



Monitorare e risolvere i problemi

StorageGRID software

NetApp
December 03, 2025

Sommario

Monitorare e risolvere i problemi di un sistema StorageGRID	1
Monitorare il sistema StorageGRID	1
Monitorare un sistema StorageGRID	1
Visualizza e gestisci la dashboard	1
Visualizza la pagina Nodi	4
Informazioni da monitorare regolarmente	38
Gestisci gli avvisi	69
Riferimento ai file di registro	107
Configurare le destinazioni dei messaggi di controllo e dei registri	127
Utilizzare il monitoraggio SNMP	141
Raccogli dati StorageGRID aggiuntivi	152
Risoluzione dei problemi del sistema StorageGRID	187
Risoluzione dei problemi di un sistema StorageGRID	187
Risolvere i problemi relativi agli oggetti e all'archiviazione	194
Risolvere i problemi relativi ai metadati	223
Risolvere gli errori del certificato	225
Risolvere i problemi relativi al nodo di amministrazione e all'interfaccia utente	226
Risolv i problemi di rete, hardware e piattaforma	229
Risolvere i problemi di un server syslog esterno	237
Esaminare i registri di controllo	240
Messaggi e registri di controllo	240
Flusso e conservazione dei messaggi di audit	240
Accedi al file di registro di controllo	243
Rotazione del file di registro di controllo	244
Formato del file di registro di controllo	244
Formato del messaggio di controllo	257
Messaggi di audit e ciclo di vita degli oggetti	262
Messaggi di controllo	269

Monitorare e risolvere i problemi di un sistema StorageGRID

Monitorare il sistema StorageGRID

Monitorare un sistema StorageGRID

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .



Per modificare le unità di misura per i valori di archiviazione visualizzati in Grid Manager, selezionare il menu a discesa dell'utente in alto a destra di Grid Manager, quindi selezionare **Preferenze utente**.

Informazioni su questo compito

Queste istruzioni descrivono come:

- "[Visualizza e gestisci la dashboard](#)"
- "[Visualizza la pagina Nodi](#)"
- "[Monitorare regolarmente questi aspetti del sistema:](#)"
 - "[Salute del sistema](#)"
 - "[Capacità di stoccaggio](#)"
 - "[Gestione del ciclo di vita delle informazioni](#)"
 - "[Risorse di rete e di sistema](#)"
 - "[Attività degli inquilini](#)"
 - "[Operazioni di bilanciamento del carico](#)"
 - "[Conessioni di federazione della rete](#)"
- "[Gestisci gli avvisi](#)"
- "[Visualizza i file di registro](#)"
- "[Configurare i messaggi di controllo e le destinazioni dei registri](#)"
- "[Utilizzare un server syslog esterno](#)" per raccogliere informazioni di audit
- "[Utilizzare SNMP per il monitoraggio](#)"
- "[Ottieni dati StorageGRID aggiuntivi](#)", comprese metriche e diagnostica

Visualizza e gestisci la dashboard

È possibile utilizzare la dashboard per monitorare a colpo d'occhio le attività del sistema. È possibile creare dashboard personalizzate per monitorare l'implementazione di

StorageGRID.



Per modificare le unità di misura per i valori di archiviazione visualizzati in Grid Manager, selezionare il menu a discesa dell'utente in alto a destra di Grid Manager, quindi selezionare **Preferenze utente**.

La dashboard potrebbe variare in base alla configurazione del sistema.

The screenshot shows the StorageGRID dashboard with the following sections:

- Health status**: Shows 1 license issue (orange exclamation mark icon).
- Data space usage breakdown**: Shows 2.11 MB (0%) of 3.09 TB used overall across three Data Centers (Data Center 2, Data Center 3, Data Center 1).
- Total objects in the grid**: Shows 0 total objects.
- Metadata allowed space usage breakdown**: Shows 3.62 MB (0%) of 25.76 GB used in Data Center 1, with Data Center 1 having the highest metadata space usage.

Visualizza la dashboard

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

È possibile utilizzare la dashboard fornita dal sistema così com'è. Inoltre, è possibile creare dashboard personalizzate contenenti solo le schede e le 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, come avvisi attivi, utilizzo dello spazio e numero totale di oggetti nella griglia.

Scheda sulla dashboard fornita dal sistema	Contiene
Prestazione	Utilizzo dello spazio, spazio di archiviazione utilizzato nel tempo, operazioni S3, durata della richiesta, tasso di errore.
Magazzinaggio	Utilizzo delle quote dei tenant e utilizzo dello spazio logico. Previsioni sull'utilizzo dello spazio per i dati e i metadati degli utenti.
ILM	Coda di gestione del ciclo di vita delle informazioni e tasso di valutazione.
Nodi	Utilizzo di CPU, dati e memoria per nodo. Operazioni S3 per nodo. Distribuzione dal nodo al sito.

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

Gestire i dashboard

Se hai accesso Root (vedi "Autorizzazioni del gruppo amministratore"), è possibile eseguire le seguenti attività di gestione per i dashboard:

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



Se si dispone di altri permessi oltre all'accesso Root, è possibile impostare solo una dashboard attiva.

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

The screenshot shows the StorageGRID dashboard interface. At the top, there's a header bar with the title 'StorageGRID dashboard' and an 'Actions' dropdown menu containing 'Clone active dashboard' and 'Manage dashboards'. Below the header, there's a notification bar indicating 'You have 4 notifications: 1 📲 3 🔞'. The main content area has tabs for 'Overview', 'Performance', 'Storage', 'ILM', and 'Nodes'. A callout box highlights the 'Manage dashboards' button in the actions menu.

