sta per scadere.
- Torni al certificato predefinito del server invece di usare quello di un'interfaccia di gestione personalizzata.

L'esempio seguente mostra un errore relativo al certificato quando il certificato dell'interfaccia di gestione

personalizzata è scaduto:



Per garantire che le operazioni non vengano interrotte da un certificato server non valido, l'avviso **Expiration of server certificate for Management Interface** viene attivato quando il certificato server sta per scadere.

Quando usi 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.

Passaggi

Se hai ricevuto una notifica di avviso relativa a un certificato scaduto, accedi ai dettagli del certificato: . Seleziona **Configuration** > **Security** > **Certificates** e quindi "seleziona la scheda del certificato appropriata".

1. Verifica 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 sta per scadere, carica o genera un nuovo certificato.
   - Per un certificato server, vedi i passaggi per "configurare un certificato server personalizzato per Grid Manager e Tenant Manager".
   - Per un certificato client, vedi i passaggi per "configurare un certificato client".
3. In caso di errori relativi al certificato del server, prova una o entrambe le seguenti opzioni:

- Assicurati che il campo Subject Alternative Name (SAN) del certificato sia compilato e che il SAN corrisponda all'indirizzo IP o host name del nodo a cui ti stai connettendo.
- Se stai tentando di connetterti a StorageGRID utilizzando un domain name:
  i. Inserisci l'indirizzo IP del nodo amministratore anziché il domain name per aggirare l'errore di connessione e accedere al Grid Manager.
  ii. Dal Grid Manager, seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi "seleziona la scheda del certificato appropriata" per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
  iii. Nelle istruzioni per l'amministrazione StorageGRID, vedi i passaggi per "configurare un certificato server personalizzato per Grid Manager e Tenant Manager".

Risolvi i problemi relativi al nodo di amministrazione e all'interfaccia utente in StorageGRID

Puoi eseguire diverse operazioni per individuare l'origine dei problemi relativi ai nodi di amministrazione e all'interfaccia utente di StorageGRID.

Errori di accesso al nodo Admin

Se riscontri un errore quando accedi a un nodo di amministrazione StorageGRID, il tuo sistema potrebbe avere un problema con un "networking" o "hardware" problema, un problema con "Servizi del nodo amministratore", o un "problema con il database Cassandra" sui nodi di archiviazione StorageGRID connessi.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il file `Passwords.txt`.
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

Utilizza queste linee guida per la risoluzione dei problemi se visualizzi uno dei seguenti messaggi di errore quando tenti di accedere a un Admin Node:

- `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…`

Passaggi

1. Attendi 10 minuti e prova ad accedere di nuovo.

   Se l'errore non si risolve automaticamente, vai al passaggio successivo.

2. Se il tuo sistema StorageGRID ha più di un nodo amministratore, prova ad accedere al Grid Manager da un altro nodo amministratore per verificare lo stato di un nodo amministratore non disponibile.
   - Se riesci ad accedere, puoi utilizzare le opzioni **Dashboard**, **Nodes**, **Alerts** e **Support** per individuare la causa dell'errore.

- Se disponi di un solo Admin Node o non riesci ancora ad accedere, passa al passaggio successivo.

3. Determina se l'hardware del nodo è offline.
4. Se il single sign-on (SSO) è abilitato per il tuo sistema StorageGRID, segui i passaggi per "configurare il single sign-on".

   Potresti dover disabilitare e riabilitare temporaneamente il single sign-on per un singolo Admin Node per risolvere eventuali problemi.

   > Se l'SSO è abilitato, non puoi accedere utilizzando una porta con restrizioni. Devi usare la porta 443.

5. Verifica se l'account che stai utilizzando appartiene a un utente federato.

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

   - Se l'utente locale può accedere:
     i. Rivedi gli avvisi.
     ii. Seleziona **Configurazione** > **Controllo accessi** > **Federazione delle identità**.
     iii. Fai clic su **Verifica connessione** per convalidare le impostazioni di connessione per il LDAP server.
     iv. Se il test fallisce, risolvi eventuali errori di configurazione.
   - Se l'utente locale non riesce ad accedere e sei sicuro che le credenziali siano corrette, passa al passaggio successivo.

6. Utilizza Secure Shell (SSH) per accedere al nodo di amministrazione:
   a. Inserisci il seguente comando: `ssh admin@Admin_Node_IP`
   b. Inserisci la password indicata nel file `Passwords.txt`.
   c. Inserisci il seguente comando per passare all'utente root: `su -`
   d. Inserisci la password indicata nel file `Passwords.txt`.

      Quando sei connesso come root, il prompt cambia da `$` a `#`.

7. Visualizza lo stato di tutti i servizi in esecuzione sul nodo della griglia: `storagegrid-status`

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

   L'output si aggiorna 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. Conferma che il servizio nginx-gw è in esecuzione `# service nginx-gw status`
9. Usa Lumberjack per raccogliere i log: `# /usr/local/sbin/lumberjack.rb`

   Se l'autenticazione non riuscita si è verificata in passato, puoi usare le opzioni dello script Lumberjack --start e --end per specificare l'intervallo di tempo appropriato. Usa lumberjack -h per dettagli su queste opzioni.

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

10. Esamina i seguenti log:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`

- `**/*commands.txt`

11. Se non riesci a identificare alcun problema con l'Admin Node, esegui uno dei seguenti comandi per determinare gli indirizzi IP dei tre Storage Node che eseguono il servizio ADC nel tuo sito. Di solito, questi sono i primi tre Storage Node installati nel sito.

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

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

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

12. Dal nodo di amministrazione, usa ssh per accedere a ciascuno dei nodi di archiviazione ADC, usando gli indirizzi IP che hai identificato.
13. Visualizza lo stato di tutti i servizi in esecuzione sul nodo della griglia: `storagegrid-status`

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

14. Ripeti i passaggi Utilizza Lumberjack per raccogliere i log e Controlla i log per rivedere i log sui nodi di Storage.
15. Se non riesci a risolvere il problema, contatta il supporto tecnico.

    Fornisci i log raccolti al supporto tecnico. Vedi anche "Riferimento ai file di registro".

Problemi dell'interfaccia utente

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

Passaggi

1. Assicurati di utilizzare un "browser web supportato".
2. Cancella la cache del browser web.

   La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e permette all'interfaccia utente di funzionare di nuovo correttamente. Per le istruzioni, consulta la documentazione del tuo browser web.

Risolvi i problemi di rete, hardware e piattaforma in StorageGRID

Ci sono diverse attività che puoi svolgere per individuare la causa dei problemi relativi alla rete StorageGRID, all'hardware e alla piattaforma StorageGRID.

[[422-unprocessable-entity-errors]]
== Errori "422: Unprocessable Entity"

L'errore 422: Entità non elaborabile può verificarsi per diversi motivi. Controlla il messaggio di errore per capire cosa ha causato il problema.

Se visualizzi uno dei messaggi di errore elencati, segui l'azione consigliata.

Messaggio di errore	Causa principale e azione correttiva

`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`
	Questo messaggio potrebbe comparire se selezioni l'opzione **Non utilizzare TLS** per Transport Layer Security (TLS) durante la configurazione della federazione delle identità tramite Windows Active Directory (AD).
	
	L'opzione **Non usare TLS** non è supportata per i server AD che impongono la firma LDAP. Devi selezionare l'opzione **Usa STARTTLS** oppure l'opzione **Usa LDAPS** per TLS.

`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)`
	Questo messaggio viene visualizzato se provi a utilizzare un algoritmo di crittografia non supportato per stabilire una connessione Transport Layer Security (TLS) da StorageGRID a un sistema esterno utilizzato per la federazione delle identità o per i Cloud Storage Pools.
	
	Verifica gli algoritmi di cifratura offerti dal sistema esterno. Il sistema deve utilizzare uno dei "${post_edited_translations.segment}" per le connessioni TLS in uscita, come mostrato nelle istruzioni per l'amministrazione di StorageGRID.

Avviso di mancata corrispondenza MTU della Grid Network

L'avviso **Discrepanza MTU della rete Grid** viene attivato quando l'impostazione dell'unità di trasmissione massima (MTU) per l'interfaccia della rete Grid (eth0) differisce in modo significativo tra i nodi del grid.

Informazioni su questa attività

Le differenze nelle impostazioni MTU potrebbero indicare che alcune, ma non tutte, le reti eth0 sono configurate per i jumbo frame. Una discrepanza nella dimensione MTU superiore a 1000 potrebbe causare problemi di prestazioni di rete.

Passaggi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, "${post_edited_translations.segment}".
2. Elenca le impostazioni MTU per eth0 su tutti i nodi.
   - Usa la query fornita nel Grid Manager.
   - Vai su *primary Admin Node IP address*`/metrics/graph` e inserisci la seguente query: `node_network_mtu_bytes{device="eth0"}`
3. "${post_edited_translations.segment}" come necessario per garantire che siano uguali per l'interfaccia Grid Network (eth0) su tutti i nodi.
   - Per i nodi basati su Linux e VMware, usa il seguente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

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

     Nota: Sui nodi basati su Linux, se il valore MTU desiderato per la rete nel container supera il valore già configurato sull'interfaccia verso gli host, devi prima configurare l'interfaccia verso gli host con il valore MTU desiderato e poi usare lo `change-ip.py` script per cambiare il valore MTU della rete nel container.

     Usa i seguenti argomenti per modificare l'MTU sui nodi basati su Linux o VMware.

Argomenti posizionali	Descrizione
`mtu`	L'MTU da impostare. Deve essere compreso tra 1280 e 9216.
`network`	Le reti a cui applicare l'MTU. Includi uno o più dei seguenti tipi di rete: • griglia • amministratore • client

+

argomenti opzionali	Descrizione
`-h, - help`	Mostra il messaggio di aiuto ed esci.

argomenti opzionali	Descrizione
`-n node, --node node`	Il nodo. L'impostazione predefinita è il nodo locale.

4. Se hai consentito l'accesso SSH esterno, "blocco accesso" quando hai finito l'attività.

Avviso di errore del frame di ricezione della rete del nodo

Gli avvisi **Errore di ricezione del frame di rete del nodo** possono essere causati da problemi di connettività tra StorageGRID e il tuo hardware di rete. Questo avviso si risolve da solo dopo che il problema di base è stato risolto.

Informazioni su questa attività

Gli avvisi **Errore di ricezione del frame di rete del nodo** possono essere causati dai seguenti problemi con l'hardware di rete che si connette a StorageGRID:

- ${post_edited_translations.segment}
- Mancata corrispondenza tra l'MTU della porta dello switch e quella della scheda di rete
- Elevati tassi di errore di collegamento
- overrun del buffer circolare della scheda di rete

Passaggi

1. Segui i passaggi per la risoluzione dei problemi relativi a tutte le possibili cause di questo avviso, in base alla configurazione della tua rete.
2. Esegui i seguenti passaggi a seconda della causa dell'errore:

discrepanza FEC

> Questi passaggi sono applicabili solo agli avvisi di **errore di ricezione del frame di rete del nodo** causati da una mancata corrispondenza FEC sugli appliance StorageGRID.

a. Verifica lo stato FEC della porta dello switch collegato al tuo appliance StorageGRID.
b. Controlla l'integrità fisica dei cavi dall'appliance allo switch.
c. Se vuoi modificare le impostazioni FEC per provare a risolvere l'avviso, assicurati prima che l'appliance sia configurata in modalità **Auto** nella pagina Link Configuration di StorageGRID Appliance Installer (vedi le istruzioni per la tua appliance:
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 e SG1100"
   - "SG100 e SG1000"
d. Modifica le impostazioni FEC sulle porte dello switch. Le porte dell'appliance StorageGRID regoleranno le proprie impostazioni FEC per adattarsi, se possibile.

   Non puoi configurare le impostazioni FEC sulle appliance StorageGRID. Invece, le appliance tentano di rilevare e rispecchiare le impostazioni FEC sulle porte dello switch a cui sono collegate. Se i collegamenti sono forzati a velocità di rete di 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 tornerà alla modalità "no-FEC". Quando la FEC non è abilitata, le connessioni sono più suscettibili agli errori causati dal rumore elettrico.

   > Le appliance StorageGRID supportano Firecode (FC) e Reed Solomon (RS) FEC, oltre alla possibilità di non usare FEC.

Mancata corrispondenza tra l'MTU della porta dello switch e quella della scheda di rete

Se l'avviso è causato da una mancata corrispondenza tra la porta dello switch e l'MTU della scheda di rete, controlla che la dimensione MTU configurata sul nodo sia la stessa dell'impostazione MTU per la porta dello switch.

La dimensione MTU configurata sul nodo potrebbe essere inferiore all'impostazione della porta dello switch a cui il nodo è connesso. Se un nodo StorageGRID riceve un frame Ethernet più grande del suo MTU, cosa possibile con questa configurazione, potrebbe essere visualizzato l'avviso **Node network reception frame error**. Se pensi che sia questo il caso, cambia l'MTU della porta dello switch per farlo corrispondere all'MTU dell'interfaccia di rete di StorageGRID, oppure cambia l'MTU dell'interfaccia di rete di StorageGRID per farlo corrispondere alla porta dello switch, a seconda dei tuoi obiettivi o requisiti MTU end-to-end.

Per ottenere le migliori prestazioni di rete, tutti i nodi devono essere configurati con valori MTU simili sulle loro interfacce Grid Network. L'avviso **Grid Network MTU mismatch** viene attivato se si riscontra una differenza significativa nelle impostazioni MTU per la Grid Network sui singoli nodi. I valori MTU non devono essere necessariamente gli stessi per tutti i tipi di rete. Consulta Risolvi i problemi relativi all'avviso di mancata corrispondenza MTU della rete Grid per ulteriori informazioni.

Vedi anche "Modifica l'impostazione MTU".

Elevati tassi di errore di collegamento

a. Abilita FEC, se non è già abilitato.
b. Verifica che il cablaggio di rete sia di buona qualità e che non sia danneggiato o collegato in modo errato.
c. Se i cavi non sembrano essere il problema, contatta il supporto tecnico.

Potresti notare tassi di errore elevati in un ambiente con molto rumore elettrico.

overrun del buffer circolare della scheda di rete

Se l'errore è un overflow del buffer circolare della scheda di rete, contatta il supporto tecnico.

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

3. Monitora il problema e contatta il supporto tecnico se l'avviso non si risolve.

Errori di sincronizzazione temporale

Potresti riscontrare problemi di sincronizzazione dell'ora nella tua griglia.

Se riscontri problemi di sincronizzazione dell'ora, verifica di aver specificato almeno quattro sorgenti NTP esterne, ciascuna con un riferimento Stratum 3 o superiore, e che tutte le sorgenti NTP esterne funzionino correttamente e siano accessibili dai nodi StorageGRID.

Quando "specificando la sorgente NTP esterna" per un'installazione di StorageGRID a livello di produzione, non usare il servizio Windows Time (W32Time) su versioni di Windows precedenti a Windows Server 2016. Il servizio di sincronizzazione dell'ora nelle versioni precedenti di Windows non è sufficientemente preciso e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, come StorageGRID.

Linux: problemi di connettività di rete

${post_edited_translations.segment}

Clonazione dell'indirizzo MAC

In alcuni casi, i problemi di rete possono essere risolti utilizzando la clonazione dell'indirizzo MAC. Se utilizzi host virtuali, imposta il valore della chiave di clonazione dell'indirizzo MAC per ciascuna delle tue reti su "true" nel tuo file di configurazione del nodo. Questa impostazione fa sì che l'indirizzo MAC del container StorageGRID utilizzi l'indirizzo MAC dell'host. Consulta le istruzioni per "${post_edited_translations.segment}".

