



Monitorare e risolvere i problemi

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

- Monitorare e risolvere i problemi di un sistema StorageGRID 1
 - Monitorare il sistema StorageGRID 1
 - Risolvere i problemi relativi al sistema StorageGRID 187
 - Esaminare i registri di audit 239

Monitorare e risolvere i problemi di un sistema StorageGRID

Monitorare il sistema StorageGRID

Monitorare un sistema StorageGRID

Monitorare regolarmente il sistema StorageGRID per assicurarsi che funzioni come previsto.

Prima di iniziare

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



Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).

A proposito di questa attività

Queste istruzioni descrivono come:

- ["Visualizzare e gestire la dashboard"](#)
- ["Visualizzare la pagina nodi"](#)
- ["Monitorare regolarmente questi aspetti del sistema:"](#)
 - ["Stato del sistema"](#)
 - ["Capacità dello storage"](#)
 - ["Gestione del ciclo di vita delle informazioni"](#)
 - ["Risorse di rete e di sistema"](#)
 - ["Attività del tenant"](#)
 - ["Operazioni di bilanciamento del carico"](#)
 - ["Connessioni a federazione di griglie"](#)
- ["Gestire gli avvisi"](#)
- ["Visualizzare i file di registro"](#)
- ["Configurare i messaggi di audit e le destinazioni dei log"](#)
- ["Utilizzare un server syslog esterno"](#) per raccogliere le informazioni di controllo
- ["Utilizzare SNMP per il monitoraggio"](#)
- ["Ottenere ulteriori dati StorageGRID"](#), comprese le metriche e la diagnostica

Visualizzare e gestire la dashboard

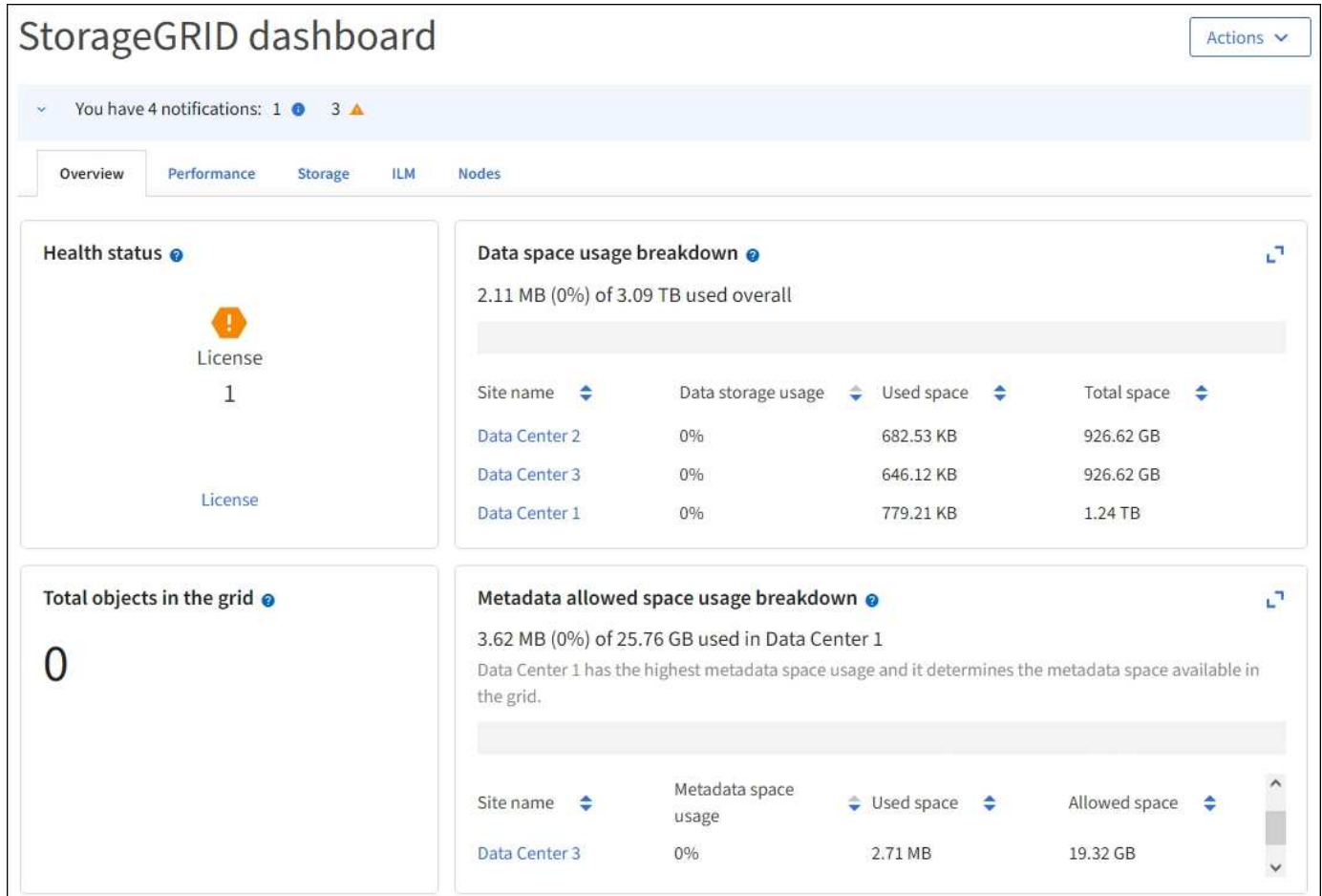
È possibile utilizzare la dashboard per monitorare le attività del sistema in un colpo d'occhio. È possibile creare dashboard personalizzati per monitorare l'implementazione

di StorageGRID.



Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).

Il dashboard potrebbe essere diverso a seconda della configurazione del sistema.



Visualizza la dashboard



La dashboard è costituita da schede che contengono informazioni specifiche sul sistema StorageGRID. Ciascuna scheda contiene le categorie di informazioni visualizzate sulle schede.

È possibile utilizzare la dashboard fornita con il sistema così com'è. Inoltre, è possibile creare dashboard personalizzati contenenti solo schede e schede rilevanti per il monitoraggio dell'implementazione di StorageGRID.

Le schede della dashboard fornite dal sistema contengono schede con i seguenti tipi di informazioni:

Scheda sulla dashboard fornita dal sistema	Contiene
Panoramica	Informazioni generali sulla griglia, ad esempio avvisi attivi, utilizzo dello spazio e oggetti totali nella griglia.

Scheda sulla dashboard fornita dal sistema	Contiene
Performance	Utilizzo dello spazio, storage utilizzato nel tempo, S3 operazioni, durata della richiesta, tasso di errore.
Storage	Utilizzo delle quote dei tenant e dello spazio logico. Previsioni di utilizzo dello spazio per i dati e i metadati dell'utente.
ILM	Coda di gestione del ciclo di vita delle informazioni e tasso di valutazione.
Nodi	Utilizzo di CPU, dati e memoria per nodo. S3 operazioni per nodo. Distribuzione da nodo a sito.

Alcune schede possono essere massimizzate per una visualizzazione più semplice. Selezionare l'icona Ingrandisci  nell'angolo superiore destro della scheda. Per chiudere una scheda ingrandita, selezionare l'icona Riduci a icona  o selezionare **Chiudi**.

Gestire i dashboard

Se si dispone dell'accesso root (vedere "[Autorizzazioni del gruppo di amministrazione](#)"), è possibile eseguire le seguenti attività di gestione per i dashboard:

- Crea una dashboard personalizzata da zero. È possibile utilizzare dashboard personalizzati per controllare quali informazioni StorageGRID vengono visualizzate e come sono organizzate.
- Clonare una dashboard per creare dashboard personalizzati.
- Impostare una dashboard attiva per un utente. La dashboard attiva può essere la dashboard fornita dal sistema o una dashboard personalizzata.
- Impostare una dashboard predefinita, che è quella visualizzata da tutti gli utenti, a meno che non attivino la propria dashboard.
- Modificare il nome di una dashboard.
- Modificare una dashboard per aggiungere o rimuovere schede e schede. È possibile avere un minimo di 1 e un massimo di 20 schede.
- Rimuovere una dashboard.



Se si dispone di altre autorizzazioni oltre all'accesso root, è possibile impostare solo una dashboard attiva.

Per gestire i dashboard, selezionare **azioni > Gestisci dashboard**.



Configurare i dashboard

Per creare una nuova dashboard clonando la dashboard attiva, selezionare **azioni** > **Clona dashboard attiva**.

Per modificare o clonare una dashboard esistente, selezionare **azioni** > **Gestisci dashboard**.



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

Durante la configurazione di una dashboard, è possibile:

- Aggiungere o rimuovere le schede
- Rinominare le schede e assegnarle nomi univoci
- Aggiungere, rimuovere o riorganizzare (trascinare) le schede per ciascuna scheda
- Selezionare le dimensioni delle singole schede selezionando **S**, **M**, **L** o **XL** nella parte superiore della scheda

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

Visualizzare la pagina nodi

Visualizzare la pagina nodi

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

La tabella Nodes (nodi) elenca informazioni riepilogative per l'intera griglia, ciascun sito e ciascun 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 sono presenti avvisi attivi, non viene visualizzata alcuna icona.



Quando un nodo non è connesso alla griglia, ad esempio durante l'aggiornamento o uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della griglia. Dopo che un nodo si ricollega alla griglia, attendere alcuni minuti per consentire la stabilizzazione dei valori.



Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).






Le schermate mostrate sono esempi. I risultati possono variare a seconda della versione di StorageGRID in uso.

Nodes



View the list and status of sites and grid nodes.

Search... Total node count: 12

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
^ DC1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	6%
 DC1-ARC1	Archive Node	—	—	1%
 DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%

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
	<p>Non connesso - Sconosciuto</p> <p>Per un motivo sconosciuto, un nodo viene disconnesso o i servizi sul nodo vengono inaspettatamente disattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato o il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione dell'alimentazione o di un'interruzione imprevista.</p> <p>Potrebbe essere attivato anche l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.</p>	<p>Richiede un'attenzione immediata. "Selezionare ciascun avviso" e seguire le azioni consigliate.</p> <p>Ad esempio, potrebbe essere necessario riavviare un servizio che ha arrestato o riavviato l'host per il nodo.</p> <p>Nota: Un nodo potrebbe apparire come sconosciuto durante le operazioni di shutdown gestite. In questi casi, è possibile ignorare lo stato Unknown (Sconosciuto).</p>
	<p>Non connesso - amministrazione non attiva</p> <p>Per un motivo previsto, il nodo non è connesso alla rete.</p> <p>Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.</p> <p>In base al problema sottostante, questi nodi tornano spesso online senza alcun intervento.</p>	<p>Determinare se eventuali avvisi influiscono su questo nodo.</p> <p>Se sono attivi uno o più avvisi, "Selezionare ciascun avviso" seguire le azioni consigliate.</p>


Se un nodo è disconnesso dalla griglia, potrebbe essere presente un avviso sottostante, ma viene visualizzata solo l'icona "non connesso". Per visualizzare gli avvisi attivi per un nodo, selezionare 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:** Esiste una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. È necessario risolvere immediatamente il problema sottostante. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.

 **Maggiore:** Esiste una condizione anomala che influisce sulle operazioni correnti o si avvicina alla soglia per un avviso critico. È necessario analizzare gli avvisi principali e risolvere eventuali problemi sottostanti per assicurarsi che le condizioni anomale non interrompano il normale funzionamento di un nodo o servizio StorageGRID.

 **Minore:** Il sistema funziona normalmente, ma esiste una condizione anomala che potrebbe influire sulla capacità del sistema di funzionare se continua. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per garantire che non causino problemi più gravi.

Visualizza i dettagli di un sistema, sito o nodo

Per filtrare le informazioni visualizzate nella tabella Nodes (nodi), inserire una stringa di ricerca nel campo **Search** (Ricerca). È possibile eseguire una ricerca in base al nome del sistema, al nome visualizzato o al tipo (ad esempio, immettere **gat** per individuare rapidamente tutti i nodi gateway).

Per visualizzare le informazioni relative a griglia, sito o nodo:

- Selezionare il nome della griglia per visualizzare un riepilogo aggregato delle statistiche per l'intero sistema StorageGRID.
- Selezionare un sito specifico del data center per visualizzare un riepilogo aggregato delle statistiche per tutti i nodi del sito.
- Selezionare un nodo specifico per visualizzare informazioni dettagliate relative a tale nodo.

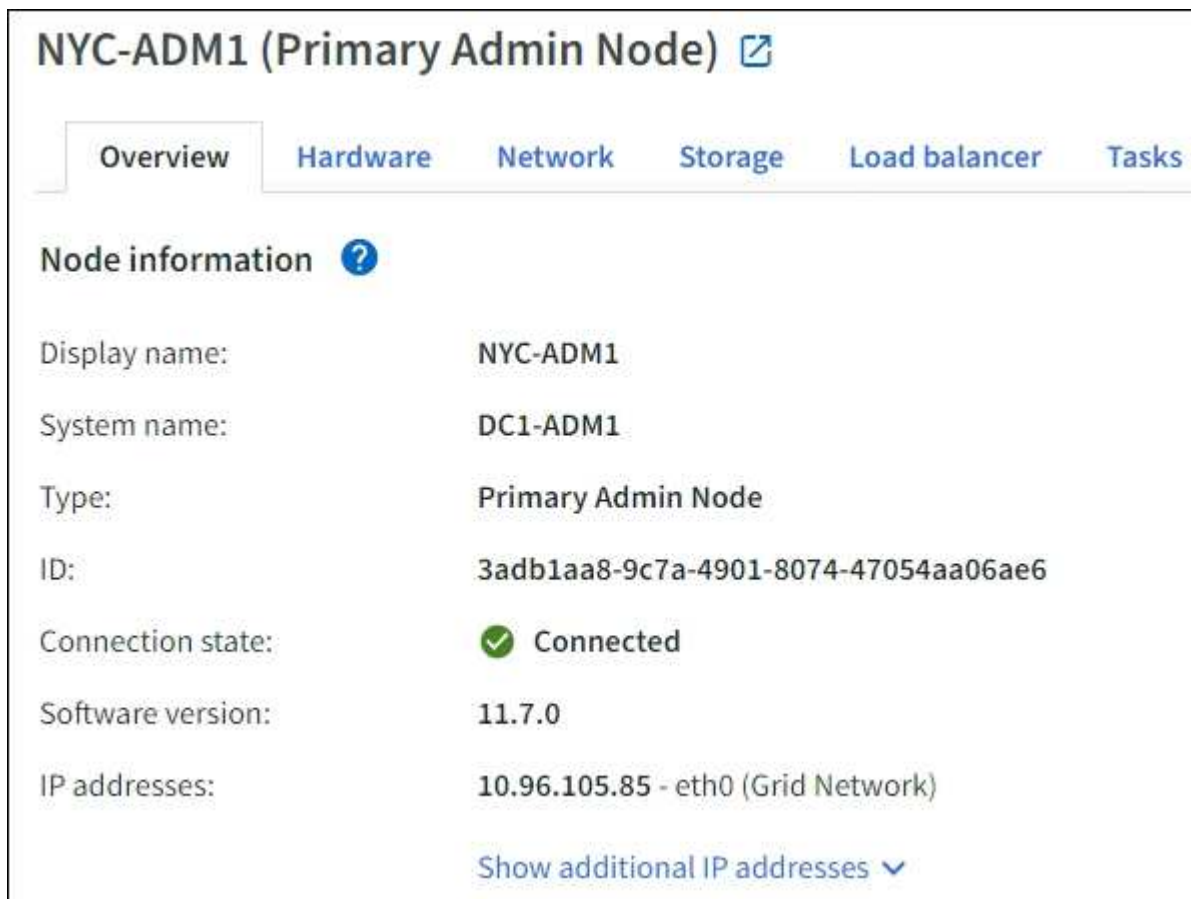
Visualizzare la scheda Panoramica

La scheda Panoramica fornisce informazioni di base su ciascun nodo. Inoltre, vengono visualizzati tutti gli avvisi che attualmente influiscono sul nodo.

Viene visualizzata la scheda Overview (Panoramica) per tutti i nodi.

Informazioni sul nodo

La sezione Node Information (informazioni nodo) della scheda Overview (Panoramica) elenca le informazioni di base sul nodo.



NYC-ADM1 (Primary Admin Node) [↗](#)


Overview Hardware Network Storage Load balancer Tasks


Node information [?](#)



Display name:	NYC-ADM1
System name:	DC1-ADM1
Type:	Primary Admin Node
ID:	3adb1aa8-9c7a-4901-8074-47054aa06ae6
Connection state:	✔ Connected
Software version:	11.7.0
IP addresses:	10.96.105.85 - eth0 (Grid Network)

[Show additional IP addresses](#) ▼

Le informazioni generali per un nodo includono quanto segue:

- **Nome visualizzato** (visualizzato solo se il nodo è stato rinominato): Il nome visualizzato corrente per il nodo. Utilizzare la ["Rinominare la griglia, i siti e i nodi"](#) procedura per aggiornare questo valore.
- **Nome sistema**: Il nome immesso per il nodo durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni StorageGRID interne e non possono essere modificati.
- **Tipo**: Il tipo di nodo — nodo amministrativo, nodo amministrativo primario, nodo di archiviazione o nodo gateway.
- **ID**: Identificatore univoco del nodo, chiamato anche UUID.
- **Stato connessione**: Uno dei tre stati. Viene visualizzata l'icona dello stato più grave.
 - **Sconosciuto** : per un motivo sconosciuto, il nodo non è connesso alla rete oppure uno o più servizi sono inattesi. Ad esempio, la connessione di rete tra i nodi è stata persa, l'alimentazione è inattiva o un servizio è inattivo. Potrebbe essere attivato anche l'avviso **Impossibile comunicare con il nodo**. Potrebbero essere attivi anche altri avvisi. Questa situazione richiede un'attenzione immediata.

 Un nodo potrebbe apparire come sconosciuto durante le operazioni di shutdown gestite. In questi casi, è possibile ignorare lo stato Unknown (Sconosciuto).

 - **Amministrativamente inattivo** : il nodo non è connesso alla rete per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.
 - **Connesso** : il nodo è collegato alla rete.
- **Storage utilizzato**: Solo per nodi di storage.
 - **Dati oggetto**: Percentuale dello spazio utilizzabile totale per i dati oggetto che è stato utilizzato nel nodo di storage.
 - **Metadati oggetto**: Percentuale dello spazio totale consentito per i metadati oggetto utilizzati nel nodo di storage.
- **Versione software**: La versione di StorageGRID installata sul nodo.
- **Gruppi ha**: Solo per nodi Admin Node e Gateway. Viene visualizzato 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. Fare clic su **Show additional IP addresses** (Mostra indirizzi IP aggiuntivi) per visualizzare gli indirizzi IPv4 e IPv6 e le mappature dell'interfaccia del nodo.

Avvisi

La sezione Avvisi della scheda Panoramica elenca qualsiasi ["avvisi che attualmente interessano questo nodo e che non sono stati tacitati"](#). Selezionare il nome dell'avviso per visualizzare ulteriori dettagli e le azioni consigliate.

Alerts

Alert name	Severity	Time triggered	Current values
Low installed node memory The amount of installed memory on a node is low.	✖ Critical	11 hours ago	Total RAM size: 8.37 GB

Gli avvisi sono inclusi anche per "stati di connessione del nodo".

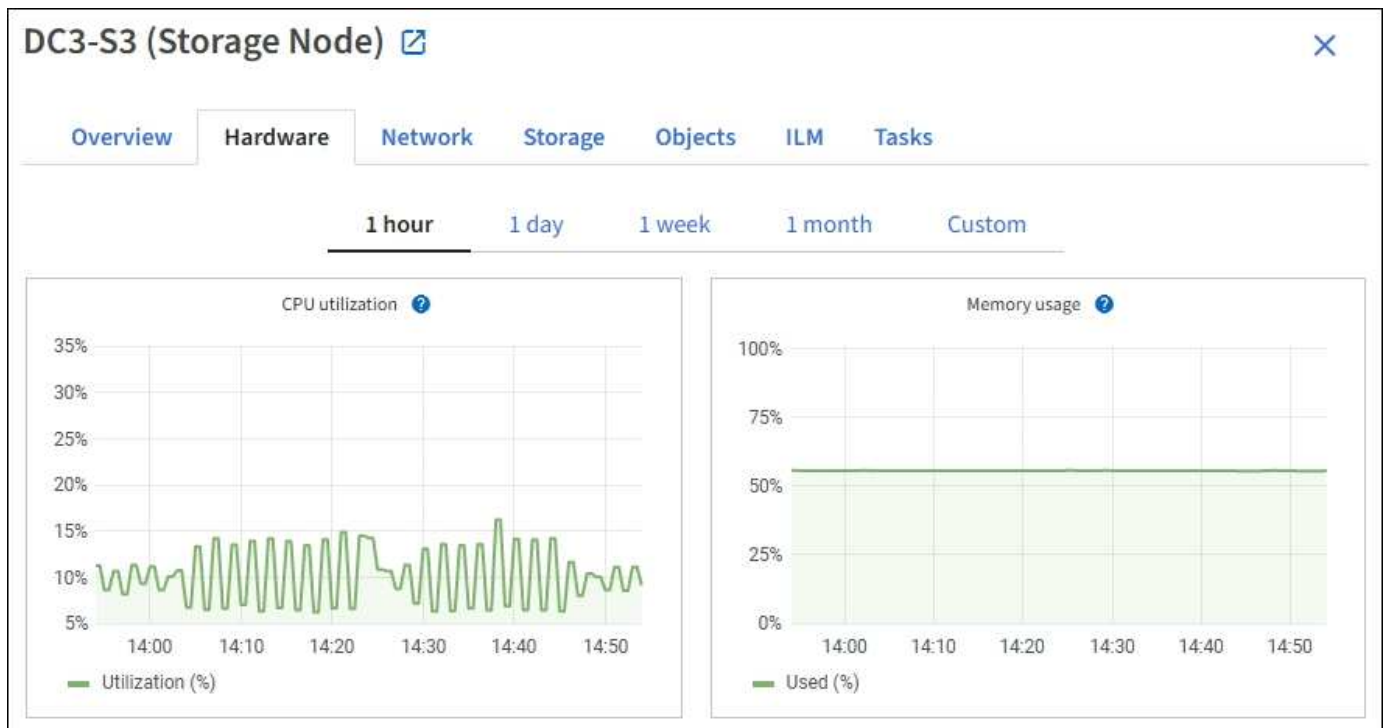
Visualizzare la scheda hardware

La scheda hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo, oltre a informazioni aggiuntive sull'hardware delle appliance.



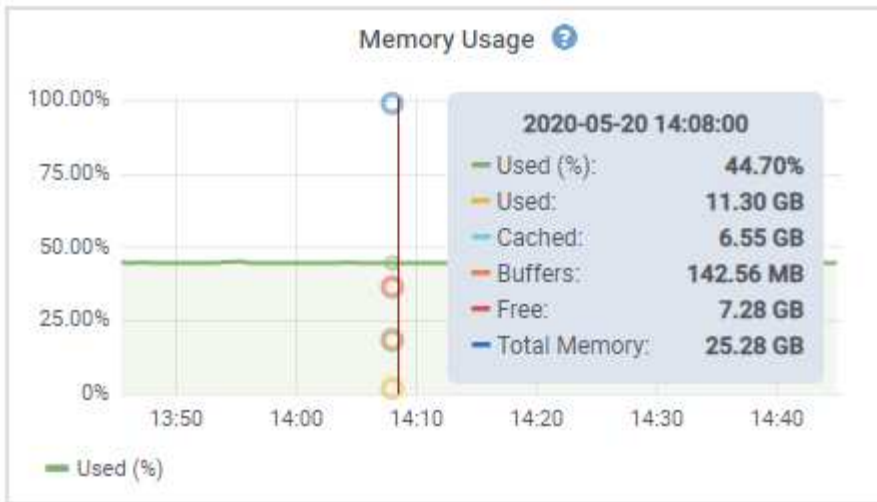
Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio di questa pagina.

Viene visualizzata la scheda hardware per tutti i nodi.



Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.

Per visualizzare i dettagli relativi all'utilizzo della CPU e della memoria, posizionare 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 Nodes (nodi) elenca le informazioni sullo stato di salute del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ciascun nodo di storage dell'appliance. È inoltre possibile visualizzare memoria, hardware di storage, versione del firmware del controller, risorse di rete, interfacce di rete, indirizzi di rete e ricevere e trasmettere dati.

Fasi

1. Dalla pagina Nodes (nodi), selezionare un nodo di storage dell'appliance.
2. Selezionare **Panoramica**.

La sezione Node information (informazioni nodo) della scheda Overview (Panoramica) visualizza informazioni riepilogative per il nodo, ad esempio il nome, il tipo, l'ID e lo stato di connessione del nodo. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

- **eth**: Rete griglia, rete amministrativa o rete client.
- **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte 1 GbE fisiche dell'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia di rete amministrativa StorageGRID (eth1). È possibile lasciare altre interfacce mtc disponibili per la connettività locale temporanea per un tecnico del data center.

Overview **Hardware** Network Storage Objects ILM Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021
 Type: Storage Node
 ID: f0890e03-4c72-401f-ae92-245511a38e51
 Connection state: ✔ Connected
 Storage used: Object data 7% [?](#)
 Object metadata 5% [?](#)
 Software version: 11.6.0 (build 20210915.1941.afce2d9)
 IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ↕	IP address ↕
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

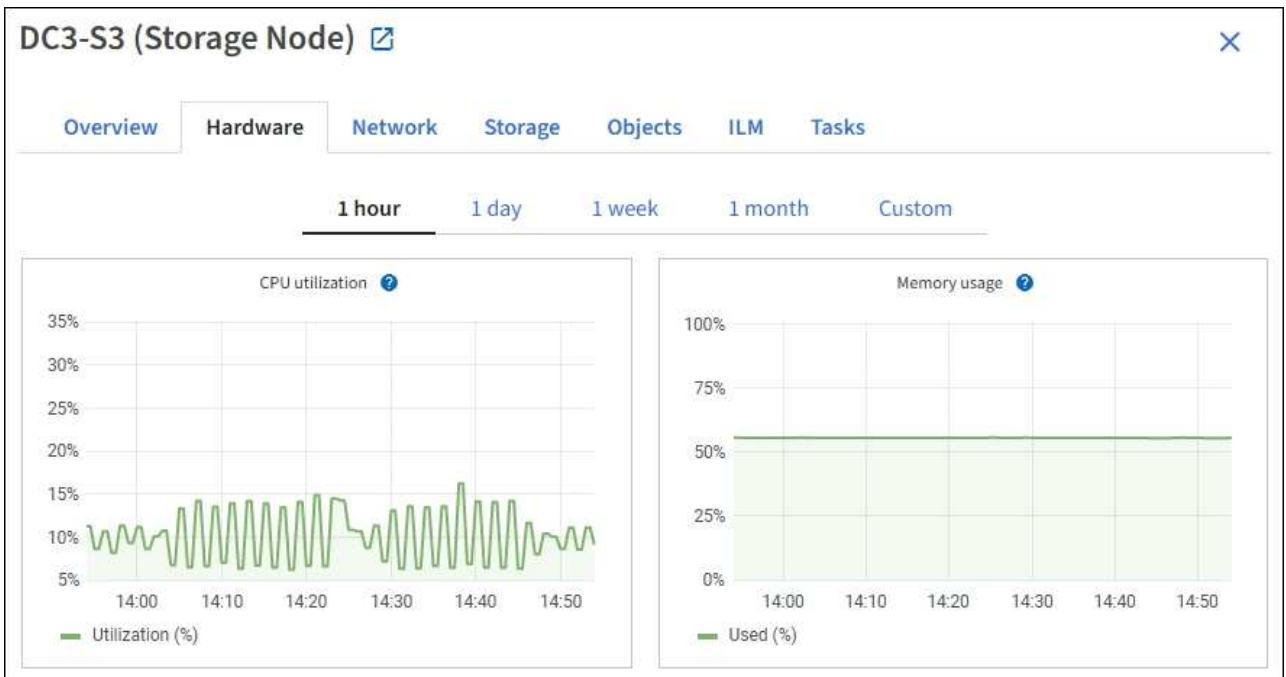
Alerts

Alert name ↕	Severity ? ↕	Time triggered ↕	Current values
ILM placement unachievable ↗	! Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

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

3. Selezionare **hardware** per visualizzare ulteriori informazioni sull'appliance.

- a. Visualizzare i grafici relativi all'utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.



- b. Scorrere 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 e lo stato di ciascun componente.



Alcuni campi, ad esempio Compute controller BMC IP e Compute hardware, vengono visualizzati solo per le appliance dotate di tale funzionalità.

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

StorageGRID Appliance

Appliance model: ?	SG6060	
Storage controller name: ?	StorageGRID-Lab79-SG6060-7-134	
Storage controller A management IP: ?	10.2	
Storage controller B management IP: ?	10.2	
Storage controller WWID: ?	6d039ea0000173e50000000065b7b761	
Storage appliance chassis serial number: ?	721924500068	
Storage controller firmware version: ?	08.53.00.09	
Storage controller SANtricity OS version: ?	11.50.3R2	
Storage controller NVRAM version: ?	N280X-853834-DG1	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller B: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	4.00 TB	
Storage RAID mode: ?	DDP16	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Degraded	
Compute controller BMC IP: ?	10.2	
Compute controller serial number: ?	721917500060	
Compute hardware: ?	Needs Attention	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Failed	
Compute controller power supply B: ?	Nominal	

Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?	Power supply status ?	Drawer status ?	Fan status
721924500068	99	Nominal	N/A	Nominal	Nominal	Nominal

Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello di questo dispositivo StorageGRID mostrato in SANtricity OS.
Nome dello storage controller	Il nome dell'appliance StorageGRID visualizzato in SANtricity OS.
Storage controller A IP di gestione	Indirizzo IP per la porta di gestione 1 sul controller di storage A. si utilizza questo IP per accedere al sistema operativo SANtricity 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. si utilizza questo IP per accedere al sistema operativo SANtricity e risolvere i problemi di storage. Alcuni modelli di appliance non dispongono di un controller di storage B.

Nella tabella Appliances	Descrizione
WWID dello storage controller	L'identificatore mondiale dello storage controller mostrato in SANtricity OS.
Numero di serie dello chassis dell'appliance di storage	Il numero di serie dello chassis dell'appliance.
Versione del firmware del controller di storage	La versione del firmware del controller di storage per l'appliance.
Versione del sistema operativo SANtricity dello storage controller	Versione del sistema operativo SANtricity dello storage controller A.
Versione NVSRAM del controller di storage	<p>Versione NVSRAM dello storage controller come indicato da System Manager di SANtricity.</p> <p>Per i modelli SG6060 e SG6160, se tra le due centraline è presente una mancata corrispondenza della versione NVSRAM, viene visualizzata la versione del controller A. Se la centralina A non è installata o funzionante, viene visualizzata la versione della centralina B.</p>
Hardware per lo storage	<p>Lo stato generale dell'hardware del controller dello storage. Se Gestore di sistema di SANtricity riporta lo stato di intervento richiesto per l'hardware di storage, anche il sistema StorageGRID riporta questo valore.</p> <p>Se lo stato è "richiede attenzione", controllare prima lo storage controller utilizzando il sistema operativo SANtricity. Quindi, assicurarsi che non esistano altri avvisi che si applicano al controller di elaborazione.</p>
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Controller dello storage A	Lo stato dello storage controller A.
Controller dello storage B	Lo stato del controller di storage B. alcuni modelli di appliance non dispongono di un controller di storage B.
Alimentazione a del controller storage	Lo stato dell'alimentatore A per il controller dello storage.
Alimentazione controller storage B	Lo stato dell'alimentazione B del controller di storage.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).

Nella tabella Appliances	Descrizione
Dimensioni del disco per i dati di storage	<p>Le dimensioni effettive di un'unità dati.</p> <p>Per il modello SG6160, vengono visualizzate anche le dimensioni dell'unità cache.</p> <p>Nota: Per i nodi con shelf di espansione, utilizzare Dimensioni del disco dati per ogni shelf invece. Le dimensioni effettive del disco potrebbero differire in base allo shelf.</p>
Storage RAID mode (modalità RAID storage)	La modalità RAID configurata per l'appliance.
Connettività dello storage	Lo stato di connettività dello storage.
Alimentatore generale	Lo stato di tutti gli alimentatori dell'apparecchio.
IP BMC del controller di calcolo	<p>L'indirizzo IP della porta BMC (Baseboard Management Controller) nel controller di calcolo. Questo IP viene utilizzato per connettersi all'interfaccia BMC per monitorare e diagnosticare l'hardware dell'appliance.</p> <p>Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.</p>
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.
Hardware di calcolo	Lo stato dell'hardware del controller di calcolo. Questo campo non viene visualizzato per i modelli di appliance che non dispongono di hardware di calcolo e storage separati.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di calcolo.
Temperatura dello chassis del controller di calcolo	Lo stato della temperatura del controller di calcolo.

+

Nella tabella Storage shelf	Descrizione
Numero di serie dello shelf chassis	Il numero di serie dello chassis dello shelf di storage.

Nella tabella Storage shelf	Descrizione
ID shelf	L'identificativo numerico dello shelf di storage. <ul style="list-style-type: none"> • 99: Shelf dello storage controller • 0: Primo shelf di espansione • 1: Secondo shelf di espansione <p>Nota: gli scaffali di espansione si applicano solo ai modelli SG6060 e SG6160.</p>
Stato dello shelf	Lo stato generale dello shelf di storage.
Stato IOM	Lo stato dei moduli di input/output (IOM) in qualsiasi shelf di espansione. N/D se non si tratta di uno shelf di espansione.
Stato dell'alimentatore	Lo stato generale degli alimentatori per lo shelf di storage.
Stato del cassetto	Lo stato dei cassettei nello shelf di archiviazione. N/D se il ripiano non contiene cassettei.
Stato della ventola	Lo stato generale delle ventole di raffreddamento nello shelf di storage.
Slot per dischi	Il numero totale di slot per dischi nello shelf di storage.
Dischi dati	Il numero di dischi nello shelf di storage utilizzati per lo storage dei dati.
dimensione del disco dati	La dimensione effettiva di un'unità dati nello shelf di storage.
Dischi cache	Il numero di dischi nello shelf di storage utilizzati come cache.
Dimensione dell'unità cache	La dimensione dell'unità cache più piccola nello shelf di storage. Normalmente, le unità cache sono tutte delle stesse dimensioni.
Stato della configurazione	Lo stato di configurazione dello shelf di storage.

a. Verificare che tutti gli stati siano "nominale".

Se uno stato non è "nominale", esaminare eventuali avvisi correnti. Puoi anche utilizzare Gestione di sistema di SANtricity per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

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

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



a. Consultare 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	

Utilizzare la seguente tabella con i valori nella colonna **Speed** della tabella Network Interfaces (interfacce di rete) per determinare se le porte di rete 10/25-GbE dell'appliance sono state configurate per l'utilizzo della modalità Active/backup o LACP.



I valori mostrati nella tabella presuppongono che siano utilizzati tutti e quattro i collegamenti.

Modalità link	Modalità bond	Velocità di collegamento HIC singola (hic1, hic2, hic3, hic4)	Velocità rete client/griglia prevista (eth0,eth2)
Aggregato	LACP	25	100
Corretto	LACP	25	50
Corretto	Attivo/Backup	25	25
Aggregato	LACP	10	40
Corretto	LACP	10	20
Corretto	Attivo/Backup	10	10

Consultare "[Configurare i collegamenti di rete](#)" per ulteriori informazioni sulla configurazione delle porte 10/25-GbE.

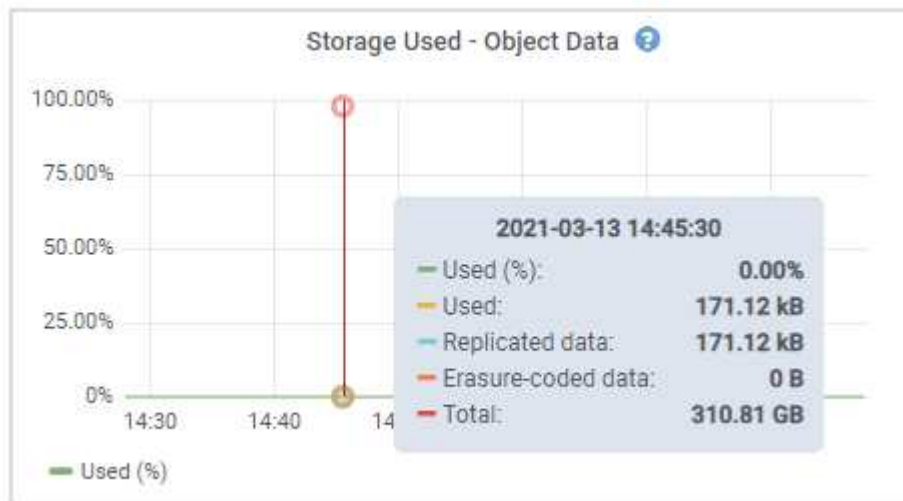
b. Consultare la sezione comunicazione di rete.

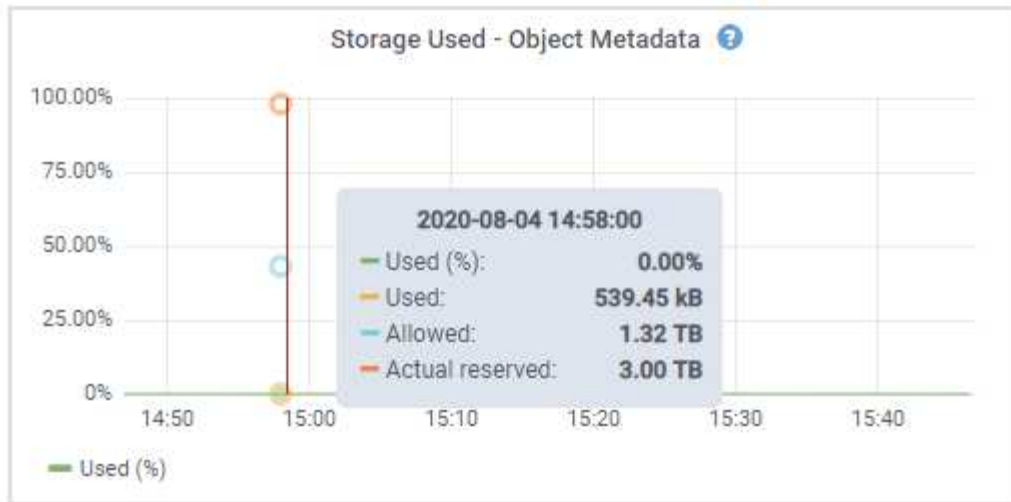
Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché altre metriche di ricezione e trasmissione.

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. Selezionare **Storage** per visualizzare i grafici che mostrano le percentuali di storage utilizzate nel tempo per i dati degli oggetti e i metadati degli oggetti, nonché informazioni su dischi, volumi e archivi di oggetti.





- a. Scorrere verso il basso per visualizzare le quantità di storage disponibili per ciascun volume e archivio di oggetti.

Il nome internazionale di ciascun disco corrisponde all'identificativo mondiale del volume (WWID) visualizzato quando si visualizzano le proprietà standard del volume in SANtricity OS (il software di gestione collegato al controller di storage dell'appliance).

Per semplificare l'interpretazione delle statistiche di lettura e scrittura dei dischi relative ai punti di montaggio del volume, la prima parte del nome visualizzato nella colonna **Name** della tabella Disk Devices (periferiche disco) (ovvero *sdc*, *sdd*, *sde* e così via) corrisponde al valore visualizzato nella colonna **Device** della tabella Volumes (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 informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway

La pagina Nodes (nodi) elenca le informazioni sullo stato del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ogni appliance di servizi utilizzata come nodo di amministrazione o nodo gateway. È inoltre possibile visualizzare memoria, hardware di storage, risorse di rete, interfacce di rete, indirizzi di rete, e ricevere e trasmettere dati.

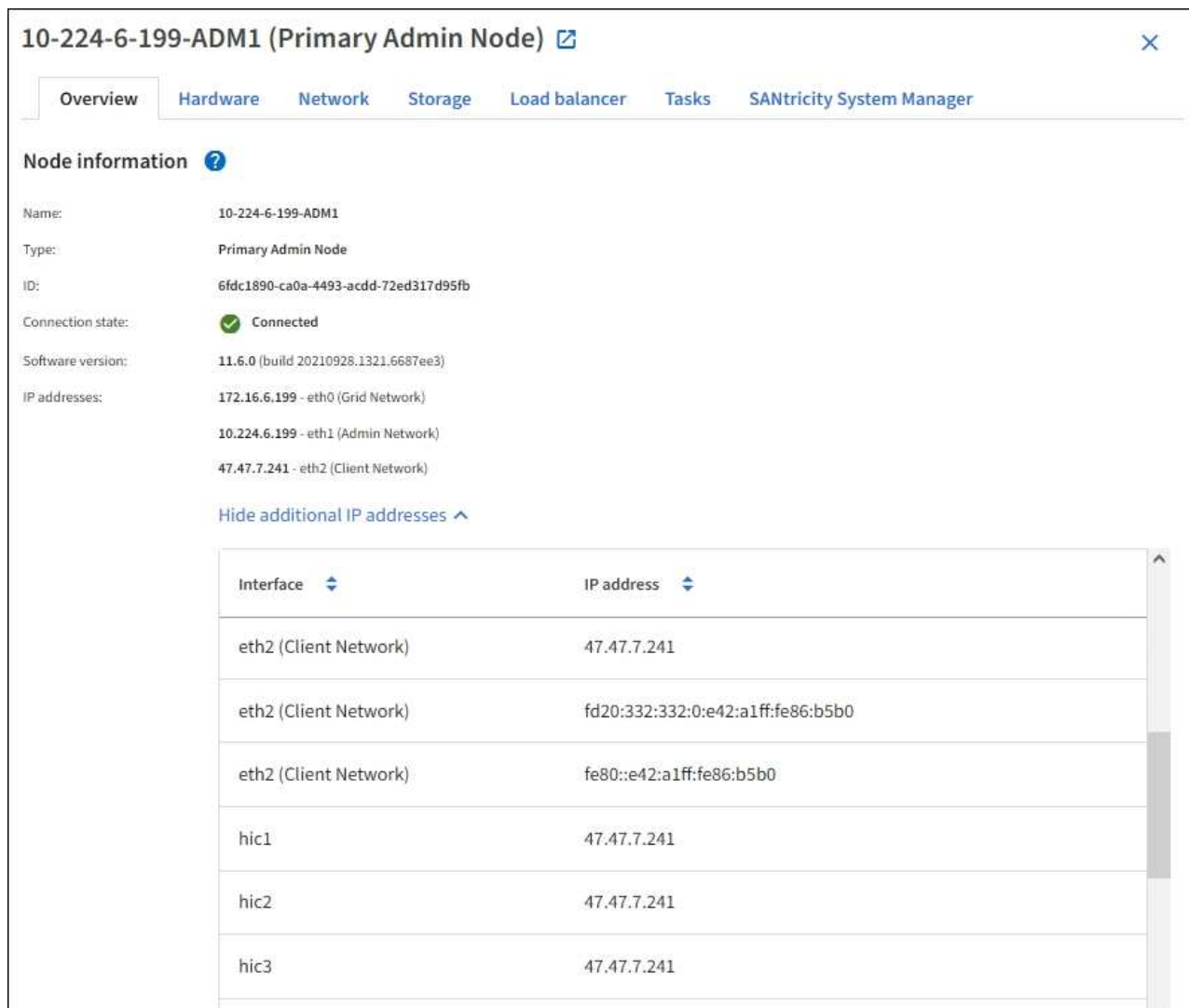
Fasi

1. Dalla pagina Nodes (nodi), selezionare un nodo Admin dell'appliance o un nodo Gateway dell'appliance.
2. Selezionare **Panoramica**.

La sezione Node information (informazioni nodo) della scheda Overview (Panoramica) visualizza informazioni riepilogative per il nodo, ad esempio il nome, il tipo, l'ID e lo stato di connessione del nodo.

L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

- **Adllb** e **adlli**: Visualizzato se si utilizza il bonding Active/backup per l'interfaccia di Admin Network
- **eth**: Rete griglia, rete amministrativa o rete client.
- **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte 1-GbE fisiche dell'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia Admin Network (eth1). È possibile lasciare altre interfacce mtc disponibili per la connettività locale temporanea per un tecnico del data center.



10-224-6-199-ADM1 (Primary Admin Node)

Overview | Hardware | Network | Storage | Load balancer | Tasks | SANtricity System Manager

Node information

Name: 10-224-6-199-ADM1
Type: Primary Admin Node
ID: 6fdc1890-ca0a-4493-acdd-72ed317d95fb
Connection state: ✔ Connected
Software version: 11.6.0 (build 20210928.1321.6687ee3)
IP addresses: 172.16.6.199 - eth0 (Grid Network)
10.224.6.199 - eth1 (Admin Network)
47.47.7.241 - eth2 (Client Network)

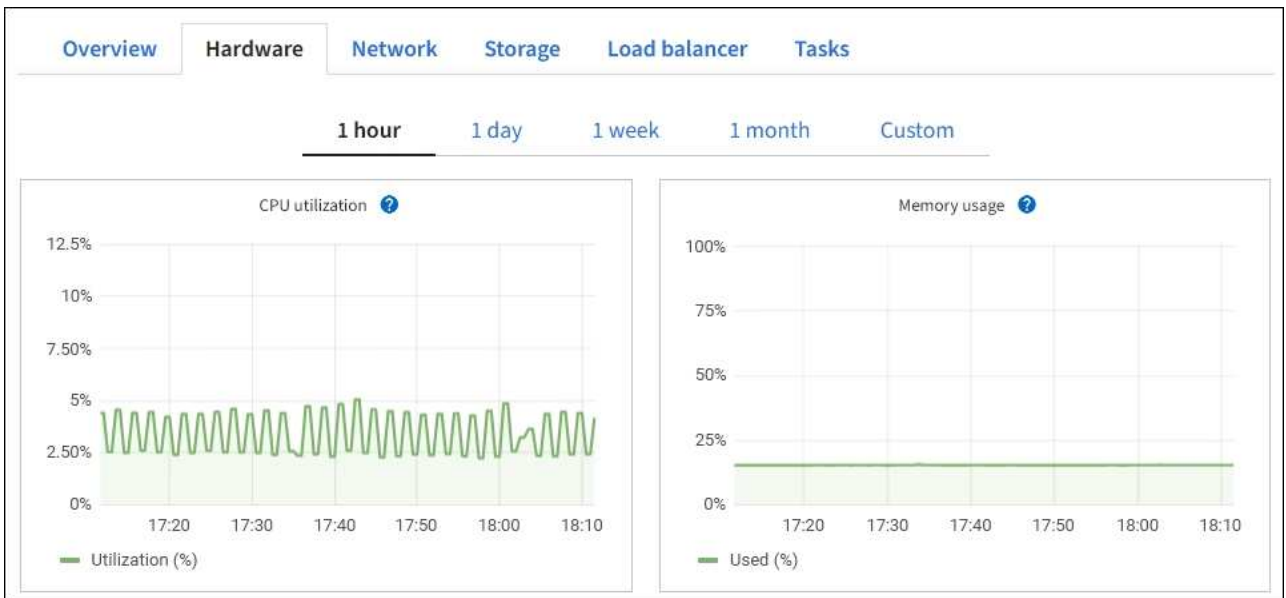
[Hide additional IP addresses](#)

Interface	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

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

3. Selezionare **hardware** per visualizzare ulteriori informazioni sull'appliance.

- Visualizzare i grafici relativi all'utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.



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

StorageGRID Appliance		
Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello dell'appliance StorageGRID.

Nella tabella Appliances	Descrizione
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).
Dimensioni del disco per i dati di storage	Le dimensioni effettive di un'unità dati.
Storage RAID mode (modalità RAID storage)	La modalità RAID per l'appliance.
Alimentatore generale	Lo stato di tutti gli alimentatori dell'apparecchio.
IP BMC del controller di calcolo	L'indirizzo IP della porta BMC (Baseboard Management Controller) nel controller di calcolo. È possibile utilizzare questo IP per connettersi all'interfaccia BMC per 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	Lo stato dell'hardware del controller di calcolo.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di calcolo.
Temperatura dello chassis del controller di calcolo	Lo stato della temperatura del controller di calcolo.

a. Verificare che tutti gli stati siano "nominale".

Se uno stato non è "nominale", esaminare eventuali avvisi correnti.

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

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



a. Consultare 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	

Utilizzare la seguente tabella con i valori nella colonna **Speed** della tabella Network Interfaces (interfacce di rete) per determinare se le quattro porte di rete 40/100-GbE dell'appliance sono state configurate per l'utilizzo della modalità Active/backup o LACP.



I valori mostrati nella tabella presuppongono che siano utilizzati tutti e quattro i collegamenti.

Modalità link	Modalità bond	Velocità di collegamento HIC singola (hic1, hic2, hic3, hic4)	Velocità rete client/griglia prevista (eth0, eth2)
Aggregato	LACP	100	400
Corretto	LACP	100	200
Corretto	Attivo/Backup	100	100
Aggregato	LACP	40	160
Corretto	LACP	40	80
Corretto	Attivo/Backup	40	40

b. Consultare la sezione comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché 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. Selezionare **Storage** per visualizzare le informazioni relative ai dischi e ai volumi sull'appliance di servizi.

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Load balancer](#)[Tasks](#)

Disk devices

Name ? ↕	World Wide Name ? ↕	I/O load ? ↕	Read rate ? ↕	Write rate ? ↕
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 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	84.63 GB 	Unknown

Visualizzare la scheda rete

La scheda Network (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.

Viene visualizzata la scheda Network (rete) per tutti i nodi, ciascun sito e l'intera griglia.

Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.

Per i nodi, la tabella interfacce di rete fornisce informazioni sulle porte di rete fisiche di ciascun nodo. La tabella delle comunicazioni di rete fornisce dettagli sulle operazioni di ricezione e trasmissione di ciascun nodo e sui contatori di guasti segnalati dai driver.

DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

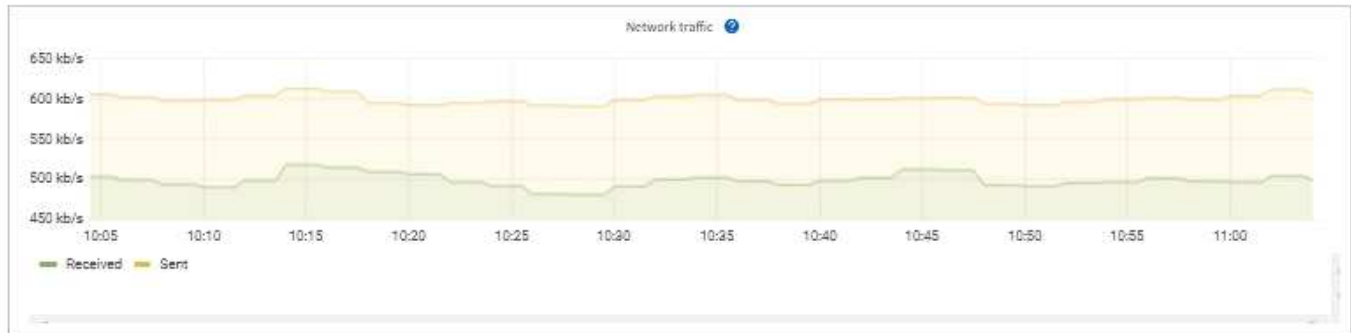
1 hour

1 day

1 week

1 month

Custom



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

Informazioni correlate

["Monitorare le connessioni di rete e le performance"](#)

Visualizzare la scheda Storage (archiviazione)

La scheda Storage riepiloga la disponibilità dello storage e altre metriche di storage.

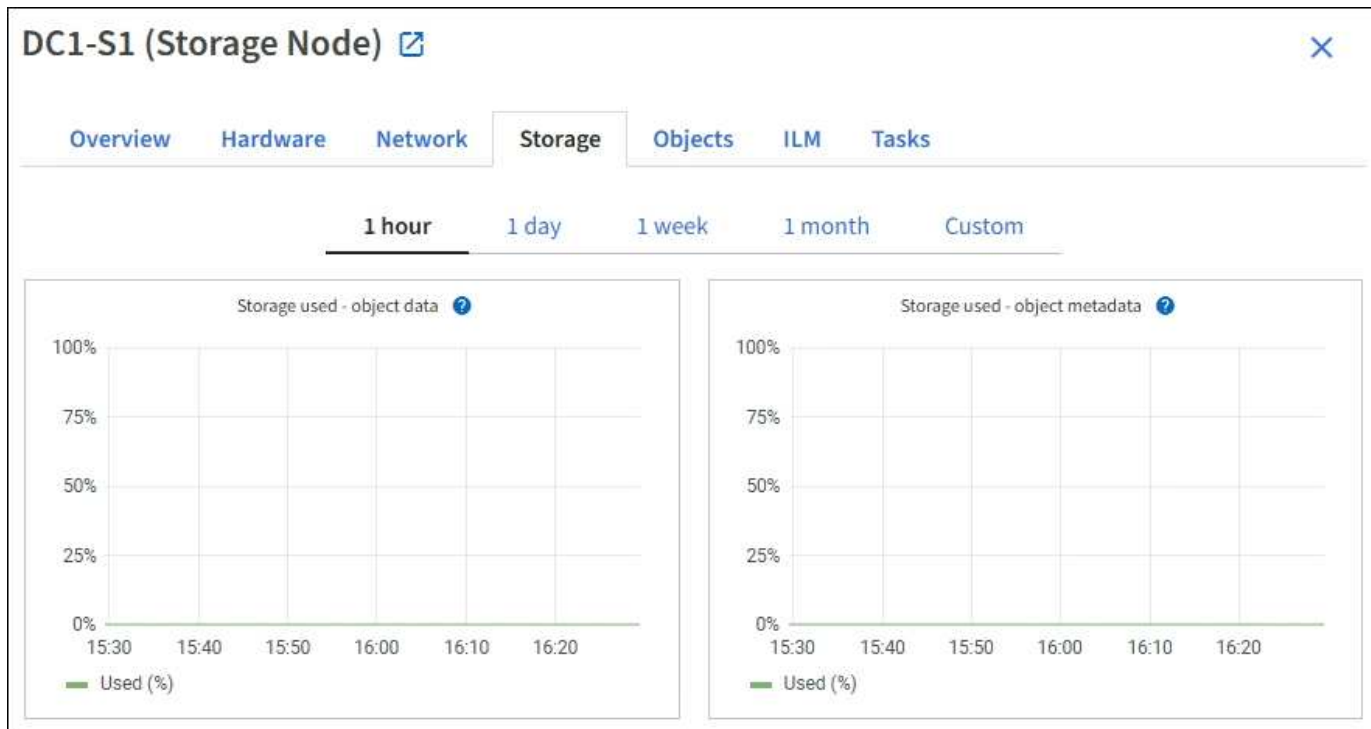
Viene visualizzata la scheda Storage (archiviazione) per tutti i nodi, ciascun sito e l'intera griglia.

Grafici utilizzati per lo storage

Per i nodi di storage, ciascun sito e l'intero grid, la scheda Storage include grafici che mostrano la quantità di storage utilizzata dai dati degli oggetti e dai metadati degli oggetti nel tempo.



Quando un nodo non è connesso alla griglia, ad esempio durante l'aggiornamento o uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della griglia. Dopo che un nodo si ricollega alla griglia, attendere alcuni minuti per consentire la stabilizzazione dei valori.



Dischi, volumi e tabelle di archiviazione degli oggetti

Per tutti i nodi, la scheda Storage contiene i dettagli relativi ai dischi e ai volumi sul nodo. Per i nodi di storage, la tabella degli archivi di oggetti fornisce informazioni su ciascun volume di storage.

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

["Monitorare la capacità dello storage"](#)

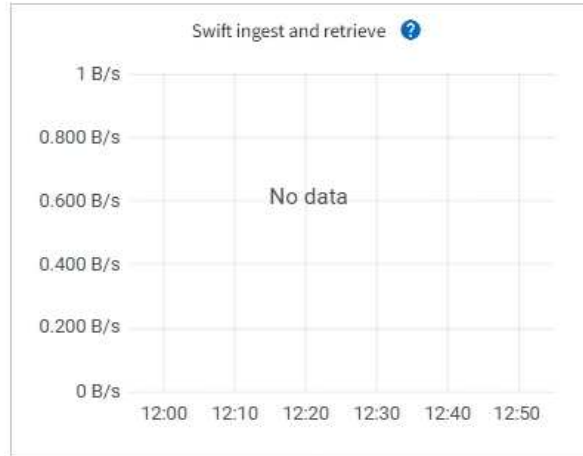
Visualizzare la scheda oggetti

La scheda oggetti fornisce informazioni su ["Tassi di acquisizione e recupero pari a S3 volte"](#).

Viene visualizzata la scheda oggetti per ciascun nodo di storage, ciascun sito e l'intera griglia. Per i nodi di storage, la scheda oggetti fornisce anche conteggi di oggetti e informazioni sulle query dei metadati e sulla verifica in background.