Configurare i dashboard

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

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



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

Quando si configura una dashboard, è possibile:

- Aggiungere o rimuovere schede
- Rinomina le schede e assegna nomi univoci alle nuove schede
- Aggiungi, rimuovi o riorganizza (trascina) le schede per ogni scheda
- Seleziona la dimensione delle singole carte selezionando **S, M, L o XL** nella parte superiore della carta

The screenshot shows the 'Configure dashboard' interface. At the top, there are tabs for Overview, Performance, Storage, ILM, and Nodes, with 'Overview' selected. Below the tabs, there's a 'Tab name' field containing 'Overview'. A 'Select cards' button is visible. The main area has two sections: 'Health status' and 'Data space usage breakdown'. The 'Health status' section shows 1 license with a warning icon. The 'Data space usage breakdown' section shows data for three Data Centers:

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

Visualizza la pagina Nodi

Visualizza la pagina Nodi

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

Nella tabella Nodi sono elencate le informazioni riepilogative per l'intera griglia, per ciascun sito e per ciascun nodo. Se un nodo è disconnesso o ha un avviso attivo, accanto al nome del nodo viene visualizzata un'icona. Se il nodo è connesso e non ha avvisi attivi, non viene visualizzata alcuna icona.

- Quando un nodo non è connesso alla rete, ad esempio durante un aggiornamento o in uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della rete. Dopo che un nodo si è ricollegato alla rete, attendere alcuni minuti affinché i valori si stabilizzino.
- Per modificare le unità di misura per i valori di archiviazione visualizzati in Grid Manager, selezionare il menu a discesa dell'utente in alto a destra di Grid Manager, quindi selezionare **Preferenze utente**.
- Gli screenshot mostrati sono esempi. I risultati potrebbero variare a seconda della versione StorageGRID .

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%

Icône dello stato della connessione

Se un nodo è disconnesso dalla rete, accanto al nome del nodo viene visualizzata una delle seguenti icône.

Icona	Descrizione	Azione richiesta
	<p>Non connesso - Sconosciuto</p> <p>Per un motivo sconosciuto, un nodo è disconnesso oppure i servizi sul nodo sono inaspettatamente inattivi. Ad esempio, un servizio sul nodo potrebbe essere interrotto oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un'interruzione imprevista.</p> <p>Potrebbe anche essere attivato l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.</p>	<p>Richiede attenzione immediata. "Seleziona ogni avviso" e seguire le azioni consigliate.</p> <p>Ad esempio, potrebbe essere necessario riavviare un servizio che si è arrestato o riavviare l'host per il nodo.</p> <p>Nota: un nodo potrebbe apparire come Sconosciuto durante le operazioni di arresto gestito. In questi casi è possibile ignorare lo stato Sconosciuto.</p>
	<p>Non connesso - Amministrativamente inattivo</p> <p>Per un motivo prevedibile, il nodo non è connesso alla griglia.</p> <p>Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.</p> <p>In base al problema di fondo, questi nodi spesso tornano online senza alcun intervento.</p>	<p>Determina se ci sono avvisi che interessano questo nodo.</p> <p>Se uno o più avvisi sono attivi, "Seleziona ogni avviso" e seguire le azioni consigliate.</p>

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

Icone di avviso

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

Critico: si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID . Bisogna affrontare immediatamente il problema di fondo. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.

Grave: Esiste una condizione anomala che sta influenzando le operazioni in corso o che si sta avvicinando alla soglia di un avviso critico. È necessario esaminare gli avvisi principali e risolvere eventuali problemi sottostanti per garantire che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID .

Minore: Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe compromettere la capacità del sistema di funzionare se continua a verificarsi tale condizione. È opportuno monitorare e risolvere gli avvisi minori che non si risolvono da soli, per evitare che diano origine a problemi più seri.

Visualizza i dettagli di un sistema, sito o nodo

Per filtrare le informazioni mostrate nella tabella Nodi, immettere una stringa di ricerca nel campo **Cerca**. È possibile effettuare la ricerca per nome del sistema, nome visualizzato o tipo (ad esempio, immettere **gat** per individuare rapidamente tutti i nodi gateway).

Per visualizzare le informazioni sulla griglia, sul sito o sul nodo:

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

Visualizza la scheda Panoramica

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

La scheda Panoramica viene visualizzata per tutti i nodi.

Informazioni sul nodo

La sezione Informazioni sul nodo della scheda 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** (mostrato solo se il nodo è stato rinominato): il nome visualizzato corrente per il nodo. Utilizzare il "[Rinomina griglia, siti e nodi](#)" procedura per aggiornare questo valore.
- **Nome del sistema**: il nome immesso per il nodo durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni interne StorageGRID 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, noto anche come UUID.
- **Stato della connessione**: uno dei tre stati. Viene mostrata l'icona per lo stato più grave.
 - **Sconosciuto***  : Per un motivo sconosciuto, il nodo non è connesso alla rete oppure uno o più servizi sono inaspettatamente inattivi. Ad esempio, la connessione di rete tra i nodi è stata interrotta, l'alimentazione è interrotta o un servizio non è disponibile. Potrebbe anche essere attivato 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 arresto gestito. In questi casi è possibile ignorare lo stato Sconosciuto.

- ***Amministrativamente inattivo***  : Il nodo non è connesso alla rete per un motivo prevedibile. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.
- ***Collegato***  : Il nodo è connesso alla rete.

- **Archiviazione utilizzata**: solo per nodi di archiviazione.
 - **Dati oggetto**: percentuale dello spazio totale utilizzabile per i dati oggetto che è stato utilizzato sul nodo di archiviazione.
 - **Metadati oggetto**: percentuale dello spazio totale consentito per i metadati oggetto utilizzato sul nodo di archiviazione.
- **Versione software**: la versione di StorageGRID installata sul nodo.
- **Gruppi HA**: solo per nodi amministrativi e nodi gateway. Viene mostrato se un'interfaccia di rete sul nodo è inclusa in un gruppo ad alta disponibilità e se tale interfaccia è l'interfaccia primaria.
- **Indirizzi IP**: gli indirizzi IP del nodo. Fare clic su **Mostra indirizzi IP aggiuntivi** per visualizzare gli indirizzi IPv4 e IPv6 del nodo e le mappature delle interfacce.