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

Per ulteriori informazioni, consulta le istruzioni per "${post_edited_translations.segment}".

Modalità promiscua

Se non vuoi usare la clonazione degli indirizzi MAC e preferisci permettere a tutte le interfacce di ricevere e trasmettere dati per indirizzi MAC diversi da quelli assegnati dall'hypervisor, assicurati che le proprietà di sicurezza a livello di switch virtuale e di port group siano impostate su **Accetta** per Modalità promiscua, Modifiche indirizzo MAC e Trasmissioni falsificate. I valori impostati sullo switch virtuale possono essere sovrascritti dai valori a livello di port group, quindi assicurati che le impostazioni siano le stesse in entrambi i punti.

Per ulteriori informazioni sull'utilizzo della modalità promiscua, consulta le istruzioni per "${post_edited_translations.segment}".

${post_edited_translations.segment}

Un nodo Linux in stato orfano di solito indica che il servizio storagegrid o il demone del nodo StorageGRID che controlla il container si sono arrestati in modo imprevisto.

Informazioni su questa attività

Se un nodo Linux segnala di trovarsi in uno stato orfano, dovresti:

- Controlla i registri per errori e messaggi.
- Prova ad avviare di nuovo il nodo.
- Se necessario, usa i comandi del motore del container per arrestare il container del nodo esistente.
- Riavvia il nodo.

Passaggi

1. Controlla i log sia del demone del servizio che del nodo orfano per errori evidenti o messaggi relativi a un'uscita imprevista.
2. Accedi all'host come root o usando un account con permessi sudo.
3. Tenta di avviare nuovamente 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, arresta il motore dei container e tutti i processi di controllo storagegrid-node. Ad esempio:`sudo docker stop --time secondscontainer-name`

Per `seconds`, inserisci il numero di secondi che vuoi attendere prima che il container si arresti (di solito 15 minuti o meno). Per esempio:

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

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

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

Linux: Risolvi i problemi relativi al supporto IPv6

Potresti dover abilitare il supporto IPv6 nel kernel se hai installato nodi StorageGRID su host Linux e noti che gli indirizzi IPv6 non sono stati assegnati ai container dei nodi come previsto.

Informazioni su questa attività

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

1. Seleziona **Nodes** e seleziona il nodo.
2. Seleziona **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, segui questi passaggi per abilitare il supporto IPv6 nel kernel.

Passaggi

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

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

Il risultato dovrebbe essere 0.

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

> Se il risultato non è 0, consulta la documentazione del sistema operativo per modificare `sysctl` le impostazioni. Poi, imposta il valore su 0 prima di continuare.

3. Entra nel container 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 dovrebbe essere 1.

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

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

5. Esci dal container: `exit`

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

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

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

7. Individua le due righe seguenti e rimuovi i tag di commento. Poi salva e chiudi il file.

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

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

8. Esegui questi comandi per riavviare il container StorageGRID:

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

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

Risoluzione dei problemi dei messaggi di errore del server syslog esterno per StorageGRID

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

Questi errori vengono mostrati dalla procedura guidata Configura server syslog esterno se hai problemi a inviare messaggi di prova per verificare che il server syslog esterno sia configurato correttamente.

Problemi durante l'esecuzione potrebbero essere segnalati dall'"Errore di inoltro del server syslog esterno"avviso. Se ricevi questo avviso, segui le istruzioni nell'avviso per reinviare i messaggi di test così puoi ottenere messaggi di errore dettagliati.

Per ulteriori informazioni sull'invio di informazioni di controllo a un syslog server esterno, consulta:

- "Considerazioni sull'utilizzo di un syslog server esterno"
- "Configura la gestione dei log e il server syslog esterno"

Messaggio di errore	Descrizione e azioni consigliate
Impossibile risolvere il nome host	L'FQDN che hai inserito per il syslog server non può essere risolto in un indirizzo IP. 1. Verifica il nome host che hai inserito. Se hai inserito un indirizzo IP, assicurati che sia un indirizzo IP valido nel formato W.X.Y.Z ("punti decimali"). 2. Verifica che i DNS server siano configurati correttamente. 3. Conferma che ogni nodo possa accedere agli indirizzi IP del DNS server.
Connessione rifiutata	La connessione TCP o TLS al syslog server è stata rifiutata. Potrebbe non esserci alcun servizio in ascolto sulla porta TCP o TLS per l'host, oppure un firewall potrebbe bloccare l'accesso. 1. Verifica di aver inserito il FQDN o l'indirizzo IP, la porta e il protocollo corretti per il syslog server. 2. Conferma che l'host per il servizio syslog stia eseguendo un demone syslog in ascolto sulla porta specificata. 3. Conferma che un firewall non stia bloccando l'accesso alle connessioni TCP/TLS dai nodi all'indirizzo IP e alla porta del syslog server.
Rete irraggiungibile	Il syslog server non si trova su una sottorete collegata direttamente. Un router ha restituito un messaggio di errore ICMP per indicare che non poteva inoltrare i messaggi di test dai nodi elencati al syslog server. 1. Verifica di aver inserito il FQDN o l'indirizzo IP corretto per il syslog server. 2. Per ogni nodo elencato, controlla l'elenco delle sottoreti della Grid Network, gli elenchi delle sottoreti delle Admin Networks e i gateway della Client Network. Conferma che siano configurati per instradare il traffico al syslog server tramite l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host irraggiungibile	Il syslog server si trova su una sottorete collegata direttamente (sottorete utilizzata dai nodi elencati per i loro indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di prova, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del syslog server. 1. Verifica di aver inserito il FQDN o l'indirizzo IP corretto per il syslog server. 2. Verifica che l'host su cui è in esecuzione il servizio syslog sia attivo.

Messaggio di errore	Descrizione e azioni consigliate
Connessione scaduta	È stato effettuato un tentativo di connessione TCP/TLS, ma non è stata ricevuta alcuna risposta dal syslog server per un lungo periodo di tempo. Potrebbe esserci un errore di configurazione del routing oppure un firewall potrebbe bloccare il traffico senza inviare alcuna risposta (una configurazione comune). 1. Verifica di aver inserito il FQDN o l'indirizzo IP corretto per il syslog server. 2. Per ogni nodo elencato, controlla la Grid Network Subnet List, le Admin Networks Subnet Lists e i gateway della Client Network. Conferma che siano configurati per instradare il traffico verso il syslog server utilizzando l'interfaccia di rete e il gateway (Grid, Admin o Client) tramite cui ti aspetti che il syslog server venga raggiunto. 3. Conferma che un firewall non stia bloccando l'accesso alle connessioni TCP/TLS dai nodi elencati all'indirizzo IP e alla porta del syslog server.
Connessione chiusa dal partner	È stata stabilita con successo una connessione TCP al server syslog, ma è stata successivamente chiusa. Le possibili cause sono le seguenti: • Il syslog server potrebbe essere stato riavviato o riavviato. • Il nodo e il syslog server 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. Per risolvere questo problema: 1. Verifica di aver inserito il FQDN o l'indirizzo IP, la porta e il protocollo corretti per il syslog server. 2. Se usi TLS, assicurati che anche il server syslog usi TLS. Se usi TCP, assicurati che anche il server syslog usi TCP. 3. Controlla che un firewall intermedio non sia configurato per chiudere le connessioni TCP inattive.
errore del certificato TLS	Il certificato del server ricevuto dal syslog server non era compatibile con il pacchetto di certificati CA e il certificato client che hai fornito. 1. Conferma che il pacchetto di certificati CA e il certificato client (se presente) siano compatibili con il certificato del server sul syslog server. 2. Conferma che le identità nel certificato del syslog server includano i valori IP o FQDN previsti.
Inoltro sospeso	I record di syslog non vengono più inoltrati al syslog server e StorageGRID non riesce a rilevare il motivo. Esamina i log di debug forniti con questo errore per tentare di determinarne la causa principale.

Messaggio di errore	Descrizione e azioni consigliate
Sessione TLS terminata	Il syslog server ha terminato la sessione TLS e StorageGRID non riesce a rilevare il motivo. 1. Esamina i log di debug forniti con questo errore per tentare di determinarne la causa principale. 2. Verifica di aver inserito il FQDN o l'indirizzo IP, la porta e il protocollo corretti per il syslog server. 3. Se usi TLS, assicurati che anche il server syslog usi TLS. Se usi TCP, assicurati che anche il server syslog usi TCP. 4. Conferma che il pacchetto di certificati CA e il certificato client (se presente) siano compatibili con il certificato del server del syslog server. 5. Conferma che le identità nel certificato del syslog server includano i valori IP o FQDN previsti.
La query dei risultati non è riuscita	Il nodo di amministrazione utilizzato per la configurazione e il test del server syslog non è in grado di richiedere i risultati dei test dai nodi elencati. Uno o più nodi potrebbero essere inattivi. 1. Segui le procedure standard di risoluzione dei problemi per assicurarti che i nodi siano online e che tutti i servizi previsti siano in esecuzione. 2. Riavvia il servizio miscd sui nodi elencati.

Scopri i problemi di memorizzazione nella cache del bilanciatore del carico in StorageGRID

Scopri i possibili problemi con la cache del load balancer e come risolverli.

Determina se una richiesta è stata un cache hit

- L'intestazione X-Cache viene impostata nella risposta alle richieste gestite dal servizio di cache. Codici possibili:
  - `HIT`: L'oggetto è stato servito dalla cache
  - `PARTIAL-HIT`: Il bucket/la chiave aveva un record nella cache, ma non è stato possibile fornire l'intero intervallo richiesto dalla cache
  - `STALE`Il bucket/la chiave aveva un record nella cache, ma l'oggetto è stato aggiornato dall'ultima volta che è stato servito dalla cache.
  - `MISS`: L'oggetto non era presente nella cache
- Il `nginx-gw/endpoint-access.log.gz`record per la richiesta include "unix:/run/cache-svc/cache-svc.sock" per le richieste gestite dalla cache.
- Il `cache-svc/cache-svc.log` riporta un messaggio come "Request 320390: completed successfully (cache hit)" oppure "Request 320375: completed successfully (cache miss)." Trova il percorso richiesto cercando altri record con la stessa stringa "Request <*number*>".

Basso cache hit rate

- Si potrebbero verificare bassi cache hit rate quando viene aggiunto un nuovo workload o quando cambia il working set a cui accede un workload. In queste situazioni, l'hit rate dovrebbe aumentare nel tempo.
- Se più carichi di lavoro utilizzano la cache, considera di aggiungere criteri di classificazione del traffico per isolare le parti dei carichi di lavoro gestite dalla cache. Le metriche di cache hit rate sono disponibili per ciascun criterio di classificazione del traffico. Se alcuni carichi di lavoro non ottengono buoni cache hit rate, considera di spostarli su altri endpoint in cui la cache non è abilitata.
- Valuta il tasso di svuotamento della cache. Se la cache è troppo piccola per contenere il working set, si verificheranno alti tassi di svuotamento e questo potrebbe contribuire a un hit rate più basso.
- Potrebbero essere disponibili opzioni per migliorare gli hit rate di determinati carichi di lavoro nell'ambito di FPVR.

Prestazioni scarse

- Valuta l'hit rate della cache. Un basso hit rate della cache può portare a prestazioni complessive basse.
- Valuta il tasso di eviction della cache. Durante l'eviction alcune risorse di storage vengono utilizzate per rimuovere gli oggetti esistenti dal disco. Se il processo di eviction non riesce a tenere il passo con l'accesso di nuovi oggetti, il sistema potrebbe raggiungere le soglie hard watermark e iniziare a bypassare la cache.
- Verifica i limiti di rete utilizzando le diagnostiche "Utilizzo di ricezione delle interfacce di rete" e "Utilizzo di trasmissione delle interfacce di rete".

${post_edited_translations.segment}

${post_edited_translations.segment}

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di audit e dei log di audit di StorageGRID. Puoi utilizzare queste informazioni per leggere e analizzare la traccia di audit dell'attività di sistema.

Queste istruzioni sono per gli amministratori responsabili della produzione di report sull'attività e sull'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID.

Per utilizzare il file di log di testo, devi avere accesso alla condivisione di audit configurata sull'Admin Node.

Per informazioni sulla configurazione dei livelli dei messaggi di audit e sull'utilizzo di un server syslog esterno, vedi "Configura la gestione dei log e il server syslog esterno".

Come i messaggi di controllo si spostano attraverso il sistema StorageGRID nel file di log audit.log per la conservazione

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. Dovresti capire come questi messaggi di audit si spostano attraverso il sistema StorageGRID fino al file `audit.log`.

I seguenti workflow per i messaggi di audit e la conservazione dei messaggi di audit sono applicabili solo se StorageGRID è configurato per **nodi Admin/nodi locali** o **nodo Admin e server syslog esterno**. Se StorageGRID è configurato per "Solo nodi locali" (impostazione predefinita) o "Server syslog esterno", i messaggi di audit vengono salvati localmente su ciascun nodo nel file `/var/local/log/localaudit.log`

e non possono essere elaborati dai nodi Admin o dai nodi Storage.

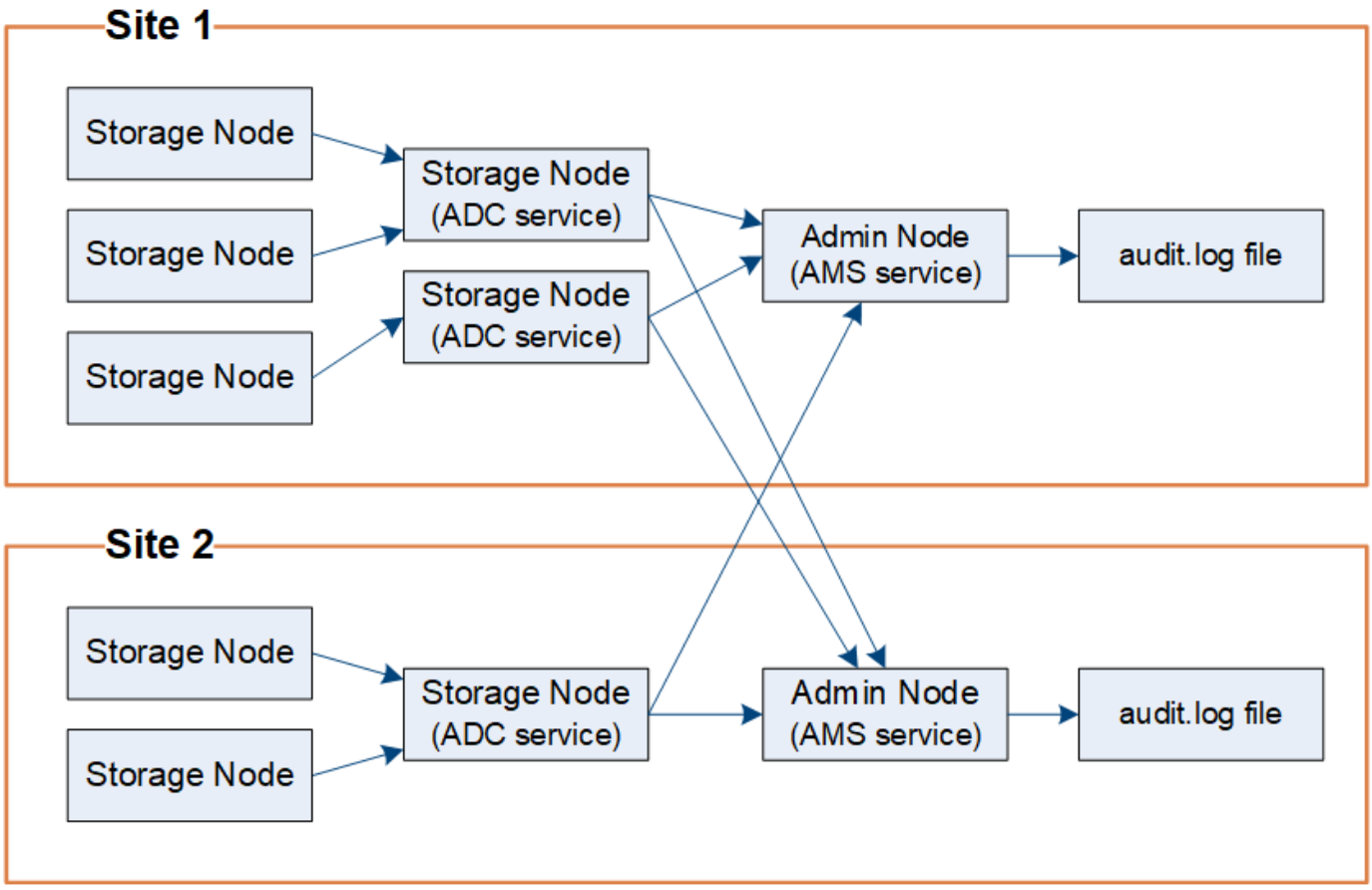
${post_edited_translations.segment}

${post_edited_translations.segment}

Come mostrato nel diagramma di flusso dei messaggi di audit, ciascun nodo StorageGRID invia i propri messaggi di audit a uno dei servizi ADC presso il sito del data center. Il servizio ADC viene abilitato automaticamente per i primi tre Storage Node installati in ciascun sito.