Overview Hardware Network Storage **Objects** ILM Tasks

1 hour 1 day 1 week 1 month Custom



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

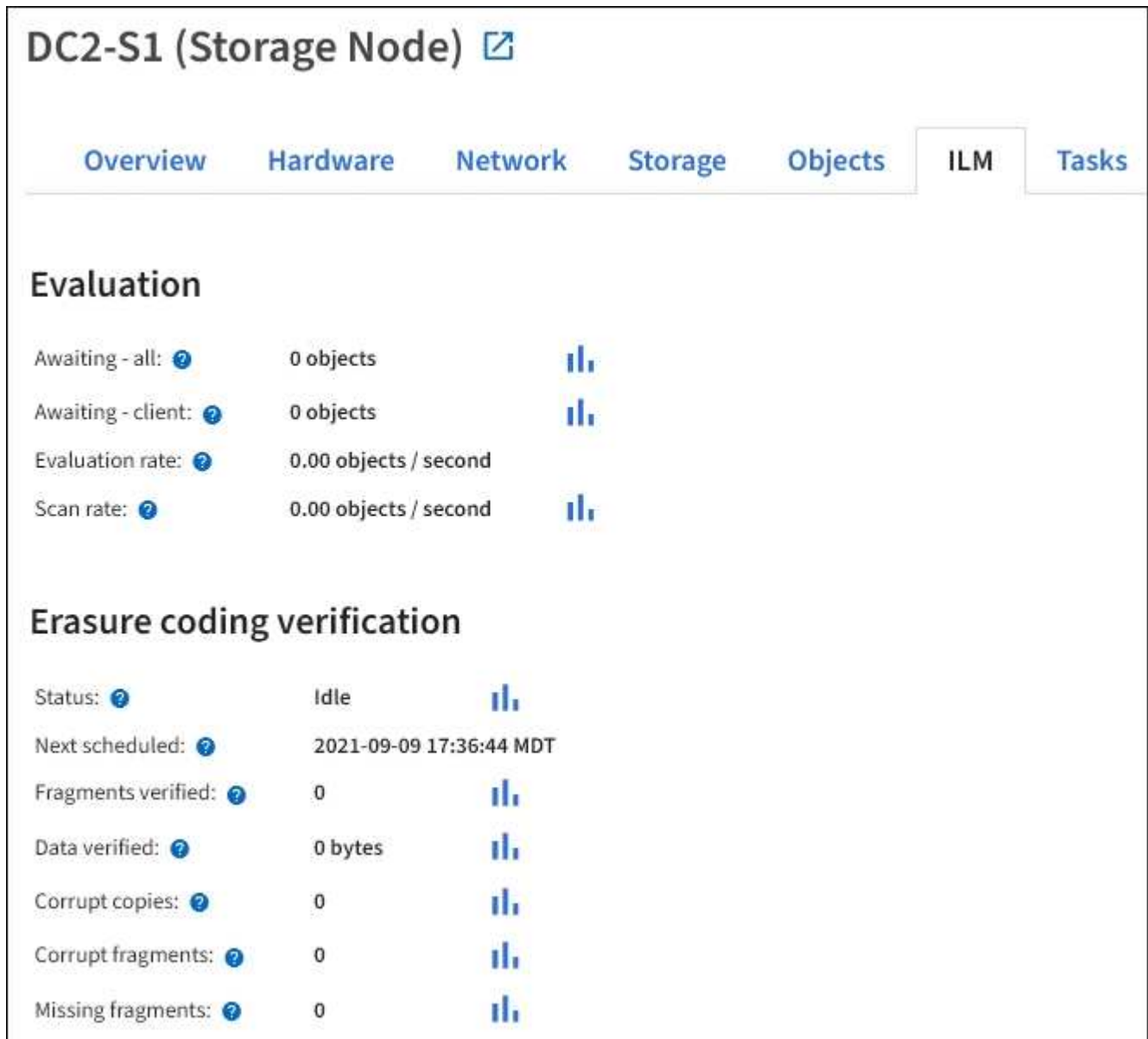
Quarantined objects: [?](#) 0

Visualizzare la scheda ILM

La scheda ILM fornisce informazioni sulle operazioni di Information Lifecycle management (ILM).

Viene visualizzata la scheda ILM per ciascun nodo di storage, ciascun sito e l'intera griglia. Per ogni sito e griglia, la scheda ILM mostra un grafico della coda ILM nel tempo. Per la griglia, questa scheda fornisce anche il tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

Per i nodi storage, la scheda ILM fornisce dettagli sulla valutazione ILM e sulla verifica in background per gli oggetti sottoposti a erasure coding.



Informazioni correlate

- ["Monitorare la gestione del ciclo di vita delle informazioni"](#)
- ["Amministrare StorageGRID"](#)

Utilizzare la scheda attività

Viene visualizzata la scheda attività per tutti i nodi. È possibile utilizzare questa scheda per rinominare o riavviare un nodo o per impostare un nodo appliance in modalità di manutenzione.

Per i requisiti e le istruzioni completi per ciascuna opzione di questa scheda, vedere quanto segue:

- ["Rinominare la griglia, i siti e i nodi"](#)
- ["Nodo di reboot grid"](#)
- ["Impostare l'apparecchio in modalità di manutenzione"](#)

Visualizzare la scheda bilanciamento del carico

La scheda bilanciamento del carico include i grafici delle performance e diagnostici relativi al funzionamento del servizio bilanciamento del carico.

Viene visualizzata la scheda Load Balancer (bilanciamento carico) per i nodi Admin e Gateway, per ciascun sito e per l'intera griglia. Per ogni sito, la scheda bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i nodi del sito. Per l'intera griglia, la scheda bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i siti.

Se non viene eseguito alcun i/o attraverso il servizio di bilanciamento del carico o non è configurato alcun bilanciamento del carico, i grafici visualizzano "Nessun dato".



Richiesta di traffico

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



Questo valore viene aggiornato al completamento di ogni richiesta. Di conseguenza, questo valore potrebbe differire dal throughput in tempo reale a bassi tassi di richiesta o per richieste di durata molto lunga. La scheda Network (rete) consente di ottenere una vista più realistica del comportamento corrente della rete.

Tasso di richiesta in entrata

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

Durata media della richiesta (non errore)

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

Tasso di risposta agli errori

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

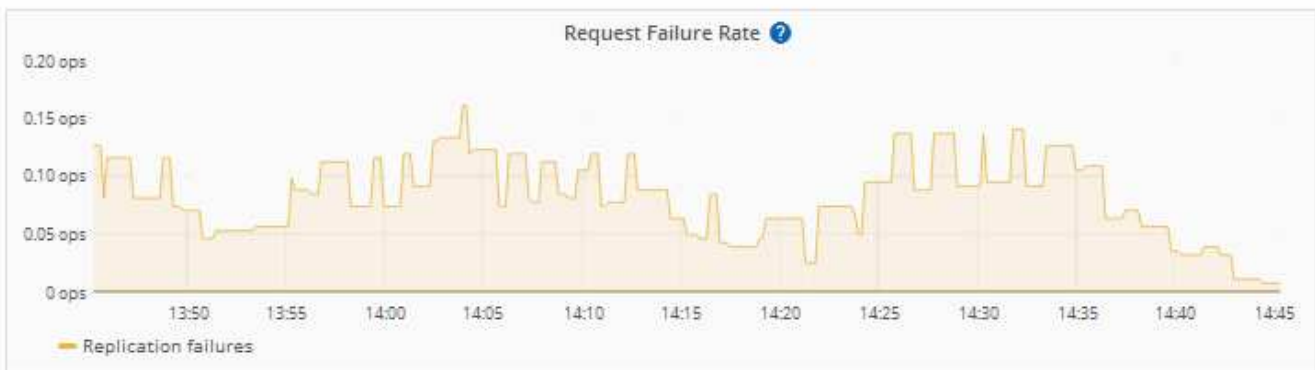
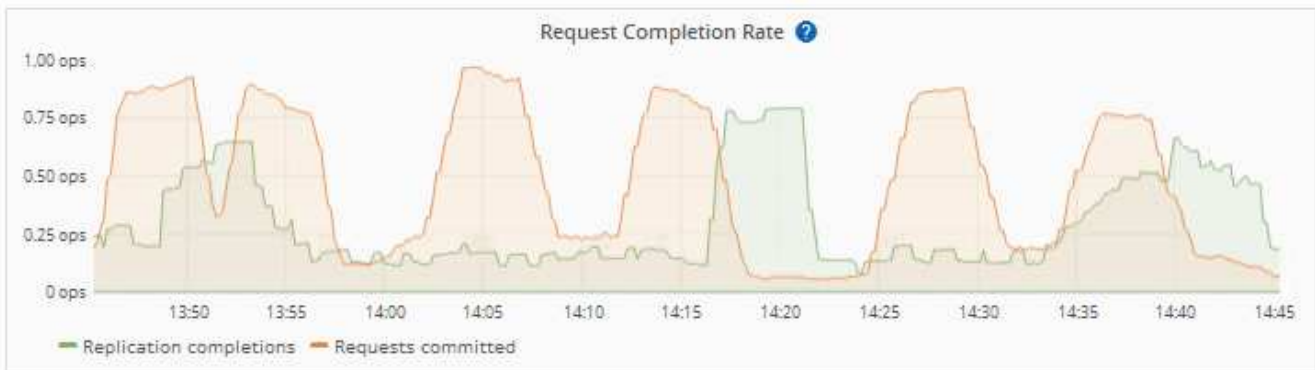
Informazioni correlate

- ["Monitorare le operazioni di bilanciamento del carico"](#)
- ["Amministrare StorageGRID"](#)

Visualizzare la scheda Platform Services (servizi piattaforma)

La scheda Platform Services (servizi piattaforma) fornisce informazioni sulle operazioni di servizio della piattaforma S3 in un sito.

Viene visualizzata la scheda Platform Services (servizi piattaforma) per ciascun sito. Questa scheda fornisce informazioni sui servizi della piattaforma S3, come la replica CloudMirror e il servizio di integrazione della ricerca. I grafici di questa scheda mostrano metriche come il numero di richieste in sospeso, la percentuale di completamento della richiesta e la percentuale di guasti della richiesta.



Per ulteriori informazioni sui servizi della piattaforma S3, inclusi i dettagli sulla risoluzione dei problemi, vedere ["Istruzioni per l'amministrazione di StorageGRID"](#).

Visualizzare la scheda Gestisci unità

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

Utilizzando la scheda Gestisci unità, è possibile effettuare le seguenti operazioni:

- Visualizzare un layout delle unità di storage dei dati nell'appliance
- Visualizza una tabella in cui sono elencati ogni tipo, posizione, stato, versione del firmware e numero di serie del disco
- Eseguire le funzioni di risoluzione dei problemi e manutenzione su ciascuna unità

Per accedere alla scheda Gestisci unità, è necessario disporre di ["Autorizzazione di accesso root o amministratore dell'appliance di storage"](#).

Per informazioni sull'utilizzo della scheda Gestisci unità, vedere ["Utilizzare la scheda Gestisci unità"](#).

Visualizza la scheda SANtricity System Manager (solo e-Series)

La scheda Gestore di sistema di SANtricity consente di accedere a Gestore di sistema di SANtricity senza dover configurare o collegare la porta di gestione dell'appliance di storage. È possibile utilizzare questa scheda per esaminare le informazioni ambientali e di diagnostica dell'hardware, nonché i problemi relativi ai dischi.



L'accesso a Gestione di sistema SANtricity da Gestione griglia è generalmente destinato solo al monitoraggio dell'hardware dell'appliance e alla configurazione di e-Series AutoSupport. Molte funzionalità e operazioni di Gestione sistema di SANtricity, come l'aggiornamento del firmware, non si applicano al monitoraggio dell'appliance StorageGRID. Per evitare problemi, seguire sempre le istruzioni per la manutenzione dell'hardware dell'apparecchio. Per aggiornare il firmware SANtricity, consultare la ["Procedure di configurazione della manutenzione"](#) relativa all'appliance di storage.



La scheda Gestore di sistema di SANtricity viene visualizzata solo per i nodi di appliance di storage che utilizzano hardware e-Series.

Utilizzando Gestione sistema di SANtricity, è possibile effettuare le seguenti operazioni:

- Visualizza i dati sulle performance come performance a livello di array di storage, latenza i/o, utilizzo della CPU del controller di storage e throughput.
- Controllare lo stato dei componenti hardware.
- Eseguire funzioni di supporto, tra cui la visualizzazione dei dati diagnostici e la configurazione di e-Series AutoSupport.



Per utilizzare Gestore di sistema di SANtricity per configurare un proxy per AutoSupport e-Series, consultare ["Invio dei pacchetti e-Series AutoSupport tramite StorageGRID"](#).

Per accedere a Gestore di sistema di SANtricity tramite Gestione griglia, è necessario disporre di ["Autorizzazione di accesso root o amministratore dell'appliance di storage"](#).



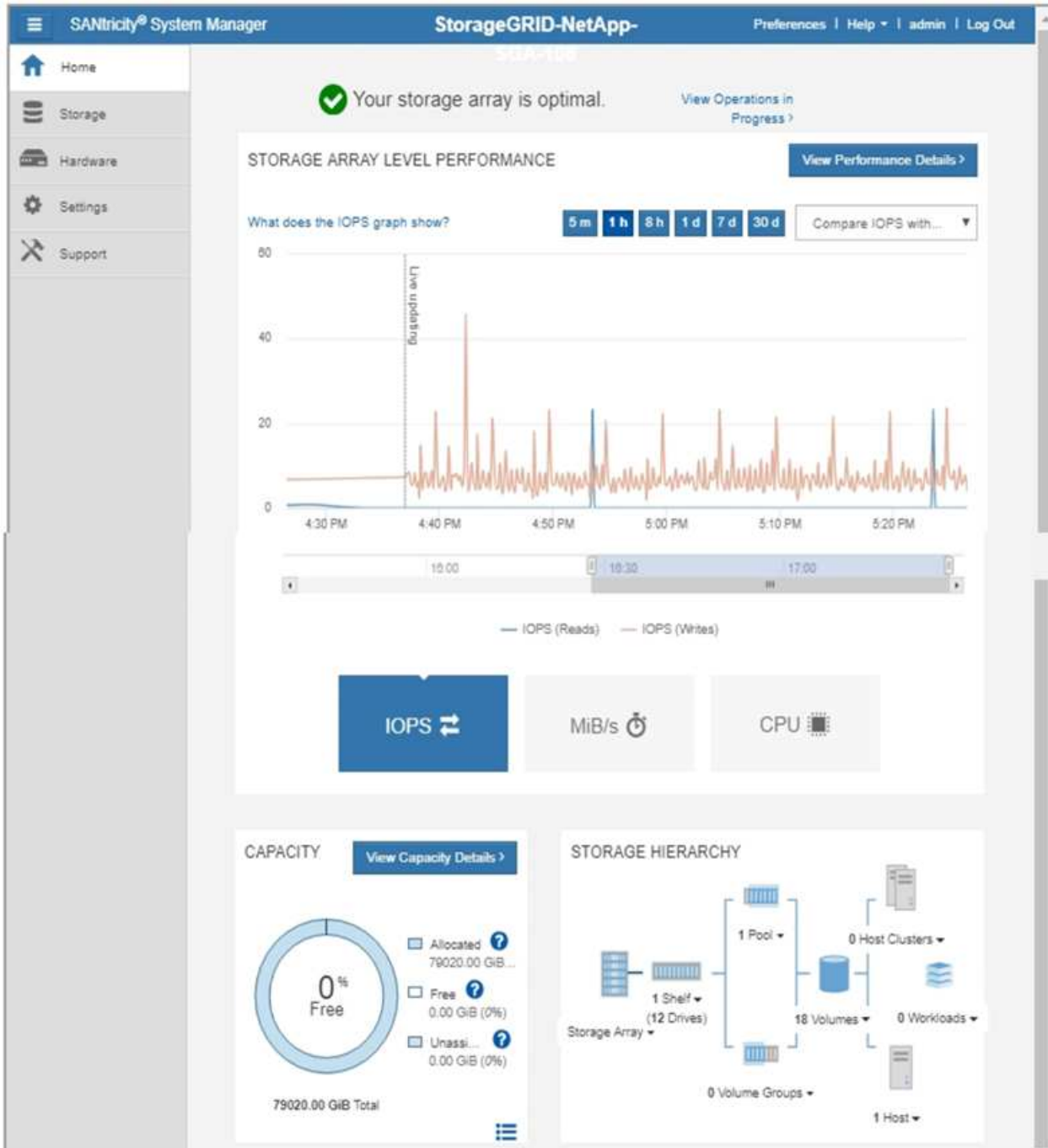
È necessario disporre del firmware SANtricity 8.70 o superiore per accedere a Gestione di sistema di SANtricity utilizzando Gestione griglia.

La scheda visualizza la home page di Gestore di sistema di SANtricity.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open SANtricity System Manager [in a new browser tab.](#)



È possibile utilizzare il collegamento Gestore di sistema di SANtricity per aprire Gestione di sistema di SANtricity in una nuova finestra del browser per una visualizzazione più semplice.

Per visualizzare i dettagli relativi all'utilizzo della capacità e delle prestazioni a livello di array di storage,

posizionare il cursore su ciascun grafico.

Per ulteriori informazioni sulla visualizzazione delle informazioni accessibili dalla scheda Gestore di sistema di SANtricity, vedere ["Documentazione di NetApp e-Series e SANtricity"](#).

Informazioni da monitorare regolarmente

Cosa e quando monitorare

Anche se il sistema StorageGRID può continuare a funzionare quando si verificano errori o parti della griglia non sono disponibili, è necessario monitorare e risolvere potenziali problemi prima che influiscano sull'efficienza o sulla disponibilità della rete.

Prima di iniziare

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

Informazioni sulle attività di monitoraggio

Un sistema occupato genera grandi quantità di informazioni. Il seguente elenco fornisce indicazioni sulle informazioni più importanti da monitorare costantemente.

Cosa monitorare	Frequenza
"Stato di salute del sistema"	Ogni giorno
Tasso a cui "Capacità di metadati e oggetti del nodo di storage" è consumato	Settimanale
"Operazioni di gestione del ciclo di vita delle informazioni"	Settimanale
"Risorse di rete e di sistema"	Settimanale
"Attività del tenant"	Settimanale
"S3 operazioni client"	Settimanale
"Operazioni di bilanciamento del carico"	Dopo la configurazione iniziale e dopo eventuali modifiche alla configurazione
"Connessioni a federazione di griglie"	Settimanale

Monitorare lo stato del sistema

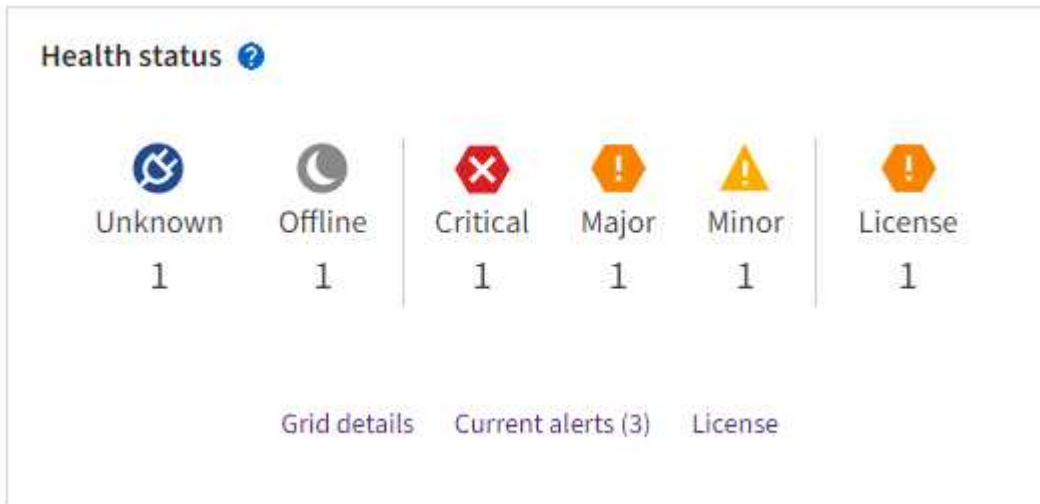
Monitorare quotidianamente lo stato di salute generale del sistema StorageGRID.

A proposito di questa attività

Il sistema StorageGRID può continuare a funzionare quando le parti della griglia non sono disponibili. I potenziali problemi indicati dagli avvisi non sono necessariamente problemi con le operazioni del sistema.

Esaminare i problemi riepilogati nella scheda di stato dello stato di salute del pannello di controllo di Grid Manager.

Per essere avvisati degli avvisi non appena vengono attivati, è possibile ["imposta le notifiche via email per gli avvisi"](#) o ["Configurare i trap SNMP"](#).






In caso di problemi, vengono visualizzati collegamenti che consentono di visualizzare ulteriori dettagli:

Collegamento	Viene visualizzato quando...
Dettagli della griglia	Tutti i nodi sono disconnessi (stato di connessione sconosciuto o amministrativamente inattivo).
Avvisi correnti (critici, maggiori, minori)	Gli avvisi sono attualmente attivo .
Avvisi risolti di recente	Avvisi attivati nella settimana precedente sono ora risolti .
Licenza	Si è verificato un problema con la licenza software per questo sistema StorageGRID. È possibile "aggiornare le informazioni sulla licenza in base alle necessità" .

Monitorare gli stati di connessione del nodo

Se uno o più nodi sono disconnessi dalla rete, potrebbero verificarsi problemi con le operazioni critiche di StorageGRID. Monitorare gli stati di connessione dei nodi e risolvere tempestivamente eventuali problemi.

Icona	Descrizione	Azione richiesta
	<p>Non connesso - Sconosciuto</p> <p>Per un motivo sconosciuto, un nodo viene disconnesso o i servizi sul nodo vengono inaspettatamente disattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato o il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione dell'alimentazione o di un'interruzione imprevista.</p> <p>Potrebbe essere attivato anche l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.</p>	<p>Richiede un'attenzione immediata. Selezionare ciascun avviso e seguire le azioni consigliate.</p> <p>Ad esempio, potrebbe essere necessario riavviare un servizio che ha arrestato o riavviato l'host per il nodo.</p> <p>Nota: Un nodo potrebbe apparire come sconosciuto durante le operazioni di shutdown gestite. In questi casi, è possibile ignorare lo stato Unknown (Sconosciuto).</p>
	<p>Non connesso - amministrazione non attiva</p> <p>Per un motivo previsto, il nodo non è connesso alla rete.</p> <p>Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.</p> <p>In base al problema sottostante, questi nodi tornano spesso online senza alcun intervento.</p>	<p>Determinare se eventuali avvisi influiscono su questo nodo.</p> <p>Se sono attivi uno o più avvisi, selezionare ciascun avviso e seguire le azioni consigliate.</p>
	<p>Connesso</p> <p>Il nodo è collegato alla rete.</p>	<p>Non è richiesta alcuna azione.</p>

Visualizzare gli avvisi correnti e risolti




Current alerts (Avvisi correnti): Quando viene attivato un avviso, viene visualizzata un'icona di avviso sul dashboard. Nella pagina nodi viene visualizzata anche un'icona di avviso per il nodo. Se "[le notifiche e-mail di avviso sono configurate](#)", viene inviata anche una notifica e-mail, a meno che l'avviso non sia stato tacitato.

Avvisi risolti: È possibile cercare e visualizzare una cronologia degli avvisi risolti.

Se si desidera, è stato guardato il video: "[Video: Panoramica degli avvisi](#)"



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

Intestazione di colonna	Descrizione
Nome o titolo	Il nome dell'avviso e la relativa descrizione.
Severità	<p>La severità dell'avviso. Per gli avvisi correnti, se sono raggruppati più avvisi, la riga del titolo mostra il numero di istanze di tale avviso che si verificano a ogni livello di gravità.</p> <p> Critico: Esiste una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. È necessario risolvere immediatamente il problema sottostante. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.</p> <p> Maggiore: Esiste una condizione anomala che influisce sulle operazioni correnti o si avvicina alla soglia per un avviso critico. È necessario analizzare gli avvisi principali e risolvere eventuali problemi sottostanti per assicurarsi che le condizioni anomale non interrompano il normale funzionamento di un nodo o servizio StorageGRID.</p> <p> Minore: Il sistema funziona normalmente, ma esiste una condizione anomala che potrebbe influire sulla capacità del sistema di funzionare se continua. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per garantire che non causino problemi più gravi.</p>
Tempo di attivazione	<p>Current alerts (Avvisi correnti): La data e l'ora in cui l'avviso è stato attivato nell'ora locale e in UTC. Se vengono raggruppati più avvisi, la riga del titolo mostra l'ora dell'istanza più recente dell'avviso (<i>NEST</i>) e l'istanza più vecchia dell'avviso (<i>OLDEST</i>).</p> <p>Resolved alerts (Avvisi risolti): Quanto tempo fa è stato attivato l'avviso.</p>
Sito/nodo	Il nome del sito e del nodo in cui si è verificato o si è verificato l'avviso.
Stato	Se l'avviso è attivo, tacitato o risolto. Se vengono raggruppati più avvisi e nell'elenco a discesa viene selezionato tutti gli avvisi , la riga del titolo mostra quante istanze di tale avviso sono attive e quante istanze sono state tacitate.

Intestazione di colonna	Descrizione
Tempo risolto (solo avvisi risolti)	Quanto tempo fa l'avviso è stato risolto.
Valori correnti o <i>valori di dati</i>	<p>Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso Low Object Data Storage includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.</p> <p>Nota: se vengono raggruppati più avvisi correnti, i valori correnti non vengono visualizzati nella riga del titolo.</p>
Valori attivati (solo avvisi risolti)	Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso Low Object Data Storage includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.

Fasi

1. Selezionare il collegamento **Avvisi correnti** o **Avvisi risolti** per visualizzare un elenco di avvisi in tali categorie. È inoltre possibile visualizzare i dettagli di un avviso selezionando **nodi > nodo > Panoramica** e selezionando l'avviso dalla tabella Avvisi.

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

- Vengono visualizzati per primi gli avvisi attivati più di recente.
- Più avvisi dello stesso tipo vengono visualizzati come gruppo.
- Gli avvisi che sono stati tacitati non vengono visualizzati.
- Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di una severità, viene visualizzato solo l'allarme più grave. Ovvero, se vengono raggiunte soglie di allarme per i livelli di severità minori, maggiori e critici, viene visualizzato solo l'avviso critico.

La pagina degli avvisi correnti viene aggiornata ogni due minuti.

2. Per espandere gruppi di avvisi, selezionare il pulsante freccia giù ▼. Per comprimere singoli avvisi in un gruppo, selezionare il cursore su ▲ o selezionare il nome del gruppo.
3. Per visualizzare singoli avvisi invece di gruppi di avvisi, deselegionare la casella di controllo **Group alerts** (Avvisi di gruppo).
4. Per ordinare gli avvisi correnti o i gruppi di avvisi, selezionare le frecce su/giù ⬆️/⬆️ nell'intestazione di ciascuna colonna.
 - Quando si seleziona **Group alerts** (Avvisi di gruppo), vengono ordinati sia i gruppi di avvisi che i singoli avvisi all'interno di ciascun gruppo. Ad esempio, è possibile ordinare gli avvisi in un gruppo in base all'ora * attivata per trovare l'istanza più recente di un avviso specifico.
 - Quando l'opzione **Group alerts** (Avvisi di gruppo) viene deselegionata, viene ordinato l'intero elenco di avvisi. Ad esempio, è possibile ordinare tutti gli avvisi in base a **nodo/sito** per visualizzare tutti gli avvisi relativi a un nodo specifico.
5. Per filtrare gli avvisi correnti in base allo stato (**tutti gli avvisi**, **attivi** o **silenziati**), utilizzare il menu a

discesa nella parte superiore della tabella.

Vedere "[Tacitare le notifiche di avviso](#)".

6. Per ordinare gli avvisi risolti:

- Selezionare un periodo di tempo dal menu a discesa **quando attivato**.
- Selezionare una o più severità dal menu a discesa **severità**.
- Selezionare una o più regole di avviso predefinite o personalizzate dal menu a discesa **regola di avviso** per filtrare gli avvisi risolti correlati a una regola di avviso specifica.
- Selezionare uno o più nodi dal menu a discesa **nodo** per filtrare gli avvisi risolti relativi a un nodo specifico.

7. Per visualizzare i dettagli di un avviso specifico, selezionarlo. Una finestra di dialogo fornisce dettagli e azioni consigliate per l'avviso selezionato.

8. (Facoltativo) per un avviso specifico, selezionare Silence this alert (tacita questo avviso) per tacitare la regola che ha causato l'attivazione dell'avviso.

È necessario disporre di "[Gestire gli avvisi o l'autorizzazione di accesso principale](#)" per tacitare una regola di avviso.



Prestare attenzione quando si decide di tacitare una regola di avviso. Se una regola di avviso viene tacitata, è possibile che non si rilevi un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

9. Per visualizzare le condizioni correnti della regola di avviso:

a. Dai dettagli dell'avviso, selezionare **View conditions** (Visualizza condizioni).

Viene visualizzata una finestra a comparsa che elenca l'espressione Prometheus per ogni severità definita.

b. Per chiudere la finestra a comparsa, fare clic in un punto qualsiasi all'esterno della finestra a comparsa.

10. Facoltativamente, selezionare **Edit rule** (Modifica regola) per modificare la regola di avviso che ha causato l'attivazione dell'avviso.

È necessario disporre di "[Gestire gli avvisi o l'autorizzazione di accesso principale](#)" per modificare una regola di avviso.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

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

Monitorare la capacità dello storage

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

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 metadati degli oggetti. Monitorare la quantità totale di spazio consumata per gli oggetti e per i metadati degli oggetti, nonché le tendenze della quantità di spazio consumata per ciascuno di essi. Ciò consente di pianificare in anticipo l'aggiunta di nodi ed evitare interruzioni del servizio.

È possibile ["visualizzare le informazioni sulla capacità dello storage"](#) per l'intero grid, per ogni sito e per ogni nodo di storage nel sistema StorageGRID.

Monitorare la capacità di storage per l'intero grid

Monitorare la capacità di storage complessiva del grid per garantire che rimanga spazio libero adeguato per i dati degli oggetti e i metadati degli oggetti. Comprendere come la capacità dello storage cambia nel tempo può aiutarti a pianificare l'aggiunta di nodi o volumi di storage prima che la capacità dello storage utilizzabile del grid venga consumata.

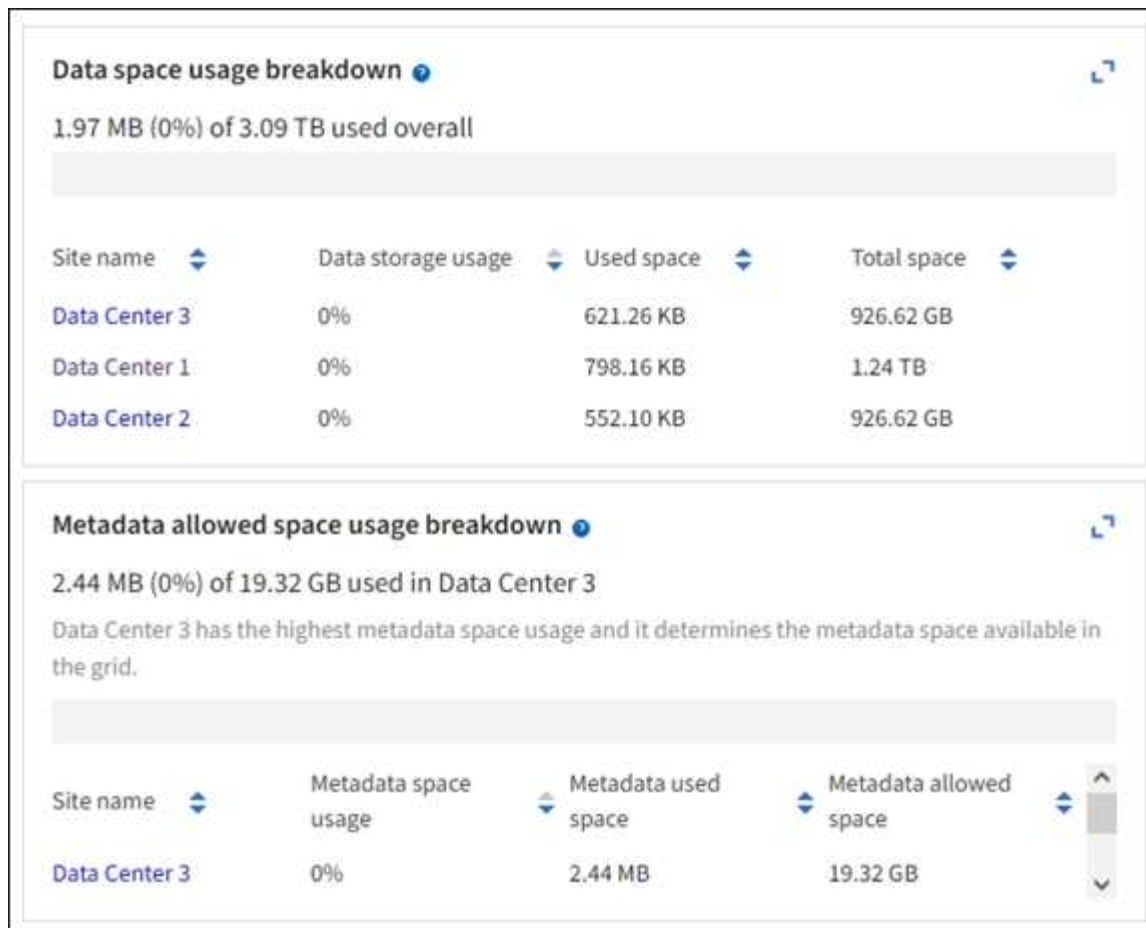
La dashboard di Grid Manager consente di valutare rapidamente la quantità di storage disponibile per l'intero grid e per ciascun data center. La pagina nodi fornisce valori più dettagliati per i dati degli oggetti e i metadati degli oggetti.

Fasi

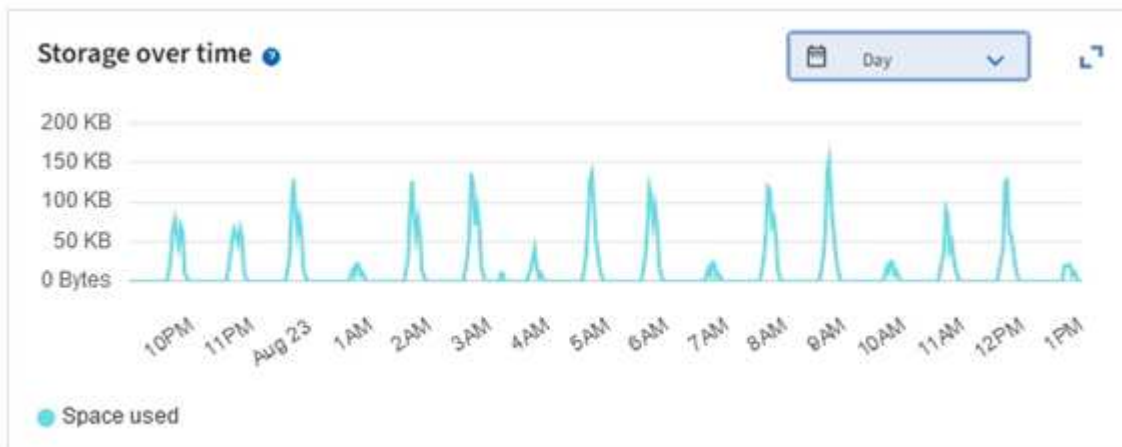
1. Valutare la quantità di storage disponibile per l'intero grid e per ciascun data center.
 - a. Selezionare **Dashboard > Overview**.
 - b. Prendere nota dei valori riportati nelle schede di analisi dell'utilizzo dello spazio dati e delle schede di analisi dell'utilizzo dello spazio consentito dai metadati. Ciascuna scheda elenca una percentuale di utilizzo dello storage, la capacità dello spazio utilizzato e lo spazio totale disponibile o consentito dal sito.



Il riepilogo non include i supporti di archiviazione.



- a. Annotare il grafico sulla scheda Storage over Time (archiviazione nel tempo). Utilizzare il menu a discesa Time Period (periodo di tempo) per determinare la velocità di utilizzo dello storage.



2. Utilizzare la pagina nodi per ulteriori dettagli sulla quantità di storage utilizzata e sulla quantità di storage disponibile nella griglia per i dati degli oggetti e i metadati degli oggetti.
 - a. Selezionare **NODI**.
 - b. Selezionare *grid* > **Storage**.



- c. Posizionare il cursore sui grafici **Storage used - Object data** e **Storage used - Object metadata** per verificare la quantità di storage a oggetti e metadati a oggetti disponibile per l'intera griglia e la quantità di storage utilizzata nel tempo.



I valori totali di un sito o di un grid non includono nodi che non hanno riportato metriche per almeno cinque minuti, come i nodi offline.

3. Pianificare un'espansione per aggiungere nodi di storage o volumi di storage prima che la capacità di storage utilizzabile del grid venga consumata.

Quando si pianifica la tempistica di un'espansione, considerare quanto tempo sarà necessario per procurarsi e installare storage aggiuntivo.



Se la policy ILM utilizza la codifica erasure, è preferibile eseguire un'espansione quando i nodi di storage esistenti sono pieni al 70% circa per ridurre il numero di nodi da aggiungere.

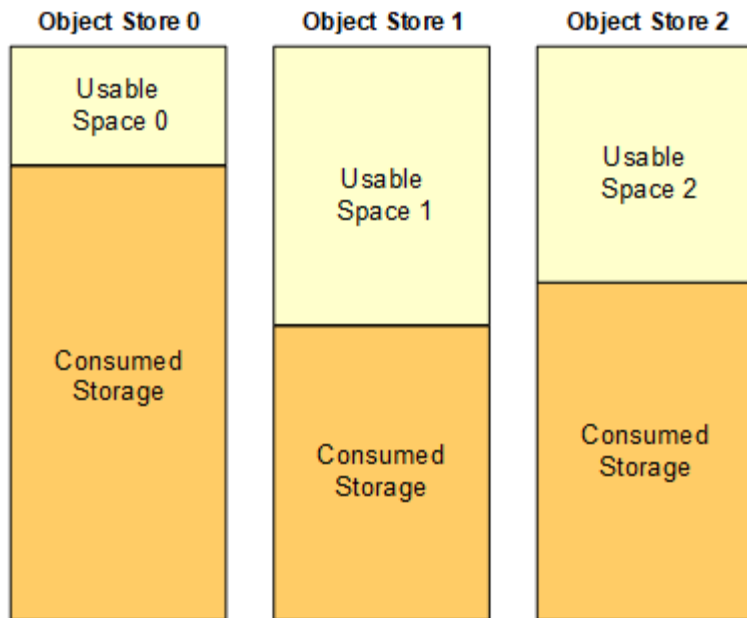
Per ulteriori informazioni sulla pianificazione di un'espansione di archiviazione, vedere "[Istruzioni per espandere StorageGRID](#)".

Monitorare la capacità di storage per ciascun nodo di storage

Monitorare lo spazio totale utilizzabile per ciascun nodo di storage per garantire che il nodo disponga di spazio sufficiente per i nuovi dati dell'oggetto.

A proposito di questa attività

Lo spazio utilizzabile è la quantità di spazio di storage disponibile per memorizzare gli oggetti. Lo spazio totale utilizzabile per un nodo di storage viene calcolato sommando lo spazio disponibile in tutti gli archivi di oggetti all'interno del nodo.



Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2

Fasi

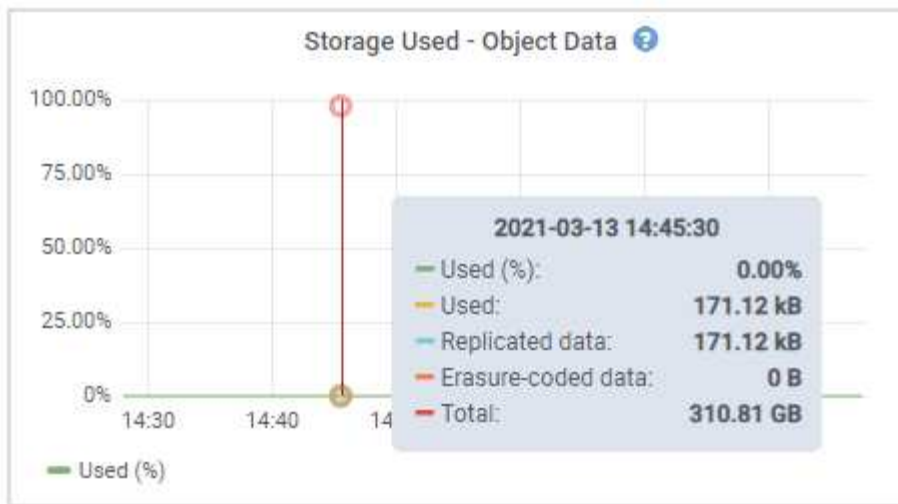
1. Selezionare **NODES > Storage Node > Storage**.

Vengono visualizzati i grafici e le tabelle del nodo.

2. Posizionare il cursore sul grafico Storage Used - Object data (Storage utilizzato - dati oggetto).


Vengono visualizzati i seguenti valori:

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



3. Esaminare i valori disponibili nelle tabelle volumi e archivi di oggetti, sotto i grafici.



Per visualizzare i grafici di questi valori, fare clic sulle icone del grafico  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

- Monitorare i valori nel tempo per stimare il tasso di consumo dello spazio di storage utilizzabile.
- Per mantenere le normali operazioni di sistema, aggiungere nodi di storage, aggiungere volumi di storage o archiviare i dati degli oggetti prima di consumare lo spazio utilizzabile.

Quando si pianifica la tempistica di un'espansione, considerare quanto tempo sarà necessario per procurarsi e installare storage aggiuntivo.



Se la policy ILM utilizza la codifica erasure, è preferibile eseguire un'espansione quando i nodi di storage esistenti sono pieni al 70% circa per ridurre il numero di nodi da aggiungere.

Per ulteriori informazioni sulla pianificazione di un'espansione di archiviazione, vedere ["Istruzioni per espandere StorageGRID"](#).

L'"Storage dei dati a oggetti basso" avviso viene attivato quando rimane spazio insufficiente per l'archiviazione dei dati oggetto su un nodo di archiviazione.

Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage

Monitorare l'utilizzo dei metadati per ciascun nodo di storage per garantire che rimanga spazio sufficiente per le operazioni essenziali del database. È necessario aggiungere nuovi nodi di storage in ogni sito prima che i metadati dell'oggetto superino il 100% dello spazio consentito per i metadati.

A proposito di questa attività

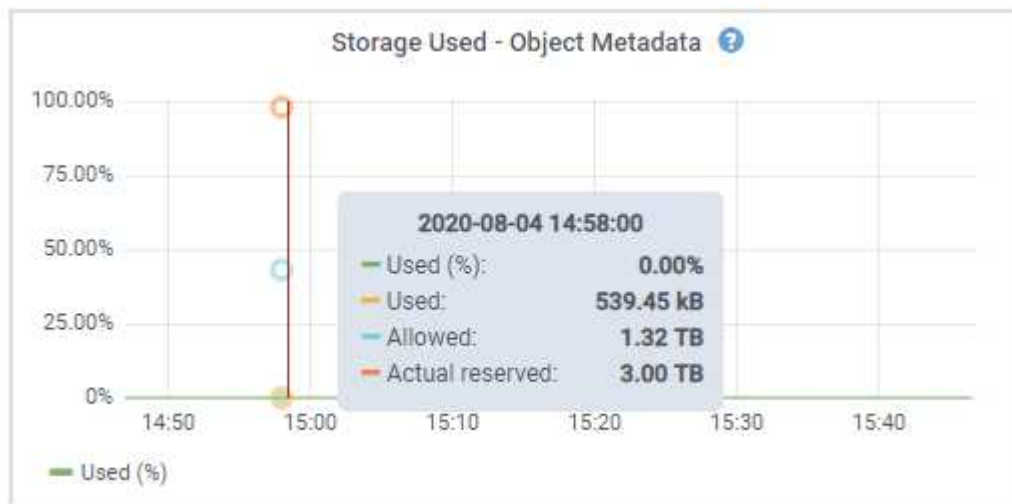
StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di storage di ogni sito utilizzando lo spazio riservato ai metadati sul volume di storage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

In alcuni casi, la capacità dei metadati degli oggetti della griglia potrebbe essere consumata più rapidamente della capacità dello storage a oggetti. Ad esempio, se in genere si acquisiscono grandi quantità di oggetti di piccole dimensioni, potrebbe essere necessario aggiungere nodi di storage per aumentare la capacità dei metadati anche se rimane sufficiente capacità di storage a oggetti.

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

Fasi

1. Selezionare **NODES > Storage Node > Storage**.
2. Posizionare il cursore sul grafico Storage Used - Object metadata (Storage utilizzato - metadati oggetto) per visualizzare i valori relativi a un orario specifico.



Utilizzato (%)

La percentuale dello spazio consentito per i metadati che è stato utilizzato su questo nodo di storage.

Metriche Prometheus: `storagegrid_storage_utilization_metadata_bytes` E.
`storagegrid_storage_utilization_metadata_allowed_bytes`

Utilizzato

I byte dello spazio di metadati consentito che sono stati utilizzati su questo nodo di storage.

Metrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Consentito

Lo spazio consentito per i metadati dell'oggetto su questo nodo di storage. Per informazioni su come questo valore è determinato per ogni nodo di archiviazione, vedere la ["Descrizione completa dello spazio consentito per i metadati"](#).

Metrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Riservato

Lo spazio effettivo riservato ai metadati su questo nodo di storage. Include lo spazio consentito e lo spazio richiesto per le operazioni essenziali dei metadati. Per informazioni su come viene calcolato questo valore per ciascun nodo di archiviazione, vedere la ["Descrizione completa dello spazio riservato effettivo per i metadati"](#).

La metrica Prometheus verrà aggiunta in una release futura.



I valori totali di un sito o di un grid non includono nodi che non hanno riportato metriche per almeno cinque minuti, come i nodi offline.

- Se il valore **utilizzato (%)** è pari o superiore al 70%, espandere il sistema StorageGRID aggiungendo nodi di storage a ciascun sito.



L'avviso **Low metadata storage** viene attivato quando il valore **used (%)** raggiunge determinate soglie. I risultati indesiderati possono verificarsi se i metadati dell'oggetto utilizzano più del 100% dello spazio consentito.

Quando si aggiungono nuovi nodi, il sistema ribilancia automaticamente i metadati degli oggetti in tutti i nodi di storage all'interno del sito. Consultare la ["Istruzioni per espandere un sistema StorageGRID"](#).

Monitorare le previsioni di utilizzo dello spazio

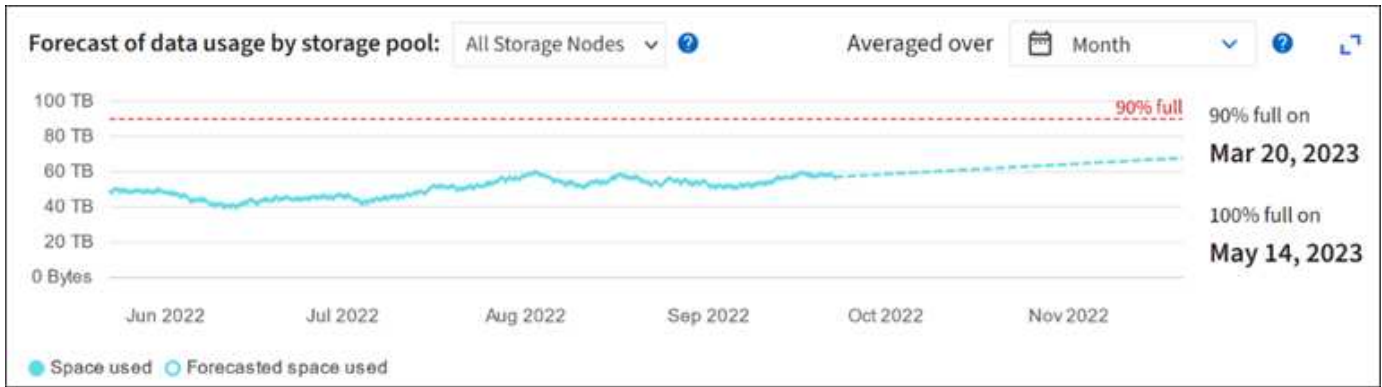
Monitorare le previsioni di utilizzo dello spazio per i dati utente e i metadati per stimare quando sarà necessario ["espandere una griglia"](#).

Se si nota che il tasso di consumo cambia nel tempo, selezionare un intervallo più breve dal menu a discesa **mediato su** per riflettere solo i modelli di acquisizione più recenti. Se si notano schemi stagionali, selezionare un intervallo più lungo.

Se si dispone di una nuova installazione StorageGRID, consentire l'accumulo di dati e metadati prima di valutare le previsioni di utilizzo dello spazio.

Fasi

- Nella dashboard, selezionare **Storage**.
- Visualizza le schede della dashboard, la previsione dell'utilizzo dei dati per pool di storage e la previsione dell'utilizzo dei metadati per sito.
- Utilizza questi valori per valutare quando sarà necessario aggiungere nuovi nodi di storage per lo storage di dati e metadati.



Monitorare la gestione del ciclo di vita delle informazioni

Il sistema ILM (Information Lifecycle Management) fornisce la gestione dei dati per tutti gli oggetti memorizzati nella griglia. È necessario monitorare le operazioni ILM per capire se la griglia è in grado di gestire il carico corrente o se sono necessarie più risorse.

A proposito di questa attività

Il sistema StorageGRID gestisce gli oggetti applicando i criteri ILM attivi. I criteri ILM e le regole ILM associate determinano il numero di copie eseguite, il tipo di copie create, il luogo in cui vengono collocate e la durata di conservazione di ciascuna copia.

L'acquisizione di oggetti e altre attività correlate agli oggetti possono superare la velocità con cui StorageGRID può valutare ILM, causando la messa in coda degli oggetti le cui istruzioni di posizionamento ILM non possono essere soddisfatte quasi in tempo reale. È necessario controllare se StorageGRID è al passo con le azioni del client.

USA la scheda del pannello di controllo di Grid Manager

Fasi

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

1. Accedi a Grid Manager.
2. Dal dashboard, selezionare la scheda ILM e annotare i valori sulla scheda coda ILM (oggetti) e sulla scheda velocità di valutazione ILM.

Sono previsti picchi temporanei nella scheda della coda ILM (oggetti) sul dashboard. Ma se la coda continua ad aumentare e non diminuisce mai, la griglia necessita di più risorse per funzionare in modo efficiente: Più nodi di storage o, se il criterio ILM colloca gli oggetti in posizioni remote, una maggiore larghezza di banda della rete.

Utilizzare la pagina NODI

Fasi

Inoltre, esaminare le code ILM utilizzando la pagina **NODI**:



I grafici della pagina **NODI** verranno sostituiti con le schede del dashboard corrispondenti in una futura versione di StorageGRID.

1. Selezionare **NODI**.

2. Selezionare **grid name > ILM**.

3. Posizionare il cursore sul grafico della coda ILM per visualizzare il valore dei seguenti attributi in un determinato momento:

- **Oggetti accodati (da operazioni client):** Il numero totale di oggetti in attesa di valutazione ILM a causa delle operazioni del client (ad esempio, acquisizione).
- **Oggetti accodati (da tutte le operazioni):** Il numero totale di oggetti in attesa di valutazione ILM.
- **Scan rate (objects/sec):** La velocità con cui gli oggetti nella griglia vengono sottoposti a scansione e messi in coda per ILM.
- **Evaluation rate (objects/sec):** La velocità corrente alla quale gli oggetti vengono valutati rispetto alla policy ILM nella griglia.

4. Nella sezione ILM Queue (coda ILM), esaminare i seguenti attributi.



La sezione coda ILM è inclusa solo per la griglia. Queste informazioni non vengono visualizzate nella scheda ILM per un sito o un nodo di storage.

- **Periodo di scansione - stimato:** Il 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.

- **Riparazioni tentate:** Il numero totale di operazioni di riparazione degli oggetti per i dati replicati che sono stati tentati. Questo numero aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Le riparazioni ILM ad alto rischio hanno la priorità se la rete diventa occupata.



La stessa riparazione dell'oggetto potrebbe aumentare di nuovo se la replica non è riuscita dopo la riparazione.

Questi attributi possono essere utili quando si monitora l'avanzamento del ripristino del volume di Storage Node. Se il numero di riparazioni tentate ha smesso di aumentare ed è stata completata una scansione completa, la riparazione probabilmente è stata completata.

Monitorare le risorse di rete e di sistema

L'integrità e la larghezza di banda della rete tra nodi e siti, nonché l'utilizzo delle risorse da parte dei singoli nodi di rete, sono fondamentali per operazioni efficienti.

Monitorare le connessioni di rete e le performance

La connettività di rete e la larghezza di banda sono particolarmente importanti se il criterio ILM (Information Lifecycle Management) copia gli oggetti replicati tra siti o archivia oggetti con codifica di cancellazione utilizzando uno schema che fornisce la protezione dalla perdita di sito. Se la rete tra siti non è disponibile, la latenza di rete è troppo elevata o la larghezza di banda della rete è insufficiente, alcune regole ILM potrebbero non essere in grado di posizionare oggetti dove previsto. Questo può portare a errori di acquisizione (quando l'opzione di acquisizione rigorosa è selezionata per le regole ILM) o a scarse performance di acquisizione e backlog ILM.

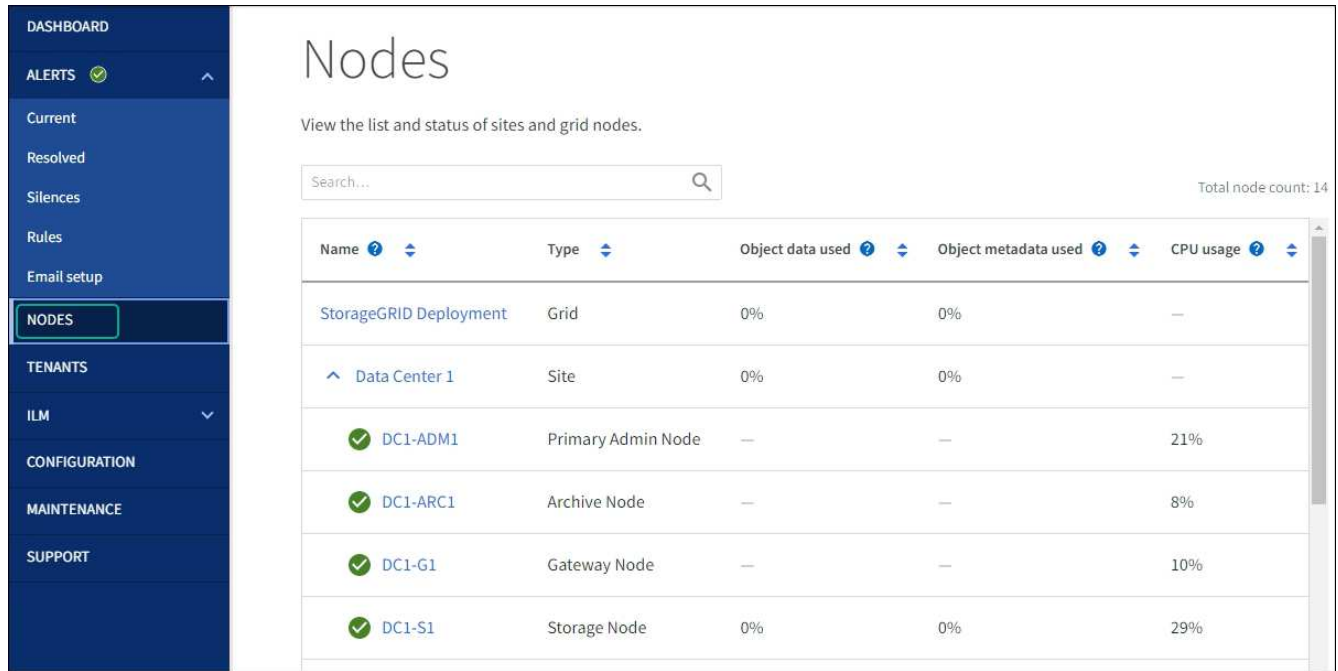
Utilizza Grid Manager per monitorare la connettività e le performance di rete, in modo da poter risolvere tempestivamente qualsiasi problema.

Inoltre, è importante "creazione di criteri di classificazione del traffico di rete" monitorare il traffico relativo a tenant, bucket, subnet o endpoint del bilanciamento del carico specifici. È possibile impostare criteri di limitazione del traffico in base alle esigenze.

Fasi

1. Selezionare **NODI**.

Viene visualizzata la pagina nodi. Ciascun nodo della griglia viene elencato in formato tabella.



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

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



a. Se è stato selezionato un nodo della griglia, scorrere verso il basso per esaminare la sezione **Network Interfaces** della pagina.

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

- b. Per i nodi della griglia, scorrere verso il basso per esaminare la sezione **Network Communication** della pagina.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché 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

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

- a. Selezionare **CONFIGURAZIONE > rete > classificazione del traffico**.

Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

- a. Per visualizzare i grafici che mostrano le metriche di rete associate a un criterio, selezionare il pulsante di opzione a sinistra del criterio, quindi fare clic su **metriche**.
- b. Esaminare i grafici per comprendere il traffico di rete associato alla policy.

Se un criterio di classificazione del traffico è progettato per limitare il traffico di rete, analizzare la

frequenza con cui il traffico è limitato e decidere se il criterio continua a soddisfare le proprie esigenze. Di tanto in tanto, ["modificare ogni policy di classificazione del traffico in base alle esigenze"](#).