Avvisi

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

Alert name	Severity	Time triggered	Current values
Low installed node memory 🔗	Critical	11 hours ago 🔗	Total RAM size: 8.37 GB

The amount of installed memory on a node is low.

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

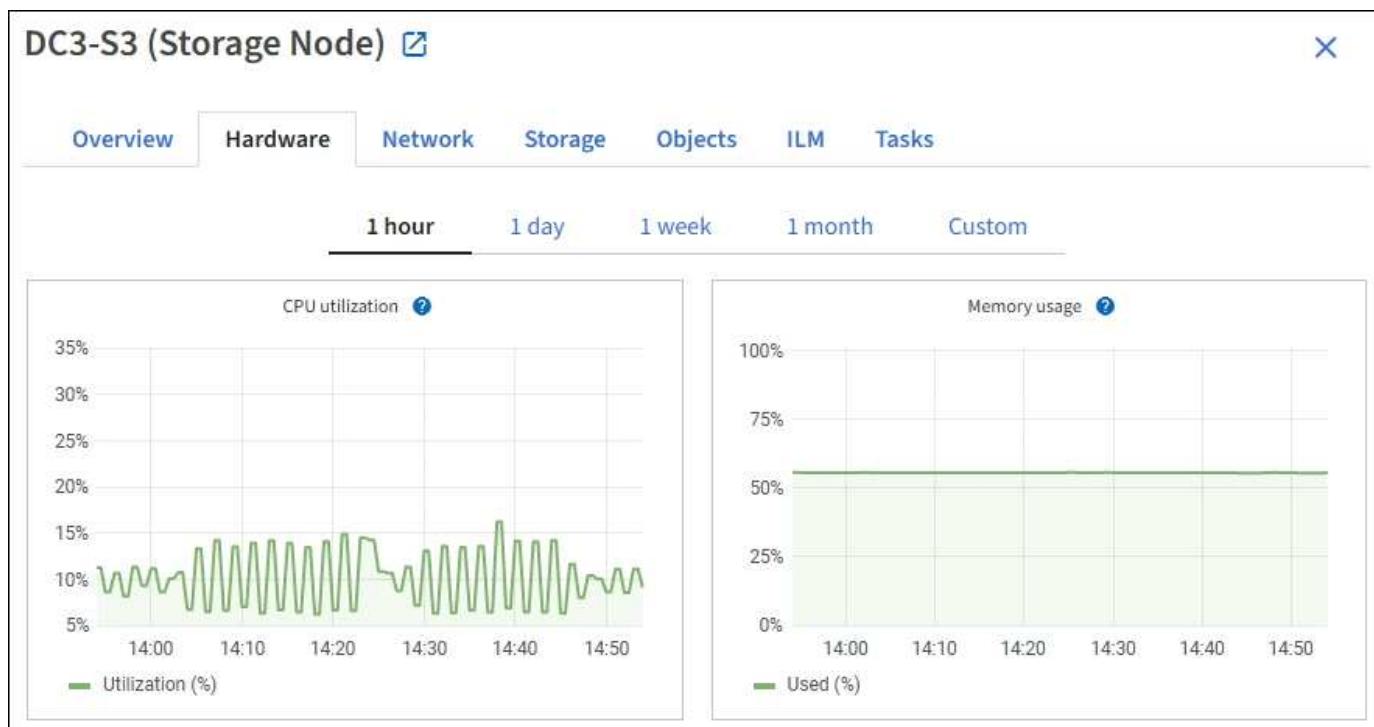
Visualizza la scheda Hardware

La scheda Hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo, nonché informazioni hardware aggiuntive sugli apparecchi.



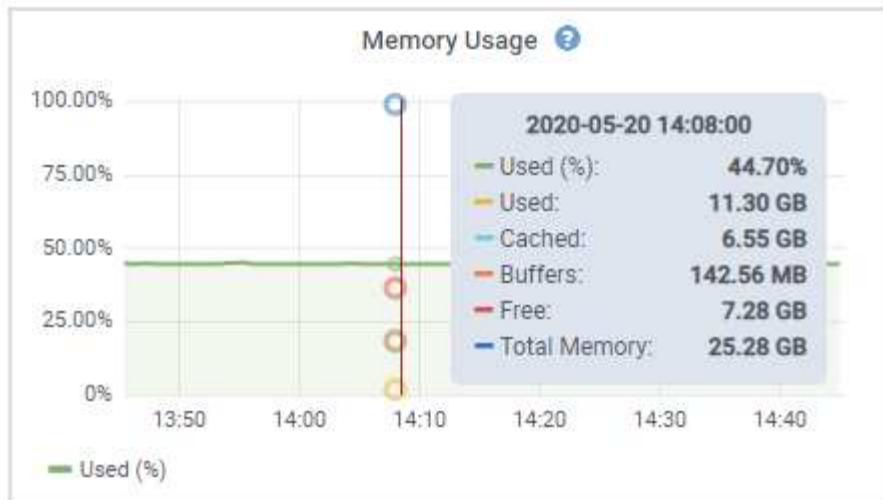
Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere agli screenshot di esempio presenti in questa pagina.

La scheda Hardware viene visualizzata per tutti i nodi.



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

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



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

Visualizza informazioni sui nodi di archiviazione dell'appliance

Nella pagina Nodi sono elencate le informazioni sullo stato del servizio e su tutte le risorse di calcolo, dei dispositivi disco e di rete per ciascun nodo di archiviazione dell'appliance. È inoltre possibile visualizzare la memoria, l'hardware di archiviazione, la versione del firmware del controller, le risorse di rete, le interfacce di rete, gli indirizzi di rete e la ricezione e la trasmissione dei dati.