A sua volta, ogni servizio ADC funge da relè e invia la propria raccolta di messaggi di audit a ogni nodo di amministrazione nel sistema StorageGRID, dando così a ciascun nodo di amministrazione una registrazione completa dell'attività di sistema.

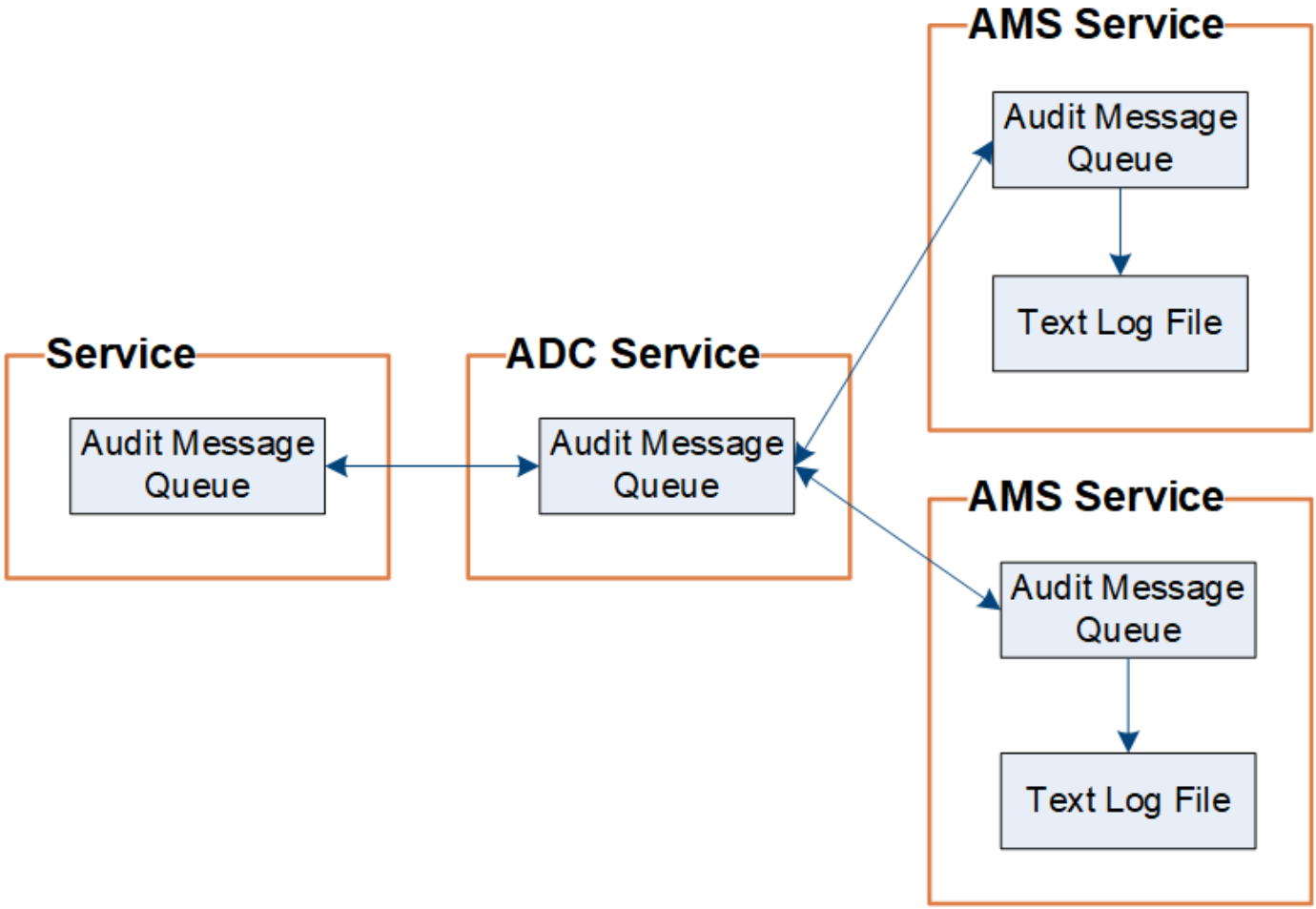
Ciascun nodo Admin memorizza i messaggi di audit in file di log di testo; il file di log attivo è denominato `audit.log`.



Conservazione dei messaggi di audit

StorageGRID utilizza un processo di copia ed eliminazione per garantire che nessun messaggio di audit venga perso prima di essere scritto nel file di log di audit.

Quando un nodo genera o inoltra un messaggio di audit, il messaggio viene memorizzato in una coda di messaggi di audit sul disco di sistema del nodo della griglia. Una copia del messaggio viene sempre conservata in una coda di messaggi di audit finché il messaggio non viene scritto nel file di log di audit nella directory dell'Admin Node `/var/local/audit/export`. Questo aiuta a prevenire la perdita di un messaggio di audit durante il trasporto.



La coda dei messaggi di audit può aumentare temporaneamente a causa di problemi di connettività di rete o di una capacità di audit insufficiente. Man mano che le code aumentano, consumano più spazio disponibile nella directory `/var/local/` di ciascun nodo. Se il problema persiste e la directory dei messaggi di audit di un nodo si riempie troppo, i singoli nodi danno priorità all'elaborazione dell'arretrato e diventano temporaneamente non disponibili per nuovi messaggi.

Nello specifico, potresti osservare i seguenti comportamenti:

- Se la `/var/local/audit/export` directory utilizzata da un Admin Node si riempie, l'Admin Node viene contrassegnato come non disponibile per i nuovi messaggi di audit finché la directory non si svuota. Le richieste client S3 non sono influenzate. L'allarme XAMS (Unreachable Audit Repositories) viene attivato quando un repository di audit non è raggiungibile.
- Se la `/var/local/` directory utilizzata da un nodo di Storage Node con il servizio ADC raggiunge il 92%, il nodo viene contrassegnato come non disponibile per i messaggi di audit finché la directory non scende all'87%. Le richieste client S3 verso altri nodi non sono influenzate. L'allarme NRLY (Available Audit Relays) viene attivato quando i relay di audit non sono raggiungibili.

  > Se non ci sono nodi di archiviazione disponibili con il servizio ADC, i nodi di archiviazione memorizzano i messaggi di audit localmente nel file `/var/local/log/localaudit.log`.

- Se la `/var/local/` directory utilizzata da un Storage Node raggiunge l'85% di riempimento, il nodo inizia a rifiutare le richieste dei client S3 con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare una crescita molto elevata delle code dei messaggi di audit:

- Interruzione di un Admin Node o di uno Storage Node con il servizio ADC. Se uno dei nodi del sistema non è disponibile, i nodi rimanenti potrebbero subire un sovraccarico.
- Un ritmo di attività sostenuto che supera la capacità di audit del sistema.
- Lo `/var/local/` spazio su un nodo di archiviazione ADC si esaurisce per motivi non correlati ai messaggi di audit. Quando succede, il nodo smette di accettare nuovi messaggi di audit e dà priorità al backlog attuale, il che può causare backlog su altri nodi.

Avviso di coda di audit di grandi dimensioni e allarme Audit Messages Queued (AMQS)

${post_edited_translations.segment}

Se viene attivato l'avviso **Coda di audit di grandi dimensioni** o l'allarme AMQS legacy, inizia verificando il carico sul sistema: se c'è stato un numero significativo di transazioni recenti, l'avviso e l'allarme dovrebbero risolversi nel tempo e puoi ignorarli.

Se l'avviso o l'allarme persiste e aumenta di gravità, visualizza un grafico della dimensione della coda. Se il numero aumenta costantemente nel corso di ore o giorni, è probabile che il carico di audit abbia superato la capacità di audit del sistema. Riduci la frequenza delle operazioni del client o diminuisci il numero di messaggi di audit registrati modificando il livello di audit per Client Writes e Client Reads su Error o Off. Vedi "Configura la gestione dei log e il server syslog esterno".

Messaggi duplicati

Il sistema StorageGRID adotta un approccio prudente in caso di guasto della rete o di un nodo. Per questo motivo, potrebbero essere presenti messaggi duplicati nel file di log.

Accedi ai file di log di audit dalla riga di comando del nodo Admin di StorageGRID

La cartella di controllo contiene il file attivo `audit.log` e tutti i file di log di controllo compressi. Puoi accedere ai file di log di controllo direttamente dalla riga di comando dell'Admin Node.

Il file `audit.log` rimane vuoto a meno che non configuri StorageGRID per **Admin Nodes/local nodes** o **Admin Node and external syslog server**. Per ulteriori informazioni, consulta "${post_edited_translations.segment}".

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Devi avere il file `Passwords.txt`.
- ${post_edited_translations.segment}

Passaggi

1. Accedi a un nodo amministratore:
   a. Inserisci il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Inserisci la password indicata nel file `Passwords.txt`.
   c. Inserisci il seguente comando per passare all'utente root: `su -`
   d. Inserisci la password indicata nel file `Passwords.txt`.

      Quando sei connesso come root, il prompt cambia da `$` a `#`.

2. Vai alla directory che contiene i file di log di controllo:

   ```
   cd /var/local/audit/export/
   ```

3. ${post_edited_translations.segment}

Scopri la rotazione dei file di log di audit in StorageGRID

Se StorageGRID è configurato per **nodi Admin/nodi locali** o **nodo Admin e server syslog esterno**, i file di log di audit vengono salvati nella directory `/var/local/audit/export/` del nodo Admin. I file di log di audit attivi sono denominati `audit.log`.

> In via opzionale, puoi modificare la destinazione dei log di audit e inviare le informazioni di audit a un server syslog esterno. I log locali dei record di audit continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Fai riferimento a "Configura i messaggi di audit e il server syslog esterno".

Una volta al giorno, il file `audit.log` attivo viene salvato e viene avviato un nuovo file `audit.log`. Il nome del file salvato indica quando è stato salvato, nel formato *`yyyy-mm-dd.txt`*. Se in un solo giorno viene creato più di un audit log, i nomi dei file utilizzano la data in cui il file è stato salvato, con l'aggiunta di un numero, nel formato *`yyyy-mm-dd.txt.n`*. Ad esempio, `2018-04-15.txt` e `2018-04-15.txt.1` sono il primo e il secondo file di log creati e salvati il 15 aprile 2018.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato *`yyyy-mm-dd.txt.gz`*, che conserva la data originale. Nel corso del tempo, lo storage dell'Admin Node allocato per i log di audit viene consumato. Uno script monitora il consumo di spazio dei log di audit e cancella i file di log secondo necessità per liberare spazio nella directory `/var/local/audit/export/`. I log di audit vengono eliminati in base alla data in cui sono stati creati. I log più vecchi vengono eliminati per primi. Puoi monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

Questo esempio mostra il file `audit.log` attivo, il file del giorno precedente (`2018-04-15.txt`, e il file compresso del giorno precedente (`2018-04-14.txt.gz`.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato del file di log di audit

Scopri il formato dei file di log di audit in StorageGRID

I file di log di audit si trovano su ogni Admin Node e contengono una raccolta di singoli messaggi di audit.

Ogni messaggio di audit contiene quanto segue:

- ${post_edited_translations.segment}

YYYY-MM-DDTHH:MM:SS.UUUUUU, dove *UUUUUU* sono microsecondi.

- Il messaggio di audit stesso, racchiuso tra parentesi quadre e che inizia con `AUDT`.

L'esempio seguente mostra tre messaggi di audit in un file di log (interruzioni di riga aggiunte per una migliore leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e ha aggiunto due oggetti a quel bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Nel loro formato predefinito, i messaggi di audit nei file di log di audit non sono facili da leggere o interpretare.

Puoi usare "strumento audit-explain" per ottenere riepiloghi semplificati dei messaggi di audit nel file di log di audit. Puoi usare "strumento audit-sum" per riepilogare quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno impiegato queste operazioni.

Utilizzare lo strumento audit-explain per tradurre i messaggi di audit di StorageGRID

Puoi usare lo `audit-explain` strumento per tradurre i messaggi di audit presenti nel registro di audit in un formato facile da leggere.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Devi avere il file `Passwords.txt`.
- ${post_edited_translations.segment}

Informazioni su questa attività

Lo strumento `audit-explain`, disponibile sull'Admin Node primario, fornisce riepiloghi semplificati dei messaggi di audit in un log di audit.

> Lo strumento `audit-explain` è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. L'elaborazione `audit-explain` delle query può consumare una grande quantità di potenza della CPU, il che potrebbe influire sulle operazioni di StorageGRID.

Questo esempio mostra l'output tipico dello `audit-explain` strumento. Questi quattro "SPUT" messaggi di audit sono stati generati quando il tenant con account ID 92484777680322627870 ha utilizzato richieste S3 PUT per creare un bucket chiamato "bucket1" e aggiungere tre oggetti a quel bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Lo `audit-explain` strumento può fare quanto segue:

- Elabora i log di controllo, sia semplici che compressi. Ad esempio:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Elabora più file contemporaneamente. Ad esempio:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- Accetta input da una pipe, che ti consente di filtrare e pre-elaborare l'input utilizzando il `grep` comando o altri mezzi. Ad esempio:

```
grep SPUT audit.log | audit-explain

grep bucket-name audit.log | audit-explain
```

Poiché i file di log di controllo possono essere molto grandi e lenti da analizzare, puoi risparmiare tempo filtrando le parti che vuoi esaminare ed eseguendo `audit-explain` su quelle parti, invece che sull'intero file.