Informazioni correlate

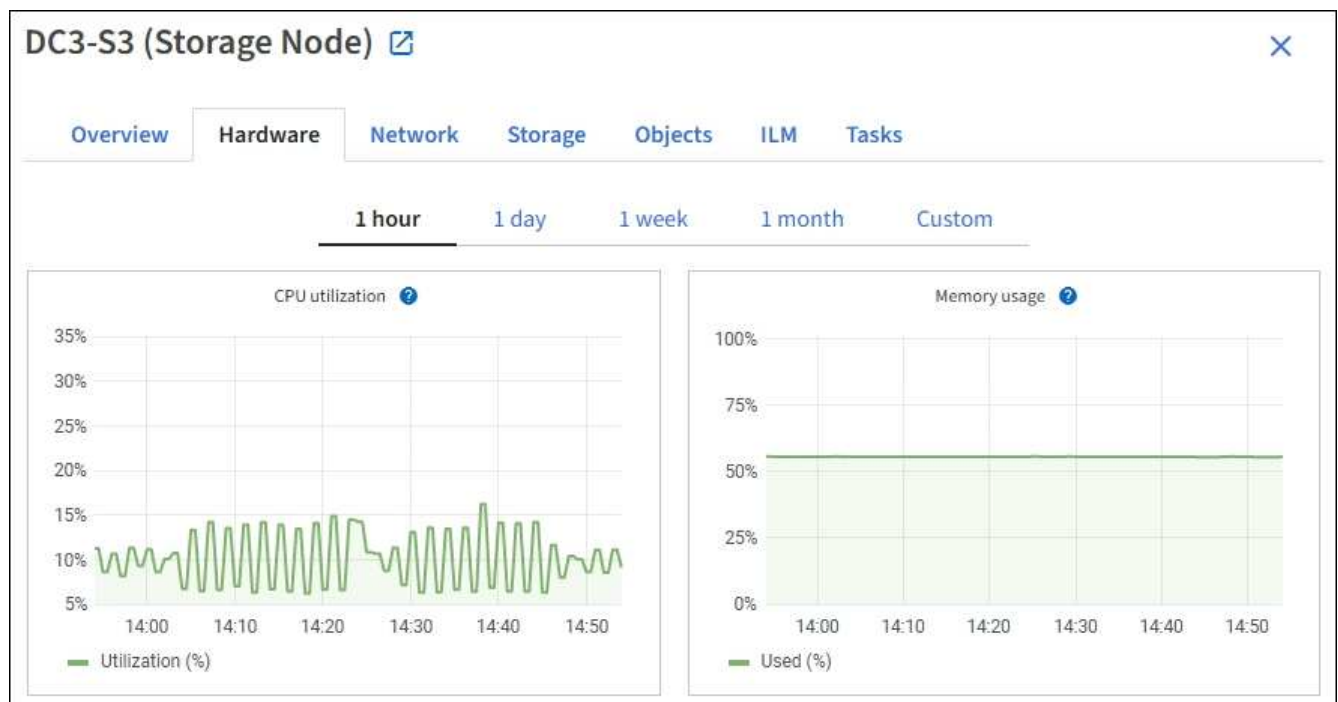
- ["Visualizzare la scheda rete"](#)
- ["Monitorare gli stati di connessione del nodo"](#)

Monitorare le risorse a livello di nodo

Monitorare i singoli nodi di griglia per verificare i livelli di utilizzo delle risorse. Se i nodi sono costantemente sovraccarichi, potrebbero essere necessari più nodi per operazioni efficienti.

Fasi

1. Dalla pagina **NODES**, selezionare il nodo.
2. Selezionare la scheda **hardware** per visualizzare i grafici relativi all'utilizzo della CPU e della memoria.



3. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.
4. Se il nodo è ospitato su un'appliance di storage o su un'appliance di servizi, scorrere verso il basso per visualizzare le tabelle dei componenti. Lo stato di tutti i componenti deve essere "nominale". Esaminare i componenti che presentano qualsiasi altro stato.

Informazioni correlate

- ["Visualizza informazioni sui nodi di storage dell'appliance"](#)
- ["Visualizza informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway"](#)

Monitorare l'attività del tenant

Tutte le attività client S3 sono associate agli account tenant StorageGRID. È possibile

utilizzare Grid Manager per monitorare l'utilizzo dello storage o il traffico di rete di tutti i tenant o di uno specifico tenant. È possibile utilizzare il registro di controllo o le dashboard Grafana per ottenere informazioni più dettagliate sull'utilizzo di StorageGRID da parte dei tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "Accesso root o autorizzazione account tenant".

Visualizza tutti i tenant

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

Fasi

1. Selezionare **TENANT**.
2. Esaminare le informazioni visualizzate nelle pagine del tenant.

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



I valori dello spazio utilizzato sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi.

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: #28a745;"></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: #ffc107;"></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: #28a745;"></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: #dc3545;"></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

3. Se si desidera, accedere a un account tenant selezionando il collegamento di accesso [→](#) nella colonna **Accedi/Copia URL**.
4. Se si desidera, copiare l'URL della pagina di accesso di un tenant selezionando il collegamento Copia URL [📄](#) nella colonna **Accedi/Copia URL**.
5. In alternativa, selezionare **Esporta in CSV** per visualizzare ed esportare un .csv file contenente i valori di utilizzo per tutti i tenant.

Viene richiesto di aprire o salvare il .csv file.

Il contenuto del .csv file è simile al seguente esempio:

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

È possibile aprire il .csv file in un foglio di calcolo o utilizzarlo in automazione.

6. Se non sono presenti oggetti nell'elenco, selezionare **azioni > Elimina** per rimuovere uno o più tenant. Vedere "[Elimina account tenant](#)".

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

Visualizzare un tenant specifico


È possibile visualizzare i dettagli di un tenant specifico.

Fasi

1. Selezionare il nome del tenant dalla pagina tenant.

Viene visualizzata la pagina dei dettagli del tenant.

Tenant 02

Tenant ID: 4103 1879 2208 5551 2180  Quota utilization: 85%
 Protocol: S3 Logical space used: 85.00 GB
 Object count: 500 Quota: 100.00 GB


[Sign in](#) [Edit](#) [Actions](#) ▾

[Space breakdown](#) [Allowed features](#)

Bucket space consumption

85.00 GB of 100.00 GB used


15.00 GB remaining (15%).







0 25% 50% 75% 100%

● bucket-01 ● bucket-02 ● bucket-03

Bucket details

[Export to CSV](#)  Displaying 3 results

Name  ▾	Region  ▾	Space used  ▾	Object count  ▾
bucket-01		40.00 GB	250
bucket-02		30.00 GB	200
bucket-03		15.00 GB	50

2. Esaminare la panoramica del tenant nella parte superiore della pagina.

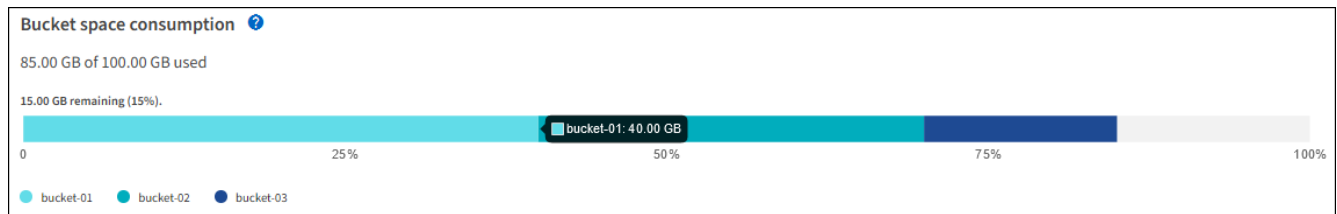
Questa sezione della pagina dei dettagli fornisce informazioni di riepilogo per il tenant, tra cui il numero di oggetti del tenant, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

3. Dalla scheda **Space disruption** (suddivisione spazio), esaminare il grafico **Space Consumption** (consumo spazio).

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

Se è stata impostata una quota per questo tenant, la quantità di quota utilizzata e rimanente viene visualizzata nel testo (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 una quantità di spazio utilizzata (ad esempio, 85.00 GB used). Il grafico a barre mostra la percentuale di quota in ciascun bucket o container. Se il tenant ha superato la quota di storage di oltre l'1% e di almeno 1 GB, il grafico mostra la quota totale e la quantità in eccesso.

È possibile posizionare il cursore sul grafico a barre per visualizzare lo storage utilizzato da ciascun bucket o container. È possibile posizionare il cursore sul segmento di spazio libero per visualizzare la quantità di spazio rimanente.



L'utilizzo delle quote si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla la quota quando un tenant avvia il caricamento degli oggetti e rifiuta le nuove ricerche se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se la quota è stata superata. Se gli oggetti vengono eliminati, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino a quando l'utilizzo della quota non viene ricalcolato. I calcoli relativi all'utilizzo delle quote possono richiedere 10 minuti o più.



L'utilizzo della quota di un tenant indica la quantità totale di dati oggetto caricati dal tenant su StorageGRID (dimensione logica). L'utilizzo della quota non rappresenta lo spazio utilizzato per memorizzare copie degli oggetti e dei relativi metadati (dimensioni fisiche).



È possibile attivare la regola di avviso **quota elevata utilizzo tenant** per determinare se i tenant consumano le proprie quote. Se attivato, questo avviso viene attivato quando un tenant utilizza il 90% della propria quota. Per istruzioni, vedere "[Modificare le regole degli avvisi](#)".

4. Dalla scheda **Space breakdown** (suddivisione spazio), rivedere i **Bucket details** (Dettagli bucket).

Questa tabella elenca i bucket S3 per il tenant. Lo spazio utilizzato è la quantità totale di dati dell'oggetto nel bucket o nel container. Questo valore non rappresenta lo spazio di storage richiesto per le copie ILM e i metadati degli oggetti.

5. Facoltativamente, selezionare **Export to CSV** (Esporta in CSV) per visualizzare ed esportare un file .csv contenente i valori di utilizzo per ciascun bucket o container.

Il contenuto di un singolo file del tenant S3 .csv è simile al 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

È possibile aprire il .csv file in un foglio di calcolo o utilizzarlo in automazione.

6. Se si desidera, selezionare la scheda **funzioni consentite** per visualizzare un elenco delle autorizzazioni e delle funzionalità attivate per il tenant. Vedere "[Modificare l'account tenant](#)" se è necessario modificare queste impostazioni.

7. Se il tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, selezionare la scheda **federazione griglia** per ulteriori informazioni sulla connessione.

Vedere "[Che cos'è la federazione di griglie?](#)" e "[Gestire i tenant consentiti per la federazione di grid](#)".

Visualizzare il traffico di rete

Se per un tenant sono in vigore criteri di classificazione del traffico, esaminare il traffico di rete per tale tenant.

Fasi

1. Selezionare **CONFIGURAZIONE > rete > classificazione del traffico**.

Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

2. Esaminare l'elenco delle policy per identificare quelle applicabili a un tenant specifico.
3. Per visualizzare le metriche associate a un criterio, selezionare il pulsante di opzione a sinistra del criterio e selezionare **metriche**.
4. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Per ulteriori informazioni, vedere ["Gestire le policy di classificazione del traffico"](#) .

Utilizzare il registro di controllo

Facoltativamente, è possibile utilizzare il registro di audit per un monitoraggio più granulare delle attività di un tenant.

Ad esempio, è possibile monitorare i seguenti tipi di informazioni:

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

I registri di audit vengono scritti in file di testo che è possibile analizzare utilizzando lo strumento di analisi dei log scelto. Ciò consente di comprendere meglio le attività del cliente o di implementare sofisticati modelli di chargeback e fatturazione.

Per ulteriori informazioni, vedere ["Esaminare i registri di audit"](#) .

Utilizza le metriche Prometheus

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

- In Grid Manager, selezionare **SUPPORT > Tools > Metrics**. È possibile utilizzare dashboard esistenti, ad esempio S3 Overview, per esaminare le attività del client.



Gli strumenti disponibili nella pagina metriche sono destinati principalmente all'utilizzo da parte del supporto tecnico. Alcune funzioni e voci di menu di questi strumenti sono intenzionalmente non funzionali.

- Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**. È possibile utilizzare le metriche nella sezione metriche dell'API Grid Management per creare regole di avviso e dashboard personalizzati per l'attività del tenant.

Per ulteriori informazioni, vedere ["Rivedere le metriche di supporto"](#) .

Monitorare S3 operazioni client

È possibile monitorare i tassi di acquisizione e recupero degli oggetti, nonché le metriche per i conteggi degli oggetti, le query e la verifica. È possibile visualizzare il numero di tentativi riusciti e non riusciti da parte delle applicazioni client di lettura, scrittura e modifica degli oggetti nel sistema StorageGRID.

Prima di iniziare

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

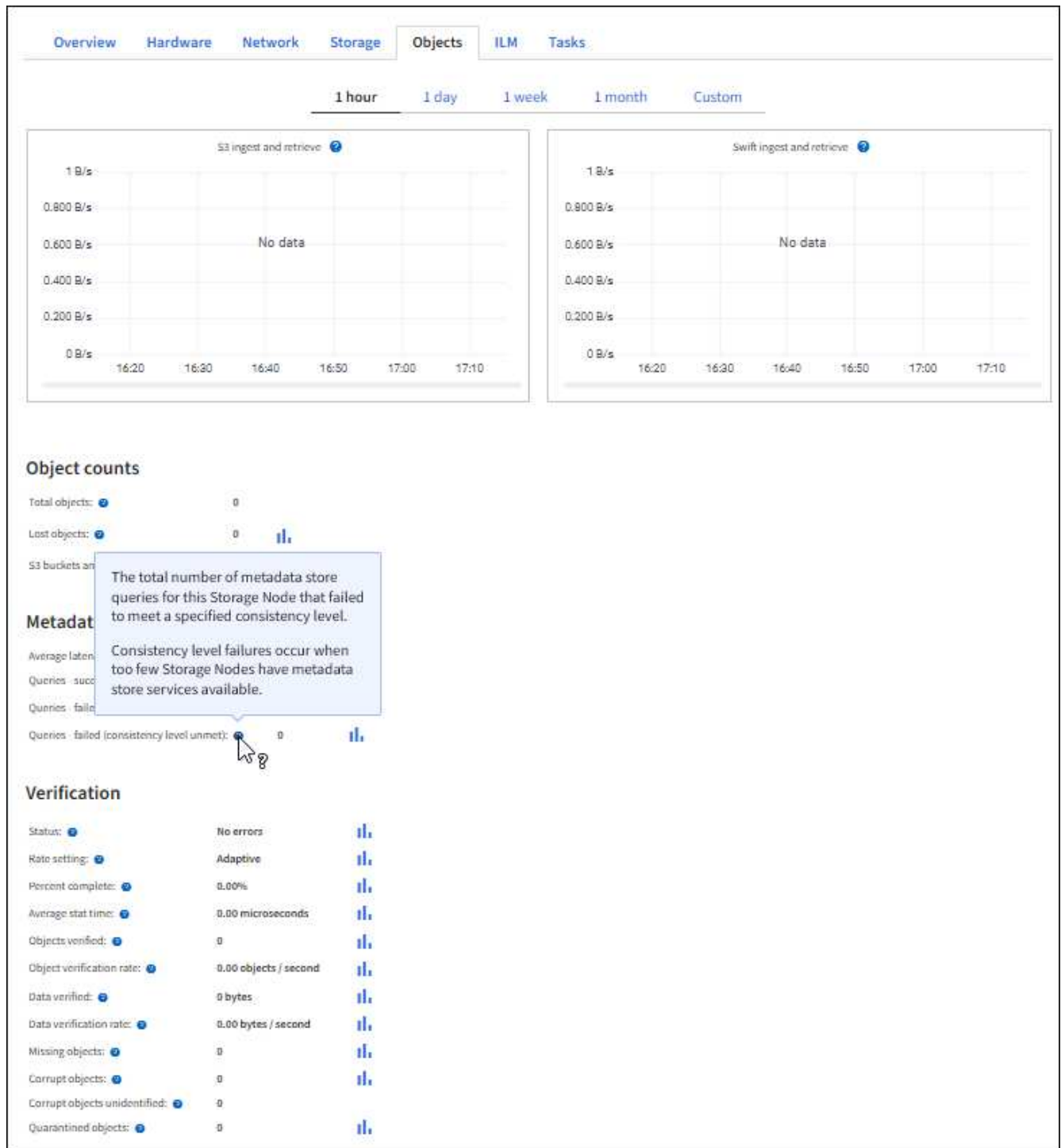
Fasi

1. Dalla dashboard, selezionare la scheda **prestazioni**.
2. Fare riferimento ai grafici S3, che riassumono il numero di operazioni client eseguite dai nodi di archiviazione e il numero di richieste API ricevute dai nodi di archiviazione durante l'intervallo di tempo selezionato.
3. Selezionare **NODI** per accedere alla pagina nodi.
4. Dalla home page dei nodi (livello griglia), selezionare la scheda **oggetti**.

Il grafico mostra i tassi di acquisizione e recupero di S3 kb dell'intero sistema StorageGRID in byte al secondo e la quantità di dati acquisiti o recuperati. È possibile selezionare un intervallo di tempo o applicare un intervallo personalizzato.

5. Per visualizzare le informazioni relative a un determinato nodo di archiviazione, selezionare il nodo dall'elenco a sinistra e selezionare la scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero per il nodo. Questa scheda include inoltre metriche per il numero di oggetti, le query sui metadati e le operazioni di verifica.



Monitorare le operazioni di bilanciamento del carico

Se si utilizza un bilanciamento del carico per gestire le connessioni client a StorageGRID, è necessario monitorare le operazioni di bilanciamento del carico dopo aver configurato il sistema inizialmente e dopo aver apportato modifiche alla configurazione o aver eseguito un'espansione.

A proposito di questa attività

È possibile utilizzare il servizio Load Balancer sui nodi Admin o Gateway o un bilanciamento del carico esterno di terze parti per distribuire le richieste dei client su più nodi di storage.

Dopo aver configurato il bilanciamento del carico, è necessario confermare che le operazioni di recupero e acquisizione degli oggetti vengono distribuite uniformemente tra i nodi di storage. Le richieste distribuite in modo uniforme garantiscono che StorageGRID rimanga reattivo alle richieste dei client sotto carico e possa contribuire a mantenere le performance dei client.

Se è stato configurato un gruppo ad alta disponibilità (ha) di nodi gateway o nodi di amministrazione in modalità Active-backup, solo un nodo del gruppo distribuisce attivamente le richieste dei client.

Per ulteriori informazioni, vedere ["Configurare connessioni client S3"](#).

Fasi

1. Se i client S3 si connettono utilizzando il servizio Load Balancer, controllare che i nodi Admin o Gateway distribuiscono attivamente il traffico come previsto:
 - a. Selezionare **NODI**.
 - b. Selezionare un nodo gateway o un nodo amministratore.
 - c. Nella scheda **Overview**, verificare se un'interfaccia di nodo è in un gruppo ha e se l'interfaccia di nodo ha il ruolo di primario.

I nodi con il ruolo di primario e i nodi che non fanno parte di un gruppo ha devono distribuire attivamente le richieste ai client.

- d. Per ogni nodo che deve distribuire attivamente le richieste client, selezionare ["Scheda bilanciamento del carico"](#).

- e. Esaminare il grafico del traffico di richiesta del bilanciamento del carico dell'ultima settimana per assicurarsi che il nodo stia distribuendo attivamente le richieste.

I nodi di un gruppo ha con backup attivo potrebbero assumere di tanto in tanto il ruolo di backup. Durante questo periodo, i nodi non distribuiscono le richieste dei client.

- f. Esaminare il grafico del tasso di richiesta in entrata del bilanciamento del carico dell'ultima settimana per esaminare il throughput degli oggetti del nodo.
 - g. Ripetere questi passaggi per ogni nodo amministratore o nodo gateway nel sistema StorageGRID.
 - h. Facoltativamente, utilizzare le policy di classificazione del traffico per visualizzare un'analisi più dettagliata del traffico fornito dal servizio Load Balancer.

2. Verificare che queste richieste vengano distribuite uniformemente ai nodi di storage.

- a. Selezionare **Storage Node > LDR > HTTP**.
 - b. Esaminare il numero di **sessioni in entrata attualmente stabilite**.
 - c. Ripetere l'operazione per ogni nodo di storage nella griglia.

Il numero di sessioni deve essere approssimativamente uguale in tutti i nodi di storage.

Monitorare le connessioni a federazione di griglie

È possibile monitorare le informazioni di base su tutto ["connessioni a federazione di griglie"](#), le informazioni dettagliate su una connessione specifica o le metriche Prometheus sulle operazioni di replica cross-grid. È possibile monitorare una connessione da entrambe le griglie.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager su una delle due griglie utilizzando un ["browser web supportato"](#).
- Si dispone del ["Autorizzazione di accesso root"](#) per la griglia a cui si è effettuato l'accesso.

Visualizza tutte le connessioni

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

Fasi

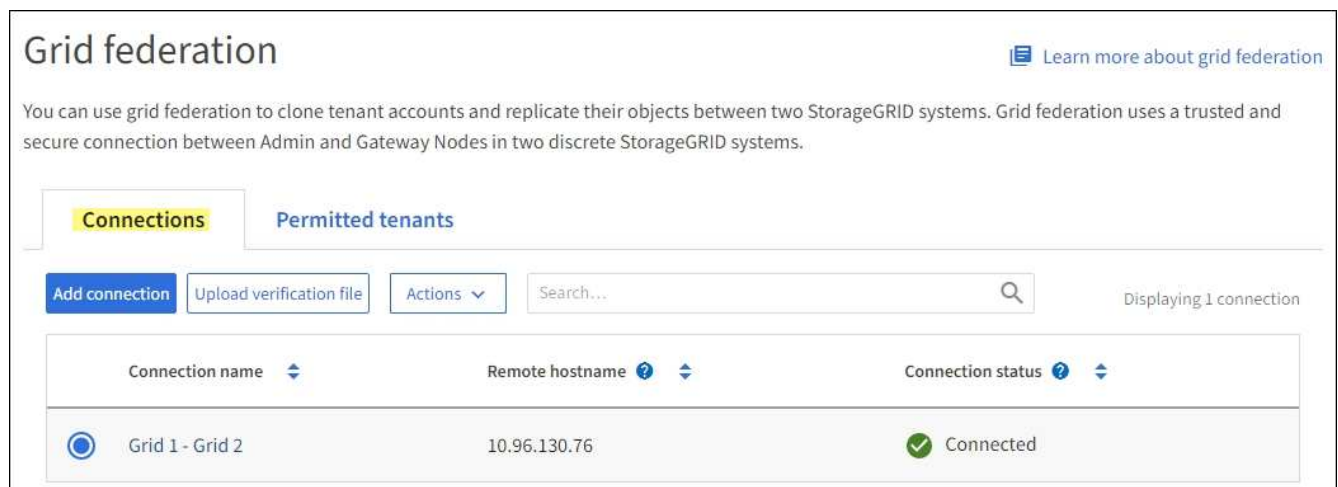
1. Selezionare **CONFIGURATION > System > Grid Federation**.

Viene visualizzata la pagina Grid Federation.

2. Per visualizzare le informazioni di base su tutte le connessioni in questa griglia, selezionare la scheda **connessioni**.

Da questa scheda è possibile:

- ["Creare una nuova connessione"](#).
- Selezionare una connessione esistente a ["modifica o verifica"](#).



Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

Connections Permitted tenants

Add connection Upload verification file Actions Search... Displaying 1 connection

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. Per visualizzare le informazioni di base per tutti gli account tenant di questa griglia che dispongono dell'autorizzazione **Usa connessione federazione griglia**, selezionare la scheda **tenant consentiti**.

Da questa scheda è possibile:

- ["Visualizza la pagina dei dettagli per ciascun tenant consentito"](#).
- Visualizzare la pagina dei dettagli per ciascuna connessione. Vedere [Visualizzare una connessione specifica](#).
- Selezionare un tenant consentito e ["rimuovere l'autorizzazione"](#).
- Verificare la presenza di errori di replica tra griglie e cancellare l'ultimo errore, se presente. Vedere ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).

Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

Connections
Permitted tenants

Remove permission
Clear error

🔍
Displaying one result

	Tenant name	Connection name	Connection status	Remote grid hostname	Last error
ⓘ	Tenant A	Grid 1 - Grid 2	✔ Connected	10.96.130.76	Check for errors

Visualizza una connessione specifica

È possibile visualizzare i dettagli di una connessione a federazione di griglie specifica.

Fasi

1. Selezionare una delle schede dalla pagina Grid Federation, quindi selezionare il nome della connessione dalla tabella.

Dalla pagina dei dettagli per la connessione, è possibile:

- Consultare le informazioni di base sullo stato della connessione, inclusi i nomi host locali e remoti, la porta e lo stato della connessione.
 - Selezionare una connessione a ["modifica, verifica o rimozione"](#).
2. Quando si visualizza una connessione specifica, selezionare la scheda **tenant consentiti** per visualizzare i dettagli relativi ai tenant consentiti per la connessione.

Da questa scheda è possibile:

- ["Visualizza la pagina dei dettagli per ciascun tenant consentito"](#).
- ["Rimuovere l'autorizzazione di un tenant"](#) per utilizzare la connessione.
- Verificare la presenza di errori di replica tra griglie e cancellare l'ultimo errore. Vedere ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64
Port: 23000
Remote hostname (other grid): 10.96.130.76
Connection status: ✔ Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

Permitted tenants [Certificates](#)

[Remove permission](#) [Clear error](#) Displaying one result

Tenant name	Last error
<input checked="" type="radio"/> Tenant A	Check for errors

3. Quando si visualizza una connessione specifica, selezionare la scheda **certificati** per visualizzare i certificati server e client generati dal sistema per questa connessione.

Da questa scheda è possibile:

- ["Ruotare i certificati di connessione"](#).
- Selezionare **Server** o **Client** per visualizzare o scaricare il certificato associato o copiare il PEM del certificato.

Grid A-Grid B

Local hostname (this grid): 10.96.106.230
Port: 23000
Remote hostname (other grid): 10.96.104.230
Connection status: ✔ Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Rotate certificates

Server

Client

Download certificate

Copy certificate PEM

Metadata [?](#)

Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230
Serial number: 30:81:B8:DD:AE:B2:86:0A
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT
Issued on: 2022-10-04T02:21:18.000Z
Expires on: 2024-10-03T19:05:13.000Z
SHA-1 fingerprint: 92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF
SHA-256 fingerprint: 54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60
Alternative names: IP Address:10.96.106.230

Certificate PEM [?](#)

```
-----BEGIN CERTIFICATE-----
MIIGdTCCBF2gAwIBAgIIMIG43a6yhgowDQYJKoZIhvcNAQENBQAwzELMAkGA1UE
BhMCMVVMxEzARBgNVBAGMCkNhbjG1mb3JuaWExEjAQBgNVBACMCV1bm55dmFsZTEU
MBQTCmV1bm55dmFsZTEU
-----END CERTIFICATE-----
```

Analisi delle metriche di replica cross-grid

Puoi utilizzare la dashboard di replica cross-grid di Grafana per visualizzare le metriche Prometheus sulle operazioni di replica cross-grid sul tuo grid.

Fasi

1. Da Grid Manager, selezionare **SUPPORT > Tools > Metrics**.



Gli strumenti disponibili nella pagina metriche sono destinati all'utilizzo da parte del supporto tecnico. Alcune funzioni e voci di menu di questi strumenti sono intenzionalmente non funzionali e sono soggette a modifiche. Vedere l'elenco di ["Metriche Prometheus comunemente utilizzate"](#).

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

Per istruzioni dettagliate, vedere ["Rivedere le metriche di supporto"](#).

3. Per riprovare la replica degli oggetti che non sono stati replicati, vedere ["Identificare e riprovare le operazioni di replica non riuscite"](#).

Gestire gli avvisi

Gestire gli avvisi

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

Gli avvisi vengono attivati a livelli di severità specifici quando le condizioni delle regole di avviso vengono valutate come vere. Quando viene attivato un avviso, si verificano le seguenti azioni:

- Sul dashboard di Grid Manager viene visualizzata un'icona di severità degli avvisi e il numero di avvisi correnti viene incrementato.
- L'avviso viene visualizzato nella pagina di riepilogo **NODI** e nella scheda **NODI > nodo > Panoramica**.
- Viene inviata una notifica e-mail, presupponendo che sia stato configurato un server SMTP e che siano stati forniti indirizzi e-mail per i destinatari.
- Viene inviata una notifica SNMP (Simple Network Management Protocol), presupponendo che l'agente SNMP StorageGRID sia stato configurato.

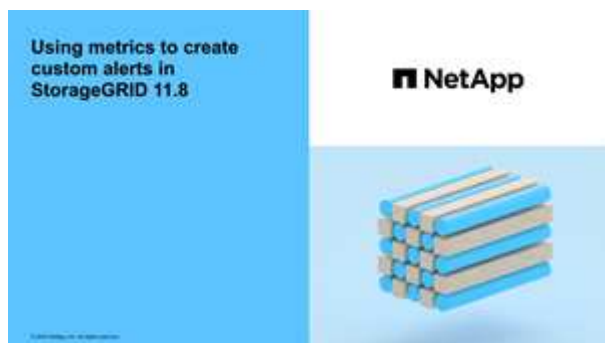
È possibile creare avvisi personalizzati, modificare o disattivare gli avvisi e gestire le notifiche degli avvisi.

Per saperne di più:

- Guarda il video: ["Video: Panoramica degli avvisi"](#)



- Guarda il video: ["Video: Avvisi personalizzati"](#)



- Consultare la ["Riferimenti agli avvisi"](#).

Visualizzare le regole degli avvisi

Le regole di avviso definiscono le condizioni che attivano "avvisi specifici". StorageGRID include una serie di regole di avviso predefinite, che è possibile utilizzare così com'è o modificare, oppure è possibile creare regole di avviso personalizzate.

È possibile visualizzare l'elenco di tutte le regole di avviso predefinite e personalizzate per scoprire quali condizioni attiveranno ciascun avviso e per verificare se gli avvisi sono disattivati.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "Gestire gli avvisi o l'autorizzazione di accesso principale".
- Se si desidera, è stato guardato il video: "Video: Panoramica degli avvisi"



Fasi

1. Selezionare **ALERTS > regole**.

Viene visualizzata la pagina regole di avviso.

Alert Rules [Learn more](#)




Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

Name	Conditions	Type	Status
<input type="radio"/> Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled

Displaying 62 alert rules.

2. Esaminare le informazioni nella tabella delle regole di avviso:

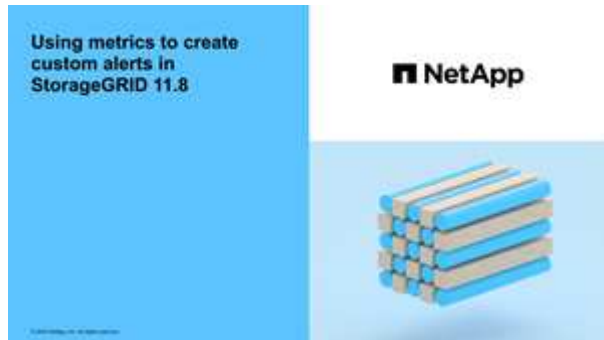
Intestazione di colonna	Descrizione
Nome	Nome univoco e descrizione della regola di avviso. Vengono elencate per prime le regole di avviso personalizzate, seguite dalle regole di avviso predefinite. Il nome della regola di avviso è l'oggetto delle notifiche e-mail.
Condizioni	<p>Le espressioni Prometheus che determinano quando viene attivato questo avviso. Un avviso può essere attivato in uno o più dei seguenti livelli di severità, ma non è richiesta alcuna condizione per ogni severità.</p> <ul style="list-style-type: none"> • Critical : esiste una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. È necessario risolvere immediatamente il problema sottostante. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati. • Maggiore : esiste una condizione anomala che influisce sulle operazioni correnti o si avvicina alla soglia per un avviso critico. È necessario analizzare gli avvisi principali e risolvere eventuali problemi sottostanti per assicurarsi che le condizioni anomale non interrompano il normale funzionamento di un nodo o servizio StorageGRID. • Minore : il sistema funziona normalmente, ma esiste una condizione anomala che potrebbe influire sulla capacità del sistema di funzionare se continua. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per garantire che non causino problemi più gravi.
Tipo	<p>Il tipo di regola di avviso:</p> <ul style="list-style-type: none"> • Default: Una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificare le condizioni e la durata di una regola di avviso predefinita. Non è possibile rimuovere una regola di avviso predefinita. • Default*: Una regola di avviso predefinita che include una condizione o una durata modificate. Se necessario, è possibile ripristinare facilmente le impostazioni predefinite originali di una condizione modificata. • Personalizzato: Una regola di avviso creata dall'utente. È possibile disattivare, modificare e rimuovere regole di avviso personalizzate.
Stato	Se questa regola di avviso è attualmente attivata o disattivata. Le condizioni per le regole di avviso disabilitate non vengono valutate, quindi non vengono attivati avvisi.

Creare regole di avviso personalizzate

È possibile creare regole di avviso personalizzate per definire le proprie condizioni di attivazione degli avvisi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).
- Si ha familiarità con ["Metriche Prometheus comunemente utilizzate"](#).
- Si comprende il ["Sintassi delle query Prometheus"](#).
- Se si desidera, è stato guardato il video: ["Video: Avvisi personalizzati"](#).



A proposito di questa attività

StorageGRID non convalida gli avvisi personalizzati. Se si decide di creare regole di avviso personalizzate, attenersi alle seguenti linee guida generali:

- Esaminare le condizioni per le regole di avviso predefinite e utilizzarle come esempi per le regole di avviso personalizzate.
- Se si definiscono più condizioni per una regola di avviso, utilizzare la stessa espressione per tutte le condizioni. Quindi, modificare il valore di soglia per ciascuna condizione.
- Controllare attentamente ogni condizione per verificare la presenza di errori di tipo e logici.
- Utilizzare solo le metriche elencate nell'API Grid Management.
- Quando si esegue il test di un'espressione utilizzando l'API Grid Management, tenere presente che una risposta "riuscita" potrebbe essere un corpo di risposta vuoto (nessun avviso attivato). Per verificare se l'avviso è effettivamente attivato, è possibile impostare temporaneamente una soglia su un valore che si prevede sia vero al momento.

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

- Non presumere che un avviso personalizzato funzioni a meno che non sia stata convalidata l'attivazione dell'avviso quando previsto.

Fasi

1. Selezionare **ALERTS > regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare **Crea regola personalizzata**.

Viene visualizzata la finestra di dialogo Create Custom Rule (Crea regola personalizzata).

Create Custom Rule

Enabled

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

5

minutes

Cancel

Save

3. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

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

4. Inserire le seguenti informazioni:

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche e-mail. I nomi delle regole di avviso possono essere compresi tra 1 e 64 caratteri.

Campo	Descrizione
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (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, immettere un'espressione Prometheus per uno o più livelli di gravità dell'avviso.

Un'espressione di base è in genere della forma:

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

Le espressioni possono essere di qualsiasi lunghezza, ma vengono visualizzate su una singola riga dell'interfaccia utente. È richiesta almeno un'espressione.

Questa espressione attiva un avviso se la quantità di RAM installata per un nodo è inferiore a 24,000,000,000 byte (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

Per visualizzare le metriche disponibili e testare le espressioni Prometheus, selezionare l'icona della guida  e seguire il collegamento alla sezione metriche dell'API di gestione griglia.

6. Nel campo **durata**, immettere il periodo di tempo in cui una condizione deve rimanere in vigore continuamente prima che l'allarme venga attivato e selezionare un'unità di tempo.

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

L'impostazione predefinita è 5 minuti.

7. Selezionare **Salva**.

La finestra di dialogo si chiude e la nuova regola di avviso personalizzata viene visualizzata nella tabella regole di avviso.

Modificare le regole degli avvisi

È possibile modificare una regola di avviso per modificare le condizioni di attivazione; per una regola di avviso personalizzata, è anche possibile aggiornare il nome della regola, la descrizione e le azioni consigliate.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[Gestire gli avvisi o l'autorizzazione di accesso principale](#)".

A proposito di questa attività

Quando si modifica una regola di avviso predefinita, è possibile modificare le condizioni per gli avvisi minori, maggiori e critici e la durata. Quando si modifica una regola di avviso personalizzata, è anche possibile modificare il nome, la descrizione e le azioni consigliate della regola.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

Fasi

1. Selezionare **ALERTS > regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione corrispondente alla regola di avviso che si desidera modificare.
3. Selezionare **Modifica regola**.

Viene visualizzata la finestra di dialogo Edit Rule (Modifica regola). Questo esempio mostra una regola di avviso predefinita: I campi Nome univoco, Descrizione e azioni consigliate sono disattivati e non possono essere modificati.

Edit Rule - Low installed node memory

Enabled

Unique Name

Description

Recommended Actions (optional)

Conditions ?

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes < 24000000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes <= 12000000000"/>

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

4. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

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



Se si disattiva la regola di avviso per un avviso corrente, è necessario attendere alcuni minuti affinché l'avviso non venga più visualizzato come avviso attivo.



In generale, la disattivazione di una regola di avviso predefinita non è consigliata. Se una regola di avviso è disattivata, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

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



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

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche e-mail. I nomi delle regole di avviso possono essere compresi tra 1 e 64 caratteri.
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (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, immettere o aggiornare l'espressione Prometheus per uno o più livelli di gravità dell'avviso.



Se si desidera ripristinare il valore originale di una condizione per una regola di avviso predefinita modificata, selezionare i tre punti a destra della condizione modificata.

Conditions

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes < 2400000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes <= 1400000000"/>





Se si aggiornano le condizioni per un avviso corrente, le modifiche potrebbero non essere implementate fino a quando la condizione precedente non viene risolta. Al successivo soddisfacimento di una delle condizioni per la regola, l'avviso rifletterà i valori aggiornati.

Un'espressione di base è in genere della forma:

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

Le espressioni possono essere di qualsiasi lunghezza, ma vengono visualizzate su una singola riga dell'interfaccia utente. È richiesta almeno un'espressione.

Questa espressione attiva un avviso se la quantità di RAM installata per un nodo è inferiore a 24,000,000,000 byte (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

7. Nel campo **durata**, immettere il periodo di tempo in cui una condizione deve rimanere in vigore continuamente prima che l'allarme venga attivato, quindi selezionare l'unità di tempo.

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

L'impostazione predefinita è 5 minuti.

8. Selezionare **Salva**.

Se è stata modificata una regola di avviso predefinita, nella colonna tipo viene visualizzato **Default***. Se è stata disattivata una regola di avviso predefinita o personalizzata, nella colonna **Status** viene visualizzato **Disabled**.

Disattiva le regole di avviso

È possibile modificare lo stato attivato/disattivato per una regola di avviso predefinita o personalizzata.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

A proposito di questa attività

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



In generale, la disattivazione di una regola di avviso predefinita non è consigliata. Se una regola di avviso è disattivata, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

Fasi

1. Selezionare **ALERTS > regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione corrispondente alla regola di avviso che si desidera attivare o disattivare.
3. Selezionare **Modifica regola**.

Viene visualizzata la finestra di dialogo Edit Rule (Modifica regola).

4. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

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



Se si disattiva la regola di avviso per un avviso corrente, è necessario attendere alcuni minuti affinché l'avviso non venga più visualizzato come avviso attivo.

5. Selezionare **Salva**.

Disabled viene visualizzato nella colonna **Status**.

Rimuovere le regole di avviso personalizzate

È possibile rimuovere una regola di avviso personalizzata se non si desidera più utilizzarla.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

Fasi

1. Selezionare **ALERTS > regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione per la regola di avviso personalizzata che si desidera rimuovere.

Non è possibile rimuovere una regola di avviso predefinita.

3. Selezionare **Rimuovi regola personalizzata**.

Viene visualizzata una finestra di dialogo di conferma.

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

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

Gestire le notifiche di avviso

Impostare le notifiche SNMP per gli avvisi

Se si desidera che StorageGRID invii notifiche SNMP quando si verificano avvisi, è necessario attivare l'agente SNMP StorageGRID e configurare una o più destinazioni trap.

È possibile utilizzare l'opzione **CONFIGURAZIONE > monitoraggio > agente SNMP** in Gestione griglia o gli endpoint SNMP per l'API di gestione griglia per attivare e configurare l'agente SNMP StorageGRID. L'agente SNMP supporta tutte e tre le versioni del protocollo SNMP.

Per informazioni sulla configurazione dell'agente SNMP, vedere ["Utilizzare il monitoraggio SNMP"](#).

Dopo aver configurato l'agente SNMP StorageGRID, è possibile inviare due tipi di notifiche basate sugli eventi:

- I trap sono notifiche inviate dall'agente SNMP che non richiedono un riconoscimento da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che si è verificato qualcosa all'interno di StorageGRID, ad esempio un avviso attivato. I trap sono supportati in tutte e tre le versioni di SNMP.
- Le informazioni sono simili alle trap, ma richiedono un riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, invia nuovamente l'informazione fino a quando non viene ricevuta una conferma o non viene raggiunto il valore massimo di ripetizione. Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche di trap e notifica vengono inviate quando viene attivato un avviso predefinito o personalizzato a qualsiasi livello di gravità. Per eliminare le notifiche SNMP per un avviso, è necessario configurare un silenzio per l'avviso. Vedere ["Tacitare le notifiche di avviso"](#).

Se la distribuzione di StorageGRID include più nodi amministrativi, il nodo amministrativo primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport e le trap SNMP e le informazioni. Se il nodo di amministrazione primario non è più disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere ["Che cos'è un nodo amministratore?"](#).

Imposta le notifiche via email per gli avvisi

Se si desidera che le notifiche e-mail vengano inviate quando si verificano avvisi, è necessario fornire informazioni sul server SMTP. È inoltre necessario immettere gli indirizzi e-mail per i destinatari delle notifiche di avviso.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

A proposito di questa attività

La configurazione dell'e-mail utilizzata per le notifiche di avviso non viene utilizzata per i pacchetti AutoSupport. Tuttavia, è possibile utilizzare lo stesso server di posta elettronica per tutte le notifiche.

Se la distribuzione di StorageGRID include più nodi amministrativi, il nodo amministrativo primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport e le trap SNMP e le informazioni. Se il nodo di amministrazione primario non è più disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere ["Che cos'è un nodo amministratore?"](#).

Fasi

1. Selezionare **ALERTS > email setup**.

Viene visualizzata la pagina Configurazione e-mail.

2. Selezionare la casella di controllo **Enable Email Notifications** (attiva notifiche e-mail) per indicare che si desidera inviare e-mail di notifica quando gli avvisi raggiungono le soglie configurate.

Vengono visualizzate le sezioni Server e-mail (SMTP), TLS (Transport Layer Security), indirizzi e-mail e

filtri.

3. Nella sezione Server e-mail (SMTP), immettere le informazioni necessarie per l'accesso al server SMTP da parte di StorageGRID.

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

Campo	Invio
Server di posta	Il nome di dominio completo (FQDN) o l'indirizzo IP del server SMTP.
Porta	Porta utilizzata per accedere al server SMTP. Deve essere compreso tra 1 e 65535.
Nome utente (opzionale)	Se il server SMTP richiede l'autenticazione, immettere il nome utente con cui eseguire l'autenticazione.
Password (opzionale)	Se il server SMTP richiede l'autenticazione, immettere la password con cui eseguire l'autenticazione.

4. Nella sezione indirizzi e-mail, immettere gli indirizzi e-mail per il mittente e per ciascun destinatario.
 - a. Per **Sender Email Address**, specificare un indirizzo e-mail valido da utilizzare come indirizzo da per le notifiche degli avvisi.

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

- b. Nella sezione destinatari, immettere un indirizzo e-mail per ciascun elenco o persona che deve ricevere un'e-mail quando si verifica un avviso.

Selezionare l'icona più  per aggiungere i destinatari.

5. Se TLS (Transport Layer Security) è richiesto per le comunicazioni con il server SMTP, selezionare **Richiedi TLS** nella sezione Transport Layer Security (TLS).

- a. Nel campo **certificato CA**, fornire il certificato CA che verrà utilizzato per verificare l'identificazione del server SMTP.

È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfogli** e selezionare il file.

È necessario fornire un singolo file contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

- b. Selezionare la casella di controllo **Send Client Certificate** (Invia certificato client) se il server di posta SMTP richiede l'invio di certificati client per l'autenticazione da parte dei mittenti di posta elettronica.

- c. Nel campo **certificato client**, fornire il certificato client con codifica PEM da inviare al server SMTP.


È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfogli** e selezionare il file.

- d. Nel campo **Private Key** (chiave privata), immettere la chiave privata per il certificato client in codifica

PEM non crittografata.

È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfoggia** e selezionare il file.



Se è necessario modificare la configurazione della posta elettronica, selezionare l'icona a forma di matita  per aggiornare questo campo.

6. Nella sezione filtri, selezionare i livelli di severità degli avvisi che devono generare le notifiche via email, a meno che la regola per uno specifico avviso non sia stata tacitata.

Severità	Descrizione
Minore, maggiore, critico	Viene inviata una notifica via email quando viene soddisfatta la condizione minore, maggiore o critica di una regola di avviso.
Importante, critico	Viene inviata una notifica via email quando viene soddisfatta la condizione principale o critica per una regola di avviso. Le notifiche non vengono inviate per avvisi minori.
Solo critico	Una notifica via email viene inviata solo quando viene soddisfatta la condizione critica per una regola di avviso. Le notifiche non vengono inviate per avvisi minori o maggiori.

7. Quando si è pronti a verificare le impostazioni e-mail, attenersi alla seguente procedura:

- a. Selezionare **Invia email di prova**.

Viene visualizzato un messaggio di conferma che indica l'invio di un'e-mail di prova.

- b. Selezionare le caselle di posta in arrivo di tutti i destinatari e confermare che è stata ricevuta un'e-mail di prova.



Se l'e-mail non viene ricevuta entro pochi minuti o se viene attivato l'avviso **errore notifica e-mail**, controllare le impostazioni e riprovare.

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



Quando si verificano le notifiche di avviso, è necessario accedere a ogni nodo amministratore per verificare la connettività. Ciò è in contrasto con il test dei pacchetti AutoSupport, in cui tutti i nodi amministrativi inviano l'e-mail di prova.

8. Selezionare **Salva**.

L'invio di un'e-mail di prova non salva le impostazioni. Selezionare **Salva**.

Le impostazioni e-mail vengono salvate.

Informazioni incluse nelle notifiche e-mail di avviso

Dopo aver configurato il server di posta SMTP, le notifiche e-mail vengono inviate ai destinatari designati quando viene attivato un avviso, a meno che la regola di avviso non venga soppressa da un silenzio. Vedere

"Tacitare le notifiche di avviso".

Le notifiche e-mail includono le seguenti informazioni:

NetApp StorageGRID

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 4
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

DC1-S2-227

Node DC1-S2-227
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

Sent from: DC1-ADM1-225 5

Didascalìa	Descrizione
1	Il nome dell'avviso, seguito dal numero di istanze attive dell'avviso.
2	La descrizione dell'avviso.
3	Qualsiasi azione consigliata per l'avviso.
4	Dettagli su ogni istanza attiva dell'avviso, inclusi il nodo e il sito interessati, la severità dell'avviso, l'ora UTC in cui è stata attivata la regola di avviso e il nome del servizio e del processo interessati.
5	Il nome host del nodo amministratore che ha inviato la notifica.

Modalità di raggruppamento degli avvisi

Per impedire l'invio di un numero eccessivo di notifiche e-mail quando vengono attivati gli avvisi, StorageGRID tenta di raggruppare più avvisi nella stessa notifica.

Fare riferimento alla tabella seguente per alcuni esempi di come StorageGRID raggruppa più avvisi nelle notifiche e-mail.

Comportamento	Esempio
<p>Ogni notifica di avviso si applica solo agli avvisi con lo stesso nome. Se vengono attivati contemporaneamente due avvisi con nomi diversi, vengono inviate due notifiche e-mail.</p>	<ul style="list-style-type: none"> • L'avviso A viene attivato su due nodi contemporaneamente. 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 ogni avviso.
<p>Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di una severità, viene inviata una notifica solo per l'avviso più grave.</p>	<ul style="list-style-type: none"> • Viene attivato l'allarme A e vengono raggiunte le soglie di allarme minore, maggiore e critico. Viene inviata una notifica per l'avviso critico.
<p>La prima volta che viene attivato un avviso, StorageGRID attende 2 minuti prima di inviare una notifica. Se durante questo periodo vengono attivati altri avvisi con lo stesso nome, StorageGRID raggruppa tutti gli avvisi nella notifica iniziale.</p>	<ol style="list-style-type: none"> 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.
<p>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 (gli avvisi correnti che non sono stati tacitati), anche se precedentemente segnalati.</p>	<ol style="list-style-type: none"> 1. L'allarme A viene attivato sul nodo 1 alle 08:00. Viene inviata una notifica alle ore 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). Vengono segnalati entrambi i nodi.
<p>Se sono presenti più avvisi correnti 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 l'avviso è stato risolto.</p>	<ol style="list-style-type: none"> 1. L'avviso A viene attivato per il nodo 1. Viene inviata una notifica. 2. L'avviso 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'avviso A viene nuovamente attivato per il nodo 2. Non viene inviata alcuna nuova notifica perché l'avviso è ancora attivo per il nodo 1.
<p>StorageGRID continua a inviare notifiche via email ogni 7 giorni fino a quando tutte le istanze dell'avviso non vengono risolte o la regola dell'avviso non viene tacitata.</p>	<ol style="list-style-type: none"> 1. L'allarme A viene attivato per il nodo 1 l'8 marzo. Viene inviata una notifica. 2. L'avviso A non viene risolto o tacitato. Ulteriori notifiche verranno inviate il 15 marzo, il 22 marzo, il 29 marzo e così via.

Risolvere i problemi relativi alle notifiche email di avviso

Se viene attivato l'avviso **errore notifica email** o non si riesce a ricevere la notifica email di avviso del test, attenersi alla procedura descritta di seguito per risolvere il problema.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

Fasi

1. Verificare le impostazioni.
 - a. Selezionare **ALERTS > email setup**.
 - b. Verificare che le impostazioni del server e-mail (SMTP) siano corrette.
 - c. Verificare di aver specificato indirizzi e-mail validi per i destinatari.
2. Controllare il filtro antispam e assicurarsi che l'e-mail non sia stata inviata a una cartella di posta indesiderata.
3. Chiedi all'amministratore dell'email di confermare che le e-mail dell'indirizzo del mittente non vengono bloccate.
4. Raccogliere un file di log per l'Admin Node, quindi contattare il supporto tecnico.

Il supporto tecnico può utilizzare le informazioni contenute nei registri per determinare l'errore. Ad esempio, il file prometheus.log potrebbe visualizzare un errore durante la connessione al server specificato.

Vedere ["Raccogliere i file di log e i dati di sistema"](#).

Tacitare le notifiche di avviso

In alternativa, è possibile configurare le silenziosità in modo da eliminare temporaneamente le notifiche di avviso.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

A proposito di questa attività

È possibile disattivare le regole di avviso sull'intera griglia, su un singolo sito o su un singolo nodo e per una o più severità. Ogni silenzio elimina tutte le notifiche per una singola regola di avviso o per tutte le regole di avviso.

Se è stato attivato l'agente SNMP, le silenziosità sopprimono anche i trap SNMP e informano.



Prestare attenzione quando si decide di tacitare una regola di avviso. Se si tacita un avviso, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

Fasi

1. Selezionare **ALERTS > silences**.

Viene visualizzata la pagina Silences (silenziosità).

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create Edit Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
<i>No results found.</i>				

2. Selezionare **Crea**.

Viene visualizzata la finestra di dialogo Crea silenzio.

Create Silence

Alert Rule

Description (optional)

Duration Minutes

Severity Minor only Minor, major Minor, major, critical

Nodes

- StorageGRID Deployment
 - Data Center 1
 - DC1-ADM1
 - DC1-G1
 - DC1-S1
 - DC1-S2
 - DC1-S3

Cancel Save

3. Selezionare o inserire le seguenti informazioni:

Campo	Descrizione
Regola di avviso	<p>Il nome della regola di avviso che si desidera disattivare. È possibile selezionare qualsiasi regola di avviso predefinita o personalizzata, anche se la regola di avviso è disattivata.</p> <p>Nota: selezionare tutte le regole se si desidera disattivare tutte le regole di avviso utilizzando i criteri specificati in questa finestra di dialogo.</p>

Campo	Descrizione
Descrizione	Facoltativamente, una descrizione del silenzio. Ad esempio, descrivi lo scopo di questo silenzio.
Durata	Per quanto tempo si desidera che questo silenzio rimanga attivo, in minuti, ore o giorni. Un silenzio può essere in vigore da 5 minuti a 1,825 giorni (5 anni). Nota: non disattivare una regola di avviso per un periodo di tempo prolungato. Se una regola di avviso viene tacitata, è possibile che non si rilevi un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica. Tuttavia, potrebbe essere necessario utilizzare un silenzio esteso se un avviso viene attivato da una configurazione specifica e intenzionale, ad esempio per gli avvisi link down dell'appliance di servizi e link down dell'appliance di storage.
Severità	Quale severità o severità degli avvisi deve essere tacitata. Se l'avviso viene attivato in una delle severità selezionate, non viene inviata alcuna notifica.
Nodi	A quale nodo o nodi si desidera applicare questo silenzio. È possibile eliminare una regola di avviso o tutte le regole dell'intera griglia, di un singolo sito o di un singolo nodo. Se si seleziona l'intera griglia, il silenzio viene applicato a tutti i siti e a tutti i nodi. Se si seleziona un sito, il silenzio si applica solo ai nodi di quel sito. Nota: non è possibile selezionare più di un nodo o più siti per ogni silenzio. Se si desidera eliminare la stessa regola di avviso su più di un nodo o più siti contemporaneamente, è necessario creare silenzi aggiuntivi.

4. Selezionare **Salva**.

5. Se si desidera modificare o terminare un silenzio prima della scadenza, è possibile modificarlo o rimuoverlo.

Opzione	Descrizione
Modificare un silenzio	<ol style="list-style-type: none"> Selezionare ALERTS > silences. Dalla tabella, selezionare il pulsante di opzione relativo al silenzio che si desidera modificare. Selezionare Modifica. Modificare la descrizione, il tempo rimanente, le severità selezionate o il nodo interessato. Selezionare Salva.

Opzione	Descrizione
Eliminare un silenzio	<p>a. Selezionare ALERTS > silences.</p> <p>b. Dalla tabella, selezionare il pulsante di opzione per il silenzio che si desidera rimuovere.</p> <p>c. Selezionare Rimuovi.</p> <p>d. Selezionare OK per confermare che si desidera rimuovere questo silenzio.</p> <p>Nota: Le notifiche verranno inviate quando viene attivato questo avviso (a meno che non venga eliminato da un altro silenzio). Se questo avviso viene attivato, potrebbero essere necessari alcuni minuti per l'invio di notifiche e-mail o SNMP e per l'aggiornamento della pagina Avvisi.</p>

Informazioni correlate

["Configurare l'agente SNMP"](#)

Riferimenti agli avvisi

Questo riferimento elenca gli avvisi predefiniti visualizzati in Grid Manager. Le azioni consigliate sono contenute nel messaggio di avviso ricevuto.

Se necessario, è possibile creare regole di avviso personalizzate per adattarsi al proprio approccio di gestione del sistema.

Alcuni avvisi predefiniti utilizzano ["Metriche Prometheus"](#).

Avvisi sull'appliance

Nome dell'avviso	Descrizione
Batteria dell'appliance scaduta	La batteria del controller di storage dell'appliance è scaduta.
Batteria dell'appliance guasta	La batteria del controller di storage dell'appliance si è guastata.
La capacità appresa della batteria dell'appliance non è sufficiente	La capacità appresa della batteria nel controller di storage dell'appliance non è sufficiente.
Batteria dell'apparecchio quasi scaduta	La batteria del controller di storage dell'appliance sta per scadere.
Batteria dell'apparecchio rimossa	La batteria nel controller di storage dell'appliance non è presente.
Batteria dell'apparecchio troppo calda	La batteria del controller di storage dell'apparecchio è surriscaldata.
Errore di comunicazione BMC dell'appliance	La comunicazione con il BMC (Baseboard Management Controller) è stata persa.

Nome dell'avviso	Descrizione
Rilevato guasto del dispositivo di avvio dell'apparecchio	È stato rilevato un problema con il dispositivo di avvio nell'apparecchio.
Periferica di backup della cache dell'appliance non riuscita	Si è verificato un errore in una periferica di backup della cache persistente.
Capacità insufficiente del dispositivo di backup della cache dell'appliance	La capacità della periferica di backup della cache è insufficiente.
Dispositivo di backup cache dell'appliance protetto da scrittura	Una periferica di backup della cache è protetta da scrittura.
Mancata corrispondenza delle dimensioni della memoria cache dell'appliance	I due controller dell'appliance hanno dimensioni della cache diverse.
Guasto della batteria CMOS dell'apparecchio	È stato rilevato un problema con la batteria CMOS dell'apparecchio.
Temperatura dello chassis del controller di calcolo dell'appliance troppo alta	La temperatura del controller di calcolo in un'appliance StorageGRID ha superato una soglia nominale.
Temperatura CPU del controller di calcolo dell'appliance troppo alta	La temperatura della CPU nel controller di calcolo di un'appliance StorageGRID ha superato una soglia nominale.
Il controller di calcolo dell'appliance richiede attenzione	È stato rilevato un guasto hardware nel controller di calcolo di un'appliance StorageGRID.
Si è verificato un problema nell'alimentatore A del controller di calcolo dell'appliance	L'alimentazione A nel controller di calcolo presenta un problema.
Si è verificato un problema nell'alimentatore B del controller di calcolo dell'appliance	L'alimentazione B nel controller di calcolo presenta un problema.
Il servizio di monitoraggio dell'hardware di calcolo dell'appliance si è bloccato	Il servizio che monitora lo stato dell'hardware dello storage si è bloccato.
Unità DAS dell'appliance che supera il limite per i dati scritti al giorno	Una quantità eccessiva di dati viene scritta su un'unità ogni giorno, il che potrebbe invalidare la garanzia.