Passi

1. Dalla pagina Nodi, seleziona un nodo di archiviazione dell'appliance.
2. Selezionare **Panoramica**.

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

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

DC2-SGA-010-096-106-021 (Storage Node)



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

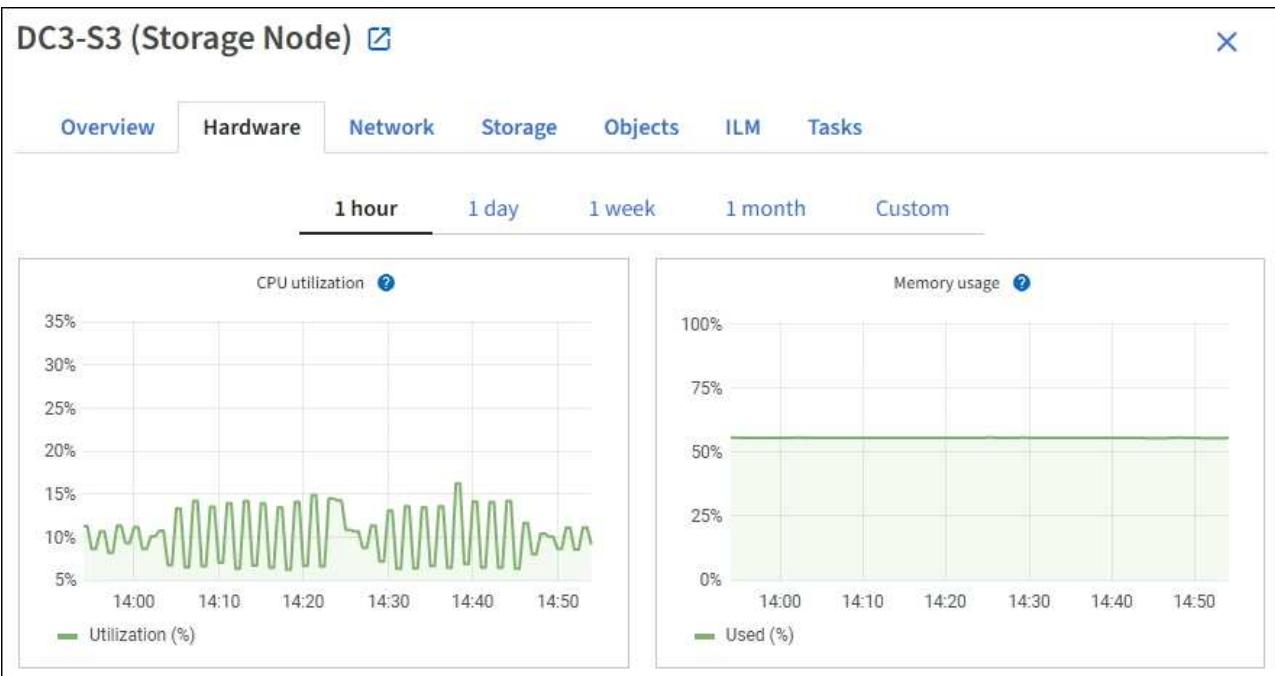
Alerts

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 tutti gli avvisi attivi per il nodo.

3. Selezionare **Hardware** per visualizzare maggiori informazioni sull'apparecchio.

- Visualizza i grafici di 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, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche 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'apparecchio. Questa tabella contiene informazioni quali il nome del modello dell'apparecchio, i nomi dei controller, i numeri di serie e gli indirizzi IP, nonché lo stato di ciascun componente.



Alcuni campi, come Compute controller BMC IP e Compute hardware, vengono visualizzati solo per gli apparecchi dotati di tale funzionalità.

I componenti per i ripiani di stoccaggio e i ripiani di espansione, se fanno parte dell'installazione, vengono visualizzati in una tabella separata sotto la tabella degli elettrodomestici.

StorageGRID Appliance

Appliance model:	SG6060
Storage controller name:	StorageGRID-Lab79-SG6060-7-134
Storage controller A management IP:	10.2 [REDACTED]
Storage controller B management IP:	10.2 [REDACTED]
Storage controller WWID:	6d039ea0000173e5000000065b7b761
Storage appliance chassis serial number:	721924500068
Storage controller firmware version:	08.53.00.09
Storage controller SANtricity OS version:	11.50.3R2
Storage controller NVSRAM version:	N280X-853834-DG1
Storage hardware:	Nominal [REDACTED]
Storage controller failed drive count:	0 [REDACTED]
Storage controller A:	Nominal [REDACTED]
Storage controller B:	Nominal [REDACTED]
Storage controller power supply A:	Nominal [REDACTED]
Storage controller power supply B:	Nominal [REDACTED]
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 [REDACTED]
Compute controller BMC IP:	10.2 [REDACTED]
Compute controller serial number:	721917500060
Compute hardware:	Needs Attention [REDACTED]
Compute controller CPU temperature:	Nominal [REDACTED]
Compute controller chassis temperature:	Nominal [REDACTED]
Compute controller power supply A:	Failed [REDACTED]
Compute controller power supply B:	Nominal [REDACTED]

Storage shelves

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

Campo nella tabella Appliance	Descrizione
Modello di elettrodomestico	Il numero di modello per questo dispositivo StorageGRID mostrato in SANtricity OS.
Nome del controller di archiviazione	Nome di questo dispositivo StorageGRID mostrato in SANtricity OS.
Controller di archiviazione A IP di gestione	Indirizzo IP per la porta di gestione 1 sul controller di archiviazione A. Utilizzare questo IP per accedere a SANtricity OS per risolvere i problemi di archiviazione.
IP di gestione del controller di archiviazione B	Indirizzo IP per la porta di gestione 1 sul controller di archiviazione B. Utilizzare questo IP per accedere a SANtricity OS per risolvere i problemi di archiviazione. Alcuni modelli di elettrodomestici non dispongono di un controller di archiviazione B.