> Lo `audit-explain` strumento non accetta file compressi come input tramite pipe. Per elaborare i file compressi, specifica i loro nomi come argomenti della riga di comando oppure usa lo `zcat` strumento per decomprimere prima i file. Ad esempio:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Usa l' `help (-h)`opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-explain -h
```

Passaggi

1. Accedi al nodo amministratore principale:
   a. Inserisci il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Inserisci la password indicata nel file `Passwords.txt`.
   c. Inserisci il seguente comando per passare all'utente root: `su -`
   d. Inserisci la password indicata nel file `Passwords.txt`.

   Quando sei connesso come root, il prompt cambia da `$` a `#`.

2. Inserisci il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e il percorso del file o dei file che desideri analizzare:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   Lo `audit-explain` strumento stampa interpretazioni leggibili dall'uomo di tutti i messaggi presenti nel file o nei file specificati.

   > Per ridurre la lunghezza delle righe e migliorare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se vuoi vedere i timestamp, usa l'opzione timestamp (`-t`.

Utilizzare lo strumento audit-sum per riepilogare i messaggi di audit di StorageGRID

Puoi usare lo strumento `audit-sum` per contare i messaggi di audit di scrittura, lettura, head ed eliminazione e per vedere il tempo minimo, massimo e medio (o la dimensione) per ciascun tipo di operazione.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Hai il file `Passwords.txt`.
- ${post_edited_translations.segment}

Informazioni su questa attività

Lo `audit-sum` strumento, disponibile sul nodo di amministrazione principale, riassume quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno impiegato queste operazioni.

> Lo `audit-sum`strumento è pensato principalmente per l'uso da parte del supporto tecnico durante le operazioni di troubleshooting. L'elaborazione delle `audit-sum`query può consumare una grande quantità di potenza della CPU, il che potrebbe influire sulle operazioni di StorageGRID.

Questo esempio mostra l'output tipico dello `audit-sum` strumento. Questo esempio mostra quanto tempo hanno impiegato le operazioni del protocollo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Lo `audit-sum`strumento fornisce conteggi e tempi per i seguenti messaggi di audit S3 e ILM in un file di log di audit.

> I codici di controllo vengono rimossi dal prodotto e dalla documentazione man mano che le funzionalità vengono deprecate. Se incontri un codice di controllo che non è presente in questo elenco, controlla le versioni precedenti di questo argomento per le release precedenti di StorageGRID. Ad esempio, "StorageGRID 11.8 Utilizzo dello strumento audit sum".

Codice	Descrizione	${post_edited_translations.segment}
IDEL	Eliminazione avviata da ILM: registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"
${post_edited_translations.segment}	S3 DELETE: Registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: S3 DELETE"

Codice	Descrizione	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment}	"SGET: S3 GET"
SHEA	${post_edited_translations.segment}	"SHEA: S3 HEAD"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"

Lo `audit-sum`strumento può fare quanto segue:

- Elabora i log di controllo, sia semplici che compressi. Ad esempio:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Elabora più file contemporaneamente. Ad esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- Accetta input da una pipe, che ti consente di filtrare e pre-elaborare l'input utilizzando il `grep` comando o altri mezzi. Ad esempio:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> Questo strumento non accetta file compressi come input tramite pipe. Per elaborare i file compressi, specifica i loro nomi come argomenti della riga di comando oppure utilizza lo `zcat` strumento per decomprimere prima i file. Ad esempio:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Puoi usare le opzioni della riga di comando per riepilogare le operazioni sui bucket separatamente da quelle sugli oggetti oppure per raggruppare i riepiloghi dei messaggi per nome del bucket, periodo di tempo o tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di operazione minimo, massimo e medio, ma puoi usare l' `size (-s)`opzione per visualizzare invece la dimensione dell'oggetto.

Usa l' `help (-h)`opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-sum -h
```

Passaggi

1. Accedi al nodo amministratore principale:

a. Inserisci il seguente comando: `ssh admin@primary_Admin_Node_IP`

b. Inserisci la password indicata nel file `Passwords.txt`.

c. Inserisci il seguente comando per passare all'utente root: `su -`

d. Inserisci la password indicata nel file `Passwords.txt`.

Quando sei connesso come root, il prompt cambia da `$` a `#`.

2. Se vuoi analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, head ed eliminazione, segui questi passaggi:

a. Inserisci il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e il percorso del file o dei file che desideri analizzare:

```
$ audit-sum /var/local/audit/export/audit.log
```

Questo esempio mostra l'output tipico dello `audit-sum` strumento. Questo esempio mostra quanto tempo hanno impiegato le operazioni del protocollo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media, con un tempo di 1,13 secondi, ma sia le operazioni SGET che SPUT (S3 PUT) mostrano tempi massimi elevati, pari a circa 1.770 secondi.

b. Per visualizzare le 10 operazioni di recupero più lente, usa il comando grep per selezionare solo i messaggi SGET e aggiungi l'opzione di output lunga (`-l` per includere i percorsi degli oggetti:

```
grep SGET audit.log | audit-sum -l
```

I risultati includono il tipo (oggetto o bucket) e il percorso, il che ti permette di cercare nel file di log di controllo altri messaggi relativi a questi specifici oggetti.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
Da questo esempio di output, puoi vedere che le tre richieste GET S3 più lente erano per oggetti di circa 5 GB di dimensione, molto più grandi rispetto agli altri oggetti. Le grandi dimensioni spiegano i tempi di recupero più lenti nel caso peggiore.

3. Se vuoi determinare quali dimensioni di oggetti vengono inseriti e recuperati dalla tua griglia, usa l'opzione dimensione (`-s`):

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

In questo esempio, la dimensione media degli oggetti per SPUT è inferiore a 2,5 MB, mentre la dimensione media per SGET è molto maggiore. Il numero di messaggi SPUT è molto più alto del numero di messaggi SGET, il che indica che la maggior parte degli oggetti non viene mai recuperata.

4. Se vuoi verificare se ieri i recuperi sono stati lenti:

   a. Esegui il comando sul file di log di audit appropriato e usa l'opzione group-by-time (`-gt`, seguita dal periodo di tempo (ad esempio, 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Questi risultati mostrano che il traffico S3 GET ha raggiunto un picco tra le 06:00 e le 07:00. I tempi massimi e medi sono entrambi considerevolmente più elevati in questo intervallo di tempo e non sono aumentati gradualmente con l'aumentare del numero di richieste. Queste metriche suggeriscono che la capacità è stata superata, probabilmente nella rete o nella capacità della grid di elaborare le richieste.

b. Per determinare la dimensione degli oggetti recuperati ogni ora ieri, aggiungi l'opzione size (`-s`) al comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Questi risultati indicano che alcuni recuperi di grandi dimensioni si sono verificati quando il traffico complessivo di recupero era al massimo.

c. Per vedere più dettagli, usa "strumento audit-explain" per rivedere tutte le operazioni SGET durante quell'ora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se ti aspetti che l'output del comando grep sia composto da molte righe, aggiungi il comando `less` per mostrare il contenuto del file di log di audit una pagina (una schermata) alla volta.

5. Se vuoi determinare se le operazioni SPUT sui bucket sono più lente delle operazioni SPUT sugli oggetti:

a. Inizia utilizzando l `-go` opzione, che raggruppa i messaggi per le operazioni su oggetti e bucket separatamente:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

I risultati mostrano che le operazioni SPUT per i bucket hanno caratteristiche prestazionali diverse rispetto alle operazioni SPUT per gli oggetti.

b. Per determinare quali bucket presentano le operazioni SPUT più lente, usa l' `-gb`opzione, che raggruppa i messaggi per bucket:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Per determinare quali bucket hanno la dimensione dell'oggetto SPUT più grande, usa sia le opzioni `-gb` che `-s`:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Formato del messaggio di audit

Scopri la struttura dei messaggi di audit di StorageGRID

${post_edited_translations.segment}

Se le informazioni di riepilogo fornite dagli "audit-explain" e "${post_edited_translations.segment}" strumenti sono insufficienti, consulta questa sezione per capire il formato generale di tutti i messaggi di audit.

${post_edited_translations.segment}

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Ogni messaggio di audit contiene una stringa di elementi attributo. L'intera stringa è racchiusa tra parentesi quadre (`[ ]`, e ogni elemento attributo nella stringa ha le seguenti caratteristiche:

- Racchiuso tra parentesi `[ ]`
- Introdotto dalla stringa `AUDT`, che indica un messaggio di audit
- Senza delimitatori (nessuna virgola o spazio) prima o dopo
- Terminato da un carattere di avanzamento riga `\n`

${post_edited_translations.segment}

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Il numero di elementi di attributo nel messaggio dipende dal tipo di evento del messaggio. Gli elementi di attributo non sono elencati in un ordine particolare.

Il seguente elenco descrive gli elementi dell'attributo:

- `ATTR` è un codice di quattro caratteri che identifica l'attributo segnalato. Alcuni attributi sono comuni a tutti i messaggi di audit, mentre altri sono specifici di un singolo evento.
- `type` è un identificatore di quattro caratteri del tipo di dati del valore, come UI64, FC32 e così via. Il tipo è racchiuso tra parentesi `( )`.
- `value` è il contenuto dell'attributo, in genere un valore numerico o testuale. I valori seguono sempre i due punti (`:`). I valori di tipo di dati CSTR sono racchiusi tra virgolette doppie " ".

Tipi di dati nei messaggi di controllo StorageGRID

${post_edited_translations.segment}

Tipo	Descrizione
UI32	Numero intero lungo senza segno (32 bit); può memorizzare i numeri da 0 a 4,294,967,295.
UI64	Numero intero lungo senza segno (64 bit); può memorizzare i numeri da 0 a 18,446,744,073,709,551,615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32 bit rappresentato da quattro caratteri ASCII come "ABCD."
IPAD	Usato per gli indirizzi IP.
${post_edited_translations.segment}	Un array di caratteri UTF-8 a lunghezza variabile. I caratteri possono essere codificati secondo le seguenti convenzioni: • La barra rovesciata è \\. • Il ritorno a capo è \r. • Le virgolette doppie sono \". • Il carattere di nuova riga è \n. • I caratteri possono essere sostituiti dai loro equivalenti esadecimali (nel formato \xHH, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento nei messaggi di audit di StorageGRID

Ogni messaggio di controllo nel registro di controllo registra dati specifici relativi a un evento di sistema.

Dopo il container di apertura `[AUDT:` che identifica il messaggio stesso, il set successivo di attributi fornisce informazioni sull'evento o sull'azione descritta dal messaggio di audit. Questi attributi sono evidenziati nel seguente esempio:

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

L' `ATYP`elemento (sottolineato nell'esempio) identifica quale evento ha generato il messaggio. Questo messaggio di esempio include il "SHEA"codice del messaggio ([ATYP(FC32):SHEA]), indicando che è stato generato da una richiesta S3 HEAD riuscita.

Elementi comuni nei messaggi di audit di StorageGRID

Tutti i messaggi di audit contengono gli elementi comuni.

Codice	Tipo	Descrizione
${post_edited_translations.segment}	FC32	ID modulo: un identificatore a quattro caratteri dell'ID modulo che ha generato il messaggio. Questo indica il segmento di codice all'interno del quale è stato generato il messaggio di audit.
${post_edited_translations.segment}	UI32	ID nodo: l'ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID. Questo ID non può essere modificato.
ASES	UI64	Identificativo della sessione di audit: nelle versioni precedenti, questo elemento indicava l'ora in cui il sistema di audit veniva inizializzato dopo l'avvio del servizio. Questo valore temporale veniva misurato in microsecondi a partire dall'epoca del sistema operativo (00:00:00 UTC del 1 gennaio 1970). **Nota:** Questo elemento è obsoleto e non compare più nei messaggi di controllo.

Codice	Tipo	Descrizione
ASQN	UI64	Conteggio sequenza: nelle versioni precedenti, questo contatore veniva incrementato per ogni messaggio di audit generato sul nodo della griglia (ANID) e azzerato al riavvio del servizio. **Nota:** Questo elemento è obsoleto e non compare più nei messaggi di controllo.
ATID	UI64	ID di tracciamento: un identificatore condiviso dal set di messaggi attivati da un singolo evento.
ATIM	UI64	Timestamp: l'ora in cui è stato generato l'evento che ha attivato il messaggio di audit, misurata in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1 gennaio 1970). Nota che la maggior parte degli strumenti disponibili per convertire il timestamp in data e ora locali si basa sui millisecondi. Potrebbe essere necessario arrotondare o troncare il timestamp registrato. L'ora leggibile dall'uomo che appare all'inizio del messaggio di audit nel `audit.log` file è l'attributo ATIM in formato ISO 8601. La data e l'ora sono rappresentate come *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, dove `T` è un carattere stringa letterale che indica l'inizio del segmento temporale della data. *`UUUUUU`* sono microsecondi.
ATYP	FC32	Tipo di evento: un identificatore a quattro caratteri dell'evento registrato. Questo determina il contenuto del "payload" del messaggio: gli attributi inclusi.
AVER	UI32	Versione: la versione del messaggio di audit. Man mano che il software StorageGRID si evolve, le nuove versioni dei servizi potrebbero includere nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti nel servizio AMS per elaborare i messaggi provenienti da versioni precedenti dei servizi.
RSLT	FC32	Risultato: il risultato di un evento, processo o transazione. Se non è rilevante per un messaggio, si usa NONE anziché SUCS per evitare che il messaggio venga filtrato accidentalmente.

Formato ed esempi del messaggio di audit StorageGRID

Puoi trovare informazioni dettagliate in ogni messaggio di audit. Tutti i messaggi di audit usano lo stesso formato.

Di seguito è riportato un esempio di messaggio di audit come potrebbe apparire nel file `audit.log`:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Il messaggio di audit contiene informazioni sull'evento registrato, oltre a informazioni sul messaggio di audit stesso.

Per identificare quale evento viene registrato dal messaggio di audit, cerca l'attributo ATYP (evidenziato di seguito):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Il valore dell'attributo ATYP è SPUT. "SPUT" rappresenta una transazione S3 PUT, che registra l'ingest di un oggetto in un bucket.

${post_edited_translations.segment}

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Per scoprire quando si è verificato l'evento PUT, nota il timestamp UTC (Universal Coordinated Time) all'inizio del messaggio di audit. Questo valore è una versione leggibile dell'attributo ATIM del messaggio di audit stesso:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM registra il tempo, in microsecondi, dall'inizio dell'epoca UNIX. Nell'esempio, il valore `1405631878959669` corrisponde a giovedì 17 luglio 2014 alle 21:17:59 UTC.

Messaggi di controllo e ciclo di vita degli oggetti

Quando i messaggi di audit vengono generati in StorageGRID

I messaggi di audit vengono generati ogni volta che un oggetto viene acquisito, recuperato o eliminato. Puoi identificare queste transazioni nel file di log di audit individuando i messaggi di audit specifici dell'API S3.

I messaggi di audit sono collegati tramite identificatori specifici per ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (bucket), S3KY (key), o entrambi
Collegamento delle operazioni interne	CBID (identificativo interno dell'oggetto)

${post_edited_translations.segment}

A causa di fattori quali le differenze di temporizzazione tra i nodi della griglia, le dimensioni degli oggetti e i ritardi di rete, l'ordine dei messaggi di audit generati dai diversi servizi può variare rispetto a quello mostrato negli esempi in questa sezione.

Messaggi di audit per le transazioni di ingestione di oggetti in StorageGRID

Puoi identificare le transazioni di acquisizione del client nel registro di controllo individuando i messaggi di controllo specifici dell'API S3.

Nella tabella seguente non sono elencati tutti i messaggi di audit generati durante una transazione di ingest. Sono inclusi solo i messaggi necessari per tracciare la transazione di ingest.

Messaggi di audit di ingest S3

Codice	Nome	Descrizione	Traccia	Vedi
SPUT	${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}	"SPUT: S3 PUT"
${post_edited_translations.segment}	${post_edited_translations.segment}	La policy ILM è stata soddisfatta per questo oggetto.	${post_edited_translations.segment}	"${post_edited_translations.segment}"

Esempio: ingest di oggetti S3

La serie di messaggi di controllo riportata di seguito è un esempio dei messaggi di controllo generati e salvati nel registro di controllo quando un client S3 inserisce un oggetto in un nodo di storage (servizio LDR).