Nome dell'avviso	Descrizione
Rilevato guasto al disco DAS dell'appliance	È stato rilevato un problema con un disco DAS (Direct-Attached Storage) nell'appliance.
Spia localizzatore unità DAS dell'appliance accesa	La spia di posizionamento dell'unità per una o più unità DAS (Direct-Attached Storage) in un nodo di archiviazione dell'appliance è accesa.
Ricostruzione del disco DAS dell'appliance	È in corso la ricostruzione di un disco DAS (Direct-Attached Storage). Questo è previsto se è stato sostituito o rimosso/reinserito di recente.
Rilevato guasto alla ventola dell'appliance	È stato rilevato un problema relativo alla ventola dell'apparecchio.
Rilevato guasto nel Fibre Channel dell'appliance	È stato rilevato un problema di collegamento Fibre Channel tra lo storage controller dell'appliance e il controller di calcolo
Errore della porta HBA Fibre Channel dell'appliance	Una porta HBA Fibre Channel si sta guastando o si è guastata.
Unità flash cache dell'appliance non ottimali	I dischi utilizzati per la cache SSD non sono ottimali.
Interconnessione dell'appliance/contenitore della batteria rimosso	Il contenitore di interconnessione/batteria non è presente.
Porta LACP dell'appliance mancante	Una porta su un'appliance StorageGRID non partecipa al bond LACP.
Rilevato guasto alla scheda NIC dell'appliance	È stato rilevato un problema con una scheda di interfaccia di rete (NIC) nell'appliance.
Alimentatore generale dell'appliance degradato	La potenza di un'appliance StorageGRID è diversa dalla tensione di esercizio consigliata.
Avviso critico SSD dell'appliance	Un'appliance SSD sta segnalando un avviso critico.
Guasto del controller dello storage dell'appliance A.	Si è verificato un errore nel controller storage A di un'appliance StorageGRID.
Guasto del controller storage dell'appliance B.	Il controller dello storage B in un'appliance StorageGRID si è guastato.
Guasto al disco del controller dello storage dell'appliance	Uno o più dischi di un'appliance StorageGRID si sono guastati o non sono ottimali.

Nome dell'avviso	Descrizione
Problema hardware del controller dello storage dell'appliance	Il software SANtricity segnala "richiede attenzione" per un componente di un'appliance StorageGRID.
Guasto all'alimentazione Del controller dello storage dell'appliance A.	L'alimentazione A di un'appliance StorageGRID non è conforme alla tensione di esercizio consigliata.
Guasto all'alimentazione B del controller storage dell'appliance	L'alimentazione B di un apparecchio StorageGRID non è conforme alla tensione di esercizio consigliata.
Il servizio di monitoraggio hardware dello storage dell'appliance si è bloccato	Il servizio che monitora lo stato dell'hardware dello storage si è bloccato.
Gli shelf di storage delle appliance sono degradati	Lo stato di uno dei componenti dello shelf di storage di un'appliance di storage è degradato.
Temperatura dell'apparecchio superata	La temperatura nominale o massima del controller di storage dell'appliance è stata superata.
Sensore di temperatura dell'apparecchio rimosso	È stato rimosso un sensore di temperatura.
Errore di avvio protetto UEFI dell'appliance	Un'appliance non è stata avviata in modo sicuro.
L'i/o del disco è molto lento	La lentezza dell'i/o del disco potrebbe influire sulle prestazioni della griglia.
Rilevato guasto alla ventola dell'appliance di storage	È stato rilevato un problema con un'unità ventola nel controller di storage di un'appliance.
La connettività dello storage dell'appliance di storage è degradata	Si è verificato un problema con una o più connessioni tra il controller di calcolo e il controller dello storage.
Dispositivo di storage inaccessibile	Impossibile accedere a un dispositivo di storage.

Avvisi di audit e syslog

Nome dell'avviso	Descrizione
I registri di controllo vengono aggiunti alla coda in-memory	Il nodo non può inviare i log al server syslog locale e la coda in-memory si sta riempiendo.

Nome dell'avviso	Descrizione
Errore di inoltrato del server syslog esterno	Il nodo non può inoltrare i log al server syslog esterno.
Coda di audit di grandi dimensioni	La coda dei dischi per i messaggi di controllo è piena. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
I registri vengono aggiunti alla coda su disco	Il nodo non può inoltrare i log al server syslog esterno e la coda su disco si sta riempiendo.

Avvisi bucket

Nome dell'avviso	Descrizione
Il bucket FabricPool ha un'impostazione di coerenza del bucket non supportata	Un bucket FabricPool utilizza il livello di coerenza disponibile o di sito sicuro, che non è supportato.
Il bucket FabricPool ha un'impostazione di versione non supportata	In un bucket FabricPool è abilitata la versione o il blocco degli oggetti S3, che non sono supportati.

Avvisi Cassandra

Nome dell'avviso	Descrizione
Errore compattatore automatico Cassandra	Si è verificato un errore nel compattatore automatico Cassandra.
Metriche del compattatore automatico Cassandra non aggiornate	Le metriche che descrivono il compattatore automatico Cassandra non sono aggiornate.
Errore di comunicazione Cassandra	I nodi che eseguono il servizio Cassandra hanno problemi di comunicazione tra loro.
Le compaction di Cassandra sono sovraccaricate	Il processo di compattazione Cassandra è sovraccarico.
Errore di scrittura Cassandra oversize	Un processo StorageGRID interno ha inviato a Cassandra una richiesta di scrittura troppo grande.
Metriche di riparazione Cassandra non aggiornate	Le metriche che descrivono i lavori di riparazione Cassandra non sono aggiornate.

Nome dell'avviso	Descrizione
Il processo di riparazione di Cassandra è lento	Il progresso delle riparazioni del database Cassandra è lento.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione Cassandra non è disponibile.
Tabella Cassandra corrotta	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva la corruzione della tabella.

Avvisi Cloud Storage Pool

Nome dell'avviso	Descrizione
Errore di connettività del pool di cloud storage	Il controllo dello stato di salute dei Cloud Storage Pools ha rilevato uno o più nuovi errori.
IAM Roles Anywhere End-Entity Certification Expiration	Il certificato IAM Roles Anywhere End-Entity sta per scadere.

Avvisi di replica cross-grid

Nome dell'avviso	Descrizione
Errore permanente della replica cross-grid	Si è verificato un errore di replica cross-grid che richiede l'intervento dell'utente per la risoluzione.
Risorse di replica cross-grid non disponibili	Le richieste di replica cross-grid sono in sospeso perché una risorsa non è disponibile.

Avvisi DHCP

Nome dell'avviso	Descrizione
Lease DHCP scaduto	Il lease DHCP su un'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 traccia

Nome dell'avviso	Descrizione
Impatto delle performance di debug	Quando la modalità di debug è attivata, le prestazioni del sistema potrebbero risentirne negativamente.

Nome dell'avviso	Descrizione
Configurazione traccia attivata	Quando la configurazione di tracce è attivata, le prestazioni del sistema potrebbero risentire negativamente.

Avvisi e-mail e AutoSupport

Nome dell'avviso	Descrizione
Impossibile inviare il messaggio AutoSupport	Impossibile inviare il messaggio AutoSupport più recente.
Errore di risoluzione del nome di dominio	Il nodo StorageGRID non è stato in grado di risolvere i nomi di dominio.
Errore di notifica e-mail	Impossibile inviare la notifica via email per un avviso.
Errori di notifica SNMP	Errori durante l'invio di notifiche di notifica SNMP a una destinazione trap.
Rilevato accesso SSH o console	Nelle ultime 24 ore, un utente ha effettuato l'accesso con la console Web o SSH.

Erasure coding (EC) alerts (Avvisi di codifica di cancellazione)

Nome dell'avviso	Descrizione
Errore di ribilanciamento EC	La procedura di ribilanciamento EC non è riuscita o è stata interrotta.
Errore di riparazione EC	Un intervento di riparazione per i dati EC non è riuscito o è stato interrotto.
Riparazione EC in stallo	Un intervento di riparazione per i dati EC si è bloccato.
Errore di verifica dei frammenti sottoposti a erasure coding	I frammenti sottoposti a erasure coding non possono più essere verificati. I frammenti corrotti potrebbero non essere riparati.

Scadenza degli avvisi relativi ai certificati

Nome dell'avviso	Descrizione
Scadenza certificato CA proxy amministratore	Uno o più certificati nel pacchetto CA del server proxy amministratore stanno per scadere.
Scadenza del certificato client	Uno o più certificati client stanno per scadere.

Nome dell'avviso	Descrizione
Scadenza del certificato server globale per S3 e Swift	Il certificato server globale per S3 e Swift sta per scadere.
Scadenza del certificato endpoint del bilanciamento del carico	Uno o più certificati endpoint per il bilanciamento del carico 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 client syslog esterno	Il certificato client per un server syslog esterno sta per scadere.
Scadenza del certificato del server syslog esterno	Il certificato del server presentato dal server syslog esterno sta per scadere.

Avvisi Grid Network

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

Avvisi di federazione delle griglie

Nome dell'avviso	Descrizione
Scadenza del certificato di federazione griglia	Uno o più certificati di federazione griglia stanno per scadere.
Errore di connessione alla federazione di griglie	La connessione a federazione di griglie tra la rete locale e remota non funziona.

Avvisi di utilizzo elevato o latenza elevata

Nome dell'avviso	Descrizione
Elevato utilizzo di heap Java	Viene utilizzata una percentuale elevata di spazio heap Java.
Latenza elevata per le query sui metadati	Il tempo medio per le query dei metadati Cassandra è troppo lungo.

Avvisi di Identity Federation

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

Avvisi ILM (Information Lifecycle Management)

Nome dell'avviso	Descrizione
Posizionamento ILM non raggiungibile	Non è possibile ottenere un'istruzione di posizionamento in una regola ILM per determinati oggetti.
Velocità di scansione ILM bassa	La velocità di scansione ILM è impostata su un valore inferiore a 100 oggetti/secondo.

Avvisi del server di gestione delle chiavi (KMS)

Nome dell'avviso	Descrizione
Scadenza del certificato CA KMS	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server di gestione delle chiavi (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 riuscita a caricarsi.
Errore di connettività KMS	Un nodo appliance non è riuscito a connettersi al server di gestione delle chiavi del proprio sito.
Nome chiave di crittografia KMS non trovato	Il server di gestione delle chiavi configurato non dispone di una chiave di crittografia corrispondente al nome fornito.
Rotazione della chiave di crittografia KMS non riuscita	Tutti i volumi dell'appliance sono stati decifrati correttamente, ma uno o più volumi non sono stati ruotati sulla chiave più recente.
KMS non configurato	Non esiste alcun server di gestione delle chiavi per questo sito.
La chiave KMS non è riuscita a decrittare un volume dell'appliance	Non è stato possibile decifrare uno o più volumi su un'appliance con crittografia del nodo abilitata con la chiave KMS corrente.

Nome dell'avviso	Descrizione
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 appliance non è stato in grado di connettersi a uno o più server nel cluster del server di gestione delle chiavi per il sito.

Avvisi per il bilanciamento del carico

Nome dell'avviso	Descrizione
Collegamenti del bilanciatore di carico a richiesta zero elevati	Una percentuale elevata di connessioni agli endpoint del bilanciatore di carico disconnesse senza eseguire richieste.

Avvisi di offset dell'orologio locale

Nome dell'avviso	Descrizione
Grande offset temporale dell'orologio locale	L'offset tra l'orologio locale e l'ora NTP (Network Time Protocol) è troppo elevato.

Avvisi di memoria insufficiente o spazio insufficiente

Nome dell'avviso	Descrizione
Bassa capacità del disco di log di audit	Lo spazio disponibile per i registri di controllo è insufficiente. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
Memoria del nodo a bassa disponibilità	La quantità di RAM disponibile su un nodo è bassa.
Spazio libero ridotto per il pool di storage	Lo spazio disponibile per memorizzare i dati dell'oggetto nel nodo di storage è basso.
Memoria del nodo installata insufficiente	La quantità di memoria installata su un nodo è bassa.
Storage dei metadati basso	Lo spazio disponibile per memorizzare i metadati degli oggetti è basso.
Capacità disco di metriche ridotte	Lo spazio disponibile per il database delle metriche è basso.
Storage dei dati a oggetti basso	Lo spazio disponibile per memorizzare i dati degli oggetti è basso.
Override del watermark di sola lettura bassa	L'override del watermark di sola lettura soft del volume di archiviazione è inferiore al watermark ottimizzato minimo per un nodo di archiviazione.

Nome dell'avviso	Descrizione
Bassa capacità del disco root	Lo spazio disponibile sul disco root è insufficiente.
Bassa capacità dei dati di sistema	Lo spazio disponibile per /var/local è basso. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
Spazio libero nella directory tmp basso	Lo spazio disponibile nella directory /tmp è insufficiente.

Avvisi di rete di nodi o nodi

Nome dell'avviso	Descrizione
Utilizzo ricezione rete amministratore	L'utilizzo della ricezione nella rete amministrativa è elevato.
Uso della trasmissione della rete di amministrazione	L'utilizzo della 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 ricadono troppo a lungo sulle porte predefinite.
Errore di connettività di rete del nodo	Si sono verificati errori durante il trasferimento dei dati tra nodi.
Errore frame ricezione rete nodo	Un'elevata percentuale di frame di rete ricevuti da un nodo presenta errori.
Nodo non sincronizzato con il server NTP	Il nodo non è sincronizzato con il server NTP (Network Time Protocol).
Nodo non bloccato con server NTP	Il nodo non è bloccato su un server NTP (Network Time Protocol).
Rete del nodo non appliance non in funzione	Uno o più dispositivi di rete sono disconnessi o non attivi.
Collegamento dell'appliance di servizi alla rete di amministrazione	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.
Collegamento dell'appliance di servizi alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa.

Nome dell'avviso	Descrizione
Collegamento dell'appliance di servizi alla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 2	La porta di rete 2 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 3	La porta di rete 3 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage in Admin Network	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.
Collegamento dell'appliance di storage alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa.
Collegamento dell'appliance di storage alla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di storage inattivo sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 2	La porta di rete 2 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 3	La porta di rete 3 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o scollegata.
Nodo di storage non 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

Nome dell'avviso	Descrizione
Utilizzo della connessione TCP	Il numero di connessioni TCP su questo nodo si avvicina al numero massimo che è possibile tenere traccia.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono o non è possibile raggiungere il nodo.
Riavvio del nodo imprevisto	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore.

Avvisi a oggetti

Nome dell'avviso	Descrizione
Controllo dell'esistenza dell'oggetto non riuscito	Il processo di controllo dell'esistenza dell'oggetto non è riuscito.
Controllo dell'esistenza dell'oggetto bloccato	Il lavoro di verifica dell'esistenza dell'oggetto si è bloccato.
Oggetti persi	Uno o più oggetti sono stati persi dalla griglia.
S3 HA POSTO la dimensione dell'oggetto troppo grande	Un client sta tentando di eseguire un'operazione PUT Object che supera i limiti di dimensione 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 sui servizi della piattaforma

Nome dell'avviso	Descrizione
Richiesta di servizi piattaforma in sospeso capacità bassa	Il numero di richieste in sospeso di Platform Services si sta avvicinando alla capacità.
Servizi della piattaforma non disponibili	In un sito sono in esecuzione o disponibili troppi nodi di storage con il servizio RSM.

Avvisi sul volume di storage

Nome dell'avviso	Descrizione
Il volume di storage richiede attenzione	Un volume di storage è offline e richiede attenzione.
Il volume di storage deve essere ripristinato	Un volume di storage è stato ripristinato e deve essere ripristinato.

Nome dell'avviso	Descrizione
Volume di storage offline	Un volume di archiviazione è stato offline per più di 5 minuti.
Tentativo di rimontaggio del volume di storage	Un volume di storage era offline e attivava un rimontaggio automatico. Ciò potrebbe indicare un problema dell'unità o errori del file system.
Ripristino volume non riuscito ad avviare la riparazione dei dati replicati	Impossibile avviare automaticamente la riparazione dei dati replicati per un volume riparato.

Avvisi dei servizi StorageGRID

Nome dell'avviso	Descrizione
servizio nginx con configurazione di backup	La configurazione del servizio nginx non è valida. È in uso la configurazione precedente.
servizio nginx-gw con configurazione di backup	La configurazione del servizio nginx-gw non è valida. È in uso la configurazione precedente.
Riavvio necessario per disattivare FIPS	Il criterio di protezione non richiede la modalità FIPS, ma il modulo di protezione crittografico NetApp è attivato.
Riavvio necessario per attivare FIPS	Il criterio di protezione richiede la modalità FIPS, ma il modulo di protezione crittografico NetApp è disattivato.
Servizio SSH con configurazione di backup	La configurazione del servizio SSH non è valida. È in uso la configurazione precedente.

Avvisi del tenant

Nome dell'avviso	Descrizione
Utilizzo elevato della quota del tenant	Viene utilizzata un'elevata percentuale di spazio di quota. Questa regola è disattivata per impostazione predefinita perché potrebbe causare un numero eccessivo di notifiche.

Metriche Prometheus comunemente utilizzate

Fare riferimento a questo elenco di metriche Prometheus comunemente utilizzate per comprendere meglio le condizioni nelle regole di avviso predefinite o per creare le condizioni per le regole di avviso personalizzate.

È anche possibile [ottenere un elenco completo di tutte le metriche](#).

Per informazioni dettagliate sulla sintassi delle query Prometheus, vedere "[Interrogazione di Prometheus](#)".

Quali sono le metriche 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 Prometheus non è pieno. Quando il `/var/local/mysql_ibdata/` volume raggiunge la capacità, vengono eliminate per prime le metriche più vecchie.

Dove vengono utilizzate le metriche Prometheus?

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

- **Pagina nodi:** I grafici e i grafici nelle schede disponibili nella pagina nodi utilizzano lo strumento di visualizzazione Grafana per visualizzare le metriche delle serie temporali raccolte da Prometheus. Grafana visualizza i dati delle serie temporali in formato grafico e grafico, mentre Prometheus funge da origine dei dati back-end.



- **Avvisi:** Gli avvisi vengono attivati a livelli di severità specifici quando le condizioni delle regole di avviso che utilizzano le metriche Prometheus valutano come vero.
- **API per la gestione dei grid:** Puoi utilizzare le metriche Prometheus in regole di avviso personalizzate o con strumenti di automazione esterni per monitorare il tuo sistema StorageGRID. Un elenco completo delle metriche Prometheus è disponibile nell'API Grid Management. (Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API > metriche**). Sebbene siano disponibili più di mille metriche, per monitorare le operazioni StorageGRID più critiche è necessario solo un numero relativamente ridotto.



Le metriche che includono *private* nei loro nomi sono destinate esclusivamente all'uso interno e sono soggette a modifiche tra le release di StorageGRID senza preavviso.

- La pagina **SUPPORT > Tools > Diagnostics** e la pagina **SUPPORT > Tools > Metrics**: Queste pagine, destinate principalmente al supporto tecnico, forniscono diversi tool e grafici che utilizzano i valori delle metriche Prometheus.



Alcune funzioni e voci di menu della pagina metriche sono intenzionalmente non funzionali 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* nei loro nomi sono solo per uso interno e sono soggette a modifiche senza preavviso tra le release di StorageGRID.

alertmanager_notifications_failed_total

Il numero totale di notifiche di avviso non riuscite.

node_filesystem_avail_bytes

La quantità di spazio del file system disponibile in byte per gli utenti non root.

Node_Memory_MemAvailable_Bytes

Campo delle informazioni sulla memoria MemAvailable_Bytes.

node_network_carrier

Valore portante di `/sys/class/net/iface`.

node_network_receive_errs_total

Statistica periferica di rete `receive_errs`.

node_network_transmit_errs_total

Statistica periferica di rete `transmit_errs`.

storagegrid_administively_down

Il nodo non è connesso alla rete per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento.

storagegrid_appliance_compute_controller_hardware_status

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

storagegrid_appliance_failed_disks

Per lo storage controller di un'appliance, il numero di dischi non ottimali.

storagegrid_appliance_storage_controller_hardware_status

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

storagegrid_content_bucket_and_containers

Il numero totale di bucket S3 e container Swift noti da questo nodo di storage.

storagegrid_content_objects

Il numero totale di oggetti dati S3 e Swift noti da questo nodo di storage. Il conteggio è valido solo per gli oggetti dati creati dalle applicazioni client che si interfacciano con il sistema tramite S3.

storagegrid_content_objects_lost

Il numero totale di oggetti che il servizio rileva come mancanti dal sistema StorageGRID. È necessario intraprendere azioni per determinare la causa della perdita e se è possibile eseguire il ripristino.

["Risolvere i problemi relativi ai dati degli oggetti persi e mancanti"](#)

storagegrid_http_sessions_incoming_tented

Il numero totale di sessioni HTTP che sono state tentate per un nodo di storage.

storagegrid_http_sessions_incoming_currently_established

Il numero di sessioni HTTP attualmente attive (aperte) sul nodo di storage.

storagegrid_http_sessions_incoming_failed

Il numero totale di sessioni HTTP che non sono riuscite a completare correttamente, 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 correttamente.

storagegrid_ilm_waiting_background_objects

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

storagegrid_ilm_waiting_client_evaluation_objects_per_second

La velocità corrente alla quale gli oggetti vengono valutati in base al criterio ILM su questo nodo.

storagegrid_ilm_waiting_client_objects

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

storagegrid_ilm_waiting_total_objects

Il numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_objects_per_second

La velocità con cui gli oggetti di proprietà di questo nodo vengono sottoposti a scansione e messi in coda per ILM.

storagegrid_ilm_scan_period_estimated_minutes

Il 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.

storagegrid_load_balancer_endpoint_cert_expiry_time

Il tempo di scadenza del certificato endpoint del bilanciamento del carico in secondi dall'epoca.

storagegrid_metadata_queries_average_latency_milliseconds

Il tempo medio richiesto per eseguire una query sull'archivio di metadati tramite questo servizio.

storagegrid_network_received_bytes

La quantità totale di dati ricevuti dall'installazione.

storagegrid_network_transmitted_bytes

La quantità totale di dati inviati dall'installazione.

storagegrid_node_cpu_utilization_percent

La percentuale di tempo CPU disponibile attualmente utilizzata da questo servizio. Indica la disponibilità del servizio. La quantità di tempo CPU disponibile dipende dal numero di CPU del server.

storagegrid_ntp_chouged_time_source_offset_millisecondi

Offset sistematico del tempo fornito da una fonte di tempo scelta. L'offset viene introdotto quando il ritardo per raggiungere un'origine temporale non è uguale al tempo richiesto per l'origine temporale per raggiungere il client NTP.

storagegrid_ntp_locked

Il nodo non è bloccato su un server NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

La quantità totale di dati acquisiti dai client S3 a questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_s3_data_transfers_bytes_retrieved

La quantità totale di dati recuperati dai client S3 da questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_s3_operations_failed

Il numero totale di operazioni S3 non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da un errore di autorizzazione S3.

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_unauthorized

Il numero totale di operazioni S3 non riuscite che sono il risultato di un errore di autorizzazione.

storagegrid_servercertificate_management_interface_cert_expiry_days

Il numero di giorni prima della scadenza del certificato dell'interfaccia di gestione.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

Il numero di giorni prima della scadenza del certificato API dello storage a oggetti.

storagegrid_service_cpu_seconds

La quantità di tempo cumulativa in cui la CPU è stata utilizzata da questo servizio dopo l'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 principale di Linux come RES.

storagegrid_service_network_received_bytes

La quantità totale di dati ricevuti dal servizio dopo l'installazione.

storagegrid_service_network_transmitted_bytes

La quantità totale di dati inviati da questo servizio.

storagegrid_service_reavvies

Il numero totale di riavvii del servizio.

storagegrid_service_runtime_seconds

Il tempo totale di esecuzione del servizio dopo l'installazione.

storagegrid_service_uptime_seconds

Il tempo totale di esecuzione del servizio dall'ultimo riavvio.

storagegrid_storage_state_current

Lo stato corrente dei servizi di storage. I valori degli attributi sono:

- 10 = non in linea
- 15 = manutenzione
- 20 = sola lettura
- 30 = Online

storagegrid_storage_status

Lo stato corrente dei servizi di storage. I valori degli attributi sono:

- 0 = Nessun errore
- 10 = in transizione
- 20 = spazio libero insufficiente
- 30 = Volume(i) non disponibile
- 40 = errore

storagegrid_storage_utilization_data_bytes

Una stima delle dimensioni totali dei dati di oggetti replicati e con erasure coding sul nodo storage.

storagegrid_storage_utilization_metadata_allowed_bytes

Lo spazio totale sul volume 0 di ciascun nodo di storage consentito per i metadati dell'oggetto. Questo valore è sempre inferiore allo spazio effettivo riservato ai metadati su un nodo, perché una parte dello spazio riservato è necessaria per le operazioni essenziali del database (come la compattazione e la riparazione) e i futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati dell'oggetto controlla la capacità complessiva degli oggetti.

storagegrid_storage_utilization_metadata_bytes

La quantità di metadati oggetto sul volume di storage 0, in byte.

storagegrid_storage_utilization_total_space_bytes

La quantità totale di spazio di storage allocato a tutti gli archivi di oggetti.

storagegrid_storage_utilization_usable_space_bytes

La quantità totale di spazio di storage a oggetti rimanente. Calcolato sommando la quantità di spazio disponibile per tutti gli archivi di oggetti sul nodo di storage.

storagegrid_swift_data_transfers_bytes_ingested

La quantità totale di dati acquisiti dai client Swift a questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_swift_data_transfers_bytes_retrieved

La quantità totale di dati recuperati dai client Swift da questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_swift_operations_failed

Il numero totale di operazioni Swift non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da un errore di autorizzazione Swift.

storagegrid_swift_operations_successful

Il numero totale di operazioni Swift riuscite (codice di stato HTTP 2xx).

storagegrid_swift_operations_inhautorizzata

Il numero totale di operazioni Swift non riuscite che sono il risultato di un errore di autorizzazione (codici di stato HTTP 401, 403, 405).

storagegrid_tenant_usage_data_bytes

La dimensione logica di tutti gli oggetti per il tenant.

storagegrid_tenant_usage_object_count

Il numero di oggetti per il tenant.

storagegrid_tenant_usage_quota_byte

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, utilizza l'API Grid Management.

1. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
2. Individuare le operazioni **metriche**.
3. Eseguire l'`GET /grid/metric-names` operazione.
4. Scarica i risultati.

Riferimenti ai file di log

Riferimenti ai file di log

StorageGRID fornisce registri utilizzati per acquisire eventi, messaggi di diagnostica e condizioni di errore. Potrebbe essere richiesto di raccogliere i file di log e inoltrarli al supporto tecnico per agevolare la risoluzione dei problemi.

I log sono classificati come segue:

- ["Log del software StorageGRID"](#)
- ["Log di implementazione e manutenzione"](#)
- ["A proposito di bycast.log"](#)



I dettagli forniti per ciascun tipo di registro sono solo a scopo di riferimento. I registri sono destinati al troubleshooting avanzato da parte del supporto tecnico. Le tecniche avanzate che implicano la ricostruzione della cronologia dei problemi utilizzando i registri di controllo e i file di log dell'applicazione esulano dall'ambito di queste istruzioni.

Accedere ai registri

Per accedere ai registri, è possibile ["raccolgere i file di log e i dati di sistema"](#) da uno o più nodi come singolo archivio di file di registro. In alternativa, se il nodo di amministrazione primario non è disponibile o non è in grado di raggiungere un nodo specifico, è possibile accedere ai singoli file di registro per ciascun nodo della griglia come segue:

1. Immettere il seguente comando: `ssh admin@grid_node_IP`
2. Immettere la password elencata nel `Passwords.txt` file.
3. Immettere il seguente comando per passare alla directory principale: `su -`
4. Immettere la password elencata nel `Passwords.txt` file.

Esportare i log nel server syslog

L'esportazione dei registri al server syslog offre le seguenti funzionalità:

- Ricevi un elenco di tutte le richieste di Grid Manager e Tenant Manager, oltre alle richieste S3 e Swift.
- Migliore visibilità delle richieste S3 che restituiscono errori, senza l'impatto sulle prestazioni causato dai metodi di registrazione degli audit.
- Accesso alle richieste del livello HTTP e ai codici di errore facili da analizzare.
- Migliore visibilità delle richieste bloccate dai classificatori del traffico nel bilanciamento del carico.

Per esportare i registri, fare riferimento alla ["Configurare i messaggi di audit e le destinazioni dei log"](#).

Categorie di file di log

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

Percorso di archiviazione	Descrizione
audit	Messaggi di audit generati durante il normale funzionamento del sistema.
log-sistema-di-base	Informazioni di base sul sistema operativo, incluse le versioni delle immagini StorageGRID.
bundle	Informazioni sulla configurazione globale (bundle).
cassandra	Informazioni sul database Cassandra e registri di riparazione Reaper.
ce	Informazioni sui VCSs relative al nodo corrente e informazioni sul gruppo EC in base all'ID del profilo.
griglia	Log generali della griglia, inclusi debug (<code>bycast.log</code>) e <code>servermanager</code> log.
grid.json	File di configurazione della griglia condiviso tra tutti i nodi. Inoltre, <code>node.json</code> è specifico per il nodo corrente.

Percorso di archiviazione	Descrizione
hagroup	Metriche e registri dei gruppi ad alta disponibilità.
installare	Gdu-server e installare i registri.
Arbitro lambda	Registri relativi alla richiesta del proxy S3 Select.
lumberjack.log	Messaggi di debug relativi alla raccolta dei log.
Metriche	Log di servizio per Grafana, Jaeger, node exporter e Prometheus.
errore	Accesso Miscd e log degli errori.
mysql	La configurazione del database MariaDB e i relativi log.
netto	Log generati da script correlati alla rete e dal servizio Dynip.
nginx	File e log di configurazione del bilanciamento del carico e della federazione di griglie. Include anche i log di traffico di Grid Manager e Tenant Manager.

Percorso di archiviazione	Descrizione
nginx-gw	<ul style="list-style-type: none"> • <code>access.log</code>: Grid Manager e Tenant Manager richiedono messaggi di registrazione. <ul style="list-style-type: none"> ◦ Questi messaggi sono preceduti da <code>mgmt</code>: quando vengono esportati utilizzando <code>syslog</code>. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$request" "\$http_host" "\$http_user_agent" "\$http_referer"</code> • <code>cgr-access.log.gz</code>: Richieste di replica cross-grid in entrata. <ul style="list-style-type: none"> ◦ Questi messaggi sono preceduti da <code>cgr</code>: quando vengono esportati utilizzando <code>syslog</code>. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$supstream_addr" "\$request" "\$http_host"</code> • <code>endpoint-access.log.gz</code>: S3 e Swift richiedono di caricare gli endpoint del bilanciatore. <ul style="list-style-type: none"> ◦ Questi messaggi sono preceduti da <code>endpoint</code>: quando vengono esportati utilizzando <code>syslog</code>. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$supstream_addr" "\$request" "\$http_host"</code> • <code>nginx-gw-dns-check.log</code>: Relativo al nuovo avviso di controllo DNS.
ntp	File di configurazione NTP e registri.
Oggetti orfani	Registri relativi agli oggetti orfani.
sistema operativo	File di stato nodo e griglia, inclusi i servizi <code>pid</code> .
altro	I file di registro in <code>/var/local/log</code> che non vengono raccolti in altre cartelle.
perf	Informazioni sulle prestazioni per CPU, rete e i/o del disco
prometheus-data	Metriche Prometheus correnti, se la raccolta di log include i dati Prometheus.
provisioning	Log relativi al processo di provisioning della griglia.
zattera	Log dal cluster Raft utilizzato nei servizi della piattaforma.

Percorso di archiviazione	Descrizione
ssh	Registri relativi alla configurazione e al servizio SSH.
snmp	Configurazione dell'agente SNMP utilizzata per l'invio di notifiche SNMP.
socket-dati	Dati socket per il debug di rete.
system-commands.txt	Output dei comandi del container StorageGRID. Contiene informazioni di sistema, ad esempio le reti e l'utilizzo del disco.
pacchetto-ripristino-sincronizzazione	Correlato al mantenimento della coerenza del pacchetto di ripristino più recente in tutti i nodi amministrativi e di archiviazione che ospitano il servizio ADC.

Log del software StorageGRID

È possibile utilizzare i registri di StorageGRID per risolvere i problemi.



Se si desidera inviare i registri a un server syslog esterno o modificare la destinazione delle informazioni di controllo, ad esempio `bycast.log` e `nms.log`, vedere ["Configurare i messaggi di audit e le destinazioni dei log"](#).

Log StorageGRID generali

Nome del file	Note	Trovato in
<code>/var/local/log/bycast.log</code>	Il file primario per la risoluzione dei problemi di StorageGRID. Selezionare SUPPORT > Tools > Grid topology . Quindi selezionare Site > Node > SSM > Events .	Tutti i nodi
<code>/var/local/log/bycast-err.log</code>	Contiene un sottoinsieme di <code>bycast.log</code> (messaggi con ERRORE DI gravità e CRITICO). I messaggi CRITICI vengono visualizzati anche nel sistema. Selezionare SUPPORT > Tools > Grid topology . Quindi selezionare Site > Node > SSM > Events .	Tutti i nodi

Nome del file	Note	Trovato in
/var/local/core/	<p>Contiene tutti i file core dump creati se il programma termina in modo anomalo. Le possibili cause includono errori di asserzione, violazioni o timeout di thread.</p> <p>Nota: Il file di <code>`/var/local/core/kexec_cmd</code> solito esiste sui nodi dell'appliance e non indica un errore.</p>	Tutti i nodi

Log relativi alla crittografia

Nome del file	Note	Trovato in
/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 di configurazioni nginx e al ricaricamento dei servizi nginx.	Tutti i nodi
/var/local/log/nginx-gw/config-generation.log	Contiene i log relativi alla generazione di configurazioni nginx-gw (e al ricaricamento dei servizi nginx-gw).	Nodi Admin e Gateway
/var/local/log/update-cipher-configurations.log	Contiene i registri relativi alla configurazione dei criteri TLS e SSH.	Tutti i nodi

Log della federazione di griglie

Nome del file	Note	Trovato in
/var/local/log/update_grid_federation_config.log	Contiene i log relativi alla generazione di configurazioni nginx e nginx-gw per le connessioni di federazione di griglie.	Tutti i nodi

Registri NMS

Nome del file	Note	Trovato in
/var/local/log/nms.log	<ul style="list-style-type: none"> • Acquisisce le notifiche da Grid Manager e Tenant Manager. • Acquisisce gli eventi correlati al funzionamento del servizio NMS. Ad esempio, notifiche e-mail e modifiche alla configurazione. • Contiene gli aggiornamenti del bundle XML risultanti dalle modifiche di configurazione apportate nel sistema. • Contiene messaggi di errore relativi al downsampling degli attributi eseguito una volta al giorno. • Contiene messaggi di errore del server Web Java, ad esempio errori di generazione pagina e errori HTTP Status 500. 	Nodi di amministrazione
/var/local/log/nms.errlog	<p>Contiene messaggi di errore relativi agli aggiornamenti del database MySQL.</p> <p>Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.</p>	Nodi di amministrazione
/var/local/log/nms.requestlog	Contiene informazioni sulle connessioni in uscita dall'API di gestione ai servizi StorageGRID interni.	Nodi di amministrazione

Log di Server Manager

Nome del file	Note	Trovato in
/var/local/log/servermanager.log	File di log per l'applicazione Server Manager in esecuzione sul server.	Tutti i nodi
/Var/local/log/GridstatBackend.errlog	File di log per l'applicazione backend della GUI di Server Manager.	Tutti i nodi
/var/local/log/gridstat.errlog	File di log per la GUI di Server Manager.	Tutti i nodi

Log dei servizi StorageGRID

Nome del file	Note	Trovato in
/var/local/log/acct.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/adc.errlog	Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.	Nodi di storage che eseguono il servizio ADC
/var/local/log/ams.errlog		Nodi di amministrazione
/var/local/log/cassandra/system.log	Informazioni per l'archivio di metadati (database Cassandra) che possono essere utilizzate se si verificano problemi durante l'aggiunta di nuovi nodi di storage o se l'attività di riparazione nodetool si blocca.	Nodi di storage
/var/local/log/cassandra-reaper.log	Informazioni per il servizio Cassandra Reaper, che esegue la riparazione dei dati nel database Cassandra.	Nodi di storage
/var/local/log/cassandra-reaper.errlog	Informazioni sugli errori 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 legacy.	Nodi di storage
/var/local/log/dds.errlog		Nodi di storage
/var/local/log/dmv.errlog		Nodi di storage
/var/local/log/dynip*	Contiene i registri relativi al servizio di dinip, che monitora la griglia per rilevare le modifiche dell'IP dinamico e aggiorna la configurazione locale.	Tutti i nodi

Nome del file	Note	Trovato in
/var/local/log/grafana.log	Log associato al servizio Grafana, utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi di amministrazione
/var/local/log/hagroups.log	Log associato ai gruppi ad alta disponibilità.	Nodi di amministrazione e nodi gateway
/var/local/log/hagroups_events.log	Tiene traccia delle modifiche di stato, come la transizione da BACKUP a MASTER o FAULT.	Nodi di amministrazione e nodi gateway
/var/local/log/idnt.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/jaeger.log	Log associato al servizio jaeger, utilizzato per la raccolta delle tracce.	Tutti i nodi
/var/local/log/kstn.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/lambda*	Contiene i registri per il servizio S3 Select.	Nodi Admin e Gateway Solo alcuni nodi Admin e Gateway contengono questo log. Consultare la "S3 selezionare requisiti e limitazioni per i nodi Admin e Gateway" .
/var/local/log/ldr.errlog		Nodi di storage
/var/local/log/miscd/*.log	Contiene i log per il servizio MISCd (Information Service Control Daemon), che fornisce un'interfaccia per eseguire query e gestire servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio per eseguire query sullo stato dei servizi in esecuzione su altri nodi.	Tutti i nodi
/var/local/log/nginx/*.log	Contiene i log per il servizio nginx, che funge da meccanismo di autenticazione e comunicazione sicura per diversi servizi grid (come Prometheus e Dynip) per poter comunicare con servizi su altri nodi tramite API HTTPS.	Tutti i nodi

Nome del file	Note	Trovato in
/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 amministrative limitate sui nodi di amministrazione.	Nodi di amministrazione e nodi gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene log di accesso relativi al traffico di replica cross-grid.	Nodi di amministrazione, nodi gateway o entrambi, in base alla configurazione della federazione di griglie. Trovato solo nella griglia di destinazione per la replica cross-grid.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene log di accesso per il servizio Load Balancer, che fornisce il bilanciamento del carico del traffico S3 dai client ai nodi storage.	Nodi di amministrazione e nodi gateway
/var/local/log/persistence*	Contiene i log per il servizio di persistenza, che gestisce i file sul disco root che devono persistere durante un riavvio.	Tutti i nodi
/var/local/log/prometheus.log	Per tutti i nodi, contiene il log del servizio dell'esportatore di nodi e il log del servizio di metriche dell'esportatore. Per i nodi di amministrazione, contiene anche i registri per i 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 storage con servizio RSM
/var/local/log/rms.errlog	Contiene i registri per il servizio RSM (Replicated state Machine Service), utilizzato per i servizi della piattaforma S3.	Nodi storage con servizio RSM
/var/local/log/ssm.errlog		Tutti i nodi
/var/local/log/update-s3vs-domains.log	Contiene i registri relativi all'elaborazione degli aggiornamenti per la configurazione dei nomi di dominio host virtuali S3.vedere le istruzioni per l'implementazione delle applicazioni client S3.	Nodi Admin e Gateway

Nome del file	Note	Trovato in
/var/local/log/update-snmp-firewall.*	Contiene i registri relativi alle porte firewall gestite per SNMP.	Tutti i nodi
/var/local/log/update-syslog.log	Contiene i registri relativi alle modifiche apportate alla configurazione syslog del sistema.	Tutti i nodi
/var/local/log/update-traffic-classes.log	Contiene i registri relativi alle modifiche apportate alla configurazione dei classificatori del traffico.	Nodi Admin e Gateway
/var/local/log/update-utcn.log	Contiene i registri relativi alla modalità di rete client non attendibile su questo nodo.	Tutti i nodi

Informazioni correlate

- ["A proposito di bycast.log"](#)
- ["UTILIZZARE L'API REST S3"](#)

Log di implementazione e manutenzione

È possibile utilizzare i registri di implementazione e manutenzione per risolvere i problemi.

Nome del file	Note	Trovato in
/var/local/log/install.log	Creato durante l'installazione del software. Contiene un record degli eventi di installazione.	Tutti i nodi
/var/local/log/expansion-progress.log	Creato durante le operazioni di espansione. Contiene un record degli eventi di espansione.	Nodi di storage
/var/local/log/pa-move.log	Creato durante l'esecuzione <code>pa-move.sh</code> dello script.	Nodo amministratore primario
/var/local/log/pa-move-new_pa.log	Creato durante l'esecuzione <code>pa-move.sh</code> dello script.	Nodo amministratore primario
/var/local/log/pa-move-old_pa.log	Creato durante l'esecuzione <code>pa-move.sh</code> dello script.	Nodo amministratore primario

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

A proposito di bycast.log

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

Il file `/var/local/log/bycast-err.log` è un sottoinsieme di `bycast.log`. Contiene messaggi di errore di severità e CRITICI.

In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere ["Configurare i messaggi di audit e le destinazioni dei log"](#).

Rotazione del file per bycast.log

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

Il file salvato viene rinominato `bycast.log.1` e il nuovo file viene denominato `bycast.log`. Quando il nuovo `bycast.log` raggiunge i 1 GB, `bycast.log.1` viene rinominato e compresso in diventa `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 versione 22nd del `bycast.log` file, 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 è necessario decomprimerlo nella stessa posizione in cui è stato scritto. La decompressione del file nella stessa posizione può interferire con gli script di rotazione del log.

In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere ["Configurare i messaggi di audit e le destinazioni dei log"](#).

Informazioni correlate

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

Messaggi nel 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 di rete.

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:

Segmento di messaggio	Valore nell'esempio
ID nodo	12455685
ID processo ADE	0357819531
Nome del modulo	SVMR
Identificatore del messaggio	EVHR
Ora di sistema UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDGH:MM:SS.UUUUUUUU)
Livello di severità	ERRORE
Numero di tracking interno	0906
Messaggio	SVMR: Controllo dello stato di salute sul volume 3 non riuscito con motivo 'TOUT'

Severità dei messaggi nel bycast.log

I messaggi in `bycast.log` sono livelli di gravità assegnati.

Ad esempio:

- **NOTA** — si è verificato un evento da registrare. La maggior parte dei messaggi di log è a questo livello.
- **ATTENZIONE** — si è verificata una condizione imprevista.
- **ERRORE** — si è verificato un errore grave che ha un impatto sulle operazioni.
- **CRITICO** — si è verificata una condizione anomala che ha interrotto le normali operazioni. È necessario risolvere immediatamente la condizione sottostante.

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 comuni in `bycast.log`. Il significato esatto di un codice non numerico dipende dal contesto in cui è riportato.

Codice di errore	Significato
SUC	Nessun errore
GERR	Sconosciuto
CANC	Annulato
ABRT	Interrotto
TOUT	Timeout
INVL	Non valido
NFND	Non trovato
VERS	Versione
CONF	Configurazione
NON RIUSCITO	Non riuscito
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	EPER	Operazione non consentita
002	ENOENT	Nessun file o directory di questo tipo
003	ESRCH	Nessun processo di questo tipo
004	EINTR	Chiamata di sistema interrotta

Numero di errore	Codice di errore	Significato
005	EIO	Errore i/O.
006	ENXIO	Nessun dispositivo o indirizzo di questo tipo
007	E2BIG	Elenco di argomenti troppo lungo
008	ENOEXEC	Errore di formato Exec
009	EBADF	Numero di file errato
010	ECHILD	Nessun processo figlio
011	EAGAIN	Riprovare
012	ENOMEM	Memoria esaurita
013	EACCES	Permesso negato
014	EFAULT	Indirizzo non valido
015	ENOTBLK	Dispositivo a blocchi richiesto
016	EBUSY	Periferica o risorsa occupata
017	EEXIST	Il file esiste
018	ESCLUDI	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo di questo tipo
020	ENOTDIR	Non 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 non disponibile sul dispositivo
029	ESPIPE	Ricerca illegale
030	EROFS	File system di sola lettura
031	EMSINK	Troppi collegamenti
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dominio della funzione
034	ERANGE	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un deadlock delle risorse
036	ENAMETOLONG	Nome file troppo lungo
037	ENOLCK	Nessun blocco di 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	Identificatore rimosso
044	ECHRNG	Numero di canale fuori intervallo
045	EL2NSYNC	Livello 2 non sincronizzato
046	EL3HLT	Livello 3 arrestato

Numero di errore	Codice di errore	Significato
047	EL3RST	Ripristino livello 3
048	ELNRNG	Numero di collegamento fuori intervallo
049	EUNATCH	Driver del protocollo non collegato
050	ENOCSI	Nessuna struttura CSI disponibile
051	EL2HLT	Livello 2 arrestato
052	EBADE	Scambio non valido
053	EBADR	Descrittore della richiesta non valido
054	ESCLUDI	Exchange pieno
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato del file di font non valido
060	ENOSTR	Il dispositivo non è un flusso
061	ENODATA	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse out of Streams
064	ENONET	La macchina non è in rete
065	ENOPKG	Pacchetto non installato
066	EREMOTE	L'oggetto è remoto
067	ENOLINK	Il collegamento è stato separato

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	PRONTO	Errore di protocollo
072	EMULTIHOP	Tentativo di multihop
073	EDOTDOT	Errore specifico RFS
074	EBADMSG	Non è un messaggio dati
075	Eoverflow	Valore troppo grande per il tipo di dati definito
076	ENOTUNIQ	Nome non univoco sulla rete
077	EBADFD	Descrittore del file in stato non valido
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 collegamento in troppe librerie condivise
083	ELIBEXEC	Impossibile eseguire direttamente una libreria condivisa
084	EILSEQ	Sequenza di byte non valida
085	ERESTART	La chiamata di sistema interrotta deve essere riavviata
086	ESTRPIPE	Errore pipe flussi
087	EUSERS	Troppi utenti

Numero di errore	Codice di errore	Significato
088	ENOTSOCK	Funzionamento socket su non socket
089	EDESTADDRREQ	Indirizzo di destinazione obbligatorio
090	EMSGSIZE	Messaggio troppo lungo
091	EPROTOTYPE	Tipo di protocollo errato per il socket
092	ENOPROTOOPT	Protocollo non disponibile
093	EPROTONOSUPPORT	Protocollo non supportato
094	SESOCKTNOSUPPORT	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 è disponibile
101	ENETUNREACH	La rete non è raggiungibile
102	ENETRESET	Connessione di rete interrotta a causa del ripristino
103	PRONTO	Il software ha causato l'interruzione della connessione
104	ECONNRESET	Connessione ripristinata da peer
105	ENOBUFS	Spazio buffer non disponibile
106	EISCONN	Endpoint di trasporto già connesso
107	ENOTCONN	Endpoint di trasporto non connesso
108	ESHUTDOWN	Impossibile inviare dopo l'arresto dell'endpoint di trasporto

Numero di errore	Codice di errore	Significato
109	ETOOMANYREFS	Troppi riferimenti: Impossibile unire
110	ETIMEDOUT	Timeout della connessione
111	ECONNREFUSED	Connessione rifiutata
112	EHOSTDOWN	Host non attivo
113	EHOSTUNREACH	Nessun percorso verso l'host
114	EALREADY	Operazione già in corso
115	EINPROGRESS	Operazione in corso
116		
117	EUCLEAN	La struttura deve essere pulita
118	ENOTNAM	Non è un file XENIX denominato
119	ENAVAIL	Nessun semaphore XENIX disponibile
120	EISNAM	È un file di tipo denominato
121	EREMOTEIO	Errore i/o remoto
122	EDQUOT	Quota superata
123	ENOMEDIUM	Nessun supporto trovato
124	EMPDIUMTYPE	Tipo di supporto errato
125	LED ECANCELED	Operazione annullata
126	ENOKEY	Chiave richiesta non disponibile
127	EKEYEXPIRED	Chiave scaduta
128	EKEYREVOKED	Chiave revocata
129	EKEYREJECTED	Chiave rifiutata dal servizio

Numero di errore	Codice di errore	Significato
130	EOWNERDEAD	Per i mutex più forti: Il proprietario è morto
131	ENOTRECOVERABLE	Per mutex affidabili: Stato non ripristinabile

Configurare le destinazioni dei messaggi di controllo e del registro

Considerazioni sull'utilizzo di un server syslog esterno

Un server syslog esterno è un server esterno a StorageGRID che può essere utilizzato per raccogliere informazioni di controllo del sistema in una singola posizione. L'utilizzo di un server syslog esterno consente di ridurre il traffico di rete sui nodi Admin e di gestire le informazioni in modo più efficiente. Per StorageGRID, il formato del pacchetto di messaggi syslog in uscita è conforme con RFC 3164.

I tipi di informazioni di controllo che è possibile inviare al server syslog esterno includono:

- Registri di audit contenenti i messaggi di audit generati durante il normale funzionamento del sistema
- Eventi correlati alla sicurezza, come accessi ed escalation a root
- Log delle applicazioni che potrebbero essere richiesti se è necessario aprire un caso di supporto per risolvere un problema riscontrato

Quando utilizzare un server syslog esterno

Un server syslog esterno è particolarmente utile se si dispone di un grid di grandi dimensioni, se si utilizzano più tipi di applicazioni S3 o se si desidera mantenere tutti i dati di revisione. L'invio di informazioni di audit a un server syslog esterno consente di:

- Raccogliere e gestire in modo più efficiente le informazioni di audit come messaggi di audit, registri delle applicazioni ed eventi di sicurezza.
- Riduci il traffico di rete sui nodi amministrativi, perché le informazioni di audit vengono trasferite direttamente dai vari nodi storage al server syslog esterno, senza dover passare attraverso un nodo amministrativo.



Quando i log vengono inviati a un server syslog esterno, i log singoli superiori a 8.192 byte vengono troncati alla fine del messaggio in conformità con le limitazioni comuni nelle implementazioni del server syslog esterno.



Per massimizzare le opzioni per il recupero completo dei dati in caso di guasto del server syslog esterno, (`localaudit.log` su ciascun nodo vengono mantenuti fino a 20 GB di registri locali dei record di controllo).

Come configurare un server syslog esterno

Per informazioni su come configurare un server syslog esterno, vedere ["Configurare i messaggi di controllo e il server syslog esterno"](#).

Se si intende configurare l'utilizzo del protocollo TLS o RELP/TLS, è necessario disporre dei seguenti certificati:

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



Se si utilizza un certificato client, è necessario utilizzare anche una chiave privata client. Se si fornisce una chiave privata crittografata, è necessario fornire anche la passphrase. L'utilizzo di una chiave privata crittografata non offre alcun vantaggio significativo in termini di sicurezza, in quanto è necessario memorizzare la chiave e la passphrase; per semplicità, si consiglia di utilizzare una chiave privata non crittografata, se disponibile.

Come valutare le dimensioni del server syslog esterno

Normalmente, il tuo grid è dimensionato per ottenere un throughput richiesto, definito in termini di operazioni S3 al secondo o byte al secondo. Ad esempio, potrebbe essere necessario che la griglia gestisca 1,000 operazioni S3 al secondo, o 2,000 MB al secondo, di acquisizione e recupero di oggetti. È necessario dimensionare il server syslog esterno in base ai requisiti dei dati del grid.

Questa sezione fornisce alcune formule euristiche che consentono di stimare la velocità e la dimensione media dei messaggi di log di vari tipi che il server syslog esterno deve gestire, espresse in termini di caratteristiche di performance note o desiderate della griglia (operazioni S3 al secondo).

Utilizzare le operazioni S3 al secondo nelle formule di stima

Se la griglia è stata dimensionata per un throughput espresso in byte al secondo, è necessario convertire questo dimensionamento in operazioni S3 al secondo per utilizzare le formule di stima. Per convertire il throughput della griglia, è necessario innanzitutto determinare la dimensione media degli oggetti, che è possibile utilizzare utilizzando le informazioni contenute nei registri di audit e nelle metriche esistenti (se presenti), oppure utilizzando la conoscenza delle applicazioni che utilizzeranno StorageGRID. Ad esempio, se la griglia è stata dimensionata per ottenere un throughput di 2,000 MB/secondo e la dimensione media dell'oggetto è di 2 MB, la griglia è stata dimensionata in modo da poter gestire 1,000 operazioni S3 al secondo (2,000 MB/2 MB).



Le formule per il dimensionamento del server syslog esterno nelle sezioni seguenti forniscono stime dei casi comuni (piuttosto che stime dei casi peggiori). A seconda della configurazione e del carico di lavoro, è possibile che venga visualizzata una velocità di messaggi syslog o un volume di dati syslog superiore o inferiore rispetto a quanto previsto dalle formule. Le formule devono essere utilizzate solo come linee guida.

Formule di stima per i log di audit

Se non si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule: Presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore):

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

Ad esempio, se la griglia è dimensionata per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 2,000 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di 1.6 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i registri di controllo, le variabili aggiuntive più importanti sono la percentuale di S3 operazioni che sono put (rispetto a GET) e la dimensione media, in byte, dei seguenti S3 campi (le abbreviazioni a 4 caratteri utilizzate nella tabella sono nomi di campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Tasto S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Utilizziamo P per rappresentare la percentuale di operazioni S3 che vengono messe, dove $0 \leq P \leq 1$ (quindi per un carico di lavoro PUT del 100%, $P = 1$ e per un carico DI lavoro GET del 100%, $P = 0$).

Utilizzare K per rappresentare la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. 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 è possibile determinare i valori per P e K, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione di Storage, Che è impostato su Error):

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

Ad esempio, se il tuo grid è dimensionato per 1,000 operazioni S3 al secondo, il tuo carico di lavoro è pari al 50% di put e i tuoi nomi account S3, nomi bucket, E i nomi degli oggetti hanno una media di 90 byte, il server

syslog esterno deve essere dimensionato per supportare 1,500 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di circa 1 MB al secondo.

Formule di stima per livelli di audit non predefiniti

Le formule fornite per i registri di controllo presuppongono l'utilizzo delle impostazioni predefinite del livello di controllo (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore). Non sono disponibili formule dettagliate per la stima del tasso e della dimensione media dei messaggi di audit per le impostazioni del livello di audit non predefinite. Tuttavia, la seguente tabella può essere utilizzata per effettuare una stima approssimativa del tasso; è possibile utilizzare la formula delle dimensioni medie fornita per i registri di controllo, ma è probabile che si verifichi 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 controllo sono impostati su Debug o Normal	Tasso del registro di controllo = 8 x S3 tasso di operazioni
Erasure coding (codifica erasure): I livelli di audit sono tutti impostati su Debug o Normal (normale)	Utilizzare la stessa formula utilizzata per le impostazioni predefinite

Formule di stima per gli eventi di sicurezza

Gli eventi di sicurezza non sono correlati con le 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 si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume di log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule:

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

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 3,300 log delle applicazioni al secondo ed essere in grado di ricevere (e memorizzare) i dati del log delle applicazioni a una velocità di circa 1.2 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i log delle applicazioni, le variabili aggiuntive più importanti sono la strategia di protezione dei dati (replica rispetto all'erasure coding), la percentuale di S3 operazioni messe (rispetto a GET/altro) e la dimensione media, in byte, dei seguenti S3 campi (le abbreviazioni di 4 caratteri utilizzate nella tabella sono i nomi dei campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.

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

Stime di dimensionamento di esempio

In questa sezione vengono illustrati esempi di utilizzo delle formule di stima per le griglie con i seguenti metodi di protezione dei dati:

- Replica
- Erasure coding

Se si utilizza la replica per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove $0 \leq P \leq 1$ (quindi per un carico di lavoro PUT del 100%, $P = 1$ e per un carico DI lavoro GET del 100%, $P = 0$).

Sia K la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. 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 K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K , è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando 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 il grid è dimensionato per 1,000 operazioni S3 al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket e i nomi degli oggetti sono in media di 90 byte, il server syslog esterno deve essere dimensionato in modo da supportare 1800 log delle applicazioni al secondo, E riceverà (e in genere memorizzerà) i dati delle applicazioni a una velocità di 0.5 MB al secondo.

Se si utilizza l'erasure coding per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove $0 \leq P \leq 1$ (quindi per un carico di lavoro PUT del 100%, $P = 1$ e per un carico DI lavoro GET del 100%, $P = 0$).

Sia K la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. 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 K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando 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 il grid è dimensionato per 1.000 S3 operazioni al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket mentre i nomi degli oggetti hanno una media di 90 byte, il server syslog esterno dovrebbe essere dimensionato in modo da supportare 2.250 registri delle applicazioni al secondo e dovrebbe essere in grado di ricevere (e generalmente archiviare) dati delle applicazioni a una velocità di 0,6 MB al secondo.

Configurare i messaggi di controllo e il server syslog esterno

È possibile configurare una serie di impostazioni relative ai messaggi di controllo. È possibile regolare il numero di messaggi di controllo registrati, definire eventuali intestazioni di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client, configurare un server syslog esterno e specificare dove vengono inviati i registri di controllo, i registri degli eventi di protezione e i registri del software StorageGRID.

I messaggi e i registri di audit registrano le attività del sistema e gli eventi di sicurezza e sono strumenti essenziali per il monitoraggio e la risoluzione dei problemi. Tutti i nodi StorageGRID generano messaggi di audit e registri per tenere traccia dell'attività e degli eventi del sistema.

In alternativa, è possibile configurare un server syslog esterno per salvare le informazioni di revisione in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto delle prestazioni della registrazione dei messaggi di controllo senza ridurre la completezza dei dati di controllo. Un server syslog esterno è particolarmente utile se si dispone di un grid di grandi dimensioni, se si utilizzano più tipi di applicazioni S3 o se si desidera mantenere tutti i dati di revisione. Per ulteriori informazioni, vedere "[Configurare i messaggi di controllo e il server syslog esterno](#)".

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[Autorizzazione di manutenzione o di accesso root](#)".
- Se si prevede di configurare un server syslog esterno, è stato esaminato il e si è "[considerazioni sull'utilizzo di un server syslog esterno](#)" certi che il server abbia capacità sufficiente per ricevere e memorizzare i file di registro.
- Se si intende configurare un server syslog esterno utilizzando il protocollo TLS o RELP/TLS, si dispone della CA del server e dei certificati client richiesti e della chiave privata del client.

Modificare i livelli dei messaggi di controllo

È possibile 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 del sistema"
Storage	Errore	"Messaggi di audit dello storage a oggetti"
Gestione	Normale	"Messaggio di audit della gestione"
Lecture del client	Normale	"Messaggi di audit in lettura del client"
Il client scrive	Normale	"Messaggi di audit di scrittura del client"
ILM	Normale	"Messaggi di controllo ILM"
Replica cross-grid	Errore	"CGRR: Richiesta di replica cross-grid"



Queste impostazioni predefinite si applicano se StorageGRID è stato installato inizialmente utilizzando la versione 10.3 o successiva. Se inizialmente è stata utilizzata una versione precedente di StorageGRID, l'impostazione predefinita per tutte le categorie è normale.