Campo nella tabella Appliance	Descrizione
WWID del controller di archiviazione	Identificatore mondiale del controller di archiviazione mostrato in SANtricity OS.
Numero di serie del telaio dell'apparecchio di archiviazione	Numero di serie del telaio dell'apparecchio.
Versione del firmware del controller di archiviazione	La versione del firmware sul controller di archiviazione per questo dispositivo.
Versione del sistema operativo SANtricity del controller di archiviazione	La versione SANtricity OS del controller di archiviazione A.
Versione NVSRAM del controller di archiviazione	<p>Versione NVSRAM del controller di archiviazione come riportato da SANtricity System Manager.</p> <p>Per SG6060 e SG6160, se c'è una mancata corrispondenza della versione NVSRAM tra i due controller, viene visualizzata la versione del controller A. Se il controller A non è installato o non è operativo, viene visualizzata la versione del controller B.</p>
Hardware di archiviazione	<p>Stato generale dell'hardware del controller di archiviazione. Se SANtricity System Manager segnala lo stato "Necessita attenzione" per l'hardware di archiviazione, anche il sistema StorageGRID segnala questo valore.</p> <p>Se lo stato è "richiede attenzione", controllare prima il controller di archiviazione utilizzando SANtricity OS. Quindi, assicurarsi che non vi siano altri avvisi applicabili al controller di elaborazione.</p>
Conteggio unità non riuscite del controller di archiviazione	Numero di unità non ottimali.
Controllore di archiviazione A	Lo stato del controller di archiviazione A.
Controllore di archiviazione B	Lo stato del controller di archiviazione B. Alcuni modelli di appliance non dispongono di un controller di archiviazione B.
Alimentatore del controller di archiviazione A	Lo stato dell'alimentatore A per il controller di archiviazione.
Alimentatore del controller di archiviazione B	Lo stato dell'alimentatore B per il controller di archiviazione.
Tipo di unità di archiviazione dati	Il tipo di unità presenti nell'appliance, ad esempio HDD (disco rigido) o SSD (unità a stato solido).

Campo nella tabella Appliance	Descrizione
Dimensioni dell'unità di archiviazione dati	<p>La dimensione effettiva di un'unità dati.</p> <p>Per il modello SG6160 viene visualizzata anche la dimensione dell'unità cache.</p> <p>Nota: Per i nodi con ripiani di espansione, utilizzare Dimensioni dell'unità dati per ogni ripiano Invece. Le dimensioni effettive dell'unità potrebbero variare a seconda dello scaffale.</p>
Modalità RAID di archiviazione	Modalità RAID configurata per l'appliance.
Connettività di archiviazione	Lo stato di connettività dell'archiviazione.
Alimentazione elettrica complessiva	Lo stato di tutte le alimentazioni elettriche dell'apparecchio.
Controller di calcolo BMC IP	<p>L'indirizzo IP della porta del controller di gestione della scheda madre (BMC) nel controller di elaborazione. Utilizzare questo IP 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	Numero di serie del controller di elaborazione.
Hardware di calcolo	Lo stato dell'hardware del controller di elaborazione. Questo campo non viene visualizzato per i modelli di appliance che non dispongono di hardware di elaborazione e hardware di archiviazione separati.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di elaborazione.
Calcola la temperatura del telaio del controller	Lo stato della temperatura del controller di calcolo.

+

Colonna nella tabella Scaffali portaoggetti	Descrizione
Numero di serie del telaio dello scaffale	Numero di serie del telaio del ripiano portaoggetti.

Colonna nella tabella Scaffali portaoggetti	Descrizione
ID scaffale	<p>Identificatore numerico per lo scaffale di stoccaggio.</p> <ul style="list-style-type: none"> • 99: Ripiano del controller di archiviazione • 0: Primo scaffale di espansione • 1: Secondo ripiano di espansione <p>Nota: i ripiani di espansione sono disponibili solo per i modelli SG6060 e SG6160.</p>
Stato di conservazione	Lo stato generale dello scaffale di stoccaggio.
Stato dell'IOM	Lo stato dei moduli di input/output (IOM) in tutti gli scaffali di espansione. N/D se non si tratta di uno scaffale di espansione.
Stato dell'alimentazione	Lo stato generale degli alimentatori per lo scaffale di stoccaggio.
Stato del cassetto	Lo stato dei cassetti nello scaffale portaoggetti. N/D se lo scaffale non contiene cassetti.
Stato del fan	Stato generale delle ventole di raffreddamento nel ripiano portaoggetti.
Slot di unità	Numero totale di slot per unità nello scaffale di archiviazione.
Unità dati	Numero di unità nello spazio di archiviazione utilizzate per l'archiviazione dei dati.
Dimensione dell'unità dati	La dimensione effettiva di un'unità dati nello spazio di archiviazione.
Unità cache	Numero di unità nello spazio di archiviazione utilizzate come cache.
Dimensioni dell'unità cache	La dimensione dell'unità cache più piccola nello spazio di archiviazione. Di solito, le unità cache hanno tutte le stesse dimensioni.
Stato di configurazione	Lo stato di configurazione dello scaffale di stoccaggio.

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

Se uno stato non è "Nominali", rivedere tutti gli avvisi correnti. È anche possibile utilizzare SANtricity System Manager per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

4. Selezionare **Rete** per visualizzare le informazioni per 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 **Velocità** nella tabella Interfacce di rete per determinare se le porte di rete 10/25-GbE sull'appliance sono state configurate per utilizzare la modalità attiva/backup o la modalità LACP.