${post_edited_translations.segment}

> Non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio qui sotto. Sono elencati solo quelli relativi alla transazione di ingestione S3 (SPUT).

Questo esempio presuppone che un bucket S3 sia già stato creato.

SPUT: S3 PUT

Il messaggio SPUT viene generato per indicare che è stata emessa una transazione S3 PUT per creare un oggetto in un bucket specifico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

${post_edited_translations.segment}

Il messaggio ORLM indica che la policy ILM è stata soddisfatta per questo oggetto. Il messaggio include il CBID dell'oggetto e il nome della regola ILM applicata.

Per gli oggetti replicati, il campo LOCS include l'ID del nodo LDR e l'ID del volume delle posizioni degli oggetti.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Per gli oggetti con codifica di cancellazione, il campo LOCS include l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

${post_edited_translations.segment}

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Messaggi di audit per le transazioni di eliminazione degli oggetti in StorageGRID

Puoi identificare le transazioni di eliminazione degli oggetti nel registro di controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

${post_edited_translations.segment}

Codice	Nome	Descrizione	Traccia	Vedi
${post_edited_translations.segment}	Eliminazione S3	${post_edited_translations.segment}	CBID, S3KY	"SDEL: S3 DELETE"

Esempio: eliminazione di un oggetto S3

Quando un client S3 elimina un oggetto da un Storage Node (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.

> Nell'esempio seguente non sono elencati tutti i messaggi di audit generati durante una transazione di eliminazione. Sono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: Eliminazione S3

L'eliminazione di un oggetto inizia quando il client invia una richiesta DeleteObject a un servizio LDR. Il messaggio contiene il bucket da cui eliminare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificarlo.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Messaggi di audit per le transazioni di recupero degli oggetti in StorageGRID

Puoi identificare le transazioni di recupero degli oggetti nel registro di controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di recupero sono elencati nella tabella seguente. Sono inclusi solo i messaggi necessari per tracciare la transazione di recupero.

Messaggi di audit del recupero S3

Codice	Nome	Descrizione	Traccia	Vedi
${post_edited_translations.segment}	S3 GET	Richiesta fatta per recuperare un oggetto da un bucket.	${post_edited_translations.segment}	"SGET: S3 GET"

Esempio: recupero di oggetti S3

Quando un client S3 recupera un oggetto da un Storage Node (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.

Nota che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti inizia quando il client invia una richiesta GetObject a un servizio LDR. Il messaggio contiene il bucket da cui recuperare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificarlo.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se la policy del bucket lo consente, un client può recuperare oggetti in modo anonimo oppure recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di audit contiene informazioni sull'account tenant del proprietario del bucket, così puoi tracciare queste richieste anonime e tra account diversi.

Nel seguente messaggio di esempio, il client invia una richiesta GetObject per un oggetto memorizzato in un bucket di cui non è proprietario. I valori per SBAI e SBAC registrano l'ID e il nome dell'account tenant del proprietario del bucket, che differiscono dall'ID e dal nome dell'account tenant del client registrati in S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

${post_edited_translations.segment}

Quando un client S3 esegue una query S3 Select su un oggetto, vengono generati messaggi di audit che

vengono salvati nel registro di audit.

Tieni presente che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

${post_edited_translations.segment}

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messaggi di controllo per gli aggiornamenti dei metadati degli oggetti S3 in StorageGRID

${post_edited_translations.segment}

${post_edited_translations.segment}

Codice	Nome	Descrizione	Traccia	Vedi
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati di un oggetto acquisito.	${post_edited_translations.segment}	"SUPD: Metadati S3 aggiornati"

${post_edited_translations.segment}

L'esempio mostra una transazione riuscita per aggiornare i metadati di un oggetto S3 esistente.

SUPD: Aggiornamento dei metadati S3

Il client S3 invia una richiesta (SUPD) per aggiornare i metadati specificati (`x-amz-meta-*`) per l'oggetto S3 (S3KY). In questo esempio, le intestazioni della richiesta sono incluse nel campo HTRH perché è stato configurato come intestazione del protocollo di audit (*Configurazione* > **Monitoraggio** > **Server di audit e syslog**). Vedi "Configura la gestione dei log e il server syslog esterno".

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Messaggi di audit

Scopri i tipi e i codici dei messaggi di audit in StorageGRID

Le descrizioni dettagliate dei messaggi di audit restituiti dal sistema sono riportate nelle sezioni seguenti. Ciascun messaggio di audit è innanzitutto elencato in una tabella che raggruppa i messaggi correlati in base alla classe di attività che il messaggio rappresenta. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposti ad audit, sia per selezionare il tipo di filtro dei messaggi di audit desiderato.

I messaggi di audit sono elencati anche in ordine alfabetico in base ai loro codici di quattro caratteri. Questo elenco alfabetico ti consente di trovare informazioni su messaggi specifici.

I codici di quattro caratteri utilizzati in questo capitolo sono i valori ATYP presenti nei messaggi di controllo, come mostrato nel seguente messaggio di esempio:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Per informazioni sull'impostazione dei livelli dei messaggi di audit, sulla modifica delle destinazioni dei log e sull'utilizzo di un server syslog esterno per le informazioni di audit, vedi "Configura la gestione dei log e il server syslog esterno"

${post_edited_translations.segment}

Messaggi di audit per gli eventi di sistema in StorageGRID

I messaggi di audit appartenenti alla categoria di audit di sistema vengono utilizzati per eventi relativi al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema (attività di griglia) e alle operazioni di backup dei servizi.

Codice	Titolo e descrizione del messaggio	Vedi
${post_edited_translations.segment}	${post_edited_translations.segment}	"${post_edited_translations.segment}"
${post_edited_translations.segment}	Frammento di dati con codifica di cancellazione corrotto: indica che è stato rilevato un frammento di dati con codifica di cancellazione corrotto.	"${post_edited_translations.segment}"
${post_edited_translations.segment}	${post_edited_translations.segment}	"${post_edited_translations.segment}"
GNRG	Registrazione GNDS: Un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.	"GNRG: Registrazione GNDS"
GNUR	${post_edited_translations.segment}	"GNUR: Annullamento della registrazione GNDS"
GTED	Attività di griglia terminata: il servizio CMN ha terminato l'elaborazione dell'attività di griglia.	"GTED: Attività di griglia terminata"
GTST	Attività di griglia avviata: il servizio CMN ha iniziato a elaborare l'attività di griglia.	"GTST: Attività di griglia avviata"
${post_edited_translations.segment}	Attività di griglia inviata: un'attività di griglia è stata inviata al servizio CMN.	"GTSU: Attività di griglia inviata"
LLST	Posizione persa: questo messaggio di controllo viene generato quando una posizione viene persa.	"${post_edited_translations.segment}"

Codice	Titolo e descrizione del messaggio	Vedi
OLST	${post_edited_translations.segment}	"OLST: Il sistema ha rilevato un oggetto smarrito"
SADD	${post_edited_translations.segment}	"SADD: Disabilita controllo di sicurezza"
${post_edited_translations.segment}	Abilitazione controllo di sicurezza: la registrazione dei messaggi di audit è stata ripristinata.	"SADE: Abilita controllo di sicurezza"
${post_edited_translations.segment}	Verifica dell'archivio di oggetti non riuscita: un blocco di contenuto non ha superato i controlli di verifica.	"${post_edited_translations.segment}"
${post_edited_translations.segment}	Object Store Verify Unknown: rilevati dati oggetto imprevisti nell'archivio di oggetti.	"${post_edited_translations.segment}"
SYSD	Arresto del nodo: è stato richiesto uno spegnimento.	"SYSD: Arresto del nodo"
SISTEMA	Arresto del nodo: un servizio ha avviato un arresto controllato.	"SYST: Arresto del nodo"
${post_edited_translations.segment}	Avvio nodo: un servizio è stato avviato; la natura dell'arresto precedente è indicata nel messaggio.	"${post_edited_translations.segment}"

Messaggi di controllo per gli eventi di storage a oggetti in StorageGRID

I messaggi di audit appartenenti alla categoria di audit dello storage a oggetti vengono utilizzati per gli eventi correlati allo storage e alla gestione degli oggetti all'interno del sistema StorageGRID. Questi includono lo storage e il recupero di oggetti, i trasferimenti da nodo grid a nodo grid e le verifiche.

> I codici di audit vengono rimossi dal prodotto e dalla documentazione man mano che le funzionalità vengono deprecate. Se incontri un codice di audit che non è elencato qui, controlla le versioni precedenti di questo argomento per le versioni precedenti di SG. Ad esempio, "Messaggi di audit dello storage a oggetti StorageGRID 11.8".

Codice	Descrizione	Vedi
BROR	Richiesta di sola lettura del bucket: un bucket è entrato o uscito dalla modalità di sola lettura.	"BROR: Richiesta di sola lettura del bucket"
${post_edited_translations.segment}	Fine invio oggetto: l'entità sorgente ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	"CBSE: Fine invio oggetto"

Codice	Descrizione	Vedi
CBRE	Fine ricezione oggetto: l'entità di destinazione ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	"CBRE: Fine ricezione oggetto"
CGRR	Richiesta di replica tra griglie: StorageGRID ha tentato un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglia.	"CGRR: Richiesta di replica cross-grid"
EBDL	${post_edited_translations.segment}	"EBDL: Eliminazione del bucket vuoto"
${post_edited_translations.segment}	Richiesta di svuotamento del bucket: un utente ha inviato una richiesta per attivare o disattivare lo svuotamento del bucket (ovvero per eliminare gli oggetti del bucket o per interrompere l'eliminazione degli oggetti).	"${post_edited_translations.segment}"
SCMT	${post_edited_translations.segment}	"SCMT: Richiesta di commit dell'object store"
${post_edited_translations.segment}	${post_edited_translations.segment}	"${post_edited_translations.segment}"

Messaggi di audit per le operazioni di lettura del client in StorageGRID

I messaggi di audit di lettura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedi
S3SL	Richiesta S3 Select: registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.	${post_edited_translations.segment}	"S3SL: richiesta S3 Select"
${post_edited_translations.segment}	${post_edited_translations.segment} **Nota:** Se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	${post_edited_translations.segment}	"SGET: S3 GET"
SHEA	${post_edited_translations.segment}	${post_edited_translations.segment}	"SHEA: S3 HEAD"

Messaggi di audit per le operazioni di scrittura del client in StorageGRID

I messaggi di audit di scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedi
${post_edited_translations.segment}	Sovrascrittura oggetto: registra una transazione per sovrascrivere un oggetto con un altro oggetto.	${post_edited_translations.segment}	"OVWR: Sovrascrittura oggetto"
${post_edited_translations.segment}	S3 DELETE: Registra una transazione riuscita per eliminare un oggetto o un bucket. **Nota:** Se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	${post_edited_translations.segment}	"SDEL: S3 DELETE"
SPOS	S3 POST: Registra una transazione riuscita per ripristinare un oggetto da AWS Glacier storage a un Cloud Storage Pool.	${post_edited_translations.segment}	"${post_edited_translations.segment}"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket. **Nota:** Se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	${post_edited_translations.segment}	"SPUT: S3 PUT"
SUPD	${post_edited_translations.segment}	${post_edited_translations.segment}	"SUPD: Metadati S3 aggiornati"

Messaggi di audit della gestione StorageGRID

La categoria Gestione registra le richieste degli utenti alla Management API.

Codice	Titolo e descrizione del messaggio	Vedi
${post_edited_translations.segment}	Messaggio di audit della Management API: un log delle richieste utente.	"${post_edited_translations.segment}"

Messaggi di audit ILM di StorageGRID

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per eventi correlati alle operazioni di gestione del ciclo di vita delle informazioni (ILM).

Codice	Titolo e descrizione del messaggio	Vedi
IDEL	Eliminazione avviata da ILM: questo messaggio di audit viene generato quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"

Codice	Titolo e descrizione del messaggio	Vedi
LKCU	Pulizia degli oggetti sovrascritti. Questo messaggio di controllo viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di storage.	"LKCU: Pulizia degli oggetti sovrascritti"
${post_edited_translations.segment}	${post_edited_translations.segment}	"${post_edited_translations.segment}"

${post_edited_translations.segment}

Messaggio di audit BROR per le richieste di sola lettura del bucket in StorageGRID

Il servizio LDR genera questo messaggio di audit quando un bucket entra o esce dalla modalità di sola lettura. Ad esempio, un bucket entra in modalità di sola lettura mentre tutti gli oggetti vengono eliminati.

Codice	Campo	Descrizione
BKHD	UUID del bucket	L'ID del bucket.
BROV	Valore della richiesta di sola lettura del bucket	Indica se il bucket viene reso di sola lettura o se sta uscendo dallo stato di sola lettura (1 = sola lettura, 0 = non sola lettura).
BROS	${post_edited_translations.segment}	Il motivo per cui il bucket viene reso di sola lettura o esce dallo stato di sola lettura. Ad esempio, emptyBucket.
S3AI	${post_edited_translations.segment}	L'ID del tenant che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

Messaggio di audit CBRB per l'inizio della ricezione dell'oggetto in StorageGRID

Durante le normali operazioni di sistema, i blocchi di contenuto vengono trasferiti continuamente tra diversi nodi man mano che si accede ai dati, e questi vengono replicati e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo a un altro, l'entità di destinazione emette questo messaggio.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	L'identificativo univoco della sessione/connessione nodo-nodo.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	${post_edited_translations.segment}
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
${post_edited_translations.segment}	Entità di origine	L'ID del nodo sorgente (mittente) del trasferimento CBID.
${post_edited_translations.segment}	Entità di destinazione	L'ID del nodo di destinazione (ricevente) del trasferimento CBID.
CTSS	Inizio conteggio sequenza	Indica il primo numero di sequenza richiesto. Se ha successo, il trasferimento inizia da questo numero di sequenza.
${post_edited_translations.segment}	${post_edited_translations.segment}	Indica l'ultimo conteggio di sequenza richiesto. In caso di esito positivo, il trasferimento viene considerato completato quando questo conteggio di sequenza è stato ricevuto.
RSLT	Stato di inizio trasferimento	${post_edited_translations.segment} SUCS: Trasferimento avviato con successo.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo elemento di contenuto, identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" a "Expected End Sequence Count". I nodi di invio e ricezione sono identificati dai relativi ID nodo. Puoi utilizzare queste informazioni per tracciare il flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

Messaggio di audit CBRE per la ricezione dell'oggetto in StorageGRID

${post_edited_translations.segment}

Codice	Campo	Descrizione
CNID	Identificatore di connessione	L'identificativo univoco della sessione/connessione nodo-nodo.
${post_edited_translations.segment}	Identificatore del blocco di contenuto	${post_edited_translations.segment}

Codice	Campo	Descrizione
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
${post_edited_translations.segment}	Entità di origine	L'ID del nodo sorgente (mittente) del trasferimento CBID.
${post_edited_translations.segment}	Entità di destinazione	L'ID del nodo di destinazione (ricevente) del trasferimento CBID.
CTSS	Inizio conteggio sequenza	Indica il numero di sequenza da cui è iniziato il trasferimento.
${post_edited_translations.segment}	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio di sequenza trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è stato positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Il risultato dell'operazione di trasferimento (dal punto di vista del soggetto mittente): ${post_edited_translations.segment} CONL: connessione persa durante il trasferimento CTMO: connessione scaduta durante la fase di stabilimento o trasferimento UNRE: ID nodo di destinazione irraggiungibile CRPT: trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di audit indica che un'operazione di trasferimento dati da nodo a nodo è stata completata. Se il risultato del trasferimento (Transfer Result) è positivo, l'operazione ha trasferito i dati da "Start Sequence Count" a "Actual End Sequence Count". I nodi di invio e ricezione sono identificati dai relativi ID nodo. Queste informazioni possono essere utilizzate per tracciare il flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare il numero di repliche.