Durante gli aggiornamenti, le configurazioni a livello di audit non saranno effettive immediatamente.

Fasi

1. Selezionare **CONFIGURATION > Monitoring > Audit and syslog server**.
2. Per ciascuna categoria di messaggi di audit, selezionare un livello di audit dall'elenco a discesa:

Livello di audit	Descrizione
Spento	Non vengono registrati messaggi di audit della categoria.
Errore	Vengono registrati solo messaggi di errore - messaggi di audit per i quali il codice risultato non è stato "riuscito" (SUCCS).
Normale	Vengono registrati i messaggi transazionali standard, ovvero i messaggi elencati in queste istruzioni per la categoria.
Debug	Obsoleto. Questo livello si comporta come il livello di audit normale.

I messaggi inclusi per qualsiasi livello specifico includono quelli che verrebbero registrati ai livelli superiori. Ad esempio, il livello normale include tutti i messaggi di errore.



Se non si richiede un record dettagliato delle operazioni di lettura del client per le applicazioni S3, modificare l'impostazione **letture del client** su **errore** per ridurre il numero di messaggi di audit registrati nel registro di audit.

3. Selezionare **Salva**.

Un banner verde indica che la configurazione è stata salvata.

Definire le intestazioni delle richieste HTTP

Facoltativamente, è possibile definire qualsiasi intestazione di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client. Queste intestazioni di protocollo si applicano solo alle richieste S3.

Fasi

1. Nella sezione **Audit Protocol headers**, definire le intestazioni di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client.

Utilizzare un asterisco (*) come carattere jolly per far corrispondere zero o più caratteri. Utilizzare la sequenza escape (\) per far corrispondere un asterisco letterale.

2. Selezionare **Add another header** (Aggiungi un'altra intestazione) per creare altre intestazioni, se necessario.

Quando le intestazioni HTTP vengono trovate in una richiesta, vengono 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 **letture client** o **scritture client** non è **disattivato**.

3. Selezionare **Salva**

Un banner verde indica che la configurazione è stata salvata.

Usa un server syslog esterno

In alternativa, è possibile configurare un server syslog esterno per salvare registri di controllo, registri delle applicazioni e registri di eventi di sicurezza in una posizione esterna alla griglia.



Se non si desidera utilizzare un server syslog esterno, ignorare questo passaggio e andare a [Selezionare le destinazioni delle informazioni di audit](#).



Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili da soddisfare i requisiti, è possibile applicare ulteriori opzioni di configurazione utilizzando gli `audit-destinations` endpoint, che si trovano nella sezione API privata di ["API di Grid Management"](#). Ad esempio, è possibile utilizzare l'API se si desidera utilizzare server syslog diversi per diversi gruppi di nodi.

Inserire le informazioni di syslog

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

Fasi

1. Dalla pagina Audit and syslog server (controllo e server syslog), selezionare **Configure external syslog server** (Configura server syslog esterno Oppure, se è stato precedentemente configurato un server syslog esterno, selezionare **Modifica server syslog esterno**).

Viene visualizzata la procedura guidata Configura server syslog esterno.

2. Per la fase **inserire le informazioni syslog** della procedura guidata, immettere un nome di dominio completo valido o un indirizzo IPv4 o IPv6 per il server syslog esterno nel campo **host**.
3. Inserire la porta di destinazione sul server syslog esterno (deve essere un numero intero compreso tra 1 e 65535). La porta predefinita è 514.
4. Selezionare il protocollo utilizzato per inviare le informazioni di audit al server syslog esterno.

Si consiglia di utilizzare **TLS** o **RELP/TLS**. Per utilizzare una di queste opzioni, è necessario caricare un certificato del server. L'utilizzo dei certificati consente di proteggere le connessioni tra la griglia e il server syslog esterno. Per ulteriori informazioni, vedere "[Gestire i certificati di sicurezza](#)".

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



Il protocollo RELP (Reliable Event Logging Protocol) estende le funzionalità del protocollo syslog per fornire un'erogazione affidabile dei messaggi di evento. L'utilizzo di RELP può contribuire a prevenire la perdita di informazioni di controllo nel caso in cui il server syslog esterno debba essere riavviato.

5. Selezionare **continua**.
6. se si seleziona **TLS** o **RELP/TLS**, caricare i certificati CA del server, il certificato client e la chiave privata del client.
 - a. Selezionare **Sfoglia** per il certificato o la chiave che si desidera utilizzare.
 - b. Selezionare il certificato o il file della chiave.
 - c. Selezionare **Open** per caricare il file.

Accanto al nome del certificato o del file della chiave viene visualizzato un segno di spunta verde che indica che il caricamento è stato eseguito correttamente.

7. Selezionare **continua**.

Gestire il contenuto syslog

È possibile selezionare le informazioni da inviare al server syslog esterno.

Fasi

1. Per la fase **Gestisci contenuto syslog** della procedura guidata, selezionare ogni tipo di informazione di audit che si desidera inviare al server syslog esterno.
 - **Invia log di audit**: Invia eventi StorageGRID e attività di sistema
 - **Invia eventi di sicurezza**: Invia eventi di sicurezza, ad esempio quando un utente non autorizzato tenta di effettuare l'accesso o un utente accede come root
 - **Invia registri applicazione**: Consente di inviare messaggi "[File di log del software StorageGRID](#)" utili per la risoluzione dei problemi, tra cui:

- `bycast-err.log`
- `bycast.log`
- `jaeger.log`
- `nms.log` (Solo nodi amministrativi)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

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

2. Utilizzare i menu a discesa per selezionare la gravità e la struttura (tipo di messaggio) per ciascuna categoria di informazioni di controllo che si desidera inviare.

L'impostazione dei valori di gravità e struttura consente di aggregare i registri in modo personalizzabile per semplificare l'analisi.

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

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

Severità	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di gravità di quando è stato registrato localmente sul nodo: <ul style="list-style-type: none"> • Per i registri di controllo, la gravità è "info". • Per gli eventi di sicurezza, i valori di gravità sono generati dalla distribuzione Linux sui nodi. • Per i registri delle applicazioni, i livelli di gravità variano tra "info" e "avviso", a seconda del problema. Ad esempio, aggiungendo un server NTP e configurando un gruppo ha si ottiene il valore "info", mentre arrestando intenzionalmente il servizio SSM o RSM si ottiene il valore "avviso". • Per i registri di accesso, la gravità è "info".
0	Emergenza: Il sistema non è utilizzabile
1	Attenzione: L'azione deve essere eseguita immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore
4	Avvertenza: Condizioni di avviso

Severità	Descrizione
5	Avviso: Condizione normale ma significativa
6	Informativo: Messaggi informativi
7	Debug: Messaggi a livello di debug

b. Per **Facility**, selezionare **Passthrough** o selezionare un valore di struttura compreso tra 0 e 23.

Se si seleziona un valore, questo verrà applicato a tutti i messaggi di questo tipo. Le informazioni sulle diverse strutture andranno perse se si sostituisce la struttura con un valore fisso.

Struttura	Descrizione
Passthrough	<p>Ogni messaggio inviato al syslog esterno per avere lo stesso valore di struttura di quando è stato collegato localmente al nodo:</p> <ul style="list-style-type: none"> • Per i registri di controllo, la struttura inviata al server syslog esterno è "local7". • Per gli eventi di sicurezza, i valori della struttura vengono generati dalla distribuzione linux sui nodi. • Per i registri delle applicazioni, i registri delle applicazioni inviati al server syslog esterno presentano i seguenti valori di struttura: <ul style="list-style-type: none"> ◦ <code>bycast.log</code>: utente o daemon ◦ <code>bycast-err.log</code>: utente, daemon, local3 o local4 ◦ <code>jaeger.log</code>: local2 ◦ <code>nms.log</code>: local3 ◦ <code>prometheus.log</code>: local4 ◦ <code>raft.log</code>: local5 ◦ <code>hagroups.log</code>: local6 • Per i registri di accesso, la struttura inviata al server syslog esterno è "local0".
0	kern (messaggi kernel)
1	utente (messaggi a livello utente)
2	mail
3	daemon (daemon di sistema)
4	auth (messaggi di sicurezza/autorizzazione)

Struttura	Descrizione
5	syslog (messaggi generati internamente da syslogd)
6	lpr (sottosistema di stampanti di linea)
7	news (sottosistema notizie di rete)
8	UUCP
9	cron (daemon di clock)
10	sicurezza (messaggi di sicurezza/autorizzazione)
11	FTP
12	NTP
13	logaudit (audit del log)
14	logalert (avviso di log)
15	clock (daemon di clock)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selezionare **continua**.

Inviare messaggi di test

Prima di iniziare a utilizzare un server syslog esterno, è necessario richiedere a tutti i nodi della griglia di inviare messaggi di test al server syslog esterno. È necessario utilizzare questi messaggi di test per

convalidare l'intera infrastruttura di raccolta dei log prima di inviare i dati al server syslog esterno.



Non utilizzare la configurazione del server syslog esterno fino a quando non si conferma che il server syslog esterno ha ricevuto un messaggio di test da ciascun nodo della griglia e che il messaggio è stato elaborato come previsto.

Fasi

1. Se non si desidera inviare messaggi di test perché si è certi che il server syslog esterno sia configurato correttamente e che sia in grado di ricevere informazioni di controllo da tutti i nodi della griglia, selezionare **Ignora e termina**.

Un banner verde indica che la configurazione è stata salvata.

2. In caso contrario, selezionare **Invia messaggi di prova** (scelta consigliata).

I risultati del test vengono visualizzati continuamente sulla pagina fino a quando non si interrompe il test. Mentre il test è in corso, i messaggi di controllo continuano a essere inviati alle destinazioni precedentemente configurate.

3. Se si ricevono errori, correggerli e selezionare di nuovo **Invia messaggi di prova**.

Per informazioni sulla risoluzione di eventuali errori, consultare la sezione "[Risolvere i problemi di un server syslog esterno](#)".

4. Attendere che venga visualizzato un banner verde che indica che tutti i nodi hanno superato il test.
5. Controllare il server syslog per determinare se i messaggi di test vengono ricevuti ed elaborati come previsto.



Se si utilizza UDP, controllare l'intera infrastruttura di raccolta dei log. Il protocollo UDP non consente un rilevamento degli errori rigoroso come gli altri protocolli.

6. Selezionare **Stop and Finish** (Interrompi e termina).

Viene nuovamente visualizzata la pagina **Audit and syslog server**. Un banner verde indica che la configurazione del server syslog è stata salvata.



Le informazioni di audit StorageGRID non vengono inviate al server syslog esterno finché non si seleziona una destinazione che include il server syslog esterno.

Selezionare le destinazioni delle informazioni di audit

È possibile specificare dove vengono inviati i registri di controllo, i registri eventi di protezione e "[Log del software StorageGRID](#)".

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



Quando si utilizza `/var/local/log/localaudit.log`, le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione. È possibile individuare il nodo con le voci più recenti utilizzando il `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` comando.

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

Fasi

1. Nella pagina Audit and syslog server (Server audit e syslog), selezionare la destinazione per le informazioni di audit.



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

Opzione	Descrizione
Solo nodi locali (impostazione predefinita)	<p>I messaggi di controllo, i registri degli eventi di protezione e i registri delle applicazioni non vengono inviati ai nodi amministrativi. Vengono invece salvati solo sui nodi che li hanno generati ("nodo locale"). Le informazioni di controllo generate su ogni nodo locale sono memorizzate in <code>/var/local/log/localaudit.log</code>.</p> <p>Nota: StorageGRID rimuove periodicamente i log locali in una rotazione per liberare spazio. Quando il file di log di 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 di 21 file. Quando viene creata la ventiduesima versione del file di log, il file di log più vecchio viene cancellato. In media, su ciascun nodo vengono memorizzati circa 20 GB di dati di log.</p>
Nodi amministrativi/nodi locali	<p>I messaggi di controllo vengono inviati al registro di controllo sui nodi Admin, mentre i registri degli eventi di protezione e i registri delle applicazioni vengono memorizzati sui nodi che li hanno generati. Le informazioni di controllo sono memorizzate nei seguenti file:</p> <ul style="list-style-type: none">• Nodi amministrativi (primario e non primario): <code>/var/local/audit/export/audit.log</code>• Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> file è in genere vuoto o mancante. Potrebbe contenere informazioni secondarie, ad esempio una copia aggiuntiva di alcuni messaggi.
Server syslog esterno	<p>Le informazioni di controllo vengono inviate a un server syslog esterno e salvate sui nodi locali (<code>/var/local/log/localaudit.log</code>). Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.</p>

Opzione	Descrizione
Nodo di amministrazione e server syslog esterno	I messaggi di controllo vengono inviati al registro di controllo (/var/local/audit/export/audit.log) sui nodi Admin e le informazioni di controllo vengono inviate al server syslog esterno e salvate sul nodo locale (/var/local/log/localaudit.log). Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.

2. Selezionare **Salva**.

Viene visualizzato un messaggio di avviso.

3. Selezionare **OK** per confermare che si desidera modificare la destinazione per le informazioni di controllo.

Un banner verde indica che la configurazione di controllo è stata salvata.

I nuovi registri vengono inviati alle destinazioni selezionate. I registri esistenti rimangono nella posizione corrente.

Utilizzare il monitoraggio SNMP

Utilizzare il monitoraggio SNMP

Se si desidera monitorare StorageGRID utilizzando il protocollo SNMP (Simple Network Management Protocol), è necessario configurare l'agente SNMP incluso in StorageGRID.

- ["Configurare l'agente SNMP"](#)
- ["Aggiornare l'agente SNMP"](#)

Funzionalità

Ogni nodo StorageGRID esegue un agente SNMP, o daemon, che fornisce un MIB. StorageGRID MIB contiene definizioni di tabella e di notifica per gli avvisi. Il MIB contiene anche informazioni sulla descrizione del sistema, come il numero di piattaforma e il numero di modello per ciascun nodo. Ogni nodo StorageGRID supporta anche un sottoinsieme di oggetti MIB-II.



Vedere ["Accedere ai file MIB"](#) se si desidera scaricare i file MIB sui nodi griglia.

Inizialmente, SNMP viene disattivato su tutti i nodi. Quando si configura l'agente SNMP, tutti i nodi StorageGRID ricevono la stessa configurazione.

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

Trappole

I trap sono notifiche inviate dall'agente SNMP che non richiedono un riconoscimento da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che si è verificato qualcosa all'interno di StorageGRID, ad esempio un avviso attivato.

I trap sono supportati in tutte e tre le versioni di SNMP.

Informa

Le informazioni sono simili alle trap, ma richiedono un riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, invia nuovamente l'informazione fino a quando non viene ricevuta una conferma o non viene raggiunto il valore massimo di tentativi.

Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche trap e inform vengono inviate nei seguenti casi:

- Viene attivato un avviso predefinito o personalizzato a qualsiasi livello di severità. Per eliminare le notifiche SNMP per un avviso, è necessario ["configurare un silenzio"](#) per tale avviso. Le notifiche di avviso vengono inviate da ["Nodo Admin mittente preferito"](#).

Ogni avviso viene associato 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 questi trap, vedere la ["Riferimenti agli avvisi"](#).

Supporto della versione SNMP

La tabella fornisce un riepilogo generale dei contenuti supportati per ciascuna versione SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Query (GET e GETNEXT)	Query MIB di sola lettura	Query MIB di sola lettura	Query MIB di sola lettura
Autenticazione e delle query	Stringa di comunità	Stringa di comunità	Utente del modello di sicurezza basato sull'utente (USM)
Notifiche (INTRAPPOL ARE e INFORMARE)	Solo trap	Trap e informa	Trap e informa
Autenticazione e delle notifiche	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Utente USM per ciascuna destinazione trap

Limitazioni

- StorageGRID supporta l'accesso MIB di sola lettura. L'accesso in lettura/scrittura non è supportato.
- Tutti i nodi della griglia ricevono la stessa configurazione.
- SNMPv3: StorageGRID non supporta la modalità di supporto per il trasporto (TSM).
- SNMPv3: L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).

- SNMPv3: L'unico protocollo per la privacy supportato è AES.

Configurare l'agente SNMP

È possibile configurare l'agente SNMP StorageGRID in modo che utilizzi un sistema di gestione SNMP di terze parti per l'accesso MIB di sola lettura e le notifiche.

Prima di iniziare

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

A proposito di questa attività

L'agente SNMP di StorageGRID supporta SNMPv1, SNMPv2c e SNMPv3. È possibile configurare l'agente per una o più versioni. Per SNMPv3, è supportata solo l'autenticazione del modello di sicurezza utente (USM).

Tutti i nodi nella griglia utilizzano la stessa configurazione SNMP.

Specificare la configurazione di base

Come prima fase, attivare l'agente SMNP StorageGRID e fornire informazioni di base.

Fasi

1. Selezionare **CONFIGURATION > Monitoring > SNMP Agent**.

Viene visualizzata la pagina SNMP Agent.

2. Per attivare l'agente SNMP su tutti i nodi della griglia, selezionare la casella di controllo **Enable SNMP** (attiva SNMP).
3. Inserire le seguenti informazioni nella sezione Configurazione di base.

Campo	Descrizione
Contatto per il sistema	Opzionale. Il contatto principale per il sistema StorageGRID, che viene restituito nei messaggi SNMP come sysContact. In genere, il contatto di sistema è un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID. Il contatto di sistema può contenere al massimo 255 caratteri.
Ubicazione del sistema	Opzionale. La posizione del sistema StorageGRID, che viene restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere una qualsiasi informazione utile per identificare la posizione del sistema StorageGRID. Ad esempio, è possibile utilizzare l'indirizzo di una struttura. Questo valore si applica a tutti i nodi nel sistema StorageGRID. La posizione del sistema può contenere al massimo 255 caratteri.

Campo	Descrizione
Attivare le notifiche dell'agente SNMP	<ul style="list-style-type: none"> • Se selezionata, l'agente SNMP StorageGRID invia notifiche trap e inform. • Se questa opzione non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.
Abilita trap di autenticazione	Se selezionata, l'agente SNMP StorageGRID invia trap di autenticazione se riceve messaggi di protocollo autenticati in modo errato.

Immettere le stringhe di comunità

Se si utilizza SNMPv1 o SNMPv2c, completare la sezione Community Strings (stringhe comunità).

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

Fasi

1. Per **comunità di sola lettura**, è possibile immettere una stringa di comunità per consentire l'accesso MIB di sola lettura agli indirizzi di agenti IPv4 e IPv6.



Per garantire la sicurezza del sistema StorageGRID, non utilizzare "public" come stringa di comunità. Se questo campo viene lasciato vuoto, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa di comunità.

Ogni stringa di community può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

2. Selezionare **Aggiungi un'altra stringa di comunità** per aggiungere altre stringhe.

Sono consentite fino a cinque stringhe.

creare destinazioni trap

Utilizzare la scheda destinazioni trap nella sezione altre configurazioni per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

Fasi

1. Per il campo **Comunità trap predefinita**, è possibile immettere la stringa di comunità predefinita che si desidera utilizzare per le destinazioni trap SNMPv1 o SNMPv2.

Se necessario, è possibile fornire una stringa di comunità diversa ("personalizzata") quando si definisce una destinazione trap specifica.

La comunità trap predefinita può contenere al massimo 32 caratteri e non può contenere spazi vuoti.

2. Per aggiungere una destinazione trap, selezionare **Crea**.
3. Selezionare la versione SNMP che verrà utilizzata per la destinazione trap.

4. Completare il modulo Crea destinazione trap per la versione selezionata.

SNMPv1

Se si seleziona SNMPv1 come versione, completare questi campi.

Campo	Descrizione
Tipo	Deve essere trap per SNMPv1.
Host	Un indirizzo IPv4 o IPv6 o un nome di dominio completo (FQDN) per ricevere il trap.
Porta	Utilizzare 162, quale porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv2c

Se si seleziona SNMPv2c come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv3

Se si seleziona SNMPv3 come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Utente USM	<p>L'utente USM che verrà utilizzato per l'autenticazione.</p> <ul style="list-style-type: none"> • Se si seleziona Trap, vengono visualizzati solo gli utenti USM senza ID motore autorevoli. • Se si seleziona inform, vengono visualizzati solo gli utenti USM con ID motore autorevoli. • Se non viene visualizzato alcun utente: <ul style="list-style-type: none"> i. Creare e salvare la destinazione trap. ii. Accedere a Creare utenti USM e creare l'utente. iii. Tornare alla scheda Destinazioni trap, selezionare la destinazione salvata dalla tabella e selezionare Modifica. iv. Selezionare l'utente.

5. Selezionare **Crea**.

La destinazione trap viene creata e aggiunta alla tabella.

Creare gli indirizzi degli agenti

Facoltativamente, utilizzare la scheda indirizzi agente nella sezione altre configurazioni per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

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

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

Campo	Descrizione
Protocollo Internet	<p>Se questo indirizzo utilizzerà IPv4 o IPv6.</p> <p>Per impostazione predefinita, SNMP utilizza IPv4.</p>

Campo	Descrizione
Protocollo di trasporto	Se questo indirizzo utilizza UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
Rete StorageGRID	La rete StorageGRID su cui l'agente ascolta. <ul style="list-style-type: none"> • Grid, Admin e Client Networks (reti Grid, Admin e Client): L'agente SNMP è in attesa di query su tutte e tre le reti. • Grid Network • Admin Network (rete amministrativa) • Rete client <p>Nota: Se si utilizza la rete client per i dati non protetti e si crea un indirizzo agente per la rete client, tenere presente che anche il traffico SNMP non sarà sicuro.</p>
Porta	Facoltativamente, il numero di porta su cui l'agente SNMP deve essere in attesa. La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta inutilizzato. Nota: Quando si salva l'agente SNMP, StorageGRID apre automaticamente le porte degli indirizzi dell'agente sul firewall interno. È necessario assicurarsi che tutti i firewall esterni consentano l'accesso a queste porte.

3. Selezionare **Crea**.

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

creare utenti USM

Se si utilizza SNMPv3, utilizzare la scheda utenti USM nella sezione altre configurazioni per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.



SNMPv3 *inform* le destinazioni devono avere utenti con ID motore. SNMPv3 la destinazione *trap* non può avere utenti con ID motore.

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

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

Campo	Descrizione
Nome utente	<p>Un nome univoco per questo utente USM.</p> <p>I nomi utente possono avere un massimo di 32 caratteri e non possono contenere spazi vuoti. Il nome utente non può essere modificato dopo la creazione dell'utente.</p>
Accesso MIB di sola lettura	Se selezionata, l'opzione consente all'utente di accedere in sola lettura al MIB.
ID motore autorevole	<p>Se l'utente verrà utilizzato in una destinazione inform, l'ID motore autorevole per questo utente.</p> <p>Inserire da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è necessario per gli utenti USM che verranno selezionati nelle destinazioni trap per gli informa. Questo valore non è consentito per gli utenti USM che verranno selezionati nelle destinazioni trap per trap.</p> <p>Nota: Questo campo non viene visualizzato se si seleziona accesso MIB di sola lettura perché gli utenti USM che hanno accesso MIB di sola lettura non possono avere ID motore.</p>
Livello di sicurezza	<p>Il livello di sicurezza per l'utente USM:</p> <ul style="list-style-type: none"> • Authprim: Questo utente comunica con autenticazione e privacy (crittografia). È necessario specificare un protocollo di autenticazione e una password, nonché un protocollo e una password per la privacy. • AuthNoPriv: Questo utente comunica con autenticazione e senza privacy (senza crittografia). Specificare un protocollo di autenticazione e una password.
Protocollo di autenticazione	Impostare sempre su SHA, che è l'unico protocollo supportato (HMAC-SHA-96).
Password	La password che l'utente utilizzerà per l'autenticazione.
Protocollo di privacy	Visualizzato solo se si seleziona authviv e si imposta sempre su AES, che è l'unico protocollo di privacy supportato.
Password	Visualizzato solo se è stato selezionato authviv . La password che l'utente utilizzerà per la privacy.

3. Selezionare **Crea**.

L'utente USM viene creato e aggiunto alla tabella.

4. Una volta completata la configurazione dell'agente SNMP, selezionare **Salva**.

La nuova configurazione dell'agente SNMP diventa attiva.

Aggiornare l'agente SNMP

È possibile disattivare le notifiche SNMP, aggiornare le stringhe di comunità o aggiungere o rimuovere indirizzi di agenti, utenti USM e destinazioni trap.

Prima di iniziare

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

A proposito di questa attività

Per informazioni dettagliate su ciascun campo nella pagina dell'agente SNMP, vedere ["Configurare l'agente SNMP"](#). È necessario selezionare **Salva** nella parte inferiore della pagina per confermare le modifiche apportate in ciascuna scheda.

Fasi

1. Selezionare **CONFIGURATION > Monitoring > SNMP Agent**.

Viene visualizzata la pagina SNMP Agent.

2. Per disattivare l'agente SNMP su tutti i nodi della griglia, deselegionare la casella di controllo **attiva SNMP** e selezionare **Salva**.

Se si riattiva l'agente SNMP, tutte le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Se si desidera, aggiornare le informazioni nella sezione Configurazione di base:

- a. Se necessario, aggiornare **System contact** e **System location**.
- b. In alternativa, selezionare o deselegionare la casella di controllo **attiva notifiche agente SNMP** per controllare se l'agente SNMP StorageGRID invia notifiche trap e inform.

Quando questa casella di controllo è deselegionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia notifiche SNMP.

- c. Facoltativamente, selezionare o deselegionare 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 autenticati in modo errato.
4. Se si utilizza SNMPv1 o SNMPv2c, è possibile aggiornare o aggiungere una comunità **di sola lettura** nella sezione Community Strings (stringhe comunità).
 5. Per aggiornare le destinazioni trap, selezionare la scheda destinazioni trap nella sezione altre configurazioni.

Utilizzare questa scheda per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

Per informazioni dettagliate su cosa immettere, vedere ["Creare destinazioni trap"](#).

- Facoltativamente, aggiornare o rimuovere la comunità trap predefinita.

Se si rimuove la comunità trap predefinita, è necessario innanzitutto verificare che tutte le destinazioni trap esistenti utilizzino una stringa di comunità personalizzata.

- Per aggiungere una destinazione trap, selezionare **Crea**.
- Per modificare una destinazione trap, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere una destinazione trap, selezionare il pulsante di opzione e selezionare **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

6. Per aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

Utilizzare questa scheda per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

Per informazioni dettagliate su cosa immettere, vedere "[Creare gli indirizzi degli agenti](#)".

- Per aggiungere un indirizzo agente, selezionare **Crea**.
- Per modificare l'indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere un indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

7. Per aggiornare gli utenti USM, selezionare la scheda utenti USM nella sezione altre configurazioni.

Utilizzare questa scheda per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

Per informazioni dettagliate su cosa immettere, vedere "[Creare utenti USM](#)".

- Per aggiungere un utente USM, selezionare **Crea**.
- Per modificare un utente USM, selezionare il pulsante di opzione e selezionare **Modifica**.

Il nome utente di un utente USM esistente non può essere modificato. Se è necessario modificare un nome utente, rimuovere l'utente e crearne uno nuovo.



Se si aggiunge o si rimuove l'ID motore autorevole di un utente e tale utente è attualmente selezionato per una destinazione, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

- Per rimuovere un utente USM, selezionare il pulsante di opzione e selezionare **Rimuovi**.



Se l'utente rimosso è attualmente selezionato per una destinazione trap, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

8. Una volta aggiornata la configurazione dell'agente SNMP, selezionare **Salva**.

Accedere ai file MIB

I file MIB contengono definizioni e informazioni sulle proprietà delle risorse e dei servizi

gestiti per i nodi della griglia. È possibile accedere ai file MIB che definiscono gli oggetti e le notifiche per StorageGRID. Questi file possono essere utili per il monitoraggio della griglia.

Per ulteriori informazioni sui file SNMP e MIB, vedere ["Utilizzare il monitoraggio SNMP"](#).

Accedere ai file MIB

Per accedere ai file MIB, procedere come segue.

Fasi

1. Selezionare **CONFIGURATION > Monitoring > SNMP Agent**.
2. Nella pagina dell'agente SNMP, selezionare il file che si desidera 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 gli oggetti e le notifiche per le appliance basate su e-Series.
 - **MIB_1_10.zip**: Definisce gli oggetti e le notifiche per le appliance con un'interfaccia BMC.



È inoltre possibile accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID StorageGRID dal file MIB:

- a. Ottenere l'OID della directory principale del MIB StorageGRID:

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Risultato: `.1.3.6.1.4.1.789.28669` (28669 È sempre l'OID per StorageGRID)

- a. Grep per l'OID StorageGRID nell'intero albero (usando `paste` per unire le linee):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



Il `snmptranslate` comando ha molte opzioni che sono utili per esplorare il MIB. Questo comando è disponibile su qualsiasi nodo StorageGRID.

Contenuto del file MIB

Tutti gli oggetti si trovano sotto l'OID StorageGRID.

Nome dell'oggetto	ID oggetto (OID)	Descrizione
		Il modulo MIB per le entità NetApp StorageGRID.

Oggetti MIB

Nome dell'oggetto	ID oggetto (OID)	Descrizione
ActiveAlertCount		Il numero di avvisi attivi in activeAlertTable.
ActiveAlertTable		Tabella degli avvisi attivi in StorageGRID.
ActiveAlertId		L'ID dell'avviso. Unico solo nel set corrente di avvisi attivi.
ActiveAlertName		Il nome dell'avviso.
ActiveAlertInstance		Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
ActiveAlertSeverity		La severità dell'avviso.
ActiveAlertStartTime		La data e l'ora di attivazione dell'avviso.

Tipi di notifica (trap)

Tutte le notifiche includono le seguenti variabili come varbind:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo di notifica	ID oggetto (OID)	Descrizione
ActiveMinorAlert		Un avviso con un livello di severità minore
ActiveMajorAlert		Un avviso con severità maggiore
ActiveCriticalAlert		Un avviso con severità critica

Raccogliere dati StorageGRID aggiuntivi

Utilizzare grafici e grafici

È possibile utilizzare grafici e report per monitorare lo stato del sistema StorageGRID e risolvere i problemi.

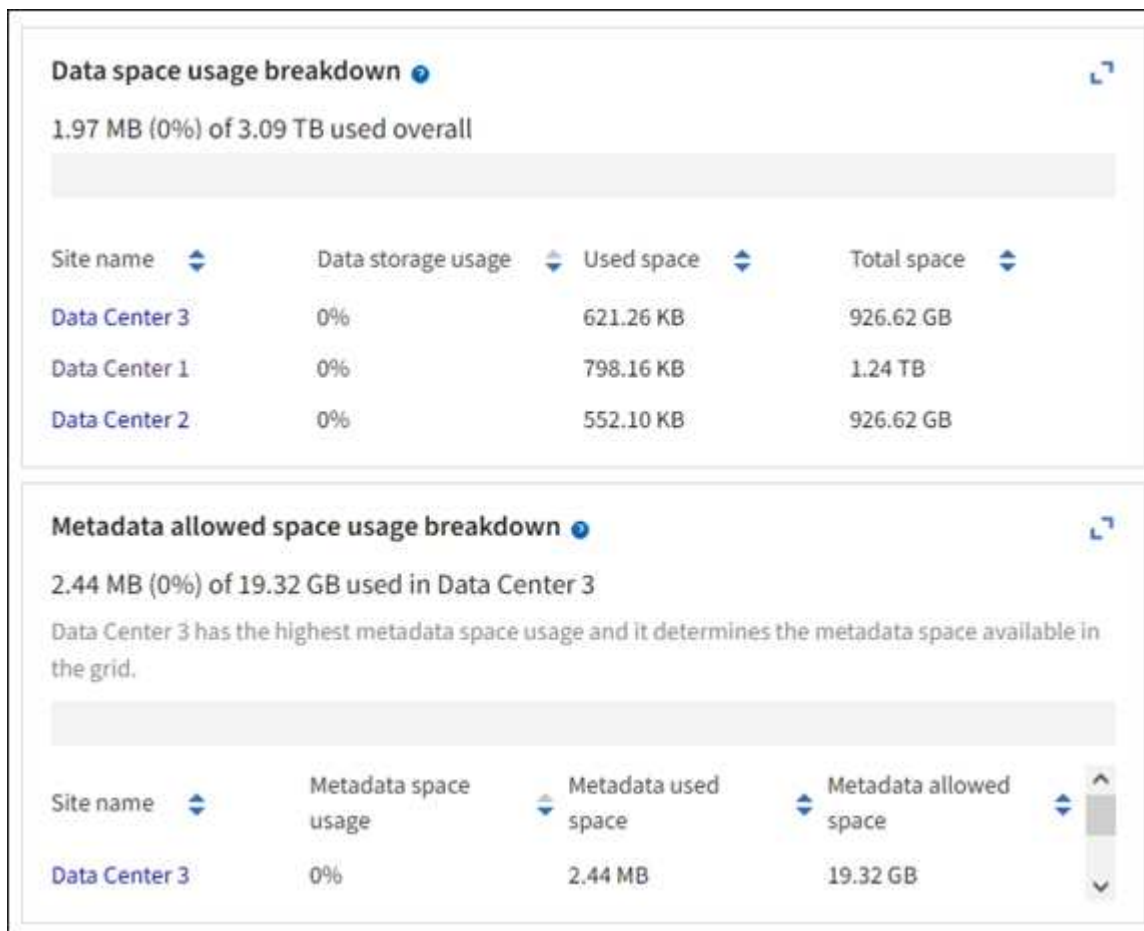


Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio di questa pagina.

Tipi di grafici

I grafici e i grafici riassumono i valori delle metriche e degli attributi specifici di StorageGRID.

La dashboard di Grid Manager include schede che riepilogano lo storage disponibile per la griglia e per ciascun sito.



Il pannello Storage Use (utilizzo storage) della dashboard di Tenant Manager visualizza quanto segue:

- Un elenco dei bucket più grandi (S3) o container (Swift) per il tenant
- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi
- La quantità totale di spazio utilizzato e, se viene impostata una quota, la quantità e la percentuale di spazio rimanente

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups

1 User
View users

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

Name: Tenant02
ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Inoltre, i grafici che mostrano come le metriche e gli attributi StorageGRID cambiano nel tempo sono disponibili dalla pagina nodi e dalla pagina **SUPPORTO > Strumenti > topologia griglia**.

Esistono quattro tipi di grafici:

- **Grafici Grafana:** Mostrati nella pagina dei nodi, i grafici Grafana vengono utilizzati per tracciare i valori delle metriche Prometheus nel tempo. Ad esempio, la scheda **NODI > rete** di un nodo di storage include un grafico Grafana per il traffico di rete.

DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

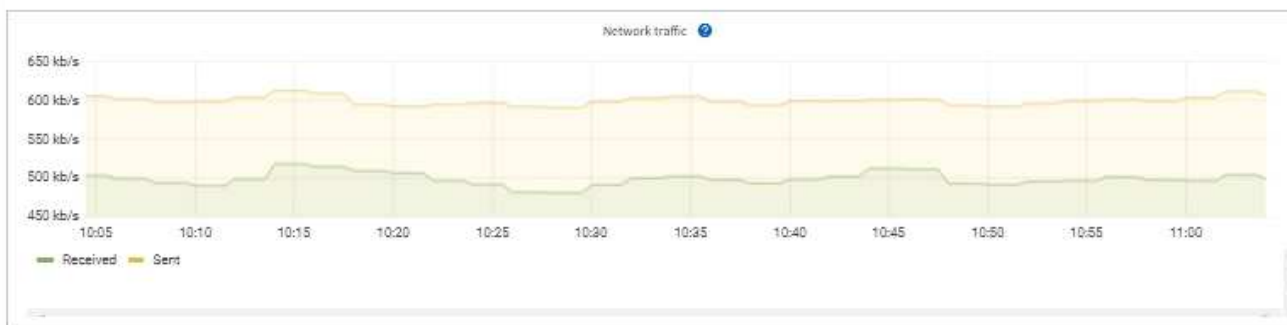
1 hour

1 day

1 week

1 month

Custom



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive


Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

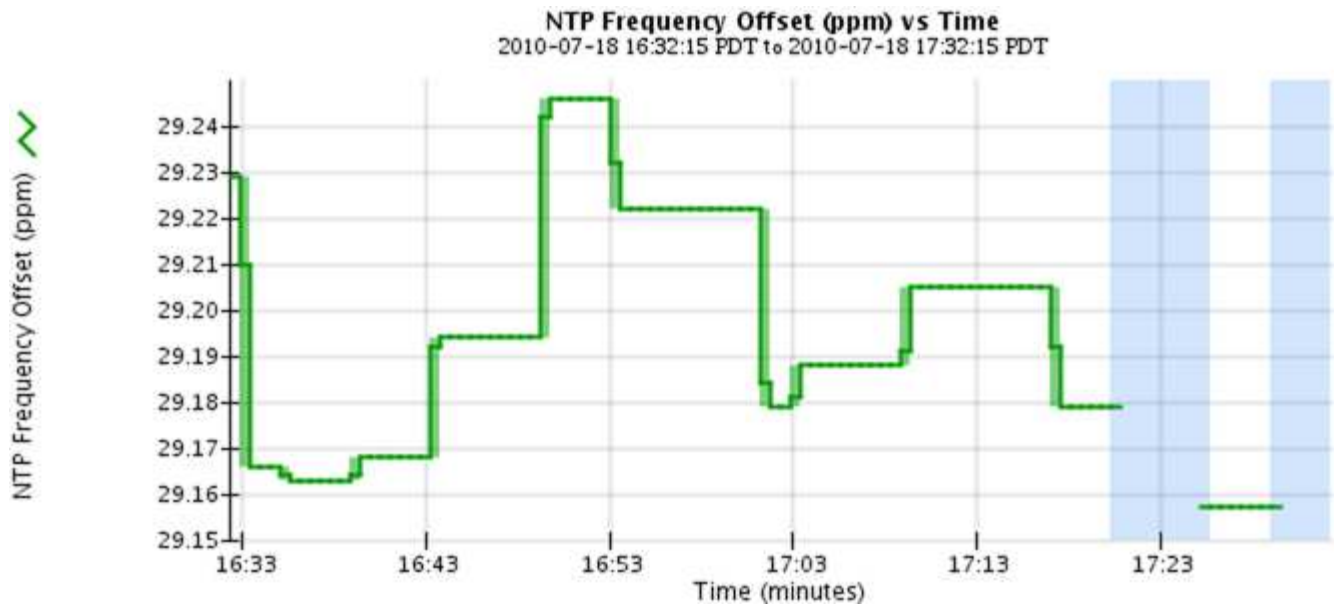
Transmit


Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

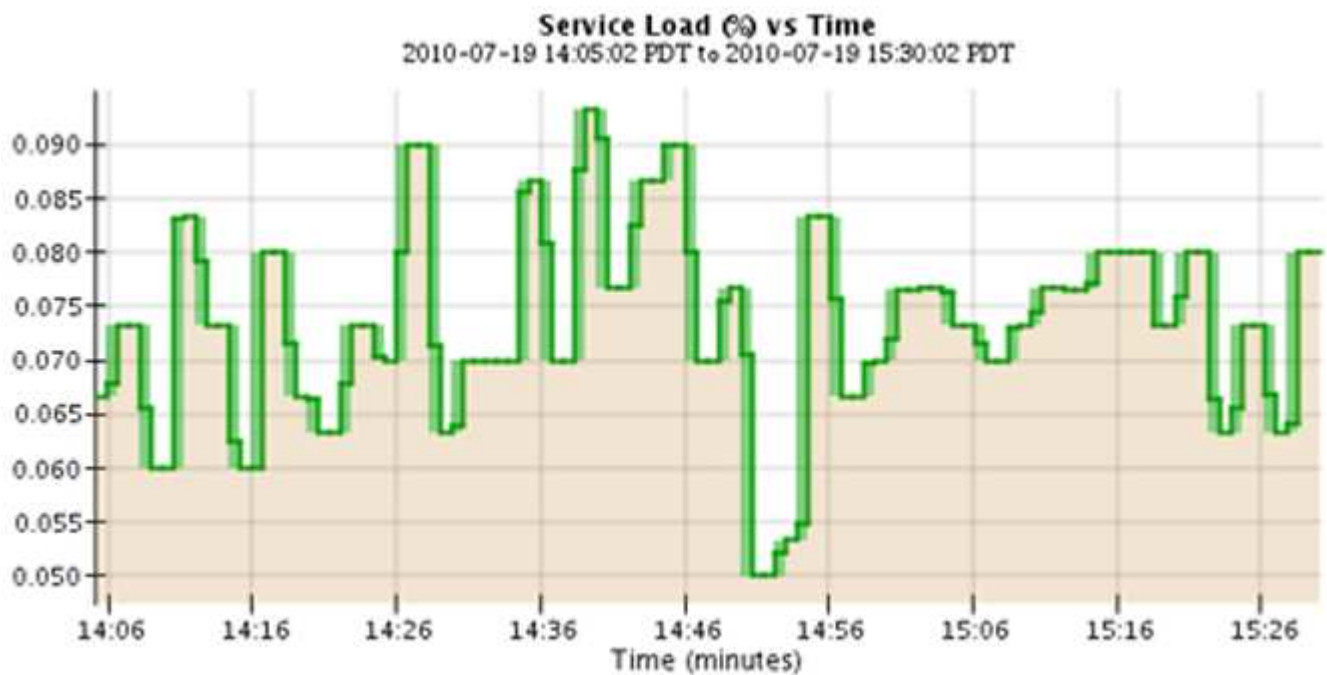


I grafici Grafana sono inclusi anche nelle dashboard predefinite disponibili nella pagina **SUPPORT > Tools > Metrics**.

- **Grafici a linee:** Disponibili dalla pagina nodi e dalla pagina **SUPPORTO > Strumenti > topologia a griglia** (selezionare l'icona del grafico  dopo un valore di dati), i grafici a linee vengono utilizzati per rappresentare graficamente i valori degli attributi StorageGRID che hanno un valore unitario (come Offset frequenza NTP, in ppm). Le modifiche al valore vengono tracciate a intervalli di dati regolari (bin) nel tempo.



- **Grafici ad area:** Disponibili dalla pagina nodi e dalla pagina **SUPPORTO > Strumenti > topologia a griglia** (selezionare l'icona del grafico  dopo un valore di dati), i grafici ad area vengono utilizzati per rappresentare graficamente le quantità di attributi volumetrici, come i conteggi degli oggetti o i valori di carico del servizio. I grafici dell'area sono simili ai grafici a linee, ma includono un'ombreggiatura marrone chiaro sotto la linea. Le modifiche al valore vengono tracciate a intervalli di dati regolari (bin) nel tempo.



- Alcuni grafici sono contrassegnati con un diverso tipo di icona del grafico  e hanno un formato diverso:

1 hour 1 day 1 week 1 month Custom

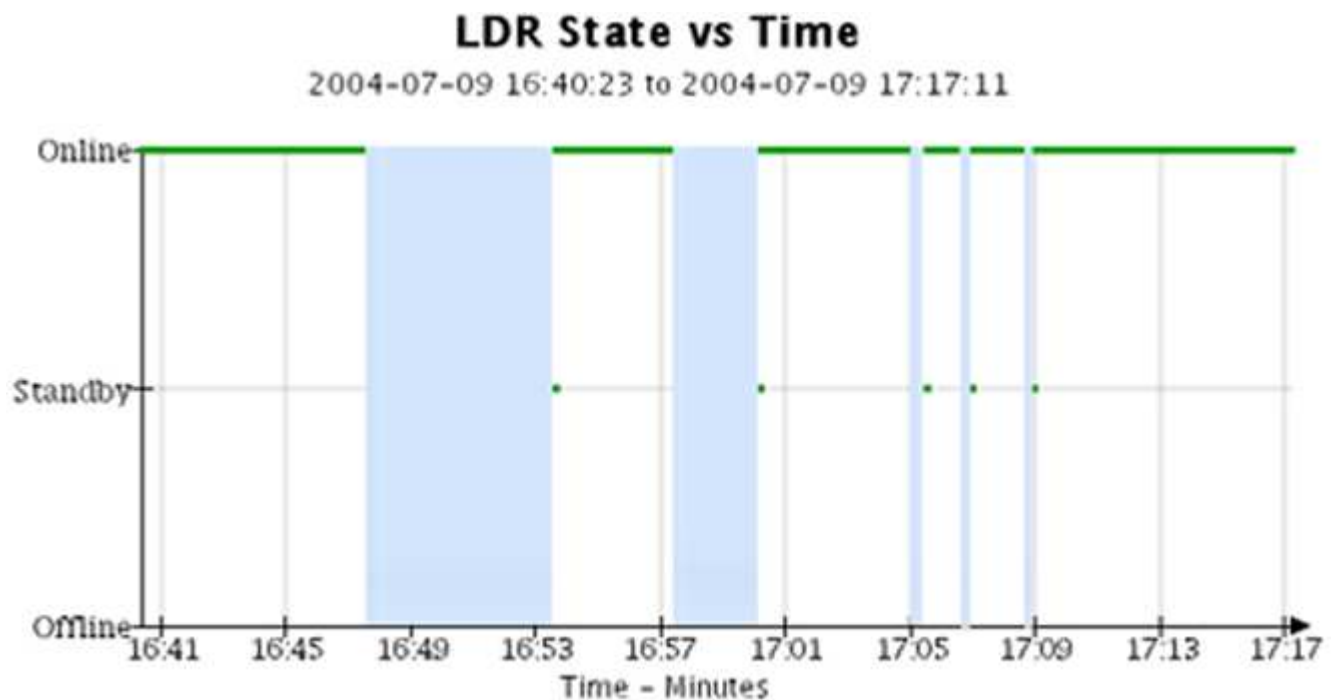
From: 2020-10-01 [calendar icon] 12 : 45 PM PDT

To: 2020-10-01 [calendar icon] 01 : 10 PM PDT Apply



Close

- **Grafico di stato:** Disponibile nella pagina **SUPPORTO > Strumenti > topologia griglia** (selezionare l'icona del grafico dopo un valore di dati), i grafici di stato vengono utilizzati per rappresentare graficamente i valori degli attributi che rappresentano stati distinti, ad esempio uno stato di servizio che può essere in linea, in standby o non in linea. I grafici di stato sono simili ai grafici a linee, ma la transizione è discontinua, ovvero il valore passa da un valore di stato all'altro.









Informazioni correlate

- "Visualizzare la pagina nodi"
- "Visualizzare l'albero topologia griglia"
- "Rivedere le metriche di supporto"

Legenda del grafico

Le linee e i colori utilizzati per disegnare i grafici hanno un significato specifico.

Esempio	Significato
	I valori degli attributi riportati vengono tracciati utilizzando linee di colore verde scuro.
	L'ombreggiatura verde chiaro intorno a linee verdi scure indica che i valori effettivi in quell'intervallo di tempo variano e sono stati "binned" (binning) per una tracciatura più rapida. La linea scura rappresenta la media ponderata. L'intervallo in verde chiaro indica i valori massimi e minimi all'interno del contenitore. L'ombreggiatura marrone chiaro viene utilizzata per i grafici dell'area per indicare i dati volumetrici.
	Le aree vuote (nessun dato plottato) indicano che i valori degli attributi non erano disponibili. Lo sfondo può essere blu, grigio o una combinazione di grigio e blu, a seconda dello stato del servizio che segnala l'attributo.
	L'ombreggiatura blu chiaro indica che alcuni o tutti i valori degli attributi in quel momento erano indeterminati; l'attributo non stava riportando i valori perché il servizio era in uno stato sconosciuto.
	L'ombreggiatura dei grigi indica che alcuni o tutti i valori degli attributi in quel momento non erano noti perché il servizio che riporta gli attributi era amministrativamente inattivo.
	Una combinazione di ombreggiature grigie e blu indica che alcuni dei valori degli attributi all'epoca erano indeterminati (perché il servizio era in uno stato sconosciuto), mentre altri non erano noti perché il servizio che riportava gli attributi era amministrativamente inattivo.

Visualizza grafici e grafici

La pagina Nodes (nodi) contiene i grafici a cui si dovrebbe accedere regolarmente per monitorare attributi come la capacità dello storage e il throughput. In alcuni casi, in particolare quando si lavora con il supporto tecnico, è possibile utilizzare la pagina **SUPPORT > Tools > Grid topology** per accedere a grafici aggiuntivi.

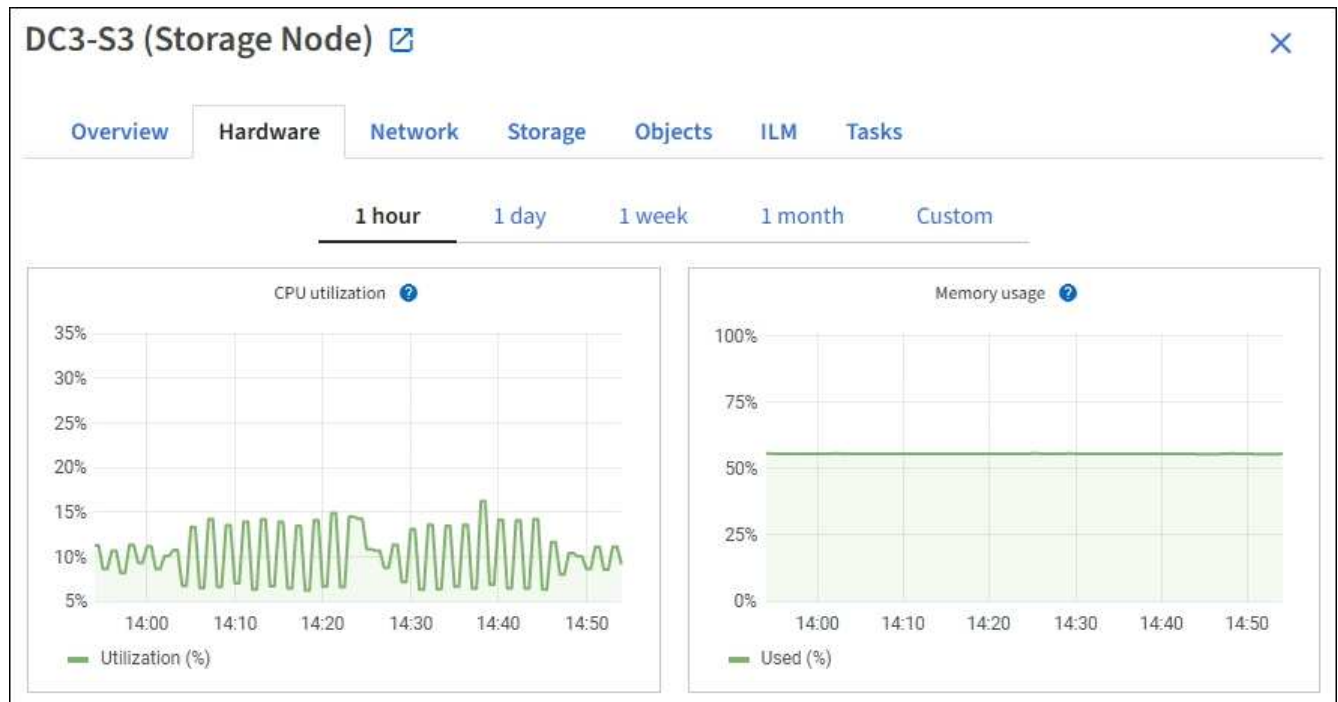
Prima di iniziare

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

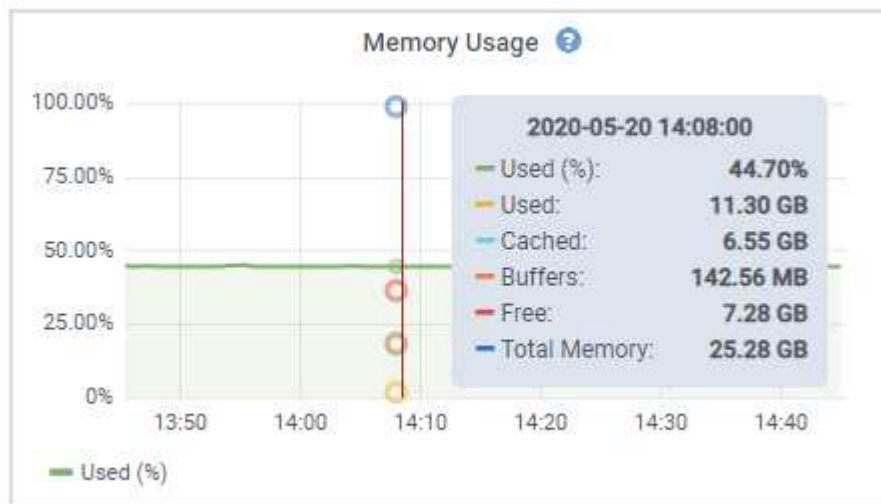
Fasi


1. Selezionare **NODI**. Quindi, selezionare un nodo, un sito o l'intera griglia.
2. Selezionare la scheda per la quale si desidera visualizzare le informazioni.

Alcune schede includono uno o più grafici Grafana, utilizzati per tracciare i valori delle metriche Prometheus nel tempo. Ad esempio, la scheda **NODI > hardware** di un nodo include due grafici Grafana.




3. Se lo si desidera, posizionare il cursore sul grafico per visualizzare valori più dettagliati per un determinato punto nel tempo.



4. In base alle esigenze, spesso è possibile visualizzare un grafico per un attributo o una metrica specifici. Dalla tabella nella pagina nodi, selezionare l'icona del grafico  a destra del nome dell'attributo.

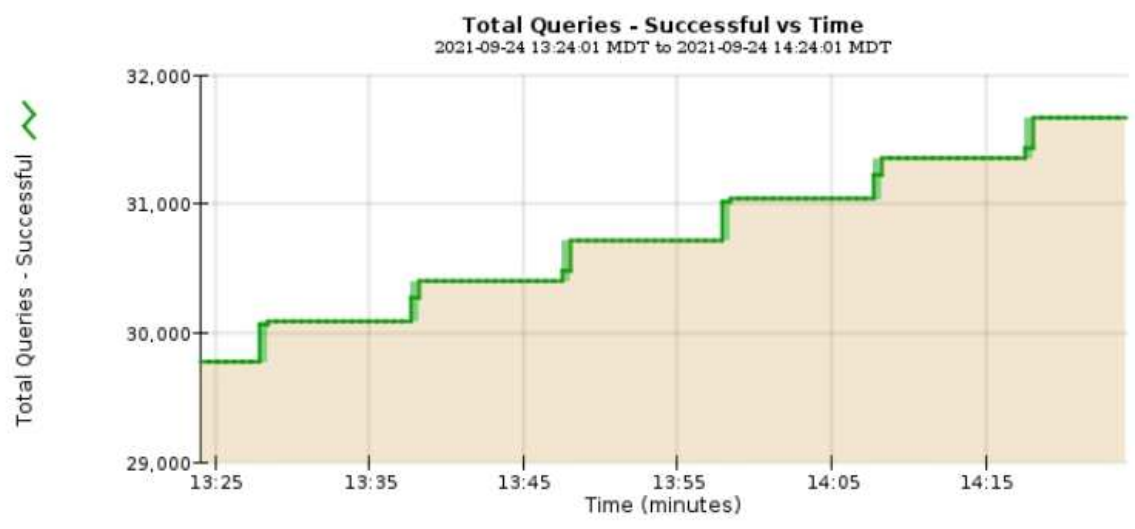


I grafici non sono disponibili per tutte le metriche e gli attributi.

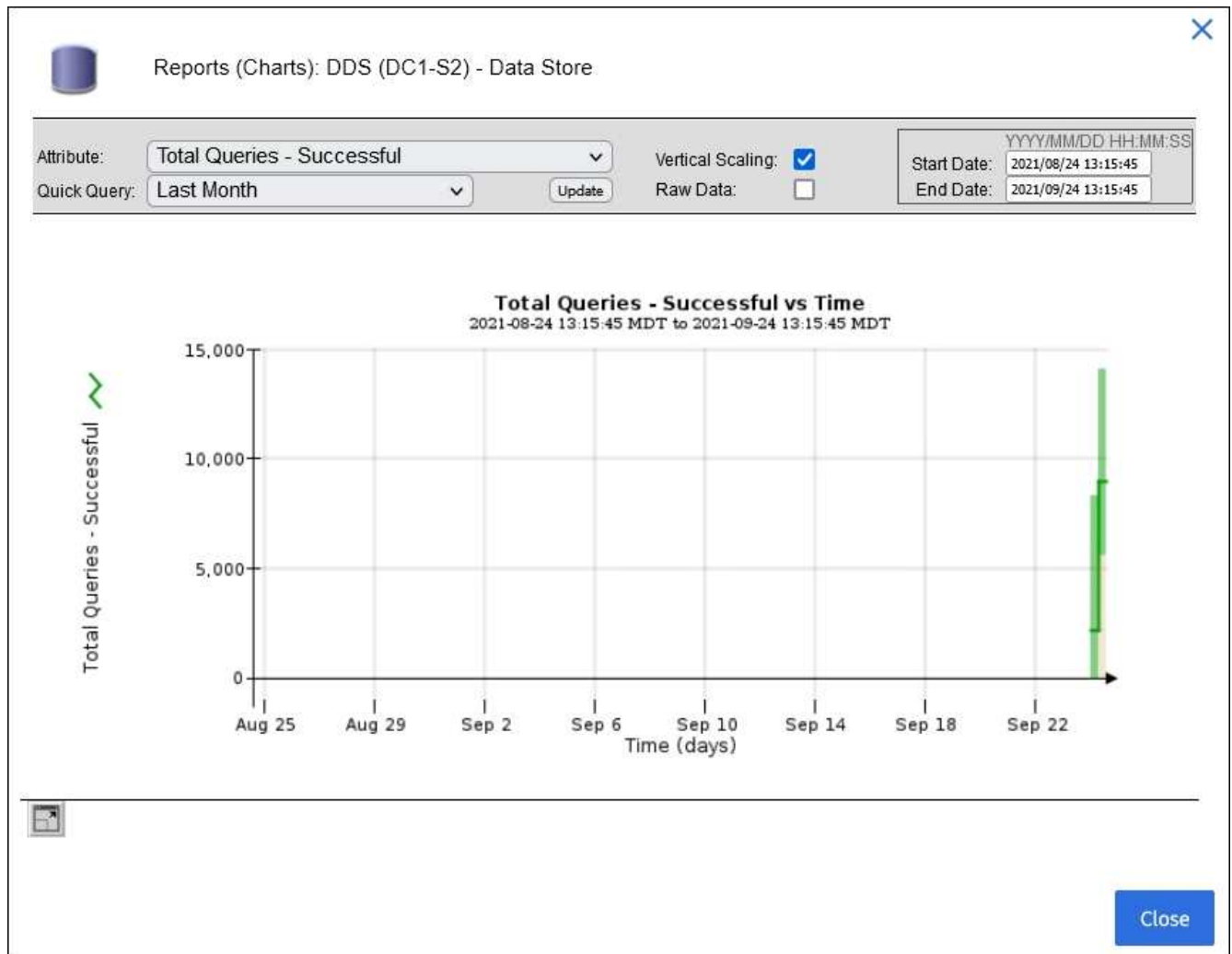
Esempio 1: Dalla scheda oggetti di un nodo di archiviazione, è possibile selezionare l'icona del grafico  per visualizzare il numero totale di query di archiviazione metadati riuscite per il nodo di archiviazione.