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

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

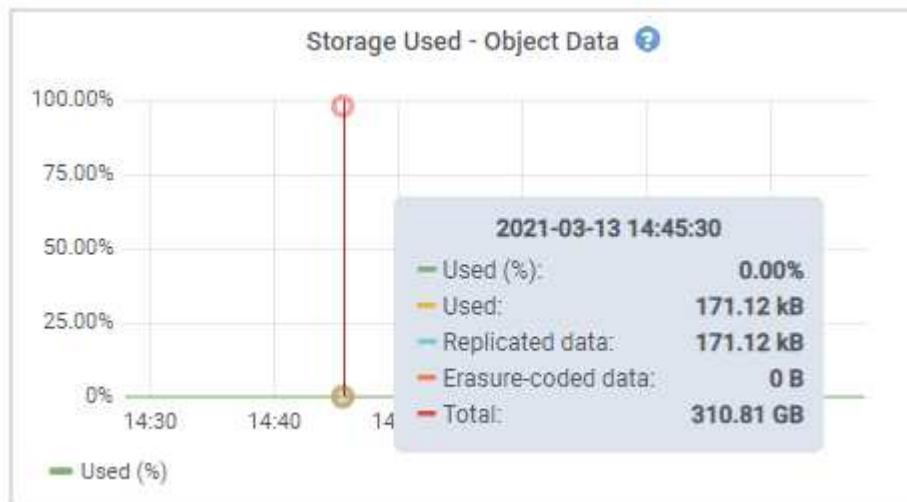
Vedere "[Configurare i collegamenti di rete](#)" per ulteriori informazioni sulla configurazione delle porte 10/25-GbE.

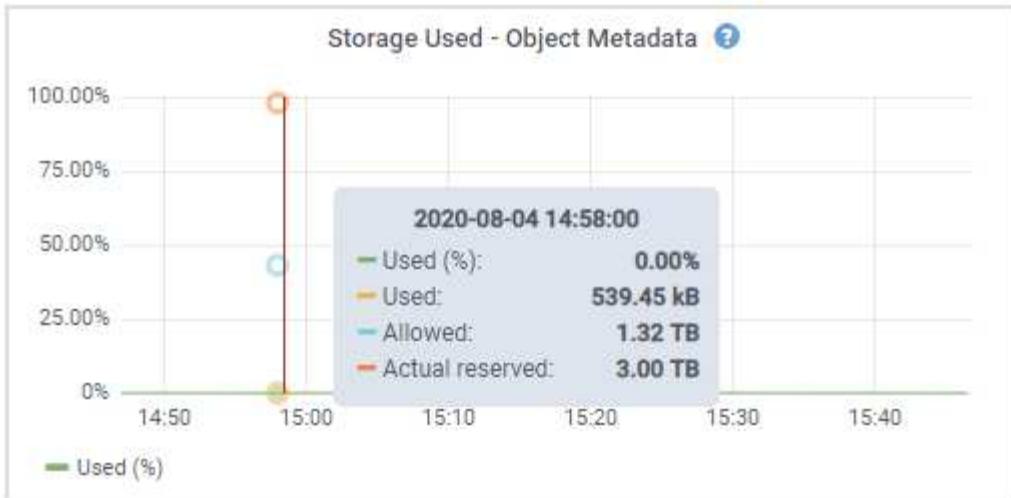
b. Rivedere la sezione Comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati su 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 **Archiviazione** per visualizzare grafici che mostrano le percentuali di spazio di archiviazione utilizzato nel tempo per i dati degli oggetti e i metadati degli oggetti, nonché informazioni su dispositivi disco, volumi e archivi di oggetti.





- a. Scorrere verso il basso per visualizzare la quantità di spazio di archiviazione disponibile per ciascun volume e archivio oggetti.

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

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

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

Volumes					
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

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

Visualizza informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway

La pagina Nodi elenca le informazioni sullo stato del servizio e su tutte le risorse di calcolo, dei dispositivi disco e di rete per ogni appliance di servizi utilizzata come nodo di amministrazione o nodo gateway. È inoltre possibile visualizzare la memoria, l'hardware di archiviazione, le risorse di rete, le interfacce di rete, gli indirizzi di rete e la ricezione e la trasmissione di dati.

Passi

1. Dalla pagina Nodi, seleziona un nodo di amministrazione dell'appliance o un nodo gateway dell'appliance.
2. Selezionare **Panoramica**.

La sezione Informazioni nodo della scheda Panoramica visualizza informazioni riepilogative sul nodo, come il nome, il tipo, l'ID e lo stato della connessione. L'elenco degli indirizzi IP include il nome

dell'interfaccia per ciascun indirizzo, come segue:

- **adlb e adlli**: visualizzati se viene utilizzato il bonding attivo/di backup per l'interfaccia di rete di amministrazione
- **eth**: Rete Grid, Rete di amministrazione o Rete client.
- **hic**: Una delle porte fisiche da 10, 25 o 100 GbE sull'appliance. Queste porte possono essere collegate tra loro e connesse alla rete StorageGRID Grid (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte fisiche da 1 GbE sull'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia di rete di amministrazione (eth1). È possibile lasciare disponibili altre interfacce mtc per la connettività locale temporanea di un tecnico nel data center.

The screenshot shows the SANtricity System Manager interface for node 10-224-6-199-ADM1. The top navigation bar includes tabs for Overview, Hardware, Network, Storage, Load balancer, Tasks, and SANtricity System Manager. The Network tab is currently selected. Below the tabs, the "Node information" section displays the following details:

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)