Messaggio di audit CBSB per l'inizio dell'invio dell'oggetto in StorageGRID

Durante il normale funzionamento del sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che i dati vengono consultati, replicati

e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, l'entità di origine emette questo messaggio.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	L'identificativo univoco della sessione/connessione nodo-nodo.
${post_edited_translations.segment}	Identificatore del blocco di contenuto	${post_edited_translations.segment}
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
${post_edited_translations.segment}	Entità di origine	L'ID del nodo sorgente (mittente) del trasferimento CBID.
${post_edited_translations.segment}	Entità di destinazione	L'ID del nodo di destinazione (ricevente) del trasferimento CBID.
CTSS	Inizio conteggio sequenza	Indica il primo numero di sequenza richiesto. Se ha successo, il trasferimento inizia da questo numero di sequenza.
${post_edited_translations.segment}	${post_edited_translations.segment}	Indica l'ultimo conteggio di sequenza richiesto. In caso di esito positivo, il trasferimento viene considerato completato quando questo conteggio di sequenza è stato ricevuto.
RSLT	Stato di inizio trasferimento	${post_edited_translations.segment} SUCS: trasferimento avviato con successo.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo elemento di contenuto, identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" a "Expected End Sequence Count". I nodi di invio e ricezione sono identificati dai relativi ID nodo. Puoi utilizzare queste informazioni per tracciare il flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

Messaggio di audit CBSE per la fine dell'invio dell'oggetto in StorageGRID

Quando il trasferimento di un blocco di contenuto da un nodo a un altro è completato, questa entità di origine emette questo messaggio.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	L'identificativo univoco della sessione/connessione nodo-nodo.
${post_edited_translations.segment}	Identificatore del blocco di contenuto	${post_edited_translations.segment}
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
${post_edited_translations.segment}	Entità di origine	L'ID del nodo sorgente (mittente) del trasferimento CBID.
${post_edited_translations.segment}	Entità di destinazione	L'ID del nodo di destinazione (ricevente) del trasferimento CBID.
CTSS	Inizio conteggio sequenza	Indica il numero di sequenza da cui è iniziato il trasferimento.
${post_edited_translations.segment}	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio di sequenza trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è stato positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Il risultato dell'operazione di trasferimento (dal punto di vista del soggetto mittente): ${post_edited_translations.segment} CONL: connessione persa durante il trasferimento CTMO: connessione scaduta durante la fase di stabilimento o trasferimento UNRE: ID nodo di destinazione irraggiungibile CRPT: trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di audit indica che un'operazione di trasferimento dati da nodo a nodo è stata completata. Se il risultato del trasferimento (Transfer Result) è positivo, l'operazione ha trasferito i dati da "Start Sequence Count" a "Actual End Sequence Count". I nodi di invio e ricezione sono identificati dai relativi ID nodo. Queste informazioni possono essere utilizzate per tracciare il flusso di dati del sistema e per individuare, tabulare e

analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare il numero di repliche.

Messaggio di audit CGRR per le richieste di replica tra griglie in StorageGRID

Questo messaggio viene generato quando StorageGRID tenta un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglia.

Codice	Campo	Descrizione
CSIZ	Dimensioni dell'oggetto	La dimensione dell'oggetto in byte. L'attributo CSIZ è stato introdotto in StorageGRID 11.8. Di conseguenza, le richieste di replica cross-grid durante un aggiornamento da StorageGRID 11.7 a 11.8 potrebbero presentare una dimensione totale dell'oggetto imprecisa.
S3AI	${post_edited_translations.segment}	L'ID del tenant che possiede il bucket da cui viene replicato l'oggetto.
GFID	ID connessione Grid federation	L'ID della connessione di federazione della griglia utilizzata per la replica tra griglie.
${post_edited_translations.segment}	Operazione CGR	Il tipo di operazione di replica cross-grid che hai tentato: • 0 = Replica oggetto • 1 = Replica oggetto multipart • 2 = Replica il marcatore di eliminazione
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket.
${post_edited_translations.segment}	ID versione	L'ID della versione specifica di un oggetto che veniva replicata.
RSLT	${post_edited_translations.segment}	Restituisce successo (SUCS) o errore generale (GERR).

Messaggio di audit EBDL per le eliminazioni di oggetti bucket vuoti in StorageGRID

Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione di svuotamento del bucket).

Codice	Campo	Descrizione
CSIZ	Dimensioni dell'oggetto	La dimensione dell'oggetto in byte.
PATH	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SEGC	UUID del container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
RSLT	${post_edited_translations.segment}	Il risultato di un evento, processo o transazione. Se non è rilevante per un messaggio, viene utilizzato NONE anziché SUCS così il messaggio non viene filtrato accidentalmente.

Messaggio di audit EBKR per richieste di bucket vuoti in StorageGRID

Questo messaggio indica che un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (cioè per eliminare gli oggetti del bucket o per interrompere l'eliminazione degli oggetti).

Codice	Campo	Descrizione
BUID	UUID del bucket	L'ID del bucket.
EBJS	Configurazione JSON del bucket vuoto	Contiene il JSON che rappresenta la configurazione corrente di Empty Bucket.
S3AI	${post_edited_translations.segment}	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

Messaggio di audit ECMC per dati con codifica di cancellazione mancanti in StorageGRID

${post_edited_translations.segment}

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il frammento mancante.

Codice	Campo	Descrizione
MCID	ID chunk	L'identificatore del frammento mancante codificato tramite cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NONE'. RSLT è un campo di messaggio obbligatorio, ma non è rilevante per questo messaggio specifico. Viene utilizzato 'NONE' anziché 'SUCS' in modo che questo messaggio non venga filtrato.

Messaggio di audit ECOC per dati con codice di cancellazione corrotti in StorageGRID

Questo messaggio di controllo indica che il sistema ha rilevato un frammento di dati con codifica di cancellazione danneggiato.

Codice	Campo	Descrizione
${post_edited_translations.segment}	ID VCS	Il nome del VCS che contiene il chunk danneggiato.
${post_edited_translations.segment}	ID volume	${post_edited_translations.segment}
CCID	ID chunk	L'identificativo del frammento corrotto codificato con cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NONE'. RSLT è un campo di messaggio obbligatorio, ma non è rilevante per questo messaggio specifico. Viene utilizzato 'NONE' anziché 'SUCS' in modo che questo messaggio non venga filtrato.

Messaggio di audit ETAF per errori di autenticazione di sicurezza in StorageGRID

Questo messaggio viene generato quando un tentativo di connessione tramite Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	L'identificativo univoco del sistema per la connessione TCP/IP tramite cui l'autenticazione non è riuscita.
RUID	Identità utente	Un identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.

Codice	Campo	Descrizione
RSLT	Codice motivo	Il motivo del fallimento: ${post_edited_translations.segment} CERM: Certificato mancante. CERT: Il certificato non è valido. CERE: Il certificato era scaduto. ${post_edited_translations.segment} CSGN: La firma del certificato non è valida. CSGU: Il firmatario del certificato era sconosciuto. UCRM: Mancavano le credenziali utente. ${post_edited_translations.segment} UCRU: Le credenziali utente non sono state consentite. ${post_edited_translations.segment}

Quando si stabilisce una connessione a un servizio sicuro che utilizza il protocollo TLS, le credenziali dell'entità remota vengono verificate utilizzando il profilo TLS e la logica aggiuntiva integrata nel servizio. Se questa autenticazione non riesce a causa di certificati o credenziali non validi, non previsti o non consentiti, viene registrato un messaggio di audit. Questo consente di eseguire query per tentativi di accesso non autorizzato e altri problemi di connessione relativi alla sicurezza.

Il messaggio potrebbe derivare da una configurazione errata di un'entità remota o da tentativi di presentare credenziali non valide o non consentite al sistema. Questo messaggio di controllo dovrebbe essere monitorato per rilevare tentativi di accesso non autorizzato al sistema.

Messaggio di audit GNRG per la registrazione GNDS in StorageGRID

Il servizio CMN genera questo messaggio di controllo quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUCS: Operazione riuscita • ${post_edited_translations.segment} • ${post_edited_translations.segment}
${post_edited_translations.segment}	ID nodo	${post_edited_translations.segment}

Codice	Campo	Descrizione
GNTP	${post_edited_translations.segment}	Il tipo di dispositivo del nodo della griglia (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	La stringa che identifica la versione del modello del dispositivo del nodo della grid nel bundle DMDL.
${post_edited_translations.segment}	Gruppo	${post_edited_translations.segment}
GNIA	Indirizzo IP	${post_edited_translations.segment}

${post_edited_translations.segment}

Messaggio di audit GNUR per l'annullamento della registrazione GNDS in StorageGRID

Il servizio CMN genera questo messaggio di controllo quando un servizio ha annullato la registrazione delle informazioni su se stesso dal sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUCS: Operazione riuscita • ${post_edited_translations.segment} • ${post_edited_translations.segment}
${post_edited_translations.segment}	ID nodo	${post_edited_translations.segment}

Messaggio di audit GTED per le attività di grid terminate in StorageGRID

Questo messaggio di controllo indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e ha spostato l'attività nella tabella storica. Se il risultato è SUCS, ABRT o ROLF, ci sarà un messaggio di controllo corrispondente "Grid Task Started". Gli altri risultati indicano che l'elaborazione di questa attività di griglia non è mai iniziata.

Codice	Campo	Descrizione
${post_edited_translations.segment}	ID attività	Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante tutto il suo ciclo di vita. **Nota:** L'ID attività viene assegnato al momento della generazione di un'attività di griglia, non al momento del suo invio. È possibile che una determinata attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Submitted, Started e Ended.
RSLT	Risultato	Risultato finale dell'attività di griglia: • SUCS: L'attività di griglia è stata completata con successo. • ABRT: L'attività di griglia è stata terminata senza errori di rollback. • ${post_edited_translations.segment} • ANNULLA: L'attività di grid è stata annullata dall'utente prima che venisse avviata. • EXPR: L'attività di griglia è scaduta prima di essere avviata. • IVLD: L'attività di grid non è valida. • AUTORIZZAZIONE: L'operazione sulla griglia non era autorizzata. • DUPL: L'attività di grid è stata rifiutata perché duplicata.

Messaggio di audit GTST per le attività di grid avviate in StorageGRID

Questo messaggio di audit indica che il servizio CMN ha iniziato a elaborare il task grid specificato. Il messaggio di audit segue immediatamente il messaggio Grid Task Submitted per i task grid avviati dal servizio interno Grid Task Submission e selezionati per l'attivazione automatica. Per i task grid inviati alla tabella Pending, questo messaggio viene generato quando l'utente avvia il task grid.

Codice	Campo	Descrizione
${post_edited_translations.segment}	ID attività	Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante tutto il suo ciclo di vita. **Nota:** L'ID attività viene assegnato al momento della generazione di un'attività di griglia, non al momento del suo invio. È possibile che una determinata attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Submitted, Started e Ended.
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: • SUCS: L'attività di grid è stata avviata correttamente.

Messaggio di audit GTSU per le attività di grid inviate in StorageGRID

${post_edited_translations.segment}

Codice	Campo	Descrizione
${post_edited_translations.segment}	ID attività	Identifica in modo univoco un'attività di griglia generata e ti permette di gestirla durante tutto il suo ciclo di vita. **Nota:** L'ID attività viene assegnato al momento della generazione di un'attività di griglia, non al momento del suo invio. È possibile che una determinata attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Submitted, Started e Ended.
TTYP	${post_edited_translations.segment}	${post_edited_translations.segment}
TVER	${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	Descrizione dell'attività	Una descrizione comprensibile all'uomo dell'attività della grid.
${post_edited_translations.segment}	Valido dopo il timestamp	L'istante più remoto (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui il grid task è valido.
${post_edited_translations.segment}	${post_edited_translations.segment}	L'ora più recente (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui l'attività di griglia è valida.
${post_edited_translations.segment}	Fonte	La fonte del compito: • TXTB: L'attività di griglia è stata inviata tramite il sistema StorageGRID come blocco di testo firmato. • GRIGLIA: L'attività di griglia è stata inviata tramite il servizio interno di invio delle attività di griglia.
${post_edited_translations.segment}	Tipo di attivazione	${post_edited_translations.segment} • AUTO: L'attività di griglia è stata inviata per l'attivazione automatica. • IN SOSPESO: L'attività di griglia è stata inserita nella tabella in sospeso. Questa è l'unica possibilità per la sorgente TXTB.

Codice	Campo	Descrizione
RSLT	Risultato	Il risultato dell'invio: • SUCS: L'attività di grid è stata inviata correttamente. • ERRORE: L'attività è stata spostata direttamente nella tabella storica.

Messaggio di audit IDEL per le eliminazioni avviate da ILM in StorageGRID

${post_edited_translations.segment}

Il messaggio IDEL viene generato in una di queste situazioni:

- **Per gli oggetti nei bucket S3 conformi**: questo messaggio viene generato quando ILM avvia il processo di eliminazione automatica di un oggetto perché il suo periodo di conservazione è scaduto (supponendo che l'impostazione di eliminazione automatica sia abilitata e che il blocco legale sia disattivato).
- **Per gli oggetti in bucket S3 non conformi**. Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto perché al momento non si applicano istruzioni di posizionamento nelle policy ILM attive all'oggetto stesso.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	${post_edited_translations.segment}	Solo per oggetti in bucket S3 conformi. 0 (falso) o 1 (vero), indica se un oggetto conforme deve essere eliminato automaticamente quando termina il suo periodo di conservazione, a meno che il bucket non sia soggetto a un blocco legale.
CMPL	${post_edited_translations.segment}	Solo per gli oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), che indica se il bucket è attualmente sottoposto a un blocco legale.
${post_edited_translations.segment}	${post_edited_translations.segment}	Solo per oggetti in bucket S3 conformi. La durata del periodo di conservazione dell'oggetto in minuti.
${post_edited_translations.segment}	Conformità: tempo di ingestione	Solo per oggetti in bucket S3 conformi. Ora di inserimento dell'oggetto. Puoi aggiungere il periodo di conservazione in minuti a questo valore per determinare quando l'oggetto può essere eliminato dal bucket.
DMRK	ID versione del marcatore di eliminazione	L'ID della versione del marcatore di eliminazione creato quando elimini un oggetto da un bucket versionato. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	La posizione di archiviazione dei dati dell'oggetto all'interno del sistema StorageGRID. Il valore per LOCS è " se l'oggetto non ha posizioni (ad esempio, è stato eliminato). CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione applicato ai dati dell'oggetto. CLDI: per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. ${post_edited_translations.segment}
PATH	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Il risultato dell'operazione ILM. SUCS: L'operazione ILM è stata un successo.
${post_edited_translations.segment}	Etichetta delle regole	• Se un oggetto in un bucket S3 conforme viene eliminato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. • Se l'oggetto viene eliminato perché non ci sono più istruzioni di posizionamento attualmente applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM che è stata applicata all'oggetto.
SGRP	${post_edited_translations.segment}	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui l'oggetto è stato acquisito.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID della versione specifica dell'oggetto eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Messaggio di audit LKCU per la pulizia degli oggetti sovrascritti in StorageGRID

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza richiedeva la pulizia per liberare spazio di storage. Un oggetto viene sovrascritto quando un client S3 scrive un oggetto in un percorso che contiene già un

oggetto. Il processo di rimozione avviene automaticamente e in background.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
${post_edited_translations.segment}	Tipo di pulizia	${post_edited_translations.segment}
LUID	UUID dell'oggetto rimosso	L'identificativo dell'oggetto che è stato rimosso.
PATH	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SEGC	UUID del container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto ancora esistente. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

Messaggio di audit LKDM per la pulizia degli oggetti trapelati in StorageGRID

Questo messaggio viene generato quando un chunk non valido viene ripulito o eliminato. Un chunk può far parte di un oggetto replicato o di un oggetto con codifica di cancellazione.