Attribute: Total Queries - Successful
Quick Query: Last Hour
Vertical Scaling:
Raw Data:
Start Date: 2021/09/24 13:24:01
End Date: 2021/09/24 14:24:01




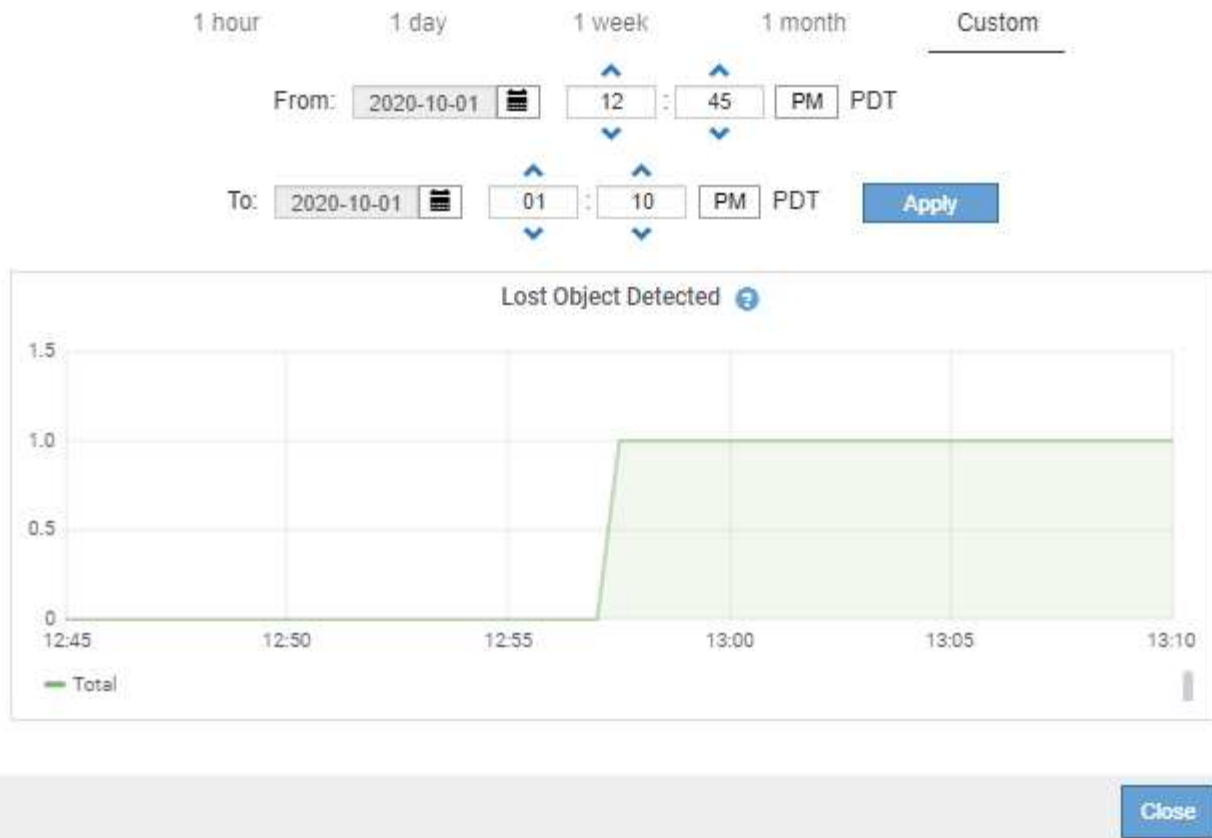
Close



Esempio 2: Dalla scheda oggetti di un nodo di archiviazione, è possibile selezionare l'icona del grafico per visualizzare il grafico Grafana del conteggio degli oggetti persi rilevati nel tempo.

Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





5. Per visualizzare i grafici degli attributi non visualizzati nella pagina nodo, selezionare **SUPPORT > Tools > Grid topology**.
6. Selezionare **grid node > component or service > Overview > Main**.

Overview | Alarms | Reports | Configuration



Main



Overview: SSM (DC1-ADM1) - Resources

Updated: 2018-05-07 16:29:52 MDT

Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

7. Selezionare l'icona del grafico  accanto all'attributo.

Il display passa automaticamente alla pagina **Report > grafici**. Il grafico visualizza i dati dell'attributo nel giorno passato.

Generare grafici

I grafici visualizzano una rappresentazione grafica dei valori dei dati degli attributi. È possibile creare report su un sito del data center, un nodo grid, un componente o un servizio.

Prima di iniziare

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

Fasi

1. Selezionare **SUPPORT > Tools > Grid topology**.
2. Selezionare **grid node > component or service > Report > grafici**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **attributo**.
4. Per forzare l'inizio dell'asse Y a zero, deselezionare la casella di controllo **Vertical Scaling** (Scala verticale).

5. Per visualizzare i valori con la massima precisione, selezionare la casella di controllo **dati non elaborati** oppure per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselegionare la casella di controllo **dati non elaborati**.
6. Selezionare il periodo di tempo per il quale si desidera creare un report dall'elenco a discesa **Query rapida**.

Selezionare l'opzione Custom Query (Query personalizzata) per selezionare un intervallo di tempo specifico.

Il grafico viene visualizzato dopo alcuni istanti. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi.

7. Se si seleziona Custom Query (Query personalizzata), personalizzare il periodo di tempo per il grafico inserendo **Data di inizio** e **Data di fine**.

Utilizzare il formato *YYYY/MM/DDHH:MM:SS* in ora locale. Gli zeri iniziali devono corrispondere al formato. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

8. Selezionare **Aggiorna**.

Dopo alcuni secondi viene generato un grafico. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi. A seconda del periodo di tempo impostato per la query, viene visualizzato un report di testo raw o aggregato.

Utilizzare report di testo

I report di testo visualizzano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. Esistono due tipi di report generati in base al periodo di tempo in cui si esegue il reporting: Report di testo raw per periodi inferiori a una settimana e report di testo aggregati per periodi superiori a una settimana.

Report di testo raw

Un report di testo raw visualizza i dettagli relativi all'attributo selezionato:

- Time Received (ora ricezione): Data e ora locali in cui un valore di esempio dei dati di un attributo è stato elaborato dal servizio NMS.
- Sample Time (ora campione): Data e ora locali in cui un valore di attributo è stato campionato o modificato all'origine.
- Value (valore): Valore dell'attributo al momento del campionamento.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Aggregare report di testo

Un report di testo aggregato visualizza i dati in un periodo di tempo più lungo (di solito una settimana) rispetto a un report di testo raw. Ciascuna voce è il risultato di un riepilogo di più valori di attributo (un aggregato di valori di attributo) da parte del servizio NMS nel tempo in una singola voce con valori medi, massimi e minimi derivati dall'aggregazione.

Ciascuna voce visualizza le seguenti informazioni:

- Aggregate time (ora aggregata): L'ultima data e ora locale in cui il servizio NMS ha aggregato (raccolto) un insieme di valori di attributo modificati.
- Average value (valore medio): La media del valore dell'attributo nel periodo di tempo aggregato.
- Minimum Value (valore minimo): Il valore minimo nel periodo di tempo aggregato.
- Maximum Value (valore massimo): Il valore massimo nel periodo di tempo aggregato.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Generare report di testo

I report di testo visualizzano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. È possibile creare report su un sito del data center, un nodo grid, un componente o un servizio.

Prima di iniziare

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

A proposito di questa attività

Per i dati degli attributi che si prevede siano in continuo cambiamento, questi dati degli attributi vengono campionati dal servizio NMS (all'origine) a intervalli regolari. Per i dati degli attributi che cambiano di rado (ad esempio, dati basati su eventi come cambiamenti di stato o stato), un valore di attributo viene inviato al servizio NMS quando il valore cambia.

Il tipo di report visualizzato dipende dal periodo di tempo configurato. Per impostazione predefinita, i report di testo aggregati vengono generati per periodi di tempo superiori a una settimana.

Il testo grigio indica che il servizio è stato amministrativamente inattivo durante il campionamento. Il testo blu indica che il servizio si trova in uno stato sconosciuto.

Fasi

1. Selezionare **SUPPORT > Tools > Grid topology**.
2. Selezionare **grid node > component o service > Report > testo**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **attributo**.
4. Selezionare il numero di risultati per pagina dall'elenco a discesa **risultati per pagina**.
5. Per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselezionare la casella di controllo **dati non elaborati**.
6. Selezionare il periodo di tempo per il quale si desidera creare un report dall'elenco a discesa **Query rapida**.

Selezionare l'opzione Custom Query (Query personalizzata) per selezionare un intervallo di tempo specifico.

Il report viene visualizzato dopo alcuni istanti. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi.

- Se si seleziona Custom Query (Query personalizzata), è necessario personalizzare il periodo di tempo per il quale si desidera creare un report inserendo **Data di inizio** e **Data di fine**.

Utilizzare il formato YYYY/MM/DDHH:MM:SS in ora locale. Gli zeri iniziali devono corrispondere al formato. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

- Fare clic su **Aggiorna**.

Dopo alcuni istanti viene generato un report di testo. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi. A seconda del periodo di tempo impostato per la query, viene visualizzato un report di testo raw o aggregato.

Esportare report di testo

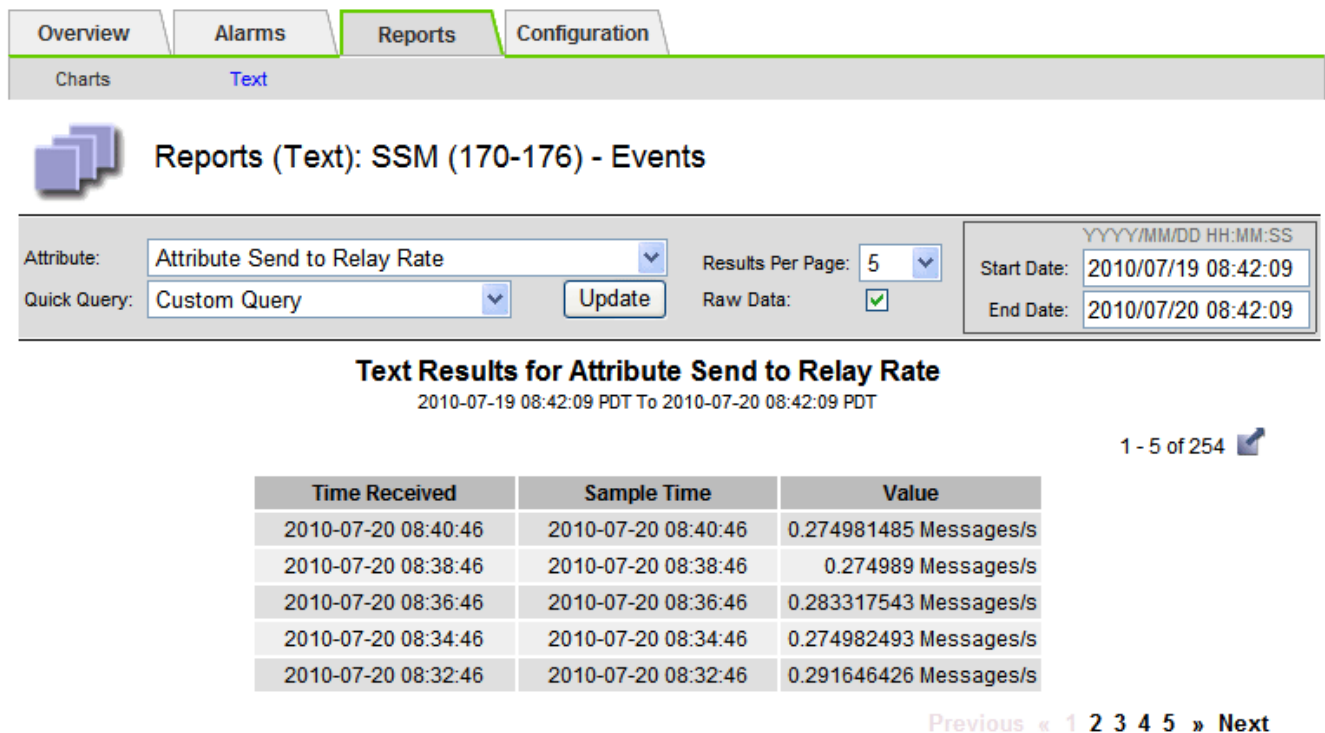
I report di testo esportati aprono una nuova scheda del browser che consente di selezionare e copiare i dati.

A proposito di questa attività

I dati copiati possono quindi essere salvati in un nuovo documento (ad esempio, un foglio di calcolo) e utilizzati per analizzare le prestazioni del sistema StorageGRID.


Fasi

- Selezionare **SUPPORT > Tools > Grid topology**.
- Creare un report di testo.
- Fare clic su *Esporta*.




Overview Alarms **Reports** Configuration

Charts **Text**

 **Reports (Text): SSM (170-176) - Events**

Attribute: Results Per Page: Start Date: YYYY/MM/DD HH:MM:SS
Quick Query: Raw Data: End Date:

Text Results for Attribute Send to Relay Rate
2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT

1 - 5 of 254 

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

Previous « 1 2 3 4 5 » Next

Viene visualizzata la finestra Export Text Report (Esporta report di testo) che visualizza il report.

Grid ID: 000 000

OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200

Node Path: Site/170-176/SSM/Events

Attribute: Attribute Send to Relay Rate (ABSR)

Query Start Date: 2010-07-19 08:42:09 PDT

Query End Date: 2010-07-20 08:42:09 PDT

Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type

2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U

2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U

2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U

2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U

2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U

2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U

2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U

2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U

2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U

2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U

2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U

2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U

2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Selezionare e copiare il contenuto della finestra Esporta report di testo.

Questi dati possono ora essere incollati in un documento di terze parti, ad esempio un foglio di calcolo.

Monitorare L'EFFICIENZA e OTTENERE le performance

È possibile monitorare le performance di alcune operazioni, come ad esempio l'archiviazione e il recupero di oggetti, per identificare le modifiche che potrebbero richiedere ulteriori analisi.

A proposito di questa attività

Per monitorare le prestazioni, è possibile eseguire comandi S3 direttamente da una workstation o utilizzando l'applicazione S3tester open-source. L'utilizzo di questi metodi consente di valutare le performance indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o problemi con una rete esterna.

Quando si eseguono i test delle operazioni PUT e GET, attenersi alle seguenti linee guida:

- Utilizzare dimensioni degli oggetti paragonabili agli oggetti che di solito si acquisiscono nella griglia.
- Eseguire operazioni su siti locali e remoti.

I messaggi in "[log di audit](#)" indicano il tempo totale necessario per eseguire determinate operazioni. Ad esempio, per determinare il tempo di elaborazione totale per una richiesta S3 GET, è possibile esaminare il valore dell'attributo TIME nel messaggio di audit SGET. È anche possibile trovare l'attributo TIME nei messaggi di controllo per le seguenti operazioni S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Durante l'analisi dei risultati, esaminare il tempo medio richiesto per soddisfare una richiesta e il throughput complessivo che è possibile ottenere. Ripetere regolarmente gli stessi test e registrare i risultati, in modo da poter identificare i trend che potrebbero richiedere un'indagine.

- È possibile "[Scarica S3tester da github](#)".

Monitorare le operazioni di verifica degli oggetti

Il sistema StorageGRID è in grado di verificare l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti danneggiati e mancanti.

Prima di iniziare

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

A proposito di 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 dell'oggetto.

La verifica in background verifica automaticamente e continuamente tutti i nodi di storage per determinare se sono presenti copie corrotte dei dati degli oggetti replicati e codificati in cancellazione. In caso di problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati dell'oggetto corrotto da copie memorizzate in un'altra parte del sistema. La verifica in background non viene eseguita sugli oggetti in un Cloud Storage Pool.



L'avviso **rilevato oggetto corrotto non identificato** viene attivato se il sistema rileva un oggetto corrotto che non può essere corretto automaticamente.

- **Il controllo dell'esistenza di oggetti** può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) dei dati dell'oggetto.

Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti consente di verificare l'integrità dei dispositivi di storage, in particolare se un recente problema hardware potrebbe aver influenzato l'integrità dei dati.

È necessario esaminare regolarmente i risultati delle verifiche in background e dei controlli sull'esistenza degli oggetti. Esaminare immediatamente eventuali istanze di dati degli oggetti corrotti o mancanti per determinare la causa principale.

Fasi

1. Esaminare i risultati delle verifiche in background:
 - a. Selezionare **NODI > nodo di storage > oggetti**.
 - b. Verificare i risultati della verifica:
 - Per controllare la verifica dei dati degli oggetti replicati, esaminare gli attributi nella sezione verifica.

Verification

Status: ?	No errors	
Percent complete: ?	0.00%	
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	

- Per controllare la verifica dei frammenti con codifica di cancellazione, selezionare **Storage Node > ILM** e controllare gli attributi nella sezione Erasure coding verification.

Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Selezionare il punto interrogativo ? accanto al nome di un attributo per visualizzare il testo della guida.

2. Esaminare i risultati dei job di controllo dell'esistenza di oggetti:
 - a. Selezionare **MANUTENZIONE > verifica dell'esistenza dell'oggetto > Cronologia lavori**.
 - b. Eseguire la scansione della colonna copie oggetto mancanti rilevate. Se un lavoro ha causato 100 o più copie di oggetti mancanti e l'avviso **oggetti persi** è stato attivato, contattare il supporto tecnico.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job Job history

Delete Search...

<input type="checkbox"/>	Job ID ?	Status ?	Nodes (volumes) ?	Missing object copies detected ?
<input type="checkbox"/>	15816859223101303015	Completed	DC2-S1 (3 volumes)	0
<input type="checkbox"/>	12538643155010477372	Completed	DC1-S3 (1 volume)	0
<input type="checkbox"/>	5490044849774982476	Completed	DC1-S2 (1 volume)	0
<input type="checkbox"/>	3395284277055907678	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0

Monitorare gli eventi

È possibile monitorare gli eventi rilevati da un nodo grid, inclusi gli eventi personalizzati creati per tenere traccia degli eventi registrati nel server syslog. Il messaggio Last Event (ultimo evento) visualizzato in Grid Manager fornisce ulteriori informazioni sull'evento più recente.

I messaggi di evento sono inoltre elencati nel `/var/local/log/bycast-err.log` file di registro. Consultare la "[Riferimenti ai file di log](#)".

L'allarme SMTT (Total events) può essere ripetutamente attivato da problemi come problemi di rete, interruzioni di corrente o aggiornamenti. Questa sezione contiene informazioni sull'analisi degli eventi, in modo da comprendere meglio il motivo per cui si sono verificati questi allarmi. Se un evento si è verificato a causa di un problema noto, è possibile ripristinare i contatori degli eventi in tutta sicurezza.

Fasi

- Esaminare gli eventi di sistema per ciascun nodo della griglia:
 - Selezionare **SUPPORT > Tools > Grid topology**.
 - Selezionare **site > grid node > SSM > Eventi > Panoramica > principale**.
- Genera un elenco di messaggi di eventi precedenti per isolare i problemi verificatisi in passato:

- Selezionare **SUPPORT > Tools > Grid topology**.
- Selezionare **site > grid node > SSM > Eventi > Report**.
- Selezionare **testo**.

L'attributo **ultimo evento** non viene visualizzato in "vista dei grafici". Per visualizzarlo:

- Modificare **attributo** in **ultimo evento**.
- Facoltativamente, selezionare un periodo di tempo per **Query rapida**.
- Selezionare **Aggiorna**.

Text Results for Last Event
2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Creare eventi syslog personalizzati

Gli eventi personalizzati consentono di tenere traccia di tutti gli eventi utente di kernel, daemon, errori e livello critico registrati sul server syslog. Un evento personalizzato può essere utile per monitorare l'occorrenza dei messaggi del registro di sistema (e quindi gli eventi di sicurezza della rete e gli errori hardware).



A proposito di questa attività

Prendere in considerazione la creazione di eventi personalizzati per monitorare i problemi ricorrenti. Le seguenti considerazioni si applicano agli eventi personalizzati.

- Dopo la creazione di un evento personalizzato, viene monitorata ogni occorrenza.
- Per creare un evento personalizzato basato su parole chiave nei `/var/local/log/messages` file, i log in tali file devono essere:
 - Generato dal kernel
 - Generato da daemon o programma utente a livello di errore o critico

Nota: non tutte le voci nei `/var/local/log/messages` file saranno abbinate a meno che non soddisfino i requisiti sopra indicati.

Fasi

1. Selezionare **SUPPORTO > Allarmi (legacy) > Eventi personalizzati**.
2. Fare clic su **Modifica**  (o **Inserisci**  se questo non è il primo evento).

3. Inserire una stringa di eventi personalizzata, ad esempio shutdown

The screenshot shows a web interface for managing events. At the top left, there is a small icon and the title "Events" with a timestamp "Updated: 2021-10-22 11:15:34 MDT". Below this, a section titled "Custom Events (1 - 1 of 1)" contains a table. The table has two columns: "Event" and "Actions". The "Event" column contains the text "shutdown". The "Actions" column contains four icons: a pencil (edit), a plus sign (add), a minus sign (delete), and a hand (stop). Below the table, there is a "Show 10 Records Per Page" dropdown menu, a "Refresh" button, and navigation links for "Previous" and "Next" (with "1" in the middle). At the bottom right, there is an "Apply Changes" button with a right-pointing arrow.

4. Selezionare **Applica modifiche**.

5. Selezionare **SUPPORT > Tools > Grid topology**.

6. Selezionare **grid node > SSM > Events**.

7. Individuare la voce per gli eventi personalizzati nella tabella Eventi e monitorare il valore per **Conteggio**.

Se il numero aumenta, viene attivato un evento personalizzato monitorato su quel nodo della griglia.

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC1-ADM1) - Events

Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State:	Connected	
Total Events:	0	
Last Event:	No Events	

Description	Count	
Abnormal Software Events	0	
Account Service Events	0	
Cassandra Errors	0	
Cassandra Heap Out Of Memory Errors	0	
Custom Events	0	
Data-Mover Service Events	0	
File System Errors	0	
Forced Termination Events	0	
Grid Node Errors	0	
Hotfix Installation Failure Events	0	
I/O Errors	0	
IDE Errors	0	
Identity Service Events	0	
Kernel Errors	0	
Kernel Memory Allocation Failure	0	
Keystone Service Events	0	
Network Receive Errors	0	
Network Transmit Errors	0	
Out Of Memory Errors	0	
Replicated State Machine Service Events	0	
SCSI Errors	0	


Azzerare il numero di eventi personalizzati

Se si desidera reimpostare il contatore solo per eventi personalizzati, è necessario utilizzare la pagina Grid Topology (topologia griglia) nel menu Support (supporto).

La reimpostazione di un contatore provoca l'attivazione dell'allarme all'evento successivo. Al contrario, quando si riconosce un allarme, questo viene riattivato solo se viene raggiunto il livello di soglia successivo.

Fasi

1. Selezionare **SUPPORT > Tools > Grid topology**.
2. Selezionare **grid node > SSM > Eventi > Configurazione > principale**.
3. Selezionare la casella di controllo **Reset** (Ripristina) per Custom Events (Eventi personalizzati).

Overview		Alarms		Reports		Configuration	
Main		Alarms					
 Configuration: SSM (DC2-ADM1) - Events Updated: 2018-04-11 10:35:44 MDT							
Description	Count			Reset			
Abnormal Software Events	0			<input type="checkbox"/>			
Account Service Events	0			<input type="checkbox"/>			
Cassandra Errors	0			<input type="checkbox"/>			
Cassandra Heap Out Of Memory Errors	0			<input type="checkbox"/>			
Custom Events	0			<input checked="" type="checkbox"/>			
File System Errors	0			<input type="checkbox"/>			
Forced Termination Events	0			<input type="checkbox"/>			

4. Selezionare **Applica modifiche**.

Esaminare i messaggi di audit

I messaggi di audit possono aiutarti a comprendere meglio le operazioni dettagliate del tuo sistema StorageGRID. È possibile utilizzare i registri di audit per risolvere i problemi e valutare le performance.

Durante il normale funzionamento del sistema, tutti i servizi StorageGRID generano messaggi di audit, come segue:

- I messaggi di audit del sistema sono correlati al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema e alle operazioni di backup del servizio.
- I messaggi di audit dello storage a oggetti sono correlati allo storage e alla gestione degli oggetti all'interno di StorageGRID, tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.
- I messaggi di controllo di lettura e scrittura del client vengono registrati quando un'applicazione client S3 richiede di creare, modificare o recuperare un oggetto.
- I messaggi di controllo della gestione registrano le richieste degli utenti all'API di gestione.

Ogni nodo amministrativo memorizza i messaggi di audit in file di testo. La condivisione dell'audit contiene il file attivo (audit.log) e i registri di audit compressi dei giorni precedenti. Ogni nodo della griglia memorizza anche una copia delle informazioni di audit generate sul nodo.

È possibile accedere ai file di log di controllo direttamente dalla riga di comando del nodo amministrativo.

StorageGRID può inviare informazioni di audit per impostazione predefinita, oppure è possibile modificare la destinazione:

- Il valore predefinito di StorageGRID per le destinazioni di audit dei nodi locali.
- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione.

- In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno.
- ["Informazioni sulla configurazione dei messaggi di controllo e delle destinazioni dei log"](#).

Per informazioni dettagliate 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, vedere ["Esaminare i registri di audit"](#).

Raccogliere i file di log e i dati di sistema

È possibile utilizzare Grid Manager per recuperare i file di log e i dati di sistema (inclusi i dati di configurazione) per il sistema StorageGRID.

Prima di iniziare

- È necessario aver effettuato l'accesso al Grid Manager sul nodo amministrativo primario utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- È necessario disporre della passphrase di provisioning.

A proposito di questa attività

È possibile utilizzare Grid Manager per raccogliere ["file di log"](#), dati di sistema e dati di configurazione da qualsiasi nodo della griglia per il periodo di tempo selezionato. I dati vengono raccolti e archiviati in un file .tar.gz che è possibile scaricare sul computer locale.

In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere ["Configurare i messaggi di audit e le destinazioni dei log"](#).

Fasi

1. Selezionare **SUPPORT > Tools > Logs**.

2. Selezionare i nodi della griglia per i quali si desidera raccogliere i file di log.

Se necessario, è possibile raccogliere i file di log per l'intera griglia o per un intero sito del data center.

3. Selezionare **ora di inizio** e **ora di fine** per impostare l'intervallo di tempo dei dati da includere nei file di log.

Se si seleziona un periodo di tempo molto lungo o si raccolgono i registri da tutti i nodi di una griglia di grandi dimensioni, l'archivio del registro potrebbe diventare troppo grande per essere memorizzato su un nodo o troppo grande per essere raccolto nel nodo di amministrazione primario per il download. In questo caso, è necessario riavviare la raccolta dei log con un set di dati più piccolo.

4. Selezionare i tipi di log che si desidera raccogliere.

- **Registri delle applicazioni:** Registri specifici delle applicazioni che il supporto tecnico utilizza più frequentemente per la risoluzione dei problemi. I log raccolti sono un sottoinsieme dei log dell'applicazione disponibili.
- **Audit Logs:** Registri contenenti i messaggi di audit generati durante il normale funzionamento del sistema.
- **Network Trace:** Registri utilizzati per il debug della rete.
- **Database Prometheus:** Metriche delle serie temporali dei servizi su tutti i nodi.

5. Se si desidera, inserire le note relative ai file di registro che si stanno raccogliendo nella casella di testo **Notes**.

È possibile utilizzare queste note per fornire informazioni di supporto tecnico sul problema che ha richiesto di raccogliere i file di log. Le note vengono aggiunte a un file denominato `info.txt`, insieme ad altre

informazioni sulla raccolta di file di registro. Il `info.txt` file viene salvato nel pacchetto di archiviazione del file di registro.

6. Inserire la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.
7. Selezionare **Collect Logs** (raccolta registri).

Quando si invia una nuova richiesta, la raccolta precedente di file di log viene eliminata.

È possibile utilizzare la pagina Logs per monitorare l'avanzamento della raccolta dei file di log per ciascun nodo della griglia.

Se viene visualizzato un messaggio di errore relativo alle dimensioni del registro, provare a raccogliere i registri per un periodo di tempo più breve o per un numero inferiore di nodi.

8. Selezionare **Download** al termine della raccolta dei file di log.

Il file `.tar.gz` contiene tutti i file di log di tutti i nodi della griglia in cui la raccolta dei log ha avuto esito positivo. All'interno del file `.tar.gz` combinato, è presente un archivio di file di log per ciascun nodo della griglia.

Al termine

Se necessario, è possibile scaricare nuovamente il pacchetto di archiviazione del file di log in un secondo momento.

In alternativa, è possibile selezionare **Delete** (Elimina) per rimuovere il pacchetto di archiviazione del file di log e liberare spazio su disco. Il pacchetto di archiviazione del file di log corrente viene automaticamente rimosso alla successiva raccolta dei file di log.

Attivare manualmente un pacchetto AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "[browser web supportato](#)".
- È necessario disporre dell'autorizzazione di accesso root o di altra configurazione della griglia.

Fasi

1. Selezionare **SUPPORTO > Strumenti > AutoSupport**.
2. Nella scheda **azioni**, selezionare **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 **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. Se si verifica un problema, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il pacchetto AutoSupport.

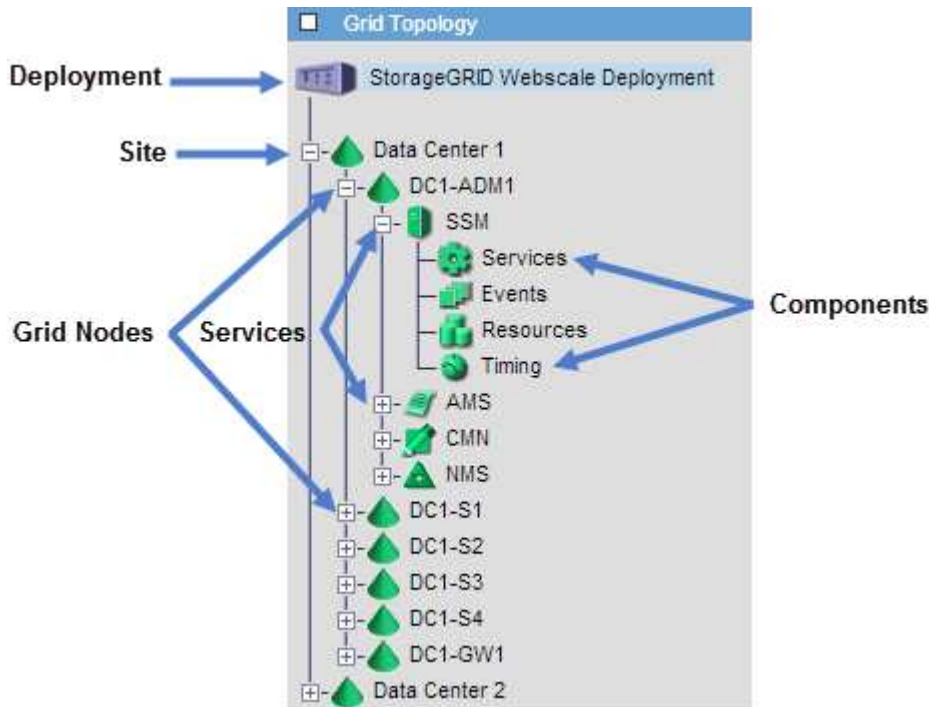


Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Visualizzare l'albero topologia griglia

L'albero topologia griglia consente di accedere a informazioni dettagliate sugli elementi del sistema StorageGRID, inclusi siti, nodi griglia, servizi e componenti. Nella maggior parte dei casi, è necessario accedere all'albero topologia griglia solo quando indicato nella documentazione o quando si lavora con il supporto tecnico.

Per accedere all'albero topologia griglia, selezionare **SUPPORTO > Strumenti > topologia griglia**.



Per espandere o comprimere l'albero topologia griglia, fare clic su **+** o **-** a livello di sito, nodo o servizio. Per espandere o comprimere tutti gli elementi dell'intero sito o di ciascun nodo, tenere premuto il tasto **<Ctrl>** e fare clic su.

Attributi StorageGRID

Gli attributi riportano valori e stati per molte delle funzioni del sistema StorageGRID. I valori degli attributi sono disponibili per ciascun nodo della griglia, per ciascun sito e per l'intera griglia.

Gli attributi StorageGRID vengono utilizzati in diversi punti del grid manager:

- Pagina **Nodes**: Molti dei valori mostrati nella pagina Nodes sono attributi StorageGRID. (Le metriche Prometheus sono visualizzate anche nelle pagine dei nodi).
- **Grid Topology tree**: I valori degli attributi vengono visualizzati nell'albero Grid Topology (**SUPPORTO > Tools > Grid Topology**).
- **Eventi**: Gli eventi di sistema si verificano quando alcuni attributi registrano una condizione di errore o di errore per un nodo, inclusi errori come gli errori di rete.

Valori degli attributi

Gli attributi vengono riportati con il massimo sforzo e sono approssimativamente corretti. In alcuni casi, gli aggiornamenti degli attributi possono andare persi, ad esempio il crash di un servizio o il guasto e la ricostruzione di un nodo di rete.

Inoltre, i ritardi di propagazione potrebbero rallentare il reporting degli attributi. I valori aggiornati per la maggior parte degli attributi vengono inviati al sistema StorageGRID a intervalli fissi. Possono essere necessari alcuni minuti prima che un aggiornamento sia visibile nel sistema e due attributi che cambiano più o meno contemporaneamente possono essere riportati in momenti leggermente diversi.

Rivedere le metriche di supporto

Durante la risoluzione di un problema, puoi lavorare con il supporto tecnico per rivedere metriche e grafici dettagliati per il tuo sistema StorageGRID.

Prima di iniziare

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

A proposito di questa attività

La pagina metriche consente di accedere alle interfacce utente Prometheus e Grafana. Prometheus è un software open-source per la raccolta di metriche. Grafana è un software open-source per la visualizzazione delle metriche.



Gli strumenti disponibili nella pagina metriche sono destinati all'utilizzo da parte del supporto tecnico. Alcune funzioni e voci di menu di questi strumenti sono intenzionalmente non funzionali e sono soggette a modifiche. Vedere l'elenco di ["Metriche Prometheus comunemente utilizzate"](#).

Fasi

1. Come indicato dal supporto tecnico, selezionare **SUPPORTO > Strumenti > metriche**.

Di seguito è riportato un esempio della pagina Metrics (metriche):

Metrics

Access charts and metrics to help troubleshoot issues.

 The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- <https://...>

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	EC Overview	Replicated Read Path Overview
Account Service Overview	Grid	S3 - Node
Alertmanager	ILM	S3 Overview
Audit Overview	Identity Service Overview	S3 Select
Cassandra Cluster Overview	Ingests	Site
Cassandra Network Overview	Node	Support
Cassandra Node Overview	Node (Internal Use)	Traces
Cross Grid Replication	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	

2. Per interrogare i valori correnti delle metriche StorageGRID e visualizzare i grafici dei valori nel tempo, fare clic sul collegamento nella sezione Prometheus.

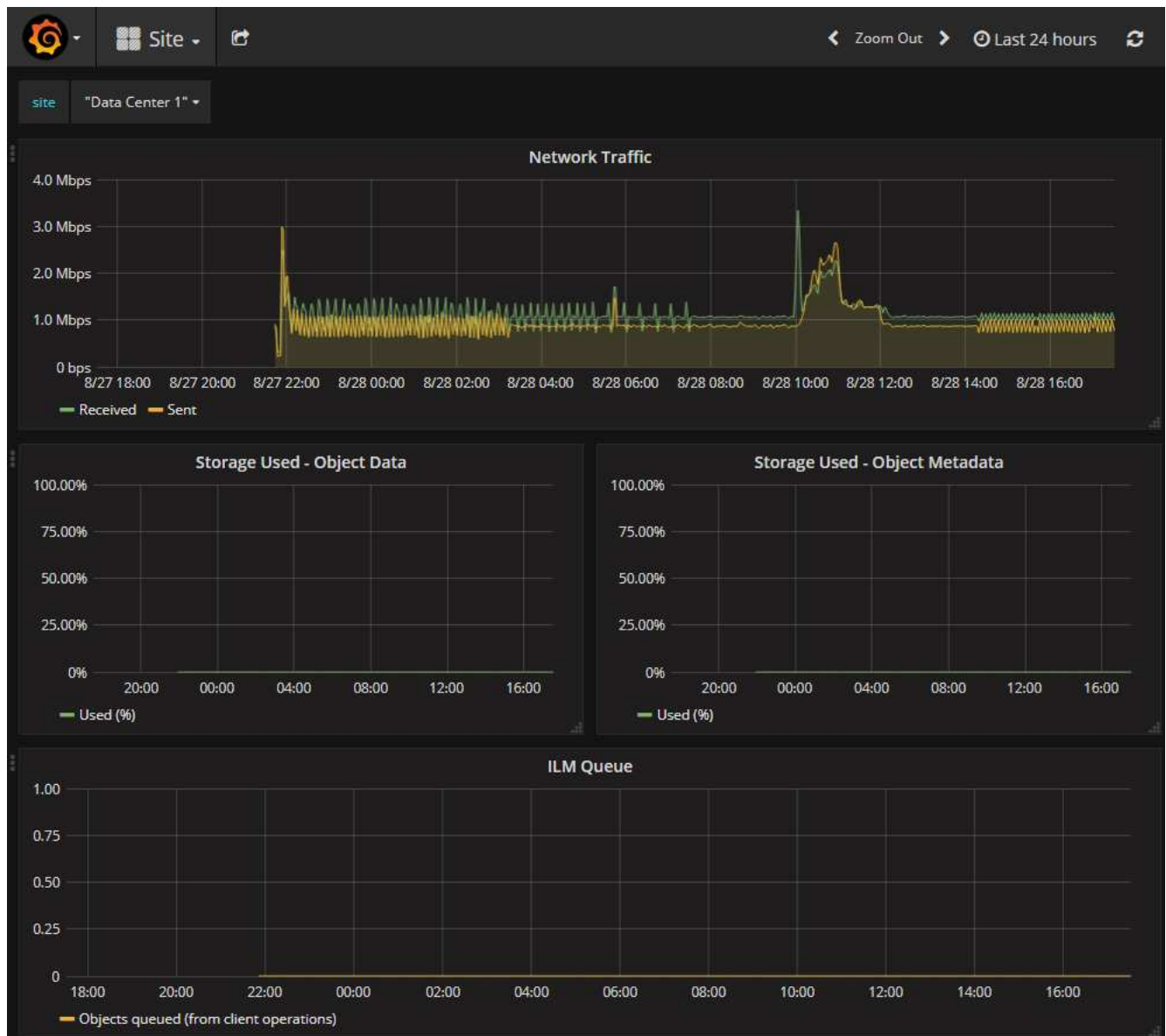
Viene visualizzata l'interfaccia Prometheus. È possibile utilizzare questa interfaccia per eseguire query sulle metriche StorageGRID disponibili e per rappresentare graficamente le metriche StorageGRID nel tempo.



Le metriche che includono *private* nei loro nomi sono destinate esclusivamente all'uso interno e sono soggette a modifiche tra le release di StorageGRID senza preavviso.

3. Per accedere alle dashboard predefinite contenenti grafici delle metriche StorageGRID nel tempo, fare clic sui collegamenti nella sezione Grafana.

Viene visualizzata l'interfaccia Grafana per il collegamento selezionato.



Eeguire la diagnostica

Durante la risoluzione di un problema, è possibile collaborare con il supporto tecnico per eseguire la diagnostica sul sistema StorageGRID e rivedere i risultati.

- ["Rivedere le metriche di supporto"](#)
- ["Metriche Prometheus comunemente utilizzate"](#)

Prima di iniziare

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

A proposito di questa attività

La pagina Diagnostics (Diagnostica) esegue una serie di controlli diagnostici sullo stato corrente 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 non rientrano nell'intervallo normale.
- ✖ **Attenzione:** Uno o più valori sono significativamente al di fuori del range normale.

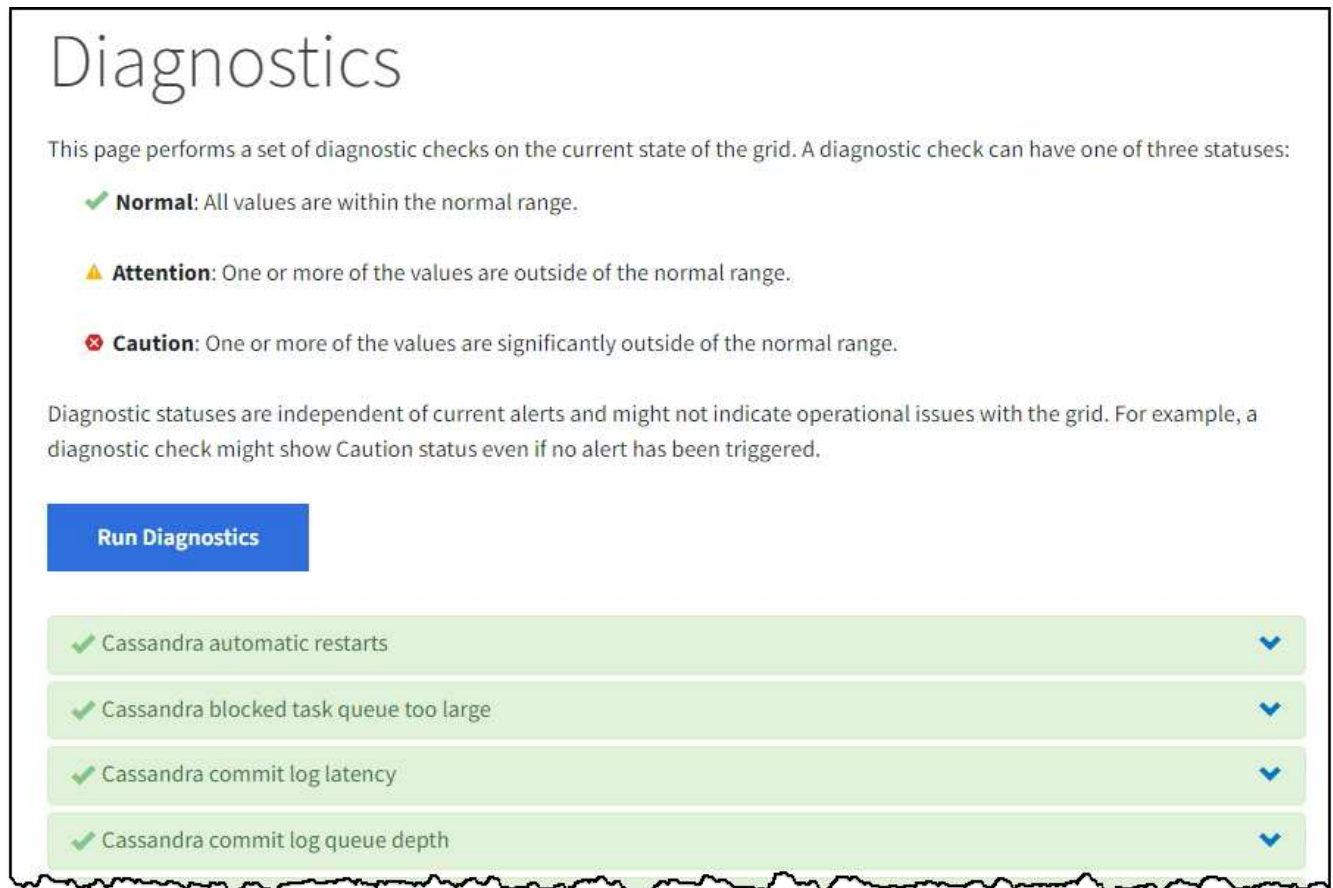
Gli stati di diagnostica sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la griglia. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato di attenzione anche se non è stato attivato alcun allarme.

Fasi

1. Selezionare **SUPPORTO > Strumenti > Diagnostica**.

Viene visualizzata la pagina Diagnostics (Diagnostica) che elenca i risultati di ciascun controllo diagnostico. I risultati vengono ordinati in base alla gravità (attenzione, attenzione e quindi normale). All'interno di ciascuna severità, i risultati sono ordinati in ordine alfabetico.

In questo esempio, tutte le diagnostiche hanno uno stato normale.



The screenshot shows a web interface titled "Diagnostics". Below the title, there is an explanatory text: "This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:". This is followed by three status definitions:

- ✓ **Normal:** All values are within the normal range.
- ⚠ **Attention:** One or more of the values are outside of the normal range.
- ✖ **Caution:** One or more of the values are significantly outside of the normal range.

 Below this, another text block states: "Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered." A blue button labeled "Run Diagnostics" is visible. At the bottom, there is a list of four diagnostic checks, each in a light green box with a checkmark icon on the left and a dropdown arrow on the right:

- ✓ Cassandra automatic restarts
- ✓ Cassandra blocked task queue too large
- ✓ Cassandra commit log latency
- ✓ Cassandra commit log queue depth

 The entire screenshot is framed with a torn paper effect at the bottom edge.

2. Per ulteriori informazioni su una diagnostica specifica, fare clic in un punto qualsiasi della riga.

Vengono visualizzati i dettagli relativi alla diagnostica e ai risultati correnti. Sono elencati i seguenti dettagli:

- **Status (Stato):** Lo stato corrente di questa diagnostica: Normal (normale), Attention (attenzione) o Caution (attenzione).
- **Query Prometheus:** Se utilizzata per la diagnostica, l'espressione Prometheus utilizzata per generare

i valori di stato. (Un'espressione Prometheus non viene utilizzata per tutte le diagnostiche).

- **Soglie:** Se disponibili per la diagnostica, le soglie definite dal sistema per ogni stato di diagnostica anomalo. (I valori di soglia non vengono utilizzati per tutte le diagnostiche).



Non puoi modificare queste soglie.

- **Valori di stato:** Una tabella che mostra lo stato e il valore della diagnostica nel 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 attenzione, quindi lo stato generale della diagnostica è normale.

✓ **CPU utilization**

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status ✓ Normal

Prometheus query `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`
[View in Prometheus](#)

Thresholds
⚠ Attention >= 75%
⊗ Caution >= 95%

Status	Instance	CPU Utilization
✓	DC1-ADM1	2.598%
✓	DC1-ARC1	0.937%
✓	DC1-G1	2.119%
✓	DC1-S1	8.708%
✓	DC1-S2	8.142%
✓	DC1-S3	9.669%
✓	DC2-ADM1	2.515%
✓	DC2-ARC1	1.152%
✓	DC2-S1	8.204%
✓	DC2-S2	5.000%
✓	DC2-S3	10.469%

3. **Opzionale:** Per visualizzare i grafici Grafana relativi a questa diagnostica, fare clic sul collegamento **dashboard Grafana**.

Questo collegamento non viene visualizzato per tutte le diagnostiche.

Viene visualizzata la dashboard Grafana correlata. In questo esempio, viene visualizzata la dashboard Node (nodo) che mostra l'utilizzo della CPU nel tempo per questo nodo e altri grafici Grafana per il nodo.



Puoi anche accedere ai dashboard di Grafana già costruiti dalla sezione Grafana della pagina **SUPPORT > Tools > Metrics**.



4. **Opzionale:** Per visualizzare un grafico dell'espressione Prometheus nel tempo, fare clic su **Visualizza in Prometheus**.

Viene visualizzato un grafico Prometheus dell'espressione utilizzata nella diagnostica.

Enable query history

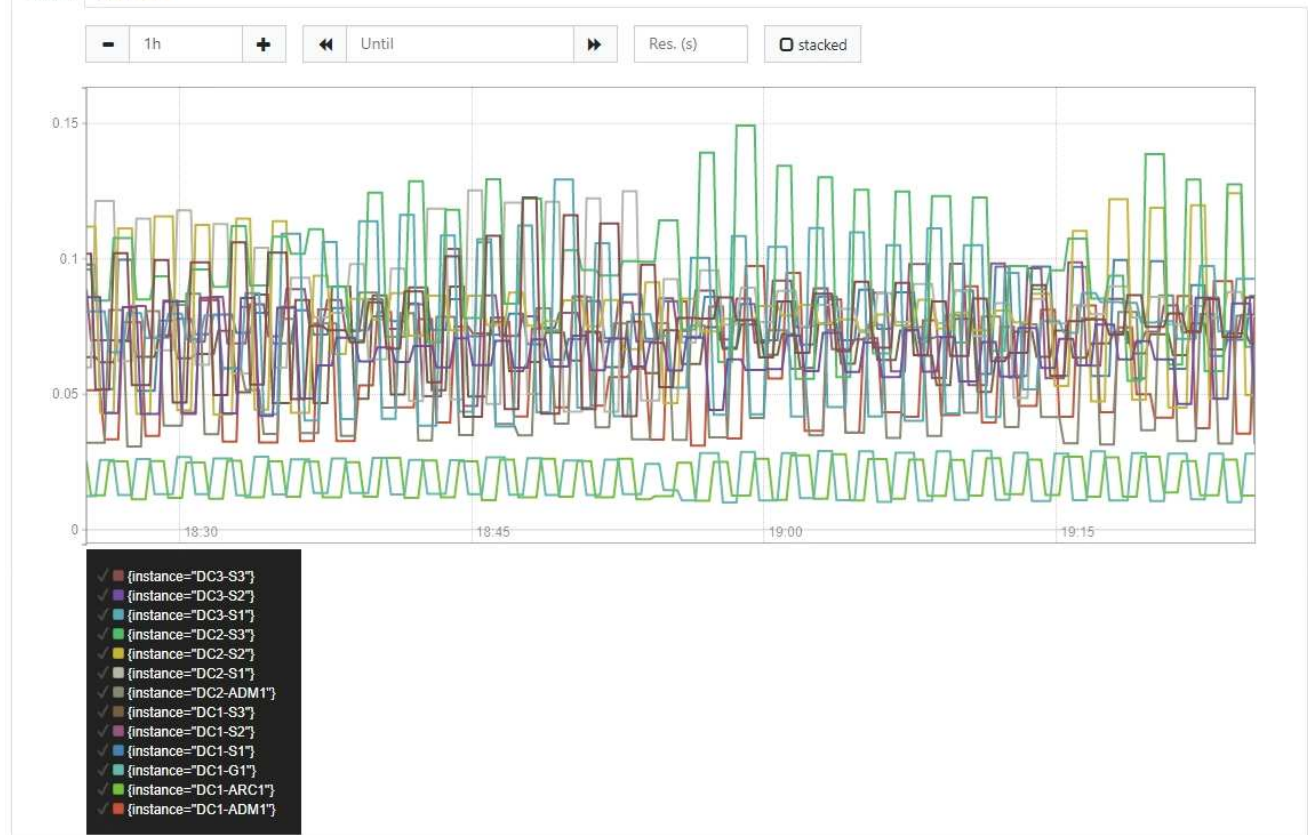
```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor -

Graph Console



Remove Graph

Add Graph

Creare applicazioni di monitoraggio personalizzate

Puoi creare dashboard e applicazioni di monitoraggio personalizzate utilizzando le metriche StorageGRID disponibili nell'API di gestione del grid.

Se si desidera monitorare le metriche non visualizzate in una pagina esistente di Grid Manager o se si desidera creare dashboard personalizzati per StorageGRID, è possibile utilizzare l'API di gestione griglia per eseguire query sulle metriche StorageGRID.

Puoi anche accedere direttamente alle metriche Prometheus con uno strumento di monitoraggio esterno, come Grafana. L'utilizzo di uno strumento esterno richiede il caricamento o la generazione di un certificato client amministrativo per consentire a StorageGRID di autenticare lo strumento per la sicurezza. Consultare la ["Istruzioni per l'amministrazione di StorageGRID"](#).

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, accedere a Grid Manager. Nella parte superiore della pagina, selezionare l'icona della guida e selezionare **documentazione API > metriche**.



GET	<code>/grid/metric-labels/{label}/values</code> Lists the values for a metric label	
GET	<code>/grid/metric-names</code> Lists all available metric names	
GET	<code>/grid/metric-query</code> Performs an instant metric query at a single point in time	
GET	<code>/grid/metric-query-range</code> Performs a metric query over a range of time	

I dettagli su come implementare un'applicazione di monitoraggio personalizzata esulano dall'ambito di questa documentazione.

Risolvere i problemi relativi al sistema StorageGRID

Risolvere i problemi di un sistema StorageGRID

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

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

definire il problema

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

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

Domanda	Esempio di risposta
Cosa fa o non fa il sistema StorageGRID? Quali sono i suoi sintomi?	Le applicazioni client segnalano che non è possibile acquisire oggetti in StorageGRID.
Quando è iniziato il problema?	L'acquisizione di oggetti è stata negata per la prima volta alle 14:50 dell'8 gennaio 2020.
Come hai notato il problema per la prima volta?	Notificato dall'applicazione client. Ha ricevuto anche notifiche email di avviso.
Il problema si verifica in modo coerente o solo a volte?	Il problema è in corso.

Domanda	Esempio di risposta
Se il problema si verifica regolarmente, quali passaggi lo causano	Il problema si verifica ogni volta che un client tenta di acquisire un oggetto.
Se il problema si verifica in modo intermittente, quando si verifica? Registrare i tempi di ciascun incidente di cui si è a conoscenza.	Il problema non è intermittente.
Hai già visto questo problema? Con quale frequenza avete avuto questo problema in passato?	Questa è la prima volta che vedo questo problema.

Valutare i rischi e l'impatto sul sistema

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

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

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

Raccogliere i dati

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

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Creare una tempistica delle modifiche recenti	Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	<ul style="list-style-type: none"> • Creare una tempistica delle modifiche recenti

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Rivedere gli avvisi	<p>Gli avvisi possono aiutare a determinare rapidamente la causa principale di un problema fornendo indizi importanti sui problemi sottostanti che potrebbero causarlo.</p> <p>Esaminare l'elenco degli avvisi correnti per verificare se StorageGRID ha identificato la causa principale di un problema.</p> <p>Rivedi gli avvisi attivati in passato per ulteriori informazioni.</p>	<ul style="list-style-type: none"> • "Visualizzare gli avvisi correnti e risolti"
Monitorare gli eventi	<p>Gli eventi includono qualsiasi errore di sistema o evento di guasto per un nodo, inclusi errori come gli errori di rete. Monitorare gli eventi per ottenere ulteriori informazioni sui problemi o per la risoluzione dei problemi.</p>	<ul style="list-style-type: none"> • "Monitorare gli eventi"
Identificare i trend utilizzando grafici e report di testo	<p>Le tendenze possono fornire indizi preziosi su quando sono comparsi i problemi per la prima volta e possono aiutarti a capire quanto rapidamente le cose stanno cambiando.</p>	<ul style="list-style-type: none"> • "Utilizzare grafici e grafici" • "Utilizzare report di testo"
Stabilire le linee di base	<p>Raccogliere informazioni sui livelli normali dei vari valori operativi. Questi valori di riferimento, e le deviazioni da queste linee di base, possono fornire indizi preziosi.</p>	<ul style="list-style-type: none"> • Stabilire le linee di base
Eseguire test di acquisizione e recupero	<p>Per risolvere i problemi di performance con acquisizione e recupero, utilizzare una workstation per memorizzare e recuperare gli oggetti. Confrontare i risultati con quelli osservati durante l'utilizzo dell'applicazione client.</p>	<ul style="list-style-type: none"> • "Monitorare L'EFFICIENZA e OTTENERE le performance"
Esaminare i messaggi di audit	<p>Esaminare i messaggi di audit per seguire in dettaglio le operazioni di StorageGRID. I dettagli nei messaggi di audit possono essere utili per la risoluzione di molti tipi di problemi, inclusi quelli relativi alle performance.</p>	<ul style="list-style-type: none"> • "Esaminare i messaggi di audit"
Controllare le posizioni degli oggetti e l'integrità dello storage	<p>In caso di problemi di storage, verificare che gli oggetti siano posizionati nel punto previsto. Verificare l'integrità dei dati dell'oggetto su un nodo di storage.</p>	<ul style="list-style-type: none"> • "Monitorare le operazioni di verifica degli oggetti" • "Confermare le posizioni dei dati degli oggetti" • "Verificare l'integrità dell'oggetto"

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Raccogliere i dati per il supporto tecnico	Il supporto tecnico potrebbe richiedere di raccogliere dati o rivedere informazioni specifiche per risolvere i problemi.	<ul style="list-style-type: none"> • "Raccogliere i file di log e i dati di sistema" • "Attivare manualmente un pacchetto AutoSupport" • "Rivedere le metriche di supporto"

Crea una timeline di modifiche recenti

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

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

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

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

Esempi di modifiche recenti significative

Ecco alcuni esempi di modifiche potenzialmente significative:

- Il sistema StorageGRID è stato recentemente installato, ampliato o ripristinato?
- Il sistema è stato aggiornato di recente? È stata applicata una correzione rapida?
- L'hardware è stato riparato o modificato di recente?
- La policy ILM è stata aggiornata?

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

Stabilire le linee di base

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

Proprietà	Valore	Come ottenere
Consumo medio di storage	GB consumati al giorno Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione). Nel grafico Storage used - Object Data (Storage utilizzato - dati oggetto), individuare un periodo in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare la quantità di storage consumata ogni giorno. È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.

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

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

Analizzare i dati


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

-analisi dipende dal problema, ma in generale:

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

Lista di controllo per le informazioni di escalation

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

	Elemento	Note
	Dichiarazione del problema	Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo coerente o intermittente? In caso di intermittenza, quali sono le volte in cui si è verificato il problema? Definire il problema
	Valutazione dell'impatto	Qual è la gravità del problema? Qual è l'impatto sull'applicazione client? <ul style="list-style-type: none"> • Il client si è connesso correttamente in precedenza? • Il client è in grado di acquisire, recuperare ed eliminare i dati?
	ID sistema StorageGRID	Selezionare MANUTENZIONE > sistema > licenza . L'ID di sistema StorageGRID viene visualizzato come parte della licenza corrente.

✓	Elemento	Note
	Versione del software	Nella parte superiore di Gestione griglia, selezionare l'icona della guida e selezionare About (informazioni su) per visualizzare la versione di StorageGRID.
	Personalizzazione	<p>Riepilogare la configurazione del sistema StorageGRID. Ad esempio, elencare quanto segue:</p> <ul style="list-style-type: none"> • Il grid utilizza la compressione dello storage, la crittografia dello storage o la conformità? • ILM produce oggetti replicati o sottoposti a erasure coding? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano i comportamenti di ingest bilanciato, rigoroso o doppio commit?
	File di log e dati di sistema	<p>Raccogliere i file di log e i dati di sistema per il sistema. Selezionare SUPPORT > Tools > Logs.</p> <p>È possibile raccogliere i log per l'intera griglia o per i nodi selezionati.</p> <p>Se si stanno raccogliendo registri solo per i nodi selezionati, assicurarsi di includere almeno un nodo di storage che dispone del servizio ADC. I primi tre nodi di storage di un sito includono il servizio ADC.</p> <p>"Raccogliere i file di log e i dati di sistema"</p>
	Informazioni di riferimento	<p>Raccogliere informazioni di riferimento relative alle operazioni di acquisizione, alle operazioni di recupero e al consumo dello storage.</p> <p>Stabilire le linee di base</p>
	Tempistiche delle modifiche recenti	<p>Creare una timeline che riepiloga le modifiche recenti apportate al sistema o al suo ambiente.</p> <p>Creare una tempistica delle modifiche recenti</p>
	Cronologia degli sforzi per diagnosticare il problema	<p>Se sono state adottate misure per diagnosticare o risolvere il problema da soli, assicurarsi di registrare i passaggi e il risultato.</p>

Risolvere i problemi relativi a oggetti e storage

Confermare le posizioni dei dati degli oggetti

A seconda del problema, potrebbe essere necessario scegliere ["confermare la posizione in cui vengono memorizzati i dati dell'oggetto"](#). Ad esempio, è possibile verificare che il

criterio ILM funzioni come previsto e che i dati degli oggetti vengano memorizzati dove previsto.

Prima di iniziare

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

Fasi

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

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

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



4. Selezionare **Cerca**.

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

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

- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

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

System Metadata

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

Replicated Copies

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

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36056",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PARTS": "2",








```

Errori dell'archivio di oggetti (volume di storage)




















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

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






























Disk devices

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

Volumes

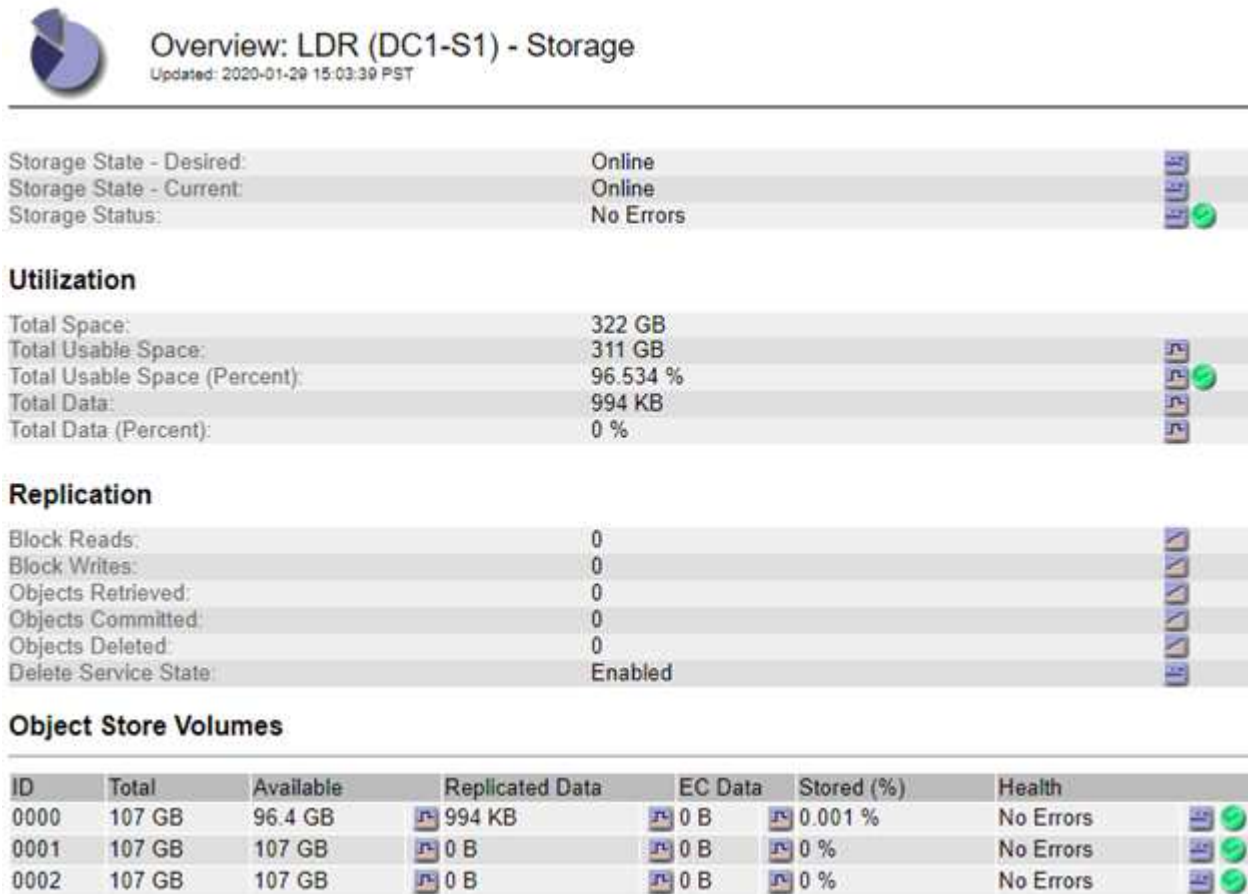
Mount point  	Device  	Status  	Size  	Available  	Write cache status  
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2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

Object stores

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

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

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



Overview: LDR (DC1-S1) - Storage
Updated: 2020-01-29 15:03:39 PST

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

Utilization

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

Replication

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

Object Store Volumes

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

A seconda della natura del guasto, i guasti relativi a un volume di memorizzazione potrebbero essere riportati in "[avvisi relativi al volume di storage](#)". In caso di guasto di un volume di storage, è necessario riparare il volume di storage guasto per ripristinare la funzionalità completa del nodo di storage il prima possibile. Se necessario, è possibile accedere alla scheda **Configurazione** e "[Posizionare il nodo di storage in uno stato di sola-lettura](#)" in modo che il sistema StorageGRID possa utilizzarlo per il recupero dei dati mentre si prepara per un ripristino completo del server.