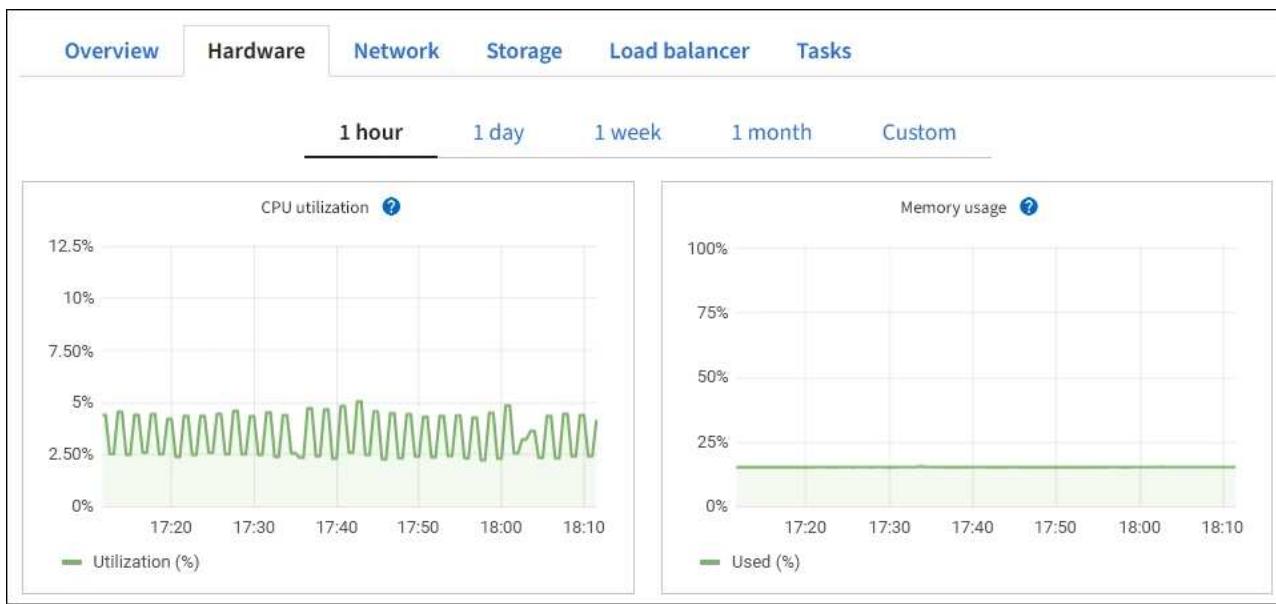
Below this, there is a link to "Hide additional IP addresses". A scrollable table lists the IP addresses assigned to various interfaces:

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 tutti gli avvisi attivi per il nodo.

3. Selezionare **Hardware** per visualizzare maggiori informazioni sull'apparecchio.

- a. Visualizza i grafici di 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, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche 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'apparecchio. Questa tabella contiene informazioni quali il nome del modello, il numero di serie, la versione del firmware del controller e lo stato di ciascun componente.

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	??

Campo nella tabella Appliance	Descrizione
Modello di elettrodomestico	Numero di modello per questo dispositivo StorageGRID .

Campo nella tabella Appliance	Descrizione
Conteggio unità non riuscite del controller di archiviazione	Numero di unità non ottimali.
Tipo di unità di archiviazione dati	Il tipo di unità presenti nell'appliance, ad esempio HDD (disco rigido) o SSD (unità a stato solido).
Dimensioni dell'unità di archiviazione dati	La dimensione effettiva di un'unità dati.
Modalità RAID di archiviazione	La modalità RAID per l'appliance.
Alimentazione elettrica complessiva	Lo stato di tutti gli alimentatori dell'apparecchio.
Controller di calcolo BMC IP	<p>L'indirizzo IP della porta del controller di gestione della scheda madre (BMC) nel controller di elaborazione. È possibile utilizzare questo IP 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	Numero di serie del controller di elaborazione.
Hardware di calcolo	Lo stato dell'hardware del controller di elaborazione.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di elaborazione.
Calcola la temperatura del telaio del controller	Lo stato della temperatura del controller di calcolo.

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

Se uno stato non è "Nominali", rivedere tutti gli avvisi correnti.

4. Selezionare **Rete** per visualizzare le informazioni per 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 **Velocità** nella tabella Interfacce di rete per determinare se le quattro porte di rete 40/100-GbE sull'appliance sono state configurate per utilizzare la modalità attiva/backup o la modalità LACP.



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

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

b. Rivedere la sezione Comunicazione di rete.

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



5. Selezionare **Archiviazione** per visualizzare informazioni sui dispositivi disco e sui volumi nell'appliance dei servizi.

DO-REF-DC1-GW1 (Gateway Node)



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

Visualizza la scheda Rete

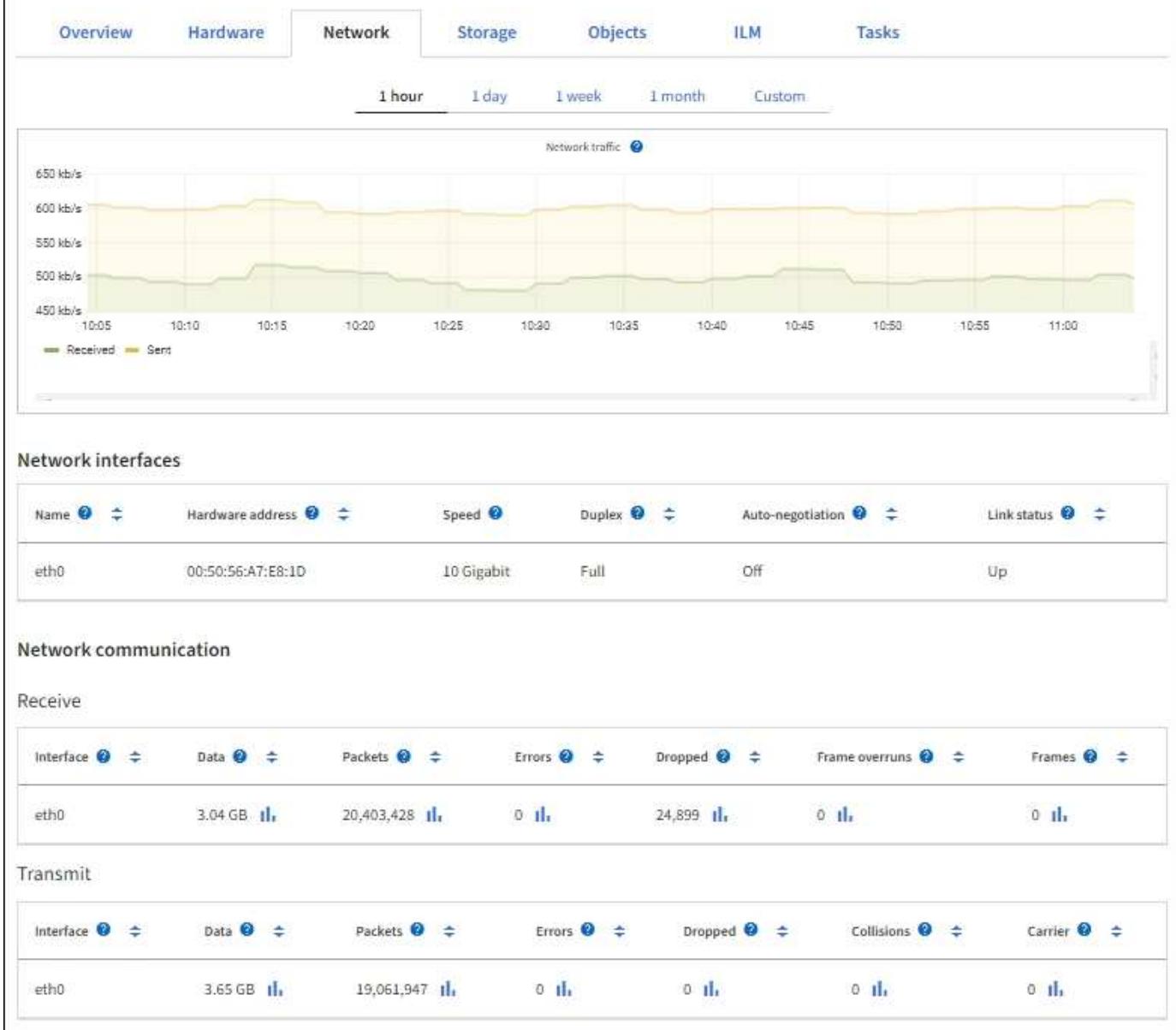
La scheda Rete visualizza un grafico che mostra il traffico di rete ricevuto e inviato su tutte le interfacce di rete sul nodo, sul sito o sulla griglia.