Codice	Campo	Descrizione
${post_edited_translations.segment}	${post_edited_translations.segment}	Il percorso del file del chunk trapelato che è stato eliminato.

CTYP	Tipo di chunk	Tipo di chunk:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

Codice	Campo	Descrizione

${post_edited_translations.segment}	Tipo di perdita	I cinque tipi di perdite che puoi rilevare:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

${post_edited_translations.segment}	Tempo di creazione del chunk	${post_edited_translations.segment}
UUID	Identificatore univoco universale	L’identificativo dell’oggetto a cui appartiene il chunk.
${post_edited_translations.segment}	Identificatore del blocco di contenuto	CBID dell’oggetto a cui appartiene il chunk trapelato.
CSIZ	Dimensione del contenuto	La dimensione del chunk in byte.

Messaggio di audit LLST per le posizioni di copia degli oggetti persi in StorageGRID

Questo messaggio viene generato ogni volta che non è possibile trovare una posizione per una copia di oggetto (replicata o codificata con cancellazione).

Codice	Campo	Descrizione
CBIL	${post_edited_translations.segment}	${post_edited_translations.segment}
ECPR	Profilo di Erasure-Coding	Per i dati degli oggetti codificati con cancellazione. L’ID del profilo di codifica con cancellazione utilizzato.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Tipo di posizione	CLDI (online): per i dati oggetto replicati ${post_edited_translations.segment} CLNL (Nearline): Per i dati oggetto replicati archiviati
NOID	ID del nodo sorgente	L'ID del nodo su cui sono state perse le posizioni.
${post_edited_translations.segment}	Percorso all'oggetto replicato	Il percorso completo della posizione su disco dei dati dell'oggetto perso. Restituito solo quando LTYP ha valore CLDI (ovvero, per gli oggetti replicati). Assume la forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Risultato	Sempre NONE. RSLT è un campo di messaggio obbligatorio, ma non è rilevante per questo messaggio. Si usa NONE anziché SUCS in modo che questo messaggio non venga filtrato.
${post_edited_translations.segment}	${post_edited_translations.segment}	UTENTE: Attivato dall'utente ${post_edited_translations.segment}
UUID	ID univoco universale	${post_edited_translations.segment}

Messaggio di audit MGAU per le richieste API di gestione in StorageGRID

La categoria Management registra le richieste degli utenti all'API di gestione. Ogni richiesta HTTP che non sia una richiesta GET o HEAD a un URI API valido registra una risposta contenente il nome utente, l'IP e il tipo di richiesta all'API. Gli URI API non validi (come /api/v3-authorize) e le richieste non valide a URI API validi non vengono registrati.

Codice	Campo	Descrizione
${post_edited_translations.segment}	${post_edited_translations.segment}	L'indirizzo IP del server (destinazione).
MDNA	domain name	${post_edited_translations.segment}
MPAT	${post_edited_translations.segment}	Il percorso della richiesta.

Codice	Campo	Descrizione
MPQP	Parametri della query di richiesta	I parametri di query per la richiesta.
MRBD	Corpo della richiesta	Il contenuto del corpo della richiesta. Sebbene il corpo della risposta venga registrato per impostazione predefinita, il corpo della richiesta viene registrato in alcuni casi quando il corpo della risposta è vuoto. Poiché le seguenti informazioni non sono disponibili nel corpo della risposta, vengono prese dal corpo della richiesta per i seguenti metodi POST: • Nome utente e ID account in **POST authorize** • Nuova configurazione delle sottoreti in **POST /grid/grid-networks/update** • Nuovi server NTP in **POST /grid/ntp-servers/update** • ID dei server decommissionati in **POST /grid/servers/decommission** **Nota:** Le informazioni sensibili vengono eliminate (per esempio, una chiave di accesso S3) oppure mascherate con asterischi (per esempio, una password).
MRMD	${post_edited_translations.segment}	Il metodo di richiesta HTTP: • POST • PUT • ELIMINA • PATCH
MRSC	Codice di risposta	Il codice di risposta.
${post_edited_translations.segment}	Corpo di risposta	Il contenuto della risposta (il corpo della risposta) viene registrato per impostazione predefinita. **Nota:** Le informazioni sensibili vengono eliminate (per esempio, una chiave di accesso S3) oppure mascherate con asterischi (per esempio, una password).
${post_edited_translations.segment}	Indirizzo IP di origine	L'indirizzo IP del client (sorgente).
${post_edited_translations.segment}	URN utente	${post_edited_translations.segment}

Codice	Campo	Descrizione
RSLT	Risultato	Restituisce SUCS (successo) oppure l'errore segnalato dal backend.

Messaggio di audit OLST per oggetti persi rilevati dal sistema in StorageGRID

${post_edited_translations.segment}

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	Il CBID dell'oggetto smarrito.
NOID	ID nodo	Se disponibile, l'ultima posizione nota diretta o near-line dell'oggetto smarrito. È possibile avere solo l'ID del nodo senza l'ID del volume se le informazioni sul volume non sono disponibili.
PATH	Bucket/chiave S3	Se disponibili, il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Questo campo ha il valore NONE. RSLT è un campo obbligatorio del messaggio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS così che questo messaggio non venga filtrato.
UUID	ID univoco universale	L'identificativo dell'oggetto smarrito all'interno del sistema StorageGRID.
VOLI	ID volume	${post_edited_translations.segment}

Messaggio di audit ORLM per le regole ILM soddisfatte in StorageGRID

Questo messaggio viene generato quando l'oggetto viene memorizzato e copiato correttamente secondo le regole ILM.

> Il messaggio ORLM non viene generato quando un oggetto viene memorizzato correttamente dalla regola predefinita "Crea 2 copie" se un'altra regola nella policy utilizza il filtro avanzato "Dimensione oggetto".

Codice	Campo	Descrizione
BUID	Header del bucket	Campo ID del bucket. Utilizzato per operazioni interne. Viene visualizzato solo se STAT è PRGD.
${post_edited_translations.segment}	Identificatore del blocco di contenuto	Il CBID dell'oggetto.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	La posizione di archiviazione dei dati dell'oggetto all'interno del sistema StorageGRID. Il valore per LOCS è " se l'oggetto non ha posizioni (ad esempio, è stato eliminato). CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione applicato ai dati dell'oggetto. CLDI: per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. ${post_edited_translations.segment}
PATH	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Il risultato dell'operazione ILM. SUCS: L'operazione ILM è stata un successo.
${post_edited_translations.segment}	Etichetta delle regole	L'etichetta leggibile assegnata alla regola ILM applicata a questo oggetto.
SEGC	UUID del container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	${post_edited_translations.segment}	CBID del container per l'oggetto segmentato. Questo valore è disponibile solo per oggetti segmentati e multipart.
${post_edited_translations.segment}	Stato	Lo stato dell'operazione ILM. ${post_edited_translations.segment} DFER: L'oggetto è stato contrassegnato per una futura rivalutazione dell'ILM. ${post_edited_translations.segment} NLOC: I dati dell'oggetto non sono più reperibili nel sistema StorageGRID. Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.

Codice	Campo	Descrizione
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID di versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Il messaggio di controllo ORLM può essere emesso più di una volta per un singolo oggetto. Ad esempio, viene emesso ogni volta che si verifica uno dei seguenti eventi:

- Le regole ILM per l'oggetto sono soddisfatte per sempre.
- ${post_edited_translations.segment}
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati di un oggetto replicato è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto danneggiato.

Informazioni correlate

- "Transazioni di ingestione degli oggetti"
- "${post_edited_translations.segment}"

Messaggio di audit OVWR per sovrascritture di oggetti in StorageGRID

${post_edited_translations.segment}

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto (nuovo)	Il CBID del nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto che stai sovrascrivendo.
${post_edited_translations.segment}	${post_edited_translations.segment}	Il CBID dell'oggetto precedente.
UUID	Identificativo univoco universale (nuovo)	${post_edited_translations.segment}

Codice	Campo	Descrizione
OUID	ID univocamente universale (precedente)	${post_edited_translations.segment}
PATH	Percorso oggetto S3	Il percorso dell'oggetto S3 utilizzato sia per l'oggetto precedente che per quello nuovo
RSLT	${post_edited_translations.segment}	Risultato della transazione di sovrascrittura dell'oggetto. Risultato è sempre: SUCS: Operazione riuscita
SGRP	${post_edited_translations.segment}	Se presente, l'oggetto sovrascritto è stato eliminato nel sito specificato, che non è il sito in cui l'oggetto sovrascritto è stato inserito.

Messaggio di audit S3SL per le richieste S3 Select in StorageGRID

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.

Codice	Campo	Descrizione
BYSC	${post_edited_translations.segment}	${post_edited_translations.segment} BYSC e BYPR potrebbero essere diversi se l'oggetto è compresso. Se l'oggetto è compresso, BYSC avrà il conteggio dei byte compressi e BYPR avrà i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "Byte scansionati" sono stati effettivamente elaborati o utilizzati da un job S3 Select.
BYRT	${post_edited_translations.segment}	Numero di byte che un job S3 Select ha restituito al client.
REPR	Record elaborati	Numero di record o righe che un processo S3 Select ha ricevuto dai nodi di archiviazione.
RERT	Record restituiti	Numero di record o righe che un job S3 Select ha restituito al client.
JOFI	Lavoro completato	Indica se il job S3 Select è terminato o meno. Se questo valore è falso, il job non è riuscito a terminare e i campi di errore probabilmente conterranno dei dati. Il client potrebbe aver ricevuto risultati parziali o nessun risultato.

Codice	Campo	Descrizione
REID	ID richiesta	${post_edited_translations.segment}
${post_edited_translations.segment}	Tempo di esecuzione	${post_edited_translations.segment}
ERMG	Messaggio di errore	Messaggio di errore generato dal job S3 Select.
${post_edited_translations.segment}	Tipo di errore	Tipo di errore che il processo S3 Select ha generato.
ERST	Stack trace dell'errore	Stacktrace dell'errore generato dal job S3 Select.
S3BK	Bucket S3	Il nome del bucket S3.
S3AK	ID della chiave di accesso S3 (mittente della richiesta)	L'ID della chiave di accesso S3 per l'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (mittente della richiesta)	${post_edited_translations.segment}
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket.

Messaggio di audit SADD per la disattivazione dell'audit di sicurezza in StorageGRID

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di audit. StorageGRID non raccoglie né invia più messaggi di audit.

Codice	Campo	Descrizione
AETM	Metodo di attivazione	Il metodo utilizzato per disabilitare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per disabilitare l'audit logging.
RSLT	Risultato	Questo campo ha il valore NONE. RSLT è un campo obbligatorio del messaggio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS così che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione era precedentemente abilitata, ma ora è stata disabilitata. Questa funzione viene in genere utilizzata solo durante l'acquisizione massiva per migliorare le prestazioni del sistema. Dopo l'attività di acquisizione massiva, la registrazione viene ripristinata (SADE) e la possibilità di disabilitare la registrazione viene quindi bloccata in modo permanente.

Messaggio di audit SADE per l'abilitazione dell'audit di sicurezza in StorageGRID

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione dei messaggi di audit. StorageGRID sta nuovamente raccogliendo e inviando i messaggi di audit.

Codice	Campo	Descrizione
AETM	Metodo di attivazione	${post_edited_translations.segment}
AEUN	Nome utente	Il nome utente che ha eseguito il comando per abilitare la registrazione degli audit.
RSLT	Risultato	Questo campo ha il valore NONE. RSLT è un campo obbligatorio del messaggio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS così che questo messaggio non venga filtrato.

Il messaggio implica che il logging era stato precedentemente disattivato (SADD), ma ora è stato ripristinato. Questo viene in genere utilizzato solo durante l'acquisizione massiva per migliorare le prestazioni del sistema. A seguito dell'attività massiva, l'auditing viene ripristinato e la possibilità di disattivare l'auditing viene quindi bloccata in modo permanente.

Messaggio di controllo SCMT per i commit dell'archivio di oggetti in StorageGRID

Il contenuto della griglia non è disponibile o riconosciuto come memorizzato finché non viene confermato (cioè finché non è stato memorizzato in modo permanente). Il contenuto memorizzato in modo permanente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene visualizzato quando un blocco di contenuto viene confermato nello storage.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto registrato nello storage permanente.
RSLT	${post_edited_translations.segment}	Stato al momento del salvataggio dell'oggetto su disco: SUCS: Oggetto salvato correttamente.

Questo messaggio indica che un determinato blocco di contenuto è stato completamente memorizzato e verificato e può ora essere richiesto. Può essere usato per tracciare il flusso di dati all'interno del sistema.

Messaggio di audit SDEL per le transazioni S3 DELETE in StorageGRID

Quando un client S3 emette una transazione DELETE, viene effettuata una richiesta di rimozione dell'oggetto o del bucket specificato, oppure di rimozione di una sottorisorsa del bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo viene impostato a 0. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	Intestazione di controllo della coerenza	Il valore dell'intestazione HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	L'identificativo univoco del sistema per la connessione TCP/IP.
CSIZ	${post_edited_translations.segment}	La dimensione dell'oggetto eliminato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	ID versione del marcatore di eliminazione	L'ID della versione del marcatore di eliminazione creato quando elimini un oggetto da un bucket versionato. Le operazioni sui bucket non includono questo campo.
GFID	${post_edited_translations.segment}	L'ID di connessione della connessione di federazione della griglia associata a una richiesta di eliminazione della replica tra griglie. Incluso solo nei log di controllo sulla grid di destinazione.
GFSA	ID account sorgente della Grid Federation	L'ID dell'account del tenant sulla griglia di origine per una richiesta di eliminazione della replica tra griglie. Incluso solo nei log di controllo sulla griglia di destinazione.
${post_edited_translations.segment}	${post_edited_translations.segment}	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate come selezionato durante la configurazione. `` `X-Forwarded-For` viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). `` `x-amz-bypass-governance-retention` viene incluso automaticamente se è presente nella richiesta.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Ultima modifica	${post_edited_translations.segment}
RSLT	${post_edited_translations.segment}	Risultato della transazione DELETE. Il risultato è sempre: SUCS: Operazione riuscita
S3AI	ID account tenant S3 (mittente della richiesta)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3AK	ID della chiave di accesso S3 (mittente della richiesta)	L'ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Il bucket o la sottorisorsa oggetto su cui stai operando, se applicabile.
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.
SAIP	${post_edited_translations.segment}	${post_edited_translations.segment}
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	L'ID account tenant del proprietario del bucket di destinazione. Usato per identificare l'accesso cross-account o l'accesso anonimo.
SGRP	${post_edited_translations.segment}	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui l'oggetto è stato acquisito.