Verificare l'integrità dell'oggetto

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

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

Che cos'è la verifica in background?

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

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

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

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



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

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

Il processo di verifica in background controlla solo gli oggetti sui nodi di storage. Non controlla gli oggetti in un Cloud Storage Pool. Gli oggetti devono avere più di quattro giorni di età per poter essere qualificati per la verifica in background.

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

Avvisi relativi alla verifica in background

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

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

Modificare il tasso di verifica in background

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

Prima di iniziare

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

A proposito di questa attività

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

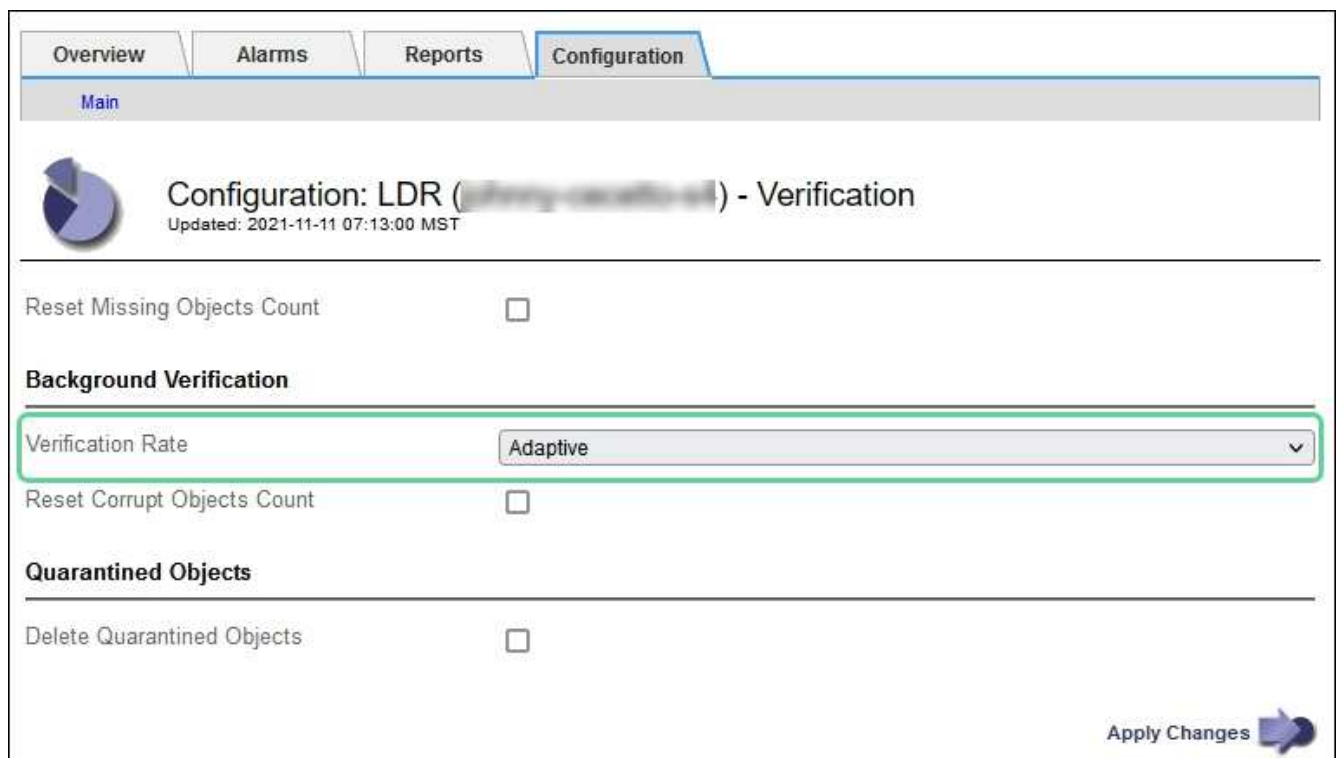
- **Adattivo:** Impostazione predefinita. L'attività è progettata per la verifica a un massimo di 4 MB/s o 10 oggetti/s (a seconda di quale valore viene superato per primo).

- Elevato: La verifica dello storage procede rapidamente, a una velocità che può rallentare le normali attività del sistema.

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

Fasi

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



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

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

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

object detected.

- c. Se vengono rilevati dati di oggetti replicati corrotti, contattare il supporto tecnico per determinare la causa principale del danneggiamento.
8. Monitorare i risultati della verifica in background per gli oggetti con codifica erasure.
- Se la verifica in background trova frammenti corrotti di dati di oggetti con codifica di cancellazione, l'attributo corrotto Fragments Detected (frammenti corrotti rilevati) viene incrementato. StorageGRID esegue il ripristino ricostruendo il frammento corrotto in posizione sullo stesso nodo di storage.
- a. Selezionare **SUPPORT > Tools > Grid topology**.
 - b. Selezionare **Storage Node > LDR > Erasure Coding**.
 - c. Nella tabella Verification Results (risultati verifica), monitorare l'attributo corrotto Fragments Detected (ECCD).
9. Una volta ripristinati automaticamente gli oggetti corrotti dal sistema StorageGRID, ripristinare il numero di oggetti corrotti.
- a. Selezionare **SUPPORT > Tools > Grid topology**.
 - b. Selezionare **Storage Node > LDR > Verification > Configuration**.
 - c. Selezionare **Ripristina conteggio oggetti corrotti**.
 - d. Fare clic su **Applica modifiche**.
10. Se sei sicuro che gli oggetti in quarantena non sono necessari, puoi eliminarli.



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

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

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

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

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

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

- **Copie replicate:** Se manca una copia dei dati degli oggetti replicati, StorageGRID tenta automaticamente di sostituire la copia da una copia memorizzata altrove nel sistema. Il nodo di storage esegue una copia esistente attraverso una valutazione ILM, che determina che il criterio ILM corrente non è più soddisfatto

per questo oggetto perché manca un'altra copia. Viene generata e posizionata una nuova copia per soddisfare i criteri ILM attivi del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa posizione in cui è stata memorizzata la copia mancante.

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

Eeguire il controllo dell'esistenza dell'oggetto

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

Prima di iniziare

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

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

A proposito di questa attività

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

Fasi

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

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

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

4. Selezionare **continua**.

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

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

6. Selezionare **continua**.

7. Selezionare la coerenza per il lavoro.

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

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

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

8. Selezionare **continua**.

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

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

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



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

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

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

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

Object existence check

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

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

Active job Job history

Status: **Accepted** Consistency control: **All**
Job ID: 2334602652907829302 Start time: 2021-11-10 14:43:02 MST
Missing object copies detected: **0** Elapsed time: —
Progress: 0% Estimated time to completion: —

Pause Cancel

Volumes Details

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

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

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

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

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

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

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

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

Object existence check

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

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

Active job | Job history

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

Displaying 4 results

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

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

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

Al termine

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

Risoluzione dei problemi S3 - Avviso DIMENSIONE oggetto troppo grande

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

Prima di iniziare

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

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

Fasi

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

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

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

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



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

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

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

Esempio di risultati del registro di controllo


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

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

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

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

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

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

Esempio di `bycast.log`

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

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

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

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

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

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

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

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

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

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

Esaminare gli oggetti persi

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

Prima di iniziare

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

A proposito di questa attività

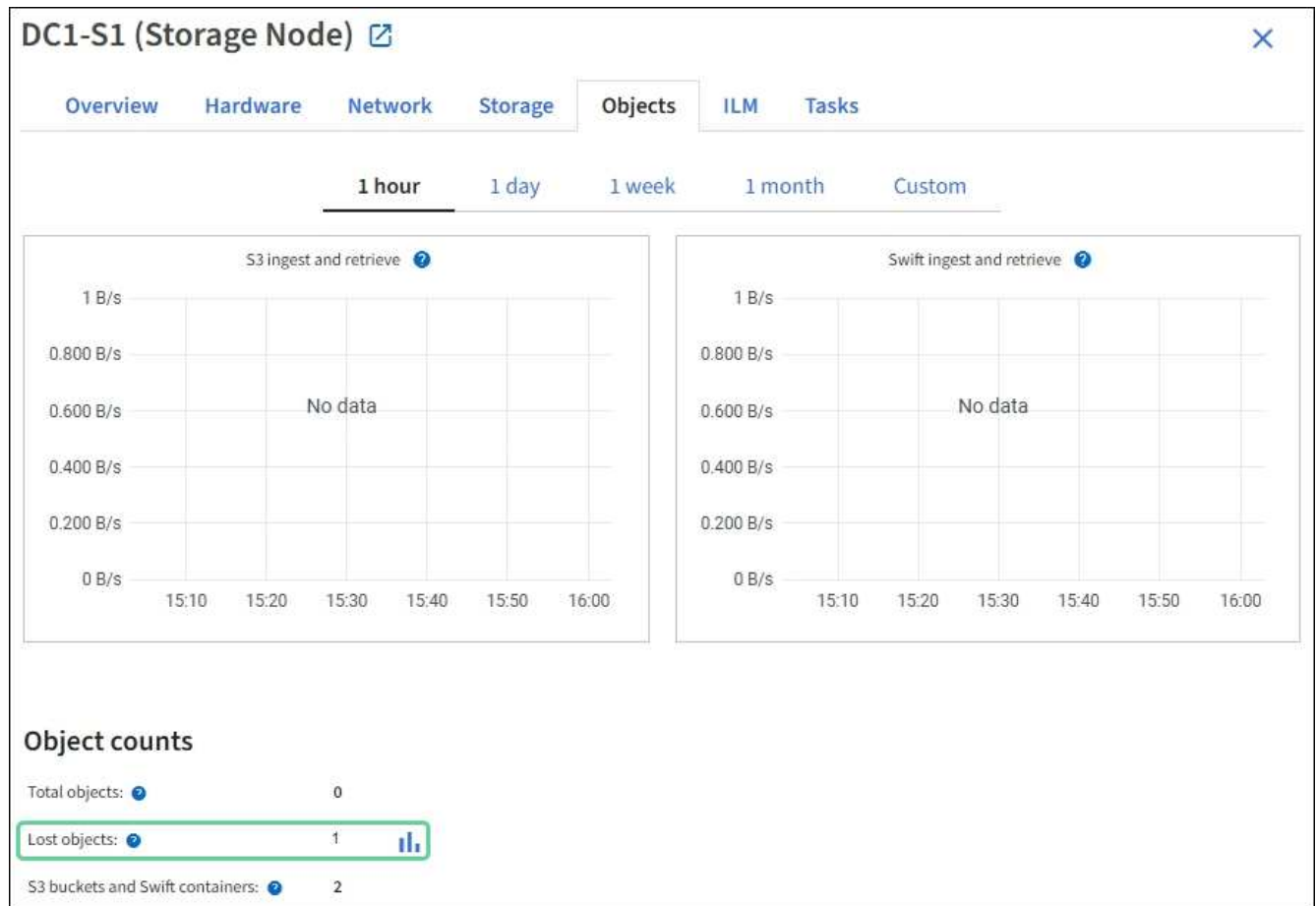
L'avviso **oggetti persi** indica che StorageGRID ritiene che non vi siano copie di un oggetto nella griglia. I dati potrebbero essere stati persi in modo permanente.

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

Fasi

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

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



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

a. Accedere al nodo Grid:

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

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



"Informazioni sulle destinazioni per le informazioni di verifica".

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

d. Annotare il valore UUID incluso nel messaggio.

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

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

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

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

Cercare e ripristinare oggetti potenzialmente persi

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

Prima di iniziare

- Si dispone dell'UUID di qualsiasi oggetto perso, come identificato in ["Esaminare gli oggetti persi"](#).
- Si dispone del `Passwords.txt` file.

A proposito di questa attività

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



Contattare il supporto tecnico per assistenza con questa procedura.

Fasi

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

a. Accedere al nodo Grid:

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

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



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

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

Ad esempio:

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

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

Ad esempio:

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

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

```
[AUDT:\[NOID\ (UI32\):12448208\] [CBIL (UI64) :0x38186FE53E3C49A5]
[UUID (CSTR) : "926026C4-00A4-449B-AC72-BCCA72DD1311"] [LTYP (FC32) :CLDI]
[PCLD\ (CSTR\): "/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6"\]
[TSRC (FC32) :SYST] [RSLT (FC32) :NONE] [AVER (UI32) :10] [ATIM (UI64) :
1581535134379225] [ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CL
SM]
[ATID (UI64) :7086871083190743409]]
```

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

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

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

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

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

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

a. Accedere al nodo Grid:

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

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

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

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

Ad esempio, immettere:

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



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

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

ripristinare l'oggetto trovato in StorageGRID.

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

Ad esempio, immettere:

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

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



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

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

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

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

Passare alla fase successiva.

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

a. Accedere al nodo Grid:

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

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

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

Ad esempio:

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

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

Ad esempio:

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

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

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

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

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

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

Ripristinare i conteggi degli oggetti persi e mancanti

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

azzerare il valore dell'attributo oggetti persi.

Prima di iniziare

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

A proposito di questa attività

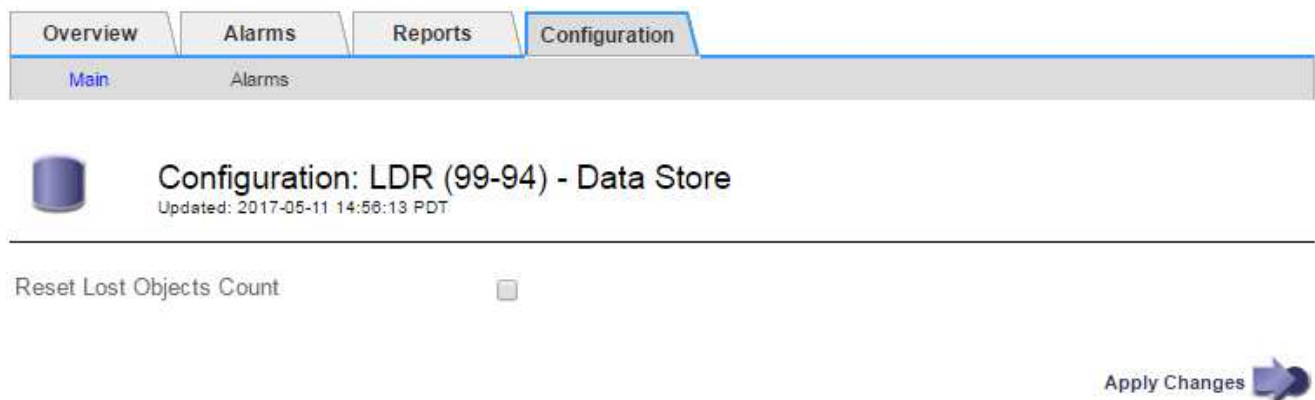
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

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

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

Fasi

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



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

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

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

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

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

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

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

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

In questa condizione:

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

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

Fasi

1. Selezionare **ALERTS > current**.

Viene visualizzata la pagina Avvisi.

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

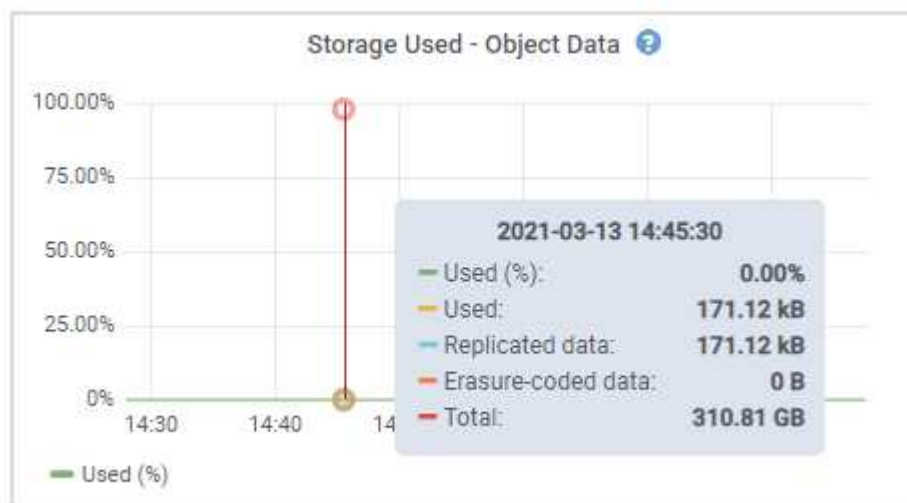


Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.

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

Vengono visualizzati i seguenti valori:

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



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

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

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

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



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

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

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, potrebbe essere

necessario risolvere l'avviso **bassa sostituzione filigrana di sola lettura**. Se possibile, aggiornare il sistema per iniziare a utilizzare i valori ottimizzati.

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

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

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

Comprendere l'avviso

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

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

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

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

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

Risolvere l'avviso

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

Prima di iniziare

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

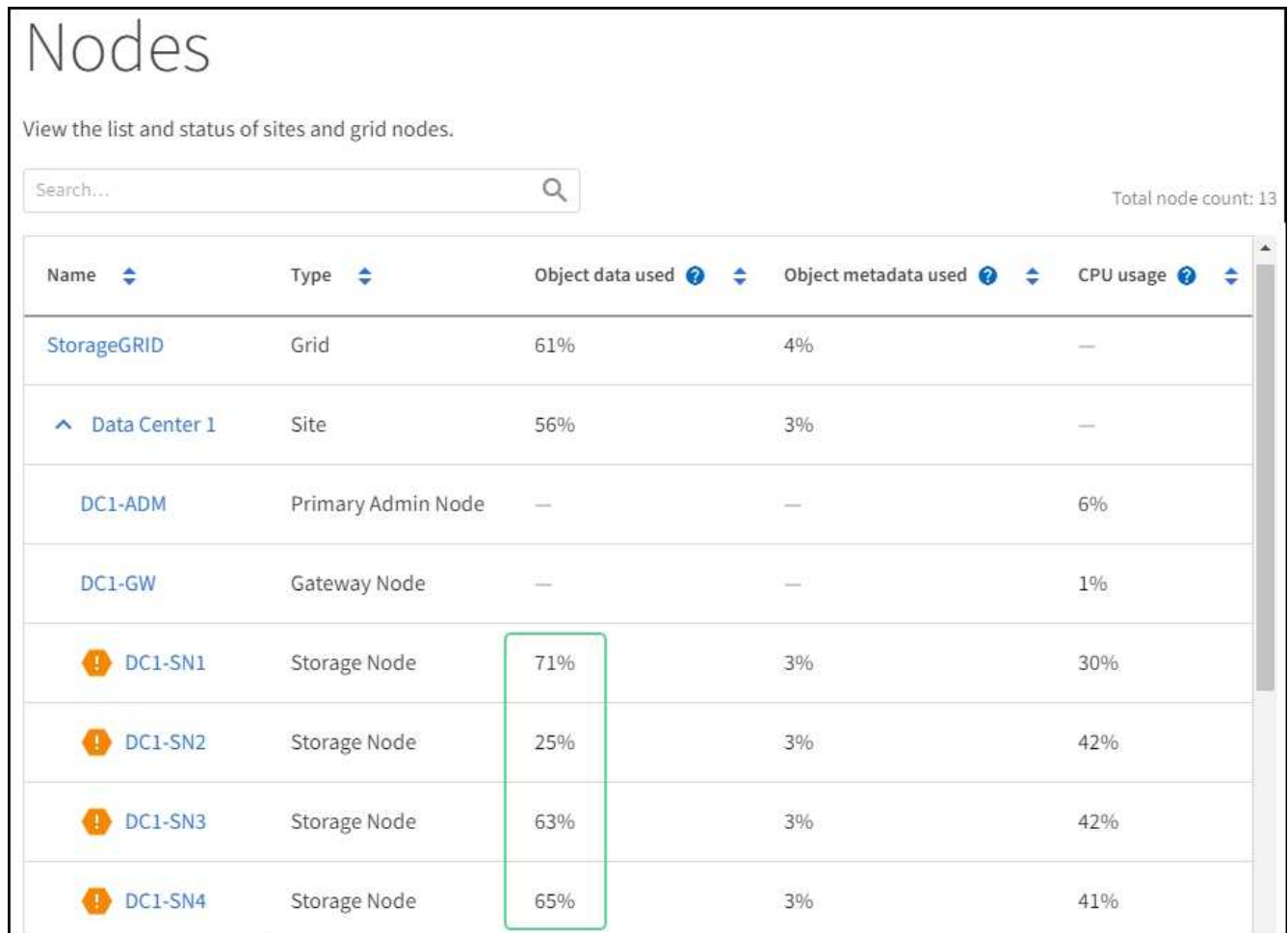
A proposito di questa attività

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

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

Fasi

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



Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

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

4. Seguire la procedura appropriata:
 - a. Se nessuno dei nodi di storage è quasi pieno (ad esempio, tutti i valori **dati oggetto utilizzati** sono inferiori al 80%), è possibile iniziare a utilizzare le impostazioni di override. Andare a [Utilizzare filigrane](#)

ottimizzate.

- b. Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se i pool di storage specifici sono quasi completi, eseguire i passaggi in [Visualizza filigrane di storage ottimizzate](#) e [Determinare se è possibile utilizzare filigrane ottimizzate](#).

Visualizza filigrane di memorizzazione ottimizzate

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

Fasi

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

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato del watermark di sola lettura soft per tutti i volumi di archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per il watermark soft di sola lettura del volume di archiviazione, viene attivato l'avviso **low Read-only watermark override** per il nodo di archiviazione.

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

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

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

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

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

Fasi

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

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

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



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

utilizza filigrane ottimizzate

Fasi

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

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

Risolvere i problemi relativi ai metadati

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

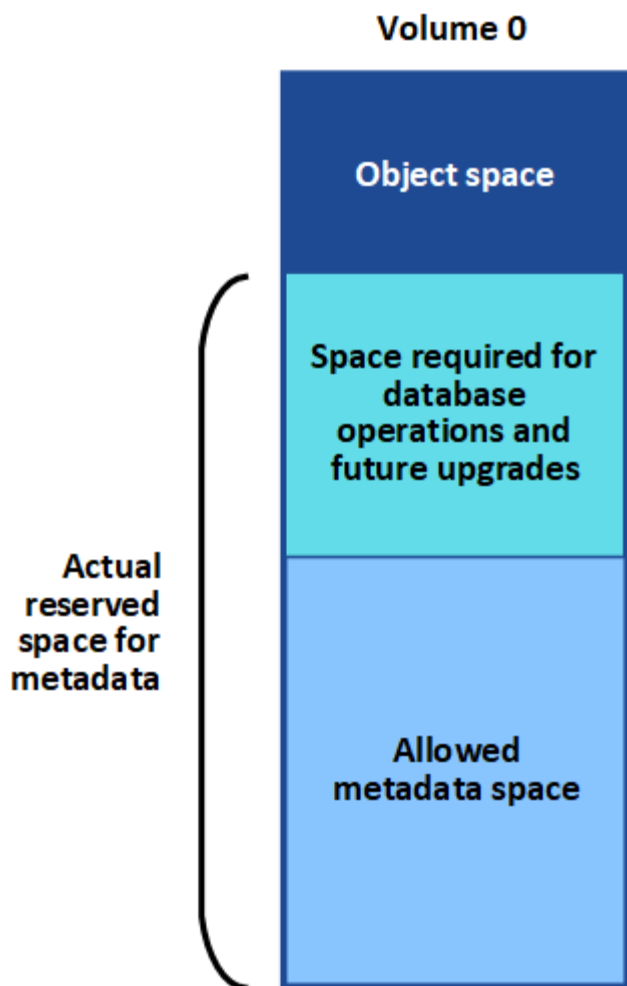
Prima di iniziare

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

A proposito di questa attività

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

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



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

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

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

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

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



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

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



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

Fasi

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



Poiché StorageGRID conserva copie complete di tutti i metadati degli oggetti in ogni sito, la capacità dei metadati dell'intera griglia è limitata dalla capacità dei metadati del sito più piccolo. Se è necessario aggiungere capacità di metadati a un sito, è necessario utilizzare anche ["espandere qualsiasi altro sito"](#) lo stesso numero di nodi di archiviazione.

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

Risolvere gli errori del certificato

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

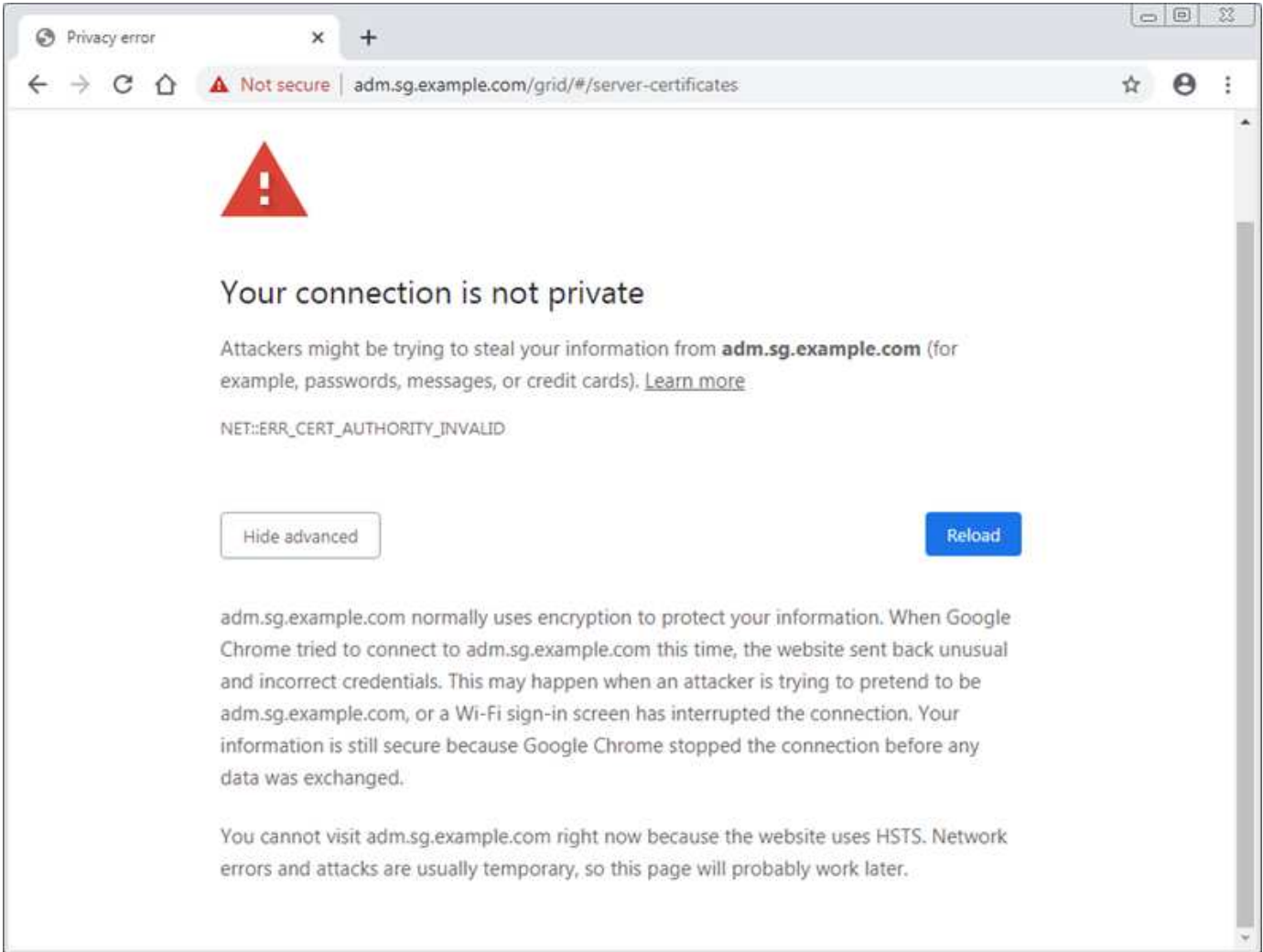
A proposito di questa attività

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

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

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

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



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

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

Fasi

Se si riceve una notifica di avviso relativa a un certificato scaduto, accedere ai dettagli del certificato: .

Selezionare **CONFIGURAZIONE > sicurezza > certificati** e quindi "[selezionare la scheda del certificato appropriata](#)".

1. Controllare il periodo di validità del certificato. + alcuni browser web e client S3 non accettano certificati con un periodo di validità superiore a 398 giorni.
2. Se il certificato è scaduto o scadrà a breve, caricare o generare un nuovo certificato.
 - Per un certificato server, vedere la procedura per "[Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager](#)".

- Per un certificato client, vedere la procedura per ["configurazione di un certificato client"](#).
3. In caso di errori del certificato del server, provare una o entrambe le seguenti opzioni:
- Assicurarsi che il campo Subject alternative Name (SAN) del certificato sia compilato e che LA SAN corrisponda all'indirizzo IP o al nome host del nodo a cui si sta effettuando la connessione.
 - Se si sta tentando di connettersi a StorageGRID utilizzando un nome di dominio:
 - i. Inserire l'indirizzo IP del nodo di amministrazione invece del nome di dominio per evitare l'errore di connessione e accedere a Grid Manager.
 - ii. Da Grid Manager, selezionare **CONFIGURAZIONE > sicurezza > certificati**, quindi ["selezionare la scheda del certificato appropriata"](#) per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
 - iii. Nelle istruzioni per l'amministrazione di StorageGRID, vedere la procedura per ["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#).

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

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

Errori di accesso al nodo amministrativo

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

Prima di iniziare

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

A proposito di questa attività

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

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

Fasi

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

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

2. Se il sistema StorageGRID dispone di più di un nodo amministrativo, provare ad accedere al Grid Manager da un altro nodo amministrativo per verificare lo stato di un nodo amministrativo non disponibile.

- Se sei in grado di effettuare l'accesso, puoi utilizzare le opzioni **Dashboard, NODES, Alerts e SUPPORT** per determinare la causa dell'errore.
- Se si dispone di un solo nodo di amministrazione o non si riesce ancora ad accedere, passare alla fase successiva.

3. Determinare se l'hardware del nodo non è in linea.

4. Se il Single Sign-on (SSO) è attivato per il sistema StorageGRID, fare riferimento alla procedura per "[configurazione del single sign-on](#)".

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



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

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

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

- Se l'utente locale può effettuare l'accesso:
 - Rivedere gli avvisi.
 - Selezionare **CONFIGURATION > Access Control > Identity Federation**.
 - Fare clic su **Test Connection** (verifica connessione) per convalidare le impostazioni di connessione per il server LDAP.
 - Se il test non riesce, risolvere eventuali errori di configurazione.
- Se l'utente locale non riesce ad accedere e si è certi che le credenziali siano corrette, passare alla fase successiva.

6. Utilizzare Secure Shell (ssh) per accedere al nodo di amministrazione:

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

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

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

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

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

```

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

```

8. Verificare che il servizio nginx-gw sia in esecuzione # `service nginx-gw status`

9. utilizzare Lumberjack per raccogliere i registri: # `/usr/local/sbin/lumberjack.rb`

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

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

10. Rivedi i seguenti log:

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

◦ `**/*commands.txt`

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

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

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

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

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

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

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

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

Problemi dell'interfaccia utente

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

Fasi

1. Assicurarsi di utilizzare un ["browser web supportato"](#).
2. Cancellare la cache del browser Web.

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

Risolvere i problemi di rete, hardware e piattaforma

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

Errori "422: Entità non elaborabile"

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

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

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

Avviso di mancata corrispondenza MTU della rete griglia

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

significativamente tra i nodi della griglia.

A proposito di questa attività

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

Fasi

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

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

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

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

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

+

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

Avviso errore frame di ricezione rete nodo

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

A proposito di questa attività

Gli avvisi **errore frame di ricezione rete nodo** possono essere causati dai seguenti problemi con l'hardware di rete che si connette a StorageGRID:

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

Fasi

1. Seguire la procedura di risoluzione dei problemi per tutte le cause potenziali di questo avviso, data la configurazione della rete in uso.
2. A seconda della causa dell'errore, attenersi alla seguente procedura:

Mancata corrispondenza FEC



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

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

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



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

Mancata corrispondenza tra porta dello switch e MTU della scheda NIC

Se l'avviso è causato da una porta dello switch e da una mancata corrispondenza della MTU della NIC, verificare che la dimensione MTU configurata sul nodo corrisponda all'impostazione MTU per la porta dello switch.

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



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



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

Elevati tassi di errore di collegamento

- a. Attivare FEC, se non è già attivato.
- b. Verificare che il cablaggio di rete sia di buona qualità e non sia danneggiato o collegato in modo errato.
- c. Se i cavi non sembrano essere il problema, contattare il supporto tecnico.



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

Buffer di anello NIC scaduto

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

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

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

Errori di sincronizzazione dell'ora

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

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



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

Linux: Problemi di connettività di rete

Potrebbero verificarsi problemi di connettività di rete per i nodi StorageGRID ospitati su host Linux.

Clonazione indirizzo MAC

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

per ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#).



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

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

Modalità promiscua

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

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

Linux: Lo stato del nodo è "orfano"

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

A proposito di questa attività

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

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

Fasi

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

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

Se il nodo è orfano, la risposta è

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

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

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

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

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

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

Linux: Risoluzione dei problemi relativi al supporto IPv6

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

A proposito di questa attività

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

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

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

Fasi

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

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

Il risultato deve essere 0.

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



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

3. Inserisci il contenitore del nodo StorageGRID: `storagegrid node enter node-name`
4. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

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

Il risultato deve essere 1.

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



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

5. Uscire dal contenitore: `exit`

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

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

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

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

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

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

8. Eseguire questi comandi per riavviare il container StorageGRID:

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

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

Risolvere i problemi di un server syslog esterno

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

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

- ["Considerazioni sull'utilizzo di un server syslog esterno"](#)
- ["Configurare i messaggi di controllo e il server syslog esterno"](#)

Messaggio di errore	Descrizione e azioni consigliate
Impossibile risolvere il nome host	<p data-bbox="472 149 1495 191">Impossibile risolvere l'FQDN immesso per il server syslog in un indirizzo IP.</p> <ol data-bbox="472 212 1495 422" style="list-style-type: none"> <li data-bbox="472 212 1495 317">1. Controllare il nome host immesso. Se è stato immesso un indirizzo IP, assicurarsi che sia un indirizzo IP valido con la notazione W.X.Y.Z ("decimale separato da punti"). <li data-bbox="472 338 1495 380">2. Verificare che i server DNS siano configurati correttamente. <li data-bbox="472 390 1495 422">3. Verificare che ciascun nodo possa accedere agli indirizzi IP del server DNS.
Connessione rifiutata	<p data-bbox="472 470 1495 575">Una connessione TCP o TLS al server syslog è stata rifiutata. Sulla porta TCP o TLS dell'host potrebbe non essere presente alcun servizio o un firewall potrebbe bloccare l'accesso.</p> <ol data-bbox="472 596 1495 842" style="list-style-type: none"> <li data-bbox="472 596 1495 680">1. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. <li data-bbox="472 690 1495 774">2. Verificare che l'host del servizio syslog stia eseguendo un daemon syslog in attesa sulla porta specificata. <li data-bbox="472 785 1495 842">3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi all'IP e alla porta del server syslog.
Rete non raggiungibile	<p data-bbox="472 890 1495 995">Il server syslog non si trova su una subnet collegata direttamente. Un router ha restituito un messaggio di errore ICMP per indicare che non è stato possibile inoltrare i messaggi di test dai nodi elencati al server syslog.</p> <ol data-bbox="472 1016 1495 1241" style="list-style-type: none"> <li data-bbox="472 1016 1495 1058">1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. <li data-bbox="472 1068 1495 1241">2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per instradare il traffico al server syslog attraverso l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host non raggiungibile	<p data-bbox="472 1289 1495 1436">Il server syslog si trova su una subnet collegata direttamente (subnet utilizzata dai nodi elencati per gli indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di test, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del server syslog.</p> <ol data-bbox="472 1457 1495 1541" style="list-style-type: none"> <li data-bbox="472 1457 1495 1499">1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. <li data-bbox="472 1509 1495 1541">2. Verificare che l'host che esegue il servizio syslog sia attivo.

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

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

Esaminare i registri di audit

Messaggi e registri di controllo

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di audit e dei registri di audit di StorageGRID. È possibile utilizzare queste informazioni per leggere e analizzare il registro di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli 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, è necessario disporre dell'accesso alla condivisione di audit configurata nel nodo di amministrazione.

Per informazioni sulla configurazione dei livelli dei messaggi di controllo e sull'utilizzo di un server syslog esterno, vedere ["Configurare i messaggi di audit e le destinazioni dei log"](#).

Controllare il flusso e la conservazione dei messaggi

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. È necessario comprendere in che modo questi messaggi di controllo passano dal sistema StorageGRID al `audit.log` file.

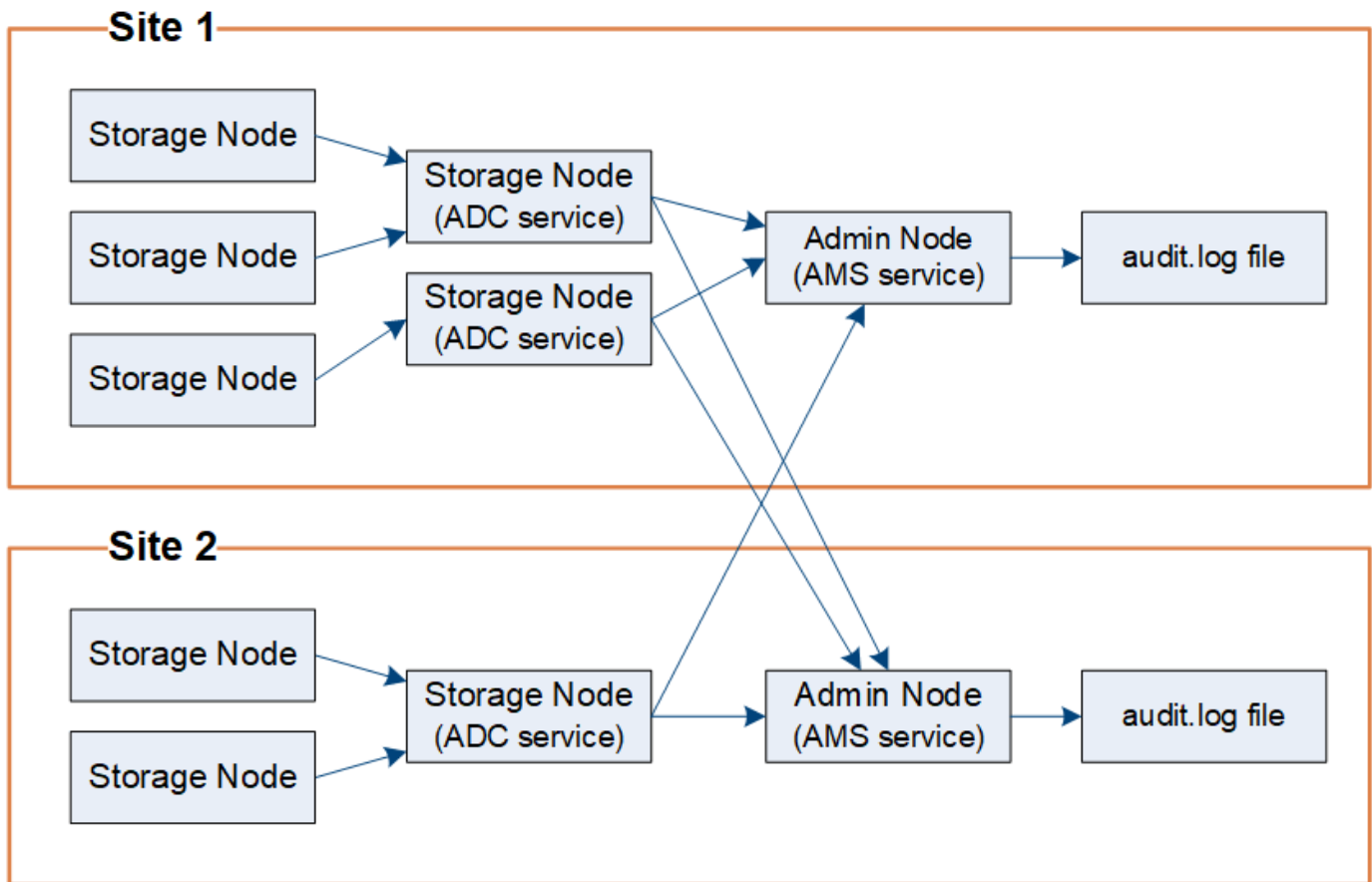
Controllare il flusso dei messaggi

I messaggi di audit vengono elaborati dai nodi di amministrazione e dai nodi di storage che dispongono di un servizio ADC (Administrative Domain Controller).

Come mostrato nel diagramma di flusso dei messaggi di audit, ciascun nodo StorageGRID invia i propri messaggi di audit a uno dei servizi ADC nel sito del data center. Il servizio ADC viene attivato automaticamente per i primi tre nodi di storage installati in ogni sito.

A sua volta, ogni servizio ADC agisce come un relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID, che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

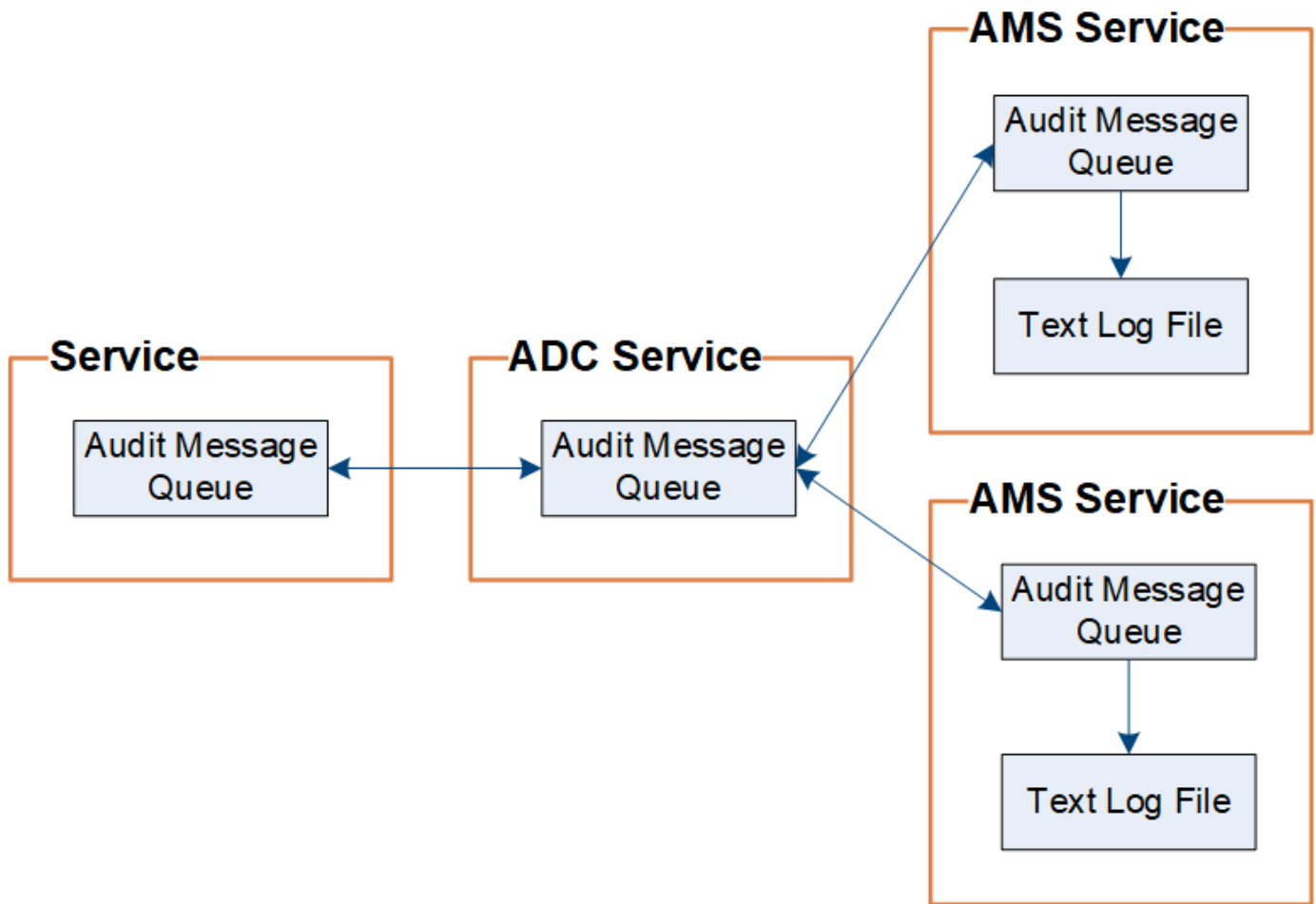
Ogni nodo amministrativo memorizza i messaggi di controllo in file di registro di testo; il file di registro attivo è denominato `audit.log`.



Controllare la conservazione dei messaggi

StorageGRID utilizza un processo di copia e cancellazione per garantire che non vengano persi messaggi di controllo prima di poter essere scritti nel registro di controllo.

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 Grid. Una copia del messaggio viene sempre conservata in una coda di messaggi di controllo finché il messaggio non viene scritto nel file di registro di controllo nella directory del nodo amministrativo `/var/local/log`. In questo modo si evita 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 capacità di audit insufficiente. Man mano che le code aumentano, consumano una quantità maggiore di spazio disponibile nella directory di ciascun nodo `/var/local/`. Se il problema persiste e la directory dei messaggi di controllo di un nodo diventa troppo piena, i singoli nodi assegneranno la priorità all'elaborazione del proprio backlog e diventeranno temporaneamente non disponibili per i nuovi messaggi.

In particolare, potrebbero verificarsi i seguenti comportamenti:

- Se la `/var/local/log` directory utilizzata da un nodo amministrativo diventa piena, il nodo amministrativo viene contrassegnato come non disponibile per i nuovi messaggi di controllo finché la directory non è più piena. S3 le richieste dei client non sono interessate. L'allarme XAMS (Unreachable Audit Repository) viene attivato quando un repository di audit non è raggiungibile.
- Se la `/var/local/` directory utilizzata da un nodo di archiviazione con il servizio ADC è piena al 92%, il nodo viene contrassegnato come non disponibile per i messaggi di controllo finché la directory non è piena solo al 87%. S3 le richieste client ad altri nodi non sono interessate. L'allarme NRLY (Available Audit Relay) viene attivato quando i relè di audit non sono raggiungibili.



Se non vi sono nodi di archiviazione disponibili con il servizio ADC, i nodi di archiviazione memorizzano i messaggi di controllo localmente nel `/var/local/log/localaudit.log` file.

- Se la `/var/local/` directory utilizzata da un nodo di archiviazione diventa piena al 85%, il nodo inizia a rifiutare le richieste client S3 con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare un aumento delle code dei messaggi di audit:

- Interruzione di un nodo amministrativo o di un nodo di storage con il servizio ADC. Se uno dei nodi del sistema non è attivo, i nodi rimanenti potrebbero diventare backlogged.
- Tasso di attività sostenuta che supera la capacità di audit del sistema.
- Lo `/var/local/` spazio su un nodo di archiviazione ADC si riempie per motivi non correlati ai messaggi di controllo. In questo caso, il nodo smette di accettare nuovi messaggi di audit e assegna la priorità al backlog corrente, che può causare backlog su altri nodi.

Avviso di coda di audit estesa e allarme di messaggi di audit in coda (AMQS)

Per facilitare il monitoraggio delle dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Large audit queue** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda Storage Node o Admin Node raggiunge determinate soglie.

Se viene attivato l'avviso **Large audit queue** o l'allarme AMQS legacy, iniziare controllando il carico sul sistema. Se si è verificato un numero significativo di transazioni recenti, l'avviso e l'allarme devono essere risolti nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di severità, visualizzare un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, il carico di audit ha probabilmente superato la capacità di audit del sistema. Ridurre la velocità di funzionamento del client o diminuire il numero di messaggi di audit registrati modificando il livello di audit per le scritture del client e le letture del client su Error (errore) o Off. Vedere "[Configurare i messaggi di audit e le destinazioni dei log](#)".

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto di rete o nodo. Per questo motivo, nel registro di controllo potrebbero essere presenti messaggi duplicati.

Accedere al file di log di audit

La condivisione di controllo contiene il file attivo `audit.log` ed eventuali file di registro di controllo compressi. È possibile accedere ai file di log di controllo direttamente dalla riga di comando del nodo amministrativo.

Prima di iniziare

- Si dispone di "[autorizzazioni di accesso specifiche](#)".
- È necessario disporre del `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

Fasi

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

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

2. Accedere alla directory contenente i file di log di controllo:

```
cd /var/local/log
```

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

Controllo della rotazione del file di log

I file dei registri di controllo vengono salvati nella directory di un nodo amministrativo `/var/local/log`. I file di registro di controllo attivi sono denominati `audit.log`.



In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno. Vedere "[Configurare i messaggi di audit e le destinazioni dei log](#)".

Una volta al giorno, il file attivo `audit.log` viene salvato e viene avviato un nuovo `audit.log` file. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`. Se in un solo giorno vengono creati più log di controllo, i nomi dei file utilizzano la data in cui il file è stato salvato, seguita da 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 registro 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. Con il passare del tempo, ciò comporta un consumo di storage allocato per i registri di controllo sul nodo di amministrazione. Uno script monitora il consumo di spazio nel registro di controllo ed elimina i file di registro come necessario per liberare spazio nella `/var/local/log` directory. I registri di audit vengono cancellati in base alla data di creazione, con la data in cui sono stati cancellati per prima. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

Questo esempio mostra il file attivo `audit.log`, il file del giorno precedente (`2018-04-15.txt`) e il file compresso per il 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

Formato del file di log di audit

I file di log di audit si trovano in ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di audit.

Ogni messaggio di audit contiene quanto segue:

- Il tempo universale coordinato (UTC) dell'evento che ha attivato il messaggio di audit (ATIM) in formato ISO 8601, seguito da uno spazio:

`YYYY-MM-DDTHH:MM:SS.UUUUUU`, dove `UUUUUU` sono microsecondi.