Codice	Campo	Descrizione
SUSR	URN utente S3 (mittente della richiesta)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Per esempio: `urn:sgws:identity::03393893651506583485:root` ${post_edited_translations.segment}
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico affidabile	Se la richiesta è stata instradata da un bilanciatore di carico Layer 7 affidabile, l'indirizzo IP del bilanciatore di carico.
UUDM	Identificatore univoco universale per un marcatore di cancellazione	L'identificatore di un marcatore di eliminazione. I messaggi del log di audit specificano UUDM o UUID, dove UUDM indica un marcatore di eliminazione creato come risultato di una richiesta di eliminazione di un oggetto e UUID indica un oggetto.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID della versione specifica dell'oggetto eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Messaggio di audit SGET per le transazioni S3 GET in StorageGRID

Quando un client S3 effettua una transazione GET, viene fatta una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket, oppure per rimuovere una sottorisorsa di un bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo viene impostato a 0. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	Intestazione di controllo della coerenza	Il valore dell'intestazione HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	L'identificativo univoco del sistema per la connessione TCP/IP.

Codice	Campo	Descrizione
CSIZ	${post_edited_translations.segment}	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	${post_edited_translations.segment}	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate come selezionato durante la configurazione. `` `X-Forwarded-For` viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). ``
LITY	ListObjectsV2	È stata richiesta una risposta in formato *v2*. Per i dettagli, vedi "AWS ListObjectsV2". Solo per operazioni GET bucket.
${post_edited_translations.segment}	Numero di child	Include chiavi e prefissi comuni. Solo per operazioni GET sui bucket.
RANG	Lettura dell'intervallo	Solo per operazioni di lettura di intervalli. Indica l'intervallo di byte letto da questa richiesta. Il valore dopo la barra (/) mostra la dimensione dell'intero oggetto.
RSLT	${post_edited_translations.segment}	Risultato della transazione GET. Il risultato è sempre: SUCS: Operazione riuscita
S3AI	ID account tenant S3 (mittente della richiesta)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3AK	ID della chiave di accesso S3 (mittente della richiesta)	L'ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Il bucket o la sottorisorsa oggetto su cui stai operando, se applicabile.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.
SAIP	${post_edited_translations.segment}	${post_edited_translations.segment}
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	L'ID account tenant del proprietario del bucket di destinazione. Usato per identificare l'accesso cross-account o l'accesso anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Per esempio: `urn:sgws:identity::03393893651506583485:root` ${post_edited_translations.segment}
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico affidabile	Se la richiesta è stata instradata da un bilanciatore di carico Layer 7 affidabile, l'indirizzo IP del bilanciatore di carico.
TRNC	Troncato o non troncato	Imposta su false se sono stati restituiti tutti i risultati. Imposta su true se sono disponibili altri risultati da restituire. Solo per le operazioni GET bucket.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID versione della versione specifica di un oggetto che è stata richiesta. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Messaggio di audit SHEA per le operazioni S3 HEAD in StorageGRID

Quando un client S3 esegue un'operazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un oggetto o di un bucket e recuperare i metadati relativi a un

oggetto. Questo messaggio viene inviato dal server se l'operazione ha esito positivo.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo viene impostato a 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	L'identificativo univoco del sistema per la connessione TCP/IP.
CSIZ	${post_edited_translations.segment}	La dimensione dell'oggetto controllato in byte. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	${post_edited_translations.segment}	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate come selezionato durante la configurazione. `` `X-Forwarded-For` viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). ``
RSLT	${post_edited_translations.segment}	Risultato della transazione GET. Il risultato è sempre: SUCS: Operazione riuscita
S3AI	ID account tenant S3 (mittente della richiesta)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3AK	ID della chiave di accesso S3 (mittente della richiesta)	L'ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.

Codice	Campo	Descrizione
SAIP	${post_edited_translations.segment}	${post_edited_translations.segment}
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	L'ID account tenant del proprietario del bucket di destinazione. Usato per identificare l'accesso cross-account o l'accesso anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Per esempio: `urn:sgws:identity::03393893651506583485:root` ${post_edited_translations.segment}
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico affidabile	Se la richiesta è stata instradata da un bilanciatore di carico Layer 7 affidabile, l'indirizzo IP del bilanciatore di carico.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID versione della versione specifica di un oggetto che è stata richiesta. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Messaggio di audit SPOS per le transazioni S3 POST in StorageGRID

Quando un client S3 invia una richiesta POST Object, il server emette questo messaggio se la transazione ha esito positivo.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato a 0.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Intestazione di controllo della coerenza	Il valore dell'intestazione HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	L'identificativo univoco del sistema per la connessione TCP/IP.
CSIZ	${post_edited_translations.segment}	La dimensione dell'oggetto recuperato in byte.
${post_edited_translations.segment}	${post_edited_translations.segment}	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate come selezionato durante la configurazione. `X-Forwarded-For` viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). (Non previsto per SPOS).
RSLT	${post_edited_translations.segment}	Risultato della richiesta RestoreObject. Risultato è sempre: SUCS: Operazione riuscita
S3AI	ID account tenant S3 (mittente della richiesta)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3AK	ID della chiave di accesso S3 (mittente della richiesta)	L'ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Il bucket o la sottorisorsa oggetto su cui stai operando, se applicabile. Imposta su "select" per un'operazione S3 Select.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.
SAIP	${post_edited_translations.segment}	${post_edited_translations.segment}
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	L'ID account tenant del proprietario del bucket di destinazione. Usato per identificare l'accesso cross-account o l'accesso anonimo.
SRCF	Configurazione della sottorisorsa	${post_edited_translations.segment}
SUSR	URN utente S3 (mittente della richiesta)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Per esempio: `urn:sgws:identity::03393893651506583485:root` ${post_edited_translations.segment}
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico affidabile	Se la richiesta è stata instradata da un bilanciatore di carico Layer 7 affidabile, l'indirizzo IP del bilanciatore di carico.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID versione della versione specifica di un oggetto che è stata richiesta. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Messaggio di audit SPUT per le transazioni S3 PUT in StorageGRID

Quando un client S3 invia una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket, oppure per rimuovere una sottorisorsa di un bucket/oggetto. Questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo viene impostato a 0. Le operazioni sui bucket non includono questo campo.
CMPS	${post_edited_translations.segment}	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).
${post_edited_translations.segment}	Intestazione di controllo della coerenza	Il valore dell'intestazione HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	L'identificativo univoco del sistema per la connessione TCP/IP.
CSIZ	${post_edited_translations.segment}	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	${post_edited_translations.segment}	L'ID di connessione della connessione di federazione della griglia associata a una richiesta PUT di replica tra griglie. Incluso solo nei log di controllo sulla griglia di destinazione.
GFSA	ID account sorgente della Grid Federation	L'ID dell'account del tenant sulla griglia di origine per una richiesta PUT di replica tra griglie. Incluso solo nei log di controllo sulla griglia di destinazione.
${post_edited_translations.segment}	${post_edited_translations.segment}	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate come selezionato durante la configurazione. `` `X-Forwarded-For` viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP). `` `x-amz-bypass-governance-retention` viene incluso automaticamente se è presente nella richiesta.
LKEN	Blocco oggetti abilitato	Valore dell'intestazione della richiesta `x-amz-bucket-object-lock-enabled`, se presente nella richiesta.
${post_edited_translations.segment}	Legal Hold di Object Lock	Valore dell'intestazione della richiesta `x-amz-object-lock-legal-hold`, se presente nella richiesta PutObject.

Codice	Campo	Descrizione
LKMD	${post_edited_translations.segment}	Valore dell'intestazione della richiesta `x-amz-object-lock-mode`, se presente nella richiesta PutObject.
LKRU	Conservazione oggetto fino alla data	Valore dell'intestazione della richiesta `x-amz-object-lock-retain-until-date`, se presente nella richiesta PutObject. I valori sono limitati a un massimo di 100 anni dalla data di acquisizione dell'oggetto.
${post_edited_translations.segment}	Ultima modifica	${post_edited_translations.segment}
RSLT	${post_edited_translations.segment}	Risultato della transazione PUT. Il risultato è sempre: SUCS: Operazione riuscita
S3AI	ID account tenant S3 (mittente della richiesta)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3AK	ID della chiave di accesso S3 (mittente della richiesta)	L'ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Il bucket o la sottorisorsa oggetto su cui stai operando, se applicabile.
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.
SAIP	${post_edited_translations.segment}	${post_edited_translations.segment}
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario del bucket)	L'ID account tenant del proprietario del bucket di destinazione. Usato per identificare l'accesso cross-account o l'accesso anonimo.
SRCF	Configurazione della sottorisorsa	La nuova configurazione della sottorisorsa (troncata ai primi 1024 caratteri).
SUSR	URN utente S3 (mittente della richiesta)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Per esempio: `urn:sgws:identity::03393893651506583485:root` ${post_edited_translations.segment}
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico affidabile	Se la richiesta è stata instradata da un bilanciatore di carico Layer 7 affidabile, l'indirizzo IP del bilanciatore di carico.
ULID	ID di caricamento	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID di versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.
VSST	${post_edited_translations.segment}	Il nuovo stato di versioning di un bucket. Vengono utilizzati due stati: "abilitato" o "sospeso". Le operazioni sugli oggetti non includono questo campo.

Messaggio di controllo SREM per la rimozione dell'archivio di oggetti in StorageGRID

Questo messaggio viene visualizzato quando un contenuto viene rimosso dallo storage persistente e non è più accessibile tramite le normali API.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto eliminato dallo storage persistente.

Codice	Campo	Descrizione
RSLT	${post_edited_translations.segment}	Indica il risultato delle operazioni di rimozione dei contenuti. L'unico valore definito è: SUCS: Contenuto rimosso dallo storage persistente

Questo messaggio di audit indica che un determinato blocco di contenuto è stato eliminato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tracciare il flusso dei contenuti eliminati all'interno del sistema.

Messaggio di audit SUPD per gli aggiornamenti dei metadati S3 in StorageGRID

Questo messaggio viene generato dall'API S3 quando un client S3 aggiorna i metadati di un oggetto acquisito. Il messaggio viene emesso dal server se l'aggiornamento dei metadati ha esito positivo.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo viene impostato a 0. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	Intestazione di controllo della coerenza	${post_edited_translations.segment}
CNID	Identificatore di connessione	L'identificativo univoco del sistema per la connessione TCP/IP.
CSIZ	${post_edited_translations.segment}	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	${post_edited_translations.segment}	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate come selezionato durante la configurazione. `X-Forwarded-For` viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	${post_edited_translations.segment}	Risultato della transazione GET. Il risultato è sempre: SUCS: riuscito

Codice	Campo	Descrizione
S3AI	ID account tenant S3 (mittente della richiesta)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica accesso anonimo.
S3AK	ID della chiave di accesso S3 (mittente della richiesta)	L'ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
${post_edited_translations.segment}	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per le richieste anonime.
SAIP	${post_edited_translations.segment}	${post_edited_translations.segment}
SBAC	Nome account tenant S3 (proprietario del bucket)	Il nome dell'account tenant per il proprietario del bucket. Usato per identificare l'accesso tra account o l'accesso anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	L'ID account tenant del proprietario del bucket di destinazione. Usato per identificare l'accesso cross-account o l'accesso anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Per esempio: `urn:sgws:identity::03393893651506583485:root` ${post_edited_translations.segment}
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico affidabile	Se la richiesta è stata instradata da un bilanciatore di carico Layer 7 affidabile, l'indirizzo IP del bilanciatore di carico.

Codice	Campo	Descrizione
UUID	Identificatore univoco universale	L'identificativo dell'oggetto all'interno del sistema StorageGRID.
${post_edited_translations.segment}	ID versione	L'ID della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Messaggio di controllo SVRF per errori di verifica dell'archivio di oggetti in StorageGRID

Questo messaggio viene visualizzato ogni volta che un blocco di contenuto non supera il processo di verifica. Ogni volta che i dati degli oggetti replicati vengono letti o scritti su disco, vengono eseguiti diversi controlli di verifica e integrità per garantire che i dati inviati all'utente richiedente siano identici ai dati originariamente acquisiti nel sistema. Se uno di questi controlli fallisce, il sistema mette automaticamente in quarantena i dati degli oggetti replicati corrotti per impedirne il recupero.

Codice	Campo	Descrizione
${post_edited_translations.segment}	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto la cui verifica non è andata a buon fine.
RSLT	${post_edited_translations.segment}	${post_edited_translations.segment} CRCF: controllo di ridondanza ciclica (CRC) non riuscito. ${post_edited_translations.segment} EHSH: Hash del contenuto crittografato inatteso. PHSH: Hash del contenuto originale inatteso. SEQC: Sequenza dati errata sul disco. PERR: Struttura del file su disco non valida. ${post_edited_translations.segment} FNAM: Nome file non valido.

Questo messaggio deve essere monitorato attentamente. Gli errori di verifica del contenuto possono indicare imminenti guasti hardware.

Per determinare quale operazione ha generato il messaggio, consulta il valore del campo AMID (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, cioè dalla verifica in background, e STOR indica che il messaggio è stato generato dal recupero dei contenuti.

Messaggio di controllo SVRU per contenuto di archivio di oggetti sconosciuto in StorageGRID

Il componente Storage del servizio LDR analizza continuamente tutte le copie dei dati degli oggetti replicati nell'archivio di oggetti. Questo messaggio viene visualizzato quando viene rilevata una copia sconosciuta o imprevista dei dati degli oggetti replicati nell'archivio di oggetti e spostata nella directory di quarantena.

Codice	Campo	Descrizione
FPTH	${post_edited_translations.segment}	${post_edited_translations.segment}
RSLT	Risultato	Questo campo ha il valore 'NONE'. RSLT è un campo obbligatorio del messaggio, ma non è rilevante per questo messaggio. Viene utilizzato 'NONE' anziché 'SUCS' affinché questo messaggio non venga filtrato.

Il messaggio di audit SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie impreviste dei dati degli oggetti nell'archivio di oggetti. Questa situazione va indagata subito per capire come sono state create queste copie, perché può indicare guasti hardware imminenti.

Messaggio di audit SYSD per arresti di nodi regolari in StorageGRID

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stata richiesta la chiusura. In genere questo messaggio viene inviato solo dopo un successivo riavvio, perché la coda dei messaggi di audit non viene svuotata prima dell'arresto. Se il servizio non è stato riavviato, cerca il messaggio SYST, inviato all'inizio della sequenza di arresto.

Codice	Campo	Descrizione
RSLT	Arresto pulito	${post_edited_translations.segment} SUCS: Il sistema è stato arrestato correttamente.

Il messaggio non indica se il server host è in fase di arresto, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare un arresto "sporco", perché il messaggio viene generato solo dagli arresti "puliti".

Messaggio di audit SYST per l'arresto del nodo in StorageGRID

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto l'arresto e che il servizio ha avviato la sua sequenza di arresto. SYST può essere utilizzato per determinare se è stato richiesto l'arresto, prima che il servizio venga riavviato (a differenza di SYSD, che di solito viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Arresto pulito	${post_edited_translations.segment} SUCS: Il sistema è stato arrestato correttamente.

Il messaggio non indica se il server host è in fase di arresto, ma solo il servizio di segnalazione. Il codice RSLT di un messaggio SYST non può indicare un arresto "sporco", perché il messaggio viene generato solo da arresti "puliti".

Messaggio di audit SYSU per il nodo avviato in StorageGRID

Quando un servizio viene riavviato, viene generato questo messaggio per indicare se l'arresto precedente è stato pulito (comandato) o disordinato (imprevisto).

Codice	Campo	Descrizione
RSLT	Arresto pulito	${post_edited_translations.segment} SUCS: Il sistema è stato spento correttamente. DSDN: Il sistema non è stato arrestato correttamente. ${post_edited_translations.segment}

Il messaggio non indica se il server host è stato avviato, ma solo se è stato avviato il servizio di reporting. Questo messaggio può essere utilizzato per:

- Individua le discontinuità nella traccia di controllo.
- Determina se un servizio si interrompe durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio che ha subito un guasto.

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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