- Il messaggio di verifica stesso, racchiuso tra parentesi quadre e che inizia con AUDT.

L'esempio seguente mostra tre messaggi di audit in un file di log di audit (interruzioni di riga aggiunte per la leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e aggiunto due oggetti a tale 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::175300642415970547
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::175300642415970547
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::175300642415970547
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. È possibile utilizzare ["tool di verifica-spiegazione"](#) per ottenere riepiloghi semplificati dei messaggi di controllo nel registro di controllo. È possibile utilizzare ["tool audit-sum"](#) per riepilogare il numero di operazioni di scrittura,

lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.

Utilizzare lo strumento di verifica e spiegazione

È possibile utilizzare `audit-explain` lo strumento per convertire i messaggi di controllo nel registro di controllo in un formato di facile lettura.

Prima di iniziare

- Si dispone di "[autorizzazioni di accesso specifiche](#)".
- È necessario disporre del `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

```
`audit-explain`Lo strumento, disponibile sul nodo amministrativo principale, fornisce riepiloghi semplificati dei messaggi di controllo in un registro di controllo.
```



`audit-explain`Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Le query di elaborazione `audit-explain` possono consumare una grande quantità di potenza della CPU, che potrebbe avere un impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico `audit-explain` dello strumento. Questi quattro "SPUT" messaggi di controllo sono stati generati quando il tenant S3 con ID account 92484777680322627870 utilizzava S3 richieste PUT per creare un bucket denominato "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 effettuare le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Elaborazione simultanea di più file. Ad esempio:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```

- Accettare l'input da una pipe, che 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 registri di controllo possono essere molto grandi e lenti da analizzare, è possibile risparmiare tempo filtrando le parti che si desidera esaminare ed eseguire `audit-explain` sulle parti, anziché sull'intero file.



`audit-explain` Lo strumento non accetta file compressi come input di pipeline. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando o utilizzare `zcat` lo strumento per decomprimere prima i file. Ad esempio:

```
zcat audit.log.gz | audit-explain
```

Utilizzare l' `help (-h)` opzione per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-explain -h
```

Fasi

1. Accedere al nodo di amministrazione principale:

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

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

2. Immettere il seguente comando, dove `/var/local/log/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

```
$ audit-explain /var/local/log/audit.log
```

`audit-explain` Lo strumento stampa interpretazioni leggibili di tutti i messaggi nel file o nei file specificati.



Per ridurre le lunghezze delle linee e agevolare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se si desidera visualizzare i timestamp, utilizzare l' `(-t)` opzione timestamp).

Utilizzare lo strumento audit-sum

È possibile utilizzare `audit-sum` lo strumento per contare i messaggi di controllo di scrittura, lettura, testa ed eliminazione e per visualizzare il tempo (o le dimensioni) minimo, massimo e medio per ogni tipo di operazione.

Prima di iniziare

- Si dispone di "autorizzazioni di accesso specifiche".
- È necessario disporre del `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

``audit-sum``Lo strumento, disponibile nel nodo amministrativo principale, riepiloga il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo necessario per tali operazioni.



`audit-sum``Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Le query di elaborazione ``audit-sum`` possono consumare una grande quantità di potenza della CPU, che potrebbe avere un impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico `audit-sum` dello strumento. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

message group average (sec)	count	min(sec)	max(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			

``audit-sum``In un audit log, il tool fornisce conteggi e tempi per i seguenti messaggi di audit S3, Swift e ILM.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione poiché le funzioni sono obsolete. Se si riscontra un codice di controllo non elencato qui, controllare le versioni precedenti di questo argomento per le versioni SG precedenti. Ad esempio, "[StorageGRID 11,8 utilizzando la documentazione dello strumento di checksum](#)".

Codice	Descrizione	Fare riferimento a.
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Registra quando ILM avvia il processo di eliminazione di un oggetto.	" IDEL: Eliminazione avviata da ILM "
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket.	" SDEL: ELIMINAZIONE S3 "
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	" SGET: S3 GET "
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	" SHEA: TESTA S3 "
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	" SPUT: S3 PUT "
WDEL	Eliminazione rapida: Registra una transazione riuscita per eliminare un oggetto o un container.	" WDEL: ELIMINAZIONE rapida "
WGET	Swift GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un container.	" WGET: Swift GET "
WHEA	Swift HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un container.	" WHEA: TESTA veloce "
WPUT	Swift PUT: Registra una transazione riuscita per creare un nuovo oggetto o container.	" WPUT: MESSA rapida "

Lo `audit-sum` strumento può effettuare le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Elaborazione simultanea di più file. Ad esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Accettare l'input da una pipe, che 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 i file compressi come input di tipo pipped. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando o utilizzare `zcat` lo strumento per decomprimere prima i file. Ad esempio:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

È possibile utilizzare le opzioni della riga di comando per riepilogare le operazioni sui bucket separatamente dalle operazioni sugli oggetti o per raggruppare i riepiloghi dei messaggi in base al nome del bucket, al periodo di tempo o al tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di funzionamento minimo, massimo e medio, ma è possibile utilizzare l'`size (-s)`opzione per esaminare le dimensioni dell'oggetto.

Utilizzare l'`help (-h)`opzione per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-sum -h
```

Fasi

1. Accedere al nodo di amministrazione principale:

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

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

2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, testa ed eliminazione, attenersi alla seguente procedura:

- a. Immettere il seguente comando, dove `/var/local/log/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

```
$ audit-sum /var/local/log/audit.log
```

Questo esempio mostra l'output tipico `audit-sum` dello strumento. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

message group average(sec)	count	min(sec)	max(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 a 1.13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano tempi lunghi nel caso peggiore di circa 1,770 secondi.

- b. Per visualizzare le operazioni di recupero 10 più lente, utilizzare il comando grep per selezionare solo i messaggi SGET e aggiungere l'opzione di output lungo (-l) per includere i percorsi oggetto:

```
grep SGET audit.log | audit-sum -l
```

I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di eseguire il grep del log di audit per altri messaggi relativi a questi oggetti specifici.

```

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/r9010aQ8JB-1566861764-4519.iso
1624414429  10.96.101.125      object    5375001556
backup/r9010aQ8JB-1566861764-6618.iso
1533143793  10.96.101.125      object    5183661466
backup/r9010aQ8JB-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, è possibile notare che le tre richieste S3 GET più lente erano per oggetti di dimensioni pari a circa 5 GB, che sono molto più grandi degli altri oggetti. Le grandi dimensioni rappresentano i tempi di recupero lenti dei casi peggiori.

3. Per determinare le dimensioni degli oggetti inseriti e recuperati dalla griglia, utilizzare l'opzione dimensioni (-s):

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

In questo esempio, la dimensione media degli oggetti per SPUT è inferiore a 2.5 MB, ma la dimensione media per SGET è molto maggiore. Il numero di messaggi SPUT è molto superiore al numero di messaggi SGET, a indicare che la maggior parte degli oggetti non viene mai recuperata.

- 4. Se si desidera determinare se i recuperi sono stati lenti ieri:
 - a. Immettere il comando nel registro di controllo appropriato e utilizzare 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 average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Questi risultati mostrano che S3 OTTIENE un incremento del traffico tra le 06:00 e le 07:00. Anche in questi casi, i tempi massimi e medi sono notevolmente più elevati e non sono aumentati gradualmente con l'aumentare del numero. Ciò suggerisce che la capacità è stata superata da qualche parte, ad esempio nella rete o nella capacità della rete di elaborare le richieste.

- b. Per determinare le dimensioni degli oggetti recuperati ogni ora ieri, aggiungere l'opzione size (-s) al comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Questi risultati indicano che si sono verificati alcuni recuperi molto grandi quando il traffico di recupero complessivo era al massimo.

c. Per ulteriori dettagli, utilizzare il ["tool di verifica-spiegazione"](#) per rivedere tutte le operazioni SGET durante quell'ora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se si prevede che l'output del comando grep sia costituito da molte righe, aggiungere il less comando per visualizzare il contenuto del file di registro di controllo una pagina (una schermata) alla volta.

5. Se si desidera determinare se le operazioni SPUT sui bucket sono più lente delle operazioni SPUT per gli oggetti:

a. Iniziare utilizzando l'`-go`opzione, che raggruppa i messaggi per le operazioni di oggetti e bucket separatamente:

```
grep SPUT sample.log | audit-sum -go
```


message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
=====			
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

I risultati mostrano che le operazioni SPUT per i bucket hanno caratteristiche di performance diverse rispetto alle operazioni SPUT per gli oggetti.

- b. Per determinare quali bucket hanno le operazioni SPUT più lente, utilizzare `-gb` l'opzione, che raggruppa i messaggi per bucket:

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ltd002 0.361	1564563	0.011	51.569

- c. Per determinare quali bucket hanno la dimensione massima dell'oggetto SPUT, utilizzare sia le `-gb` opzioni e `-s`:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ltd002 0.352	1564563	0.000	999.972

Formato del messaggio di audit

Formato del messaggio di audit

I messaggi di audit scambiati all'interno del sistema StorageGRID includono informazioni standard comuni a tutti i messaggi e contenuti specifici che descrivono l'evento o l'attività da segnalare.

Se le informazioni di riepilogo fornite dagli ["audit-spiegare"](#) strumenti e ["audit-sum"](#) non sono sufficienti, fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di controllo.

Di seguito viene riportato un esempio di messaggio di audit che potrebbe essere visualizzato nel file di log dell'audit:

```
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):9445736326500603516]]
```

Ogni messaggio di audit contiene una stringa di elementi di attributo. L'intera stringa è racchiusa tra parentesi ([]()), e ogni elemento attributo nella stringa ha le seguenti caratteristiche:

- Racchiuso tra parentesi []
- Introdotta dalla stringa AUDT, che indica un messaggio di controllo
- Senza delimitatori (senza virgole o spazi) prima o dopo
- Terminato da un carattere di avanzamento riga \n

Ogni elemento include un codice di attributo, un tipo di dati e un valore che vengono riportati in questo formato:

```
[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 dell'attributo non sono elencati in un ordine specifico.

L'elenco seguente descrive gli elementi degli attributi:

- `ATTR` è un codice di quattro caratteri per l'attributo riportato. Esistono alcuni attributi comuni a tutti i messaggi di audit e ad altri specifici degli eventi.
- `type` È un identificatore di quattro caratteri del tipo di dati di programmazione 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 di testo. I valori seguono sempre i due punti (:). I valori del tipo di dati CSTR sono racchiusi tra virgolette doppie " ".

Tipi di dati

Per memorizzare le informazioni nei messaggi di audit vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero senza segno (32 bit); può memorizzare i numeri da 0 a 4,294,967,295.
UI64	Numero intero doppio 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, ad esempio "ABCD".
IPAD	Utilizzato per gli indirizzi IP.
CSTR	Matrice a lunghezza variabile di caratteri UTF-8. È possibile eseguire l'escape dei caratteri con le seguenti convenzioni: <ul style="list-style-type: none">• La barra rovesciata è• Il ritorno a capo è• Le virgolette doppie sono " .• L'avanzamento riga (nuova riga) è il n.• I caratteri possono essere sostituiti dai rispettivi equivalenti esadecimali (nel formato HH, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento

Ogni messaggio di audit nel registro di audit registra i dati specifici di un evento di sistema.

Dopo il contenitore di apertura [AUDT: che identifica il messaggio stesso, il successivo insieme di attributi fornisce informazioni sull'evento o sull'azione descritti dal messaggio di controllo. Questi attributi sono evidenziati nel seguente esempio:

```
2018-12-05T08:24:45.921845 [AUDT:[RSLT:"60025621595611246499"] *[TIME(UI64):11454][SAIP](IPAD
BUCKET):"10.224.0 60025621595611246499.100 60025621595611246499"]
*[S3AI(CSTGSTR):[S3CSTGSTR] *[S3CSTGK]: *[S3CSTGSTGSTR] *[S3CSTGSTR]:
*[S3CSTGSTGSTR]: *[S3GSTGSTGSTR]: *[S3GSTGSTGSTR] *] *[S3K]:
*[S3CSTGSTGSTR]: *[S3K] *: *: *: *: *: *:
S3CSTGSTGSTR:15552417629170647261
12281045 1543998285921845 10 30720
```

L'`ATYP` elemento (sottolineato nell'esempio) identifica l'evento che ha generato il messaggio. Questo messaggio di esempio include il "SHEA" codice del messaggio ([ATYP(FC32):SHEA]), che indica che è stato generato da una richiesta di S3 TESTINE riuscita.

Elementi comuni nei messaggi di audit

Tutti i messaggi di audit contengono gli elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	Module ID (ID modulo): Identificatore di quattro caratteri dell'ID modulo che ha generato il messaggio. Indica il segmento di codice all'interno del quale è stato generato il messaggio di audit.
ANID	UI32	Node ID (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. Impossibile modificare questo ID.
ASE	UI64	Audit Session Identifier (identificatore sessione di audit): Nelle release precedenti, questo elemento indica l'ora in cui il sistema di audit è stato inizializzato dopo l'avvio del servizio. Questo valore di tempo è stato misurato in microsecondi 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 audit.
ASQN	UI64	Sequence Count (Conteggio sequenze): Nelle release precedenti, questo contatore è stato 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 audit.
ATID	UI64	Trace ID (ID traccia): Identificatore condiviso dalla serie di messaggi attivati da un singolo evento.

Codice	Tipo	Descrizione
ATIM	UI64	<p>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). Si noti che la maggior parte degli strumenti disponibili per la conversione dell'indicatore data e ora in data e ora locali si basano su millisecondi.</p> <p>Potrebbe essere richiesto l'arrotondamento o il troncamento dell'indicatore data e ora registrato. L'ora leggibile dall'uomo che appare all'inizio del messaggio di controllo nel <code>audit.log</code> file è l'attributo ATIM in formato ISO 8601. La data e l'ora sono rappresentate come <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, dove T è un carattere stringa letterale che indica l'inizio del segmento temporale della data. <code>UUUUUU</code> sono microsecondi.</p>
ATYP	FC32	Event Type (tipo di evento): Identificatore di quattro caratteri dell'evento registrato. Questo regola il contenuto "payload" del messaggio: Gli attributi che sono inclusi.
MEDIA	UI32	Version (versione): La versione del messaggio di audit. Man mano che il software StorageGRID si evolve, le nuove versioni dei servizi potrebbero incorporare nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti del servizio AMS per l'elaborazione dei messaggi provenienti da versioni precedenti dei servizi.
RSLT	FC32	Risultato: Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

Esempi di messaggi di audit

È possibile trovare informazioni dettagliate in ciascun messaggio di audit. Tutti i messaggi di audit utilizzano lo stesso formato.

Di seguito è riportato un esempio di messaggio di controllo che potrebbe essere visualizzato nel `audit.log` file:

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2"] [S3BK (CSTR) : "s3small11"] [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, nonché informazioni sul messaggio di audit stesso.

Per identificare l'evento registrato dal messaggio di audit, cercare 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) : "s3small11"] [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 PUT S3 KB, che registra l'acquisizione di un oggetto in un bucket.

Il seguente messaggio di audit mostra anche il bucket a cui è associato l'oggetto:

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :246979] [S3AI (CSTR) : "bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK (CSTR) : "UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR\ ) : "s3small11"] [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, prendere nota dell'indicatore orario 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) : "s3small11"] [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 viene convertito in giovedì, 17-lug-2014 21:17:59:00 UTC.

Messaggi di audit e ciclo di vita degli oggetti

Quando vengono generati i messaggi di audit?

I messaggi di audit vengono generati ogni volta che un oggetto viene acquisito, recuperato o eliminato. È possibile identificare queste transazioni nel registro di controllo individuando i messaggi di controllo specifici di API S3.

I messaggi di audit sono collegati tramite identificatori specifici di ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (bucket), S3KY (chiave) o entrambi
Collegamento delle operazioni Swift	WCON (container), WOBJ (Object) o entrambi
Collegamento delle operazioni interne	CBID (identificatore interno dell'oggetto)

Tempistiche dei messaggi di audit

A causa di fattori come le differenze di tempo tra i nodi della griglia, le dimensioni degli oggetti e i ritardi di rete, l'ordine dei messaggi di controllo generati dai diversi servizi può variare rispetto a quello mostrato negli esempi di questa sezione.

Transazioni di acquisizione degli oggetti

Nell'audit log, puoi identificare le transazioni di acquisizione dei client individuando S3 messaggi di audit specifici di API.

Non tutti i messaggi di audit generati durante una transazione di acquisizione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

S3: Acquisizione di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione S3 PUT ingest è stata completata correttamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	"ORLM: Regole oggetto soddisfatte"

Acquisizione rapida di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
WPUT	Transazione SWIFT PUT	Una transazione Swift PUT Ingest è stata completata correttamente.	CBID, WCON, WOBJ	"WPUT: MESSA rapida"
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	"ORLM: Regole oggetto soddisfatte"

Esempio: Acquisizione 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 acquisisce un oggetto in un nodo di storage (servizio LDR).

In questo esempio, il criterio ILM attivo include la regola ILM Make 2 Copies.



Non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di acquisizione S3 (SPUT).

Questo esempio presuppone che sia stato precedentemente creato un bucket S3.

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):"SGKHya1RU_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]]
```

ORLM: Regole oggetto soddisfatte

Il messaggio ORLM indica che il criterio ILM è stato soddisfatto 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 sottoposti a erasure coding, il campo LOCS include l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding

```
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]]
```

Il campo PATH include informazioni sul bucket S3 e sulla chiave o informazioni sul container Swift e sull'oggetto, a seconda dell'API utilizzata.

```
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]]
```

Transazioni di eliminazione degli oggetti

È possibile identificare le transazioni di eliminazione degli oggetti nel registro di controllo individuando i messaggi di audit S3 specifici per API.

Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

S3 eliminare i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta di eliminazione dell'oggetto da un bucket.	CBID, S3KY	"SDEL: ELIMINAZIONE S3"

Eliminazione rapida dei messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
WDEL	Eliminazione rapida	Richiesta di eliminazione dell'oggetto da un container o dal container.	CBID, WOBJ	"WDEL: ELIMINAZIONE rapida"

Esempio: Eliminazione di oggetti S3

Quando un client S3 elimina un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.



Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: S3 Elimina

L'eliminazione degli oggetti ha inizio 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 identificare l'oggetto.

```
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):"SGKHya1RU_5cLflqajtaFmxJn946lAWRjfbf33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity:70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SBA
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]]
```

Transazioni di recupero degli oggetti

È possibile identificare le transazioni di recupero degli oggetti nel registro di controllo individuando i messaggi di audit S3 specifici per API.

Non tutti i messaggi di audit generati durante una transazione di recupero sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di recupero.

Messaggi di controllo per il recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta di recupero di un oggetto da un bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Messaggi di audit per il recupero rapido

Codice	Nome	Descrizione	Traccia	Vedere
WGET	OTTENERE rapidamente	Richiesta di recupero di un oggetto da un container.	CBID, WCON, WOBJ	"WGET: Swift GET"

Esempio: Recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti ha inizio 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 identificare l'oggetto.

```
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][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\ (FC32\):SGET\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se la policy bucket lo consente, un client può recuperare in modo anonimo oggetti o 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, in modo da poter tenere traccia di queste richieste anonime e multiaccount.

Nel seguente messaggio di esempio, il client invia una richiesta GetObject per un oggetto memorizzato in un bucket che non possiede. I valori di SBAI e SBAC registrano l'ID e il nome dell'account tenant del bucket Owner, che differiscono dall'ID dell'account tenant e dal nome 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"]\[S3AI\n(CSTR):"17915054115450519830"\]\[SACC(CSTR):"s3-account-b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"]\[SBAI\n(CSTR):"43979298178977966408"\]\[SBAC(CSTR):"s3-account-a"\][S3BK(CSTR):"bucket-anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Esempio: S3 selezionare su un oggetto

Quando un client S3 esegue una query S3 Select su un oggetto, i messaggi di audit vengono generati e salvati nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

Ogni query genera due messaggi di audit: Uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "Select") e un'operazione GET standard successiva che recupera i dati dallo storage durante l'elaborazione.

```
2021-11-08T15:35:30.750038
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAIP(IPAD):"192.168.7.44"]\[S3AI(CSTR):"63147909414576125820"]\[SACC(CSTR):"Tenant1636027116"]\[S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"]\[SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"]\[SBAI(CSTR):"63147909414576125820"]\[SBAC(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 aggiornamento dei metadati

I messaggi di audit vengono generati quando un client S3 aggiorna i metadati di un oggetto.

I metadati S3 aggiornano i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati di un oggetto acquisito.	CBID, S3KY, HTRH	"SUPD: Metadati S3 aggiornati"

Esempio: Aggiornamento dei metadati S3

L'esempio mostra una transazione riuscita per aggiornare i metadati di un oggetto S3 esistente.

SUPD: Aggiornamento dei metadati S3

Il client S3 effettua una richiesta (SUPD) (`x-amz-meta-*`) per aggiornare i metadati specificati) per l'oggetto S3 (S3KY). In questo esempio, le intestazioni delle richieste sono incluse nel campo HTRH perché è stato configurato come intestazione del protocollo di audit (**CONFIGURAZIONE > monitoraggio > server di audit e syslog**). Vedere ["Configurare i messaggi di audit e le destinazioni dei log"](#).

```

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(FC
32):S3RQ]
[ATID(UI64):8987436599021955788]]

```

Messaggi di audit

Descrizioni dei messaggi di controllo

Le descrizioni dettagliate dei messaggi di controllo restituiti dal sistema sono elencate nelle sezioni seguenti. Ciascun messaggio di audit viene elencato per primo in una tabella che raggruppa i messaggi correlati in base alla classe di attività rappresentata dal messaggio. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit che per selezionare il tipo di filtro dei messaggi di audit desiderato.

I messaggi di audit sono anche elencati in ordine alfabetico in base ai codici a quattro caratteri. Questo elenco alfabetico consente di trovare informazioni su messaggi specifici.

I codici a 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, vedere ["Configurare i messaggi di audit e le destinazioni dei log"](#)

Controllare le categorie dei messaggi

Messaggi di audit del sistema

I messaggi di audit appartenenti alla categoria di audit del sistema vengono utilizzati per gli eventi correlati al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema (attività della griglia) e alle operazioni di backup del servizio.

Codice	Titolo e descrizione del messaggio	Vedere
ECMC	Manca un frammento di dati con erasure coding: Indica che è stato rilevato un frammento di dati con erasure coding mancante.	"ECMC: Frammento di dati con codice di cancellazione mancante"
ECOC	Fragment di dati con erasure coding corrotto: Indica che è stato rilevato un frammento di dati sottoposto a erasure coding corrotto.	"ECOC: Frammento di dati con codice di cancellazione corrotto"
ETAF	Autenticazione di sicurezza non riuscita: Tentativo di connessione con Transport Layer Security (TLS) non riuscito.	"ETAF: Autenticazione di sicurezza non riuscita"
GNRG	Registrazione GNDS: Un servizio aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.	"GNRG: Registrazione GNDS"
NUR	Annullamento registrazione GNDS: Un servizio non si è registrato dal sistema StorageGRID.	"GNUR: Annullamento registrazione GNDS"
GTED	Grid Task Ended (attività griglia terminata): Il servizio CMN ha terminato l'elaborazione dell'attività Grid.	"GTED: Task Grid terminato"
GTST	Grid Task Started (attività griglia avviata): Il servizio CMN ha avviato l'elaborazione dell'attività Grid.	"GTST: Task Grid avviato"
GTSU	Grid Task Submitted (attività griglia inviata): È stata inviata un'attività Grid al servizio CMN.	"GTSU: Task Grid inviato"
LLST	Location Lost (posizione persa): Questo messaggio di audit viene generato quando una posizione viene persa.	"LLST: Località persa"
OLST	Object Lost (oggetti persi): Non è possibile individuare un oggetto richiesto all'interno del sistema StorageGRID.	"OLST: Il sistema ha rilevato un oggetto perso"
SADD	Security Audit Disable (Disattiva controllo protezione): La registrazione del messaggio di controllo è stata disattivata.	"SADD: Disattivazione dell'audit di sicurezza"

Codice	Titolo e descrizione del messaggio	Vedere
SADE	Security Audit Enable (attiva controllo di sicurezza): La registrazione del messaggio di controllo è stata ripristinata.	"SADE: Abilitazione controllo di sicurezza"
SVRF	Verifica archivio oggetti non riuscita: Un blocco di contenuto non ha superato i controlli di verifica.	"SVRF: Verifica archivio oggetti non riuscita"
SVRU	Object Store Verify Unknown (verifica archivio oggetti sconosciuto): Dati di oggetti imprevisti rilevati nell'archivio oggetti.	"SVRU: Verifica archivio oggetti sconosciuta"
SYSD	Node Stop (arresto nodo): È stato richiesto lo spegnimento.	"SYSD: Interruzione nodo"
SIST	Node stopping (interruzione nodo): Un servizio ha avviato un'interruzione senza interruzioni.	"SYST: Interruzione del nodo"
SISU	Node Start (Avvio nodo): Un servizio avviato; la natura dello shutdown precedente viene indicata nel messaggio.	"SYSU: Avvio nodo"

Messaggi di audit dello storage a oggetti

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. Tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione poiché le funzioni sono obsolete. Se si riscontra un codice di controllo non elencato qui, controllare le versioni precedenti di questo argomento per le versioni SG precedenti. Ad esempio, ["Messaggi di audit dello storage a oggetti StorageGRID 11,8"](#).

Codice	Descrizione	Vedere
BROR	Bucket Read Only Request (richiesta di sola lettura bucket): Un bucket è entrato o è uscito dalla modalità di sola lettura.	"BROR: Richiesta di sola lettura bucket"
CBSE	Object Send End (fine invio oggetto): L'entità di origine ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBSE: Fine invio oggetto"
CBRE	Object Receive End (fine ricezione oggetto): L'entità di destinazione ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBRE: Fine ricezione oggetto"

Codice	Descrizione	Vedere
CGRR	Richiesta di replica cross-grid: StorageGRID ha tentato un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di grid.	"CGRR: Richiesta di replica cross-grid"
EBDL	Empty bucket Delete (Elimina bucket vuoto): Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione bucket vuoto).	"EBDL: Eliminazione bucket vuoto"
EBKR	Empty bucket Request (richiesta bucket vuoto): Un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).	"EBKR: Richiesta bucket vuoto"
SCMT	Commit dell'archivio oggetti: Un blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto.	"SCMT: Richiesta di commit dell'archivio di oggetti"
SREM	Rimozione archivio oggetti: Un blocco di contenuto è stato cancellato da un nodo griglia e non può più essere richiesto direttamente.	"SREM: Rimozione dell'archivio di oggetti"

Messaggi di audit in lettura del client

I messaggi di controllo in lettura dei client vengono registrati quando un'applicazione client S3 richiede di recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
S3SL	S3 Select request (richiesta S3 Select): Registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.	Client S3	"S3SL: Richiesta S3 Select"
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Client S3	"SHEA: TESTA S3"

Codice	Descrizione	Utilizzato da	Vedere
WGET	Swift GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un container.	Client Swift	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un container.	Client Swift	"WHEA: TESTA veloce"

Messaggi di audit di scrittura del client

I messaggi di controllo in scrittura del client vengono registrati quando un'applicazione client S3 richiede di creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Object Overwrite: Registra una transazione per sovrascrivere un oggetto con un altro oggetto.	S3 e Swift	"OVWR: Sovrascrittura degli oggetti"
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SDEL: ELIMINAZIONE S3"
SPOS	S3 POST: Registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Client S3	"SPOS: POST S3"
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 audit includerà il campo S3SR.	Client S3	"SPUT: S3 PUT"
SUPD	S3 Metadata Updated: Registra una transazione riuscita per aggiornare i metadati di un oggetto o bucket esistente.	Client S3	"SUPD: Metadati S3 aggiornati"
WDEL	Eliminazione rapida: Registra una transazione riuscita per eliminare un oggetto o un container.	Client Swift	"WDEL: ELIMINAZIONE rapida"
WPUT	Swift PUT: Registra una transazione riuscita per creare un nuovo oggetto o container.	Client Swift	"WPUT: MESSA rapida"

Messaggio di audit della gestione

La categoria Gestione registra le richieste degli utenti all'API di gestione.

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di audit API di gestione: Un registro delle richieste degli utenti.	"MGAU: Messaggio di audit della gestione"

Messaggi di controllo ILM

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per gli eventi relativi alle operazioni ILM (Information Lifecycle Management).

Codice	Titolo e descrizione del messaggio	Vedere
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"
LKCU	Pulitura oggetto sovrascritto. Questo messaggio di audit viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di storage.	"LKCU: Pulitura oggetto sovrascritta"
ORLM	Regole oggetto soddisfatte: Questo messaggio di audit viene generato quando i dati oggetto vengono memorizzati come specificato dalle regole ILM.	"ORLM: Regole oggetto soddisfatte"

Riferimento del messaggio di audit

BROR: Richiesta di sola lettura bucket

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 cancellati.

Codice	Campo	Descrizione
BKHD	UUID bucket	L'ID bucket.
BROV	Valore della richiesta di sola lettura del bucket	Se il bucket viene reso di sola lettura o se esce dallo stato di sola lettura (1 = sola lettura, 0 = non di sola lettura).
BROS	Motivo di sola lettura del bucket	Il motivo per cui il bucket viene reso di sola lettura o viene lasciato lo stato di sola lettura. Ad esempio, emptyBucket.

Codice	Campo	Descrizione
S3AI	ID account tenant S3	L'ID dell'account tenant che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

CBRB: Inizio ricezione oggetto

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
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.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da

"Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

CBRE: Fine ricezione oggetto

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
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.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.

Codice	Campo	Descrizione
RSLT	Risultato del trasferimento	<p>Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente):</p> <p>SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati.</p> <p>CONL: Connessione persa durante il trasferimento</p> <p>CTMO: Timeout della connessione durante la creazione o il trasferimento</p> <p>UNRE: ID nodo di destinazione non raggiungibile</p> <p>CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi</p>

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del 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 i conteggi delle repliche.

CBSB: Inizio invio oggetto

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	<p>Indica se il trasferimento CBID è stato avviato tramite push o pull:</p> <p>PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente.</p> <p>PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.</p>
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.

Codice	Campo	Descrizione
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

CBSE: Fine invio oggetto

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
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.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.

Codice	Campo	Descrizione
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	<p>Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente):</p> <p>SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati.</p> <p>CONL: Connessione persa durante il trasferimento</p> <p>CTMO: Timeout della connessione durante la creazione o il trasferimento</p> <p>UNRE: ID nodo di destinazione non raggiungibile</p> <p>CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi</p>

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del 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 i conteggi delle repliche.

CGRR: Richiesta di replica cross-grid

Questo messaggio viene generato quando StorageGRID tenta di eseguire un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di griglie.

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	<p>La dimensione dell'oggetto in byte.</p> <p>L'attributo CSIZ è stato introdotto in StorageGRID 11,8. Di conseguenza, le richieste di replica cross-grid su un aggiornamento da StorageGRID 11,7 a 11,8 potrebbero presentare dimensioni totali degli oggetti imprecise.</p>
S3AI	ID account tenant S3	L'ID dell'account tenant proprietario del bucket da cui l'oggetto viene replicato.

Codice	Campo	Descrizione
GFID	ID connessione federazione griglia	L'ID della connessione a federazione di griglie utilizzata per la replica cross-grid.
OPER	Funzionamento CGR	Il tipo di operazione di replica cross-grid che è stata tentata: <ul style="list-style-type: none"> • 0 = oggetto replicato • 1 = Replica oggetto multiparte • 2 = marcatore di eliminazione replicato
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.
VSID	ID versione	L'ID versione della versione specifica di un oggetto replicato.
RSLT	Codice risultato	Restituisce Successful (SUCS) o General error (GERR).

EBDL: Eliminazione bucket vuoto

Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione bucket vuota).

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	La dimensione dell'oggetto in byte.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
RSLT	Risultato dell'operazione di eliminazione	Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

EBKR: Richiesta bucket vuoto

Questo messaggio indica che un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di

oggetti).

Codice	Campo	Descrizione
BUID (BUID)	UUID bucket	L'ID bucket.
EBJS	Configurazione JSON bucket vuoto	Contiene il JSON che rappresenta la configurazione vuota corrente del bucket.
S3AI	ID account tenant S3	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

ECMC: Frammento di dati con codice di cancellazione mancante

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati con codifica di cancellazione mancante.

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il blocco mancante.
MCID	ID chunk	L'identificatore del frammento con codifica di cancellazione mancante.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

ECOC: Frammento di dati con codice di cancellazione corrotto

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati corrotto con codifica di cancellazione.

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco corrotto.
VLID	ID volume	Volume RangeDB contenente il frammento corrotto con codifica di cancellazione.
CCID	ID chunk	L'identificatore del frammento corrotto con codifica in cancellazione.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

ETAF: Autenticazione di sicurezza non riuscita

Questo messaggio viene generato quando un tentativo di connessione con Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP su cui l'autenticazione non è riuscita.
MALEDUCATO	Identità dell'utente	Identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.
RSLT	Codice di motivazione	Il motivo del guasto: SCNI: Connessione sicura non riuscita. CERM: Certificato mancante. CERT: Certificato non valido. CERE: Certificato scaduto. CER: Certificato revocato. CSGN: Firma del certificato non valida. CSGU: Il firmatario del certificato non era noto. UCRM: Credenziali utente mancanti. UCRI: Credenziali utente non valide. UCRU: Le credenziali dell'utente non sono consentite. TOUT: Timeout dell'autenticazione.

Quando viene stabilita una connessione a un servizio sicuro che utilizza TLS, le credenziali dell'entità remota vengono verificate utilizzando il profilo TLS e la logica aggiuntiva integrata nel servizio. Se l'autenticazione non riesce a causa di certificati o credenziali non validi, imprevisti o non consentiti, viene registrato un messaggio di audit. Ciò consente di eseguire query per tentativi di accesso non autorizzati e altri problemi di connessione correlati alla sicurezza.

Il messaggio potrebbe derivare da un'entità remota con una configurazione errata o da tentativi di presentare credenziali non valide o non consentite al sistema. Questo messaggio di audit deve essere monitorato per

rilevare i tentativi di accesso non autorizzato al sistema.

GNRG: Registrazione GNDS

Il servizio CMN genera questo messaggio di audit quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: <ul style="list-style-type: none">• SUC: Riuscito• SUNV: Servizio non disponibile• GERR: Altro guasto
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.
GNTTP	Tipo di dispositivo	Il tipo di dispositivo del nodo Grid (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello di dispositivo del nodo Grid nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo grid (nel contesto dei costi di collegamento e della classificazione delle query di servizio).
GNIA	Indirizzo IP	L'indirizzo IP del nodo della griglia.

Questo messaggio viene generato ogni volta che un nodo della griglia aggiorna la propria voce nel bundle dei nodi della griglia.

GNUR: Annullamento registrazione GNDS

Il servizio CMN genera questo messaggio di audit quando un servizio ha informazioni non registrate su se stesso dal sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: <ul style="list-style-type: none">• SUC: Riuscito• SUNV: Servizio non disponibile• GERR: Altro guasto
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.

GTED: Task Grid terminato

Questo messaggio di audit indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e che l'attività è stata spostata nella tabella Cronologia. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato un messaggio di audit Grid Task Started (attività griglia avviata) corrispondente. Gli altri risultati indicano che l'elaborazione di questa attività della griglia non è mai stata avviata.

Codice	Campo	Descrizione
TSID	ID attività	<p>Questo campo identifica in modo univoco un'attività Grid generata e consente di gestire l'attività Grid nel suo ciclo di vita.</p> <p>Nota: l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'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 audit inviati, avviati e terminati.</p>
RSLT	Risultato	<p>Risultato finale dello stato dell'attività Grid:</p> <ul style="list-style-type: none">• SUCS: L'attività Grid è stata completata correttamente.• ABRT: L'attività Grid è stata terminata senza un errore di rollback.• ROLF: L'attività Grid è stata terminata e non è stato possibile completare il processo di rollback.• CANC: L'attività della griglia è stata annullata dall'utente prima dell'avvio.• EXPR: L'attività Grid è scaduta prima dell'avvio.• IVLD: L'attività della griglia non era valida.• AUTH: L'attività della rete non è stata autorizzata.• DUPL: L'attività Grid è stata rifiutata come duplicata.

GTST: Task Grid avviato

Questo messaggio di audit indica che il servizio CMN ha avviato l'elaborazione dell'attività Grid specificata. Il messaggio di audit segue immediatamente il messaggio Grid Task Submitted per le attività Grid avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inoltrate nella tabella Pending (in sospeso), questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in maniera univoca un'attività grid generata e consente di gestirne l'intero ciclo di vita. Nota: l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'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 audit inviati, avviati e terminati.
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: • SUCS: L'attività Grid è stata avviata correttamente.

GTSU: Task Grid inviato

Questo messaggio di audit indica che un'attività Grid è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	Identifica in modo univoco un'attività grid generata e consente di gestarla per l'intero ciclo di vita. Nota: l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'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 audit inviati, avviati e terminati.
TTIP	Tipo di attività	Il tipo di attività della griglia.
VER	Versione attività	Un numero che indica la versione dell'attività Grid.
TDSC	Descrizione dell'attività	Una descrizione leggibile dell'attività Grid.
VAT	Valido dopo l'indicatore di data e ora	Il primo tempo (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui l'attività grid è valida.
VBTS	Valido prima dell'indicatore di data e ora	L'ultima ora (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui è valida l'attività grid.

Codice	Campo	Descrizione
TSRC	Origine	L'origine dell'attività: <ul style="list-style-type: none"> • TXTB: L'attività Grid è stata inviata tramite il sistema StorageGRID come blocco di testo firmato. • GRID: L'attività Grid è stata inviata tramite il Grid Task Submission Service interno.
ACTV	Tipo di attivazione	Il tipo di attivazione: <ul style="list-style-type: none"> • AUTO: L'attività della griglia è stata inviata per l'attivazione automatica. • PEND: L'attività Grid è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per l'origine TXTB.
RSLT	Risultato	Risultato dell'invio: <ul style="list-style-type: none"> • SUCS: L'attività Grid è stata inviata correttamente. • ERRORE: L'attività è stata spostata direttamente nella tabella storica.

IDEL: Eliminazione avviata da ILM

Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto.

Il messaggio IDEL viene generato in una delle seguenti 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 relativo periodo di conservazione è scaduto (supponendo che l'impostazione di eliminazione automatica sia attivata e che la sospensione legale sia disattivata).
- **Per oggetti in bucket S3 non conformi.** Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto poiché all'oggetto non sono attualmente applicate istruzioni di posizionamento nei criteri ILM attivi.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Compliance: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (false) o 1 (true), che indica se un oggetto conforme deve essere cancellato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a una conservazione legale.

Codice	Campo	Descrizione
CMPL	Compliance: Conservazione a fini legali	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), che indica se il bucket è attualmente in stato di conservazione legale.
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. La durata del periodo di conservazione dell'oggetto in minuti.
CTME	Compliance: Tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Il tempo di acquisizione dell'oggetto. È possibile aggiungere il periodo di conservazione in minuti a questo valore per determinare quando l'oggetto può essere cancellato dal bucket.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	<p>La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato).</p> <p>CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto.</p> <p>CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto.</p> <p>CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.</p>
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	<p>Risultato dell'operazione ILM.</p> <p>SUCS: Operazione ILM riuscita.</p>
REGOLA	Etichetta regole	<ul style="list-style-type: none"> • Se un oggetto in un bucket S3 conforme viene cancellato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. • Se l'oggetto viene eliminato perché non sono presenti ulteriori istruzioni di posizionamento attualmente applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM applicata all'oggetto.

Codice	Campo	Descrizione
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

LKCU: Pulitura oggetto sovrascritta

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 già contenente un oggetto. Il processo di rimozione avviene automaticamente e in background.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LTYP	Tipo di pulizia	<i>Solo per uso interno.</i>
LUID	UUID oggetto rimosso	L'identificativo dell'oggetto rimosso.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificativo dell'oggetto ancora esistente. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

LKDM: Pulizia degli oggetti con perdite

Questo messaggio viene generato quando un frammento fuoriuscito è stato pulito o eliminato. Un blocco può far parte di un oggetto replicato o di un oggetto codificato per la cancellazione.

Codice	Campo	Descrizione
CLOC	Posizione del frammento	Il percorso del file del blocco fuoriuscito che è stato eliminato.
CTYP	Tipo di frammento	Tipo di pezzo: ec: Erasure-coded object chunk repl: Replicated object chunk
LTYP	Tipo di perdita	I cinque tipi di perdite che possono essere rilevate: 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
CTIM	Crea il tempo	Ora in cui è stato creato il frammento fuoriuscito.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto a cui appartiene il blocco.
CBID	Identificatore del blocco di contenuto	CBID dell'oggetto a cui appartiene il blocco fuoriuscito.
CSIZ	Dimensione del contenuto	La dimensione del blocco in byte.

LLST: Località persa

Questo messaggio viene generato ogni volta che non è possibile trovare una posizione per una copia dell'oggetto (replicata o con erasure coding).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.

Codice	Campo	Descrizione
ECPR	Profilo di erasure coding	Per i dati degli oggetti con codifica erasure coding utilizzato.
LTYP	Tipo di ubicazione	CLDI (online): Per i dati degli oggetti replicati CLEC (Online): Per i dati degli oggetti con codifica erasure CLNL (Nearline): Per i dati degli oggetti replicati archiviati
NOID. (NOIDE	ID nodo di origine	L'ID del nodo in cui sono state perse le posizioni.
PCLD	Percorso dell'oggetto replicato	Il percorso completo alla posizione del disco dei dati dell'oggetto perso. Viene restituito solo quando LTYP ha un valore di CLDI (vale a dire, per gli oggetti replicati). Assume la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
RSLT	Risultato	SEMPRE NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
TSRC	Fonte di attivazione	UTENTE: Attivato dall'utente SYST: Attivato dal sistema
UUID	ID universalmente univoco	L'identificativo dell'oggetto interessato nel sistema StorageGRID.

MGAU: Messaggio di audit della gestione

La categoria Gestione registra le richieste degli utenti all'API di gestione. Ogni richiesta HTTP che non è 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-autorizza) e le richieste non valide agli URI API validi non vengono registrate.

Codice	Campo	Descrizione
MDIP	Indirizzo IP di destinazione	L'indirizzo IP del server (destinazione).
MDNA	Nome di dominio	Il nome del dominio host.
MPAT	PERCORSO di richiesta	Il percorso della richiesta.

Codice	Campo	Descrizione
MPQP	Parametri di query della richiesta	I parametri di query per la richiesta.
MRBD	Corpo della richiesta	<p>Il contenuto dell'organismo di richiesta. Mentre il corpo della risposta viene 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:</p> <ul style="list-style-type: none"> • Nome utente e ID account in POST authorize • Nuova configurazione delle subnet in POST /grid/grid-networks/update • Nuovi server NTP in POST /grid/ntp-servers/update • ID server decommissionati in POST /grid/servers/decommissionation <p>Nota: le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).</p>
MRMD	Metodo di richiesta	<p>Il metodo di richiesta HTTP:</p> <ul style="list-style-type: none"> • POST • IN PRIMO PIANO • ELIMINARE • PATCH
MRSC	Codice di risposta	Il codice di risposta.
MRSP	Corpo di risposta	<p>Il contenuto della risposta (il corpo della risposta) viene registrato per impostazione predefinita.</p> <p>Nota: le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).</p>
MSIP	Indirizzo IP di origine	L'indirizzo IP (di origine) del client.
MUN	URN utente	L'URN (Uniform resource name) dell'utente che ha inviato la richiesta.
RSLT	Risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.

OLST: Il sistema ha rilevato un oggetto perso

Questo messaggio viene generato quando il servizio DDS non riesce a individuare alcuna copia di un oggetto all'interno del sistema StorageGRID.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto perso.
NOID. (NOIDE)	ID nodo	Se disponibile, l'ultima posizione nota diretta o near-line dell'oggetto perso. Se le informazioni sul volume non sono disponibili, è possibile avere solo l'ID nodo senza un ID volume.
PERCORSO	Bucket/chiave S3	Se disponibile, il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
UUID	ID universalmente univoco	L'identificativo dell'oggetto perso nel sistema StorageGRID.
VOLO	ID volume	Se disponibile, l'ID del volume del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

ORLM: Regole oggetto soddisfatte

Questo messaggio viene generato quando l'oggetto viene memorizzato e copiato correttamente come specificato dalle regole ILM.



Il messaggio ORLM non viene generato quando un oggetto viene memorizzato correttamente dalla regola predefinita Make 2 Copies se un'altra regola del criterio utilizza il filtro avanzato dimensione oggetto.

Codice	Campo	Descrizione
BUID (BUID)	Testata benna	Campo ID bucket. Utilizzato per operazioni interne. Viene visualizzato solo se STAT è PRGD.
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	<p>La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato).</p> <p>CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto.</p> <p>CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto.</p> <p>CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.</p>
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	<p>Risultato dell'operazione ILM.</p> <p>SUCS: Operazione ILM riuscita.</p>
REGOLA	Etichetta regole	Etichetta leggibile assegnata alla regola ILM applicata a questo oggetto.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	CBID contenitore	CBID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo per gli oggetti segmentati e multiparte.
URGENZA	Stato	<p>Lo stato del funzionamento di ILM.</p> <p>FATTO: Operazioni ILM rispetto all'oggetto completate.</p> <p>DFER: L'oggetto è stato contrassegnato per la futura rivalutazione ILM.</p> <p>PRGD: L'oggetto è stato cancellato dal sistema StorageGRID.</p> <p>NLOC: I dati dell'oggetto non possono più essere trovati nel sistema StorageGRID. Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.</p>
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.

Codice	Campo	Descrizione
VSID	ID versione	L'ID 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 audit 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.
- Le regole ILM per l'oggetto sono soddisfatte per questa epoca.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati degli oggetti replicati è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto corrotto.

Informazioni correlate

- ["Transazioni di acquisizione degli oggetti"](#)
- ["Transazioni di eliminazione degli oggetti"](#)

OVWR: Sovrascrittura degli oggetti

Questo messaggio viene generato quando un'operazione esterna (richiesta dal client) causa la sovrascrittura di un oggetto da parte di un altro oggetto.

Codice	Campo	Descrizione
CBID	Content Block Identifier (nuovo)	Il CBID per il nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto da sovrascrivere.
OCBD	Content Block Identifier (precedente)	Il CBID dell'oggetto precedente.
UUID	ID universally Unique (nuovo)	L'identificativo del nuovo oggetto all'interno del sistema StorageGRID.
ID OUID	ID universally Unique (precedente)	L'identificativo dell'oggetto precedente all'interno del sistema StorageGRID.
PERCORSO	Percorso oggetto S3	Il percorso dell'oggetto S3 utilizzato sia per l'oggetto precedente che per quello nuovo

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione Object Overwrite. Il risultato è sempre: SUC: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato cancellato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto sovrascritto.

S3SL: Richiesta S3 Select

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.

Codice	Campo	Descrizione
BYSC	Byte sottoposti a scansione	Numero di byte sottoposti a scansione (ricevuti) dai nodi di storage. BYSC e BYPR potrebbero essere diversi se l'oggetto viene compresso. Se l'oggetto è compresso, BYSC avrebbe il conteggio dei byte compressi e BYPR i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "byte sottoposti a scansione" sono stati effettivamente elaborati o utilizzati da un lavoro S3 Select.
BYRT	Byte restituiti	Numero di byte restituiti al client da un lavoro S3 Select.
RPR	Record elaborati	Numero di record o righe ricevuti da un processo S3 Select dai nodi di storage.
RERT	Record restituiti	Numero di record o righe di un lavoro S3 Select restituito al client.
JOFI	Lavoro terminato	Indica se il lavoro S3 Select ha terminato o meno l'elaborazione. Se questo è falso, il lavoro non è stato completato e i campi di errore probabilmente contengono dei dati. Il client potrebbe aver ricevuto risultati parziali o non avere alcun risultato.
RID	ID richiesta	Identificatore della richiesta S3 Select.
ETM	Tempo di esecuzione	Il tempo, in secondi, impiegato per il completamento del processo S3 Select.
ERMG	Messaggio di errore	Messaggio di errore generato dal lavoro S3 Select.
EROSO	Tipo di errore	Tipo di errore generato dal lavoro S3 Select.

Codice	Campo	Descrizione
ERST	Errore StackTrace	Errore StackTrace generato dal lavoro S3 Select.
S3BK	Bucket S3	Il nome del bucket S3.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 per l'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.

SADD: Disattivazione dell'audit di sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di audit; i messaggi di audit non vengono più raccolti o consegnati.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per disattivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione era stata precedentemente attivata, ma ora è stata disattivata. Questo viene generalmente utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato (SADE) e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

SADE: Abilitazione controllo di sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione del messaggio di audit; i messaggi di audit vengono nuovamente raccolti e consegnati.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Il metodo utilizzato per attivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per attivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione è stata precedentemente disattivata (SADD), ma ora è stata ripristinata. In genere viene utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

SCMT: Commit dell'archivio di oggetti

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato fino a quando non viene assegnato (ovvero viene memorizzato in modo persistente). Il contenuto memorizzato in maniera persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene emesso quando un blocco di contenuto viene assegnato allo storage.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto impegnato nello storage permanente.
RSLT	Codice risultato	Stato al momento in cui l'oggetto è stato memorizzato sul disco: SUCS: Oggetto memorizzato correttamente.

Questo messaggio indica che un dato blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto. Può essere utilizzato per tenere traccia del flusso di dati all'interno del sistema.

SDEL: ELIMINAZIONE S3

Quando un client S3 esegue una transazione DI ELIMINAZIONE, viene effettuata una richiesta per rimuovere l'oggetto o il bucket specificato o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta di eliminazione della replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta di eliminazione della replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p><code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div> <p><code>x-amz-bypass-governance-retention</code> viene incluso automaticamente se è presente nella richiesta.</p>
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre: SUC: Riuscito

Codice	Campo	Descrizione
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.

Codice	Campo	Descrizione
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UDM	Identificatore univoco universale per un marcatore di cancellazione	L'identificatore di un marcatore di eliminazione. I messaggi del registro di controllo specificano UUDM o UUID, dove UUDM indica un marcatore di eliminazione creato come risultato di una richiesta di eliminazione dell'oggetto e UUID indica un oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SGET: S3 GET

Quando un client S3 esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>`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 controllo SAIP).</p> </div>
LITY	ListObjectsV2	È stata richiesta una risposta <i>formato v2</i> . Per ulteriori informazioni, vedere " AWS ListObjectsV2 ". Solo per operazioni CON benna GET.
NCHD	Numero di bambini	Include tasti e prefissi comuni. Solo per operazioni CON benna GET.
RANG	Range Read (lettura intervallo)	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) mostra la dimensione dell'intero oggetto.
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.

Codice	Campo	Descrizione
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
TRNC	Troncato o non troncato	Impostare su false se sono stati restituiti tutti i risultati. Impostare su true se sono disponibili ulteriori risultati da restituire. Solo per operazioni CON benna GET.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SHEA: TESTA S3

Quando un client S3 esegue una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un oggetto o bucket e recuperare i metadati relativi a un oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto controllato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div>
RSLT	Codice risultato	<p>Risultato della transazione GET. Il risultato è sempre:</p> <p>SUC: Riuscito</p>
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.

Codice	Campo	Descrizione
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SPOS: POST S3

Quando un client S3 invia una richiesta di oggetto POST, questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0.

Codice	Campo	Descrizione
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre>`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 controllo SAIP).</pre> </div> <p>(Non previsto per SPOS).</p>
RSLT	Codice risultato	<p>Risultato della richiesta RestoreObject. Il risultato è sempre:</p> <p>SUC: Riuscito</p>
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	<p>Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.</p> <p>Impostare su "SELECT" per un'operazione di selezione S3.</p>

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SPUT: S3 PUT

Quando un client S3 esegue una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di compliance	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta DI PUT di replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta DI PUT di replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p><code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div> <p><code>x-amz-bypass-governance-retention</code> viene incluso automaticamente se è presente nella richiesta.</p>
LKEN	Blocco oggetto attivato	Valore dell'intestazione della richiesta <code>x-amz-bucket-object-lock-enabled</code> , se presente nella richiesta.
LKSX	Blocco oggetto Legal Hold	Valore dell'intestazione della richiesta <code>x-amz-object-lock-legal-hold</code> , se presente nella richiesta PutObject.

Codice	Campo	Descrizione
LKMD	Modalità di conservazione del blocco degli oggetti	Valore dell'intestazione della richiesta <code>x-amz-object-lock-mode</code> , se presente nella richiesta PutObject.
LKRU	Blocco oggetto conserva fino alla data	Valore dell'intestazione della richiesta <code>x-amz-object-lock-retain-until-date</code> , se presente nella richiesta PutObject. I valori sono limitati entro 100 anni dalla data di acquisizione dell'oggetto.
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
ULID	ID upload	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID 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	Stato di versione	Il nuovo stato di versione di un bucket. Vengono utilizzati due stati: "Attivato" o "sospeso". Le operazioni sugli oggetti non includono questo campo.

SREM: Rimozione dell'archivio di oggetti

Questo messaggio viene inviato quando il contenuto viene rimosso dallo storage persistente e non è più accessibile tramite API regolari.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto cancellato dallo storage permanente.

Codice	Campo	Descrizione
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è: SUC: Contenuto rimosso dallo storage persistente

Questo messaggio di audit indica che un dato blocco di contenuto è stato cancellato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tenere traccia del flusso di contenuti cancellati all'interno del sistema.

SUPD: Metadati S3 aggiornati

Questo messaggio viene generato dall'API S3 quando un client S3 aggiorna i metadati per un oggetto acquisito. Il messaggio viene emesso dal server se l'aggiornamento dei metadati ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, quando si aggiornano le impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <pre>`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 controllo SAIP).</pre> </div>
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito

Codice	Campo	Descrizione
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.

Codice	Campo	Descrizione
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SVRF: Verifica archivio oggetti non riuscita

Questo messaggio viene emesso 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 non riesce, il sistema mette automaticamente in quarantena i dati dell'oggetto replicato corrotto per impedirne il recupero.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto che non ha superato la verifica.
RSLT	Codice risultato	Tipo di errore di verifica: CRCF: Controllo di ridondanza ciclico (CRC) non riuscito. HMAC: Controllo HMAC (hash-based message Authentication code) non riuscito. ESHS: Hash di contenuto crittografato inatteso. PSHS: Hash di contenuto originale inaspettato. SEQC: Sequenza di dati errata sul disco. PERR: Struttura del file di disco non valida. DERR: Errore del disco. FNAME: Nome file non valido.



Questo messaggio deve essere monitorato attentamente. Gli errori di verifica del contenuto possono indicare guasti hardware imminenti.

Per determinare quale operazione ha attivato il messaggio, vedere il valore del campo AMID (Module ID) (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, ovvero la verifica in background e STOR indica che il messaggio è stato attivato dal recupero del contenuto.

SVRU: Verifica archivio oggetti sconosciuta

Il componente Storage del servizio LDR esegue una scansione continua di 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	Percorso del file	Il percorso del file della copia imprevista dell'oggetto.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che 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 dell'oggetto nell'archivio di oggetti. Questa situazione deve essere esaminata immediatamente per determinare come sono state create queste copie, perché può indicare guasti hardware imminenti.

SYSD: Interruzione nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto lo shutdown. In genere, questo messaggio viene inviato solo dopo un riavvio successivo, in quanto la coda dei messaggi di controllo non viene cancellata prima dell'arresto. Se il servizio non è stato riavviato, cercare il messaggio SYST inviato all'inizio della sequenza di arresto.

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno shutdown "anomalo", perché il messaggio viene generato solo dagli shutdown "puliti".

SYST: Interruzione del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto lo shutdown e che il servizio ha avviato la sequenza di shutdown. SYST può essere utilizzato per determinare se è stato richiesto lo shutdown, prima che il servizio venga riavviato (a differenza di SYSD, che in genere viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. Il codice RSLT di un messaggio SYST non può indicare uno shutdown "dirty", perché il messaggio viene generato solo dagli shutdown "clean".

SYSU: Avvio nodo

Quando un servizio viene riavviato, questo messaggio viene generato per indicare se l'arresto precedente era pulito (comandato) o disordinato (imprevisto).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito. DSDN: Il sistema non è stato spento correttamente. VRGN: Il sistema è stato avviato per la prima volta dopo l'installazione (o la reinstallazione) del server.

Il messaggio non indica se il server host è stato avviato, ma solo il servizio di reporting. Questo messaggio può essere utilizzato per:

- Rilevare la discontinuità nel registro di controllo.
- Determinare se un servizio si guasta durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio guasto.

WDEL: ELIMINAZIONE rapida

Quando un client Swift esegue una transazione DI ELIMINAZIONE, viene inviata una richiesta per rimuovere l'oggetto o il container specificato. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui container non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div>
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	<p>Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre:</p> <p>SUC: Riuscito</p>
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni sui container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WGET: Swift GET

Quando un client Swift esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto, elencare gli oggetti in un container o elencare i container in un account. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni su account e container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"><code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</div>
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L>ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift. Le operazioni sui conti non includono questo campo.

Codice	Campo	Descrizione
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni su account e container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WHEA: TESTA veloce

Quando un client Swift esegue una transazione HEAD, viene inviata una richiesta per verificare l'esistenza di un account, un container o un oggetto e recuperare eventuali metadati pertinenti. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni su account e container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. <div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p><code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div>
RSLT	Codice risultato	Risultato dell'operazione PRINCIPALE. Il risultato è sempre: SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.

Codice	Campo	Descrizione
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni su account e container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WPUT: MESSA rapida

Quando un client Swift esegue una transazione PUT, viene inviata una richiesta per creare un nuovo oggetto o container. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <pre>`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 controllo SAIP).</pre> </div>
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUC: Riuscito

Codice	Campo	Descrizione
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L>ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni sui container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

Informazioni sul copyright

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

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.