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

Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È anche 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 su eventuali contatori di errori segnalati dal driver.

DC1-S2 (Storage Node)



Informazioni correlate

"Monitorare le connessioni e le prestazioni di rete"

Visualizza la scheda Archiviazione

La scheda Archiviazione riassume la disponibilità di archiviazione e altre metriche di archiviazione.

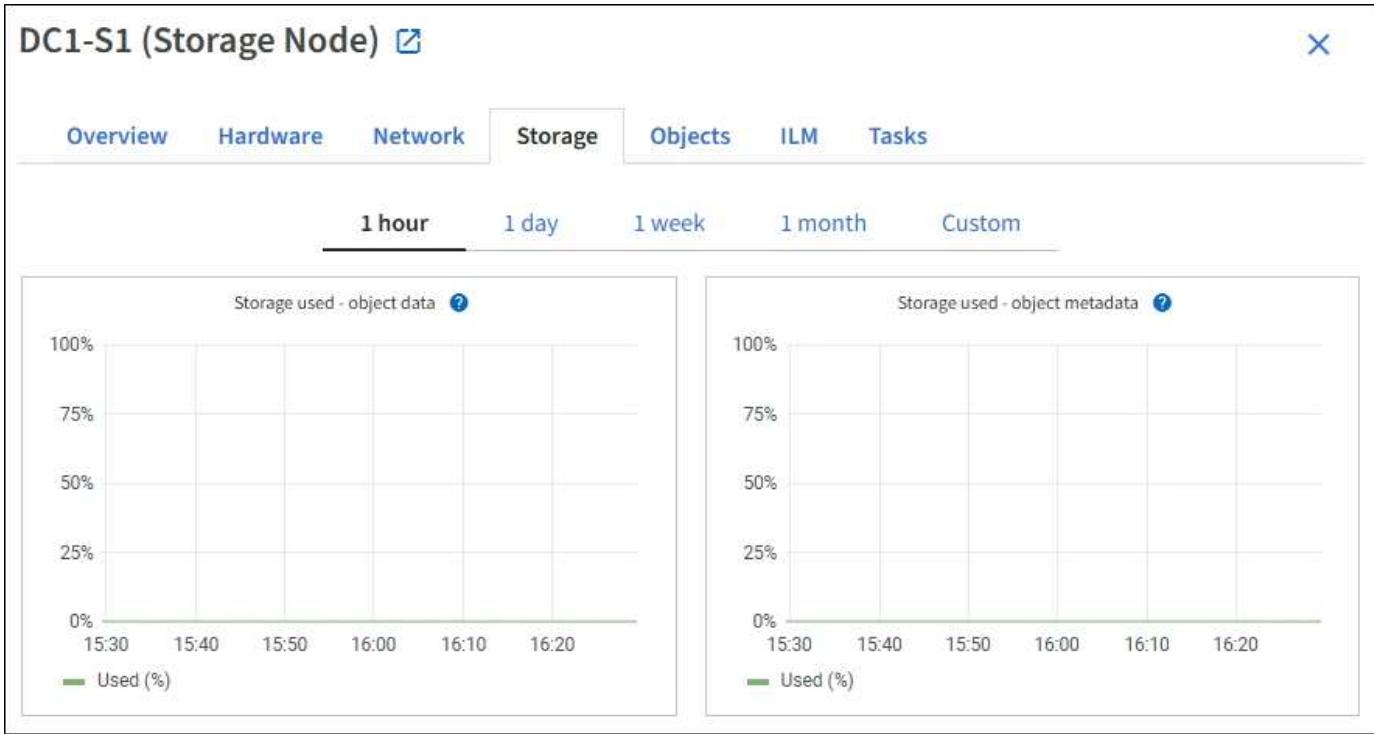
La scheda Archiviazione viene visualizzata per tutti i nodi, per ciascun sito e per l'intera griglia.

Grafici di archiviazione utilizzati

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



Quando un nodo non è connesso alla rete, ad esempio durante un aggiornamento o in uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della rete. Dopo che un nodo si è ricollegato alla rete, attendere alcuni minuti affinché i valori si stabilizzino.



Dispositivi disco, volumi e tabelle di archiviazione oggetti

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

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

Volumes					
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

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

Informazioni correlate

["Monitorare la capacità di archiviazione"](#)

Visualizza la scheda Oggetti

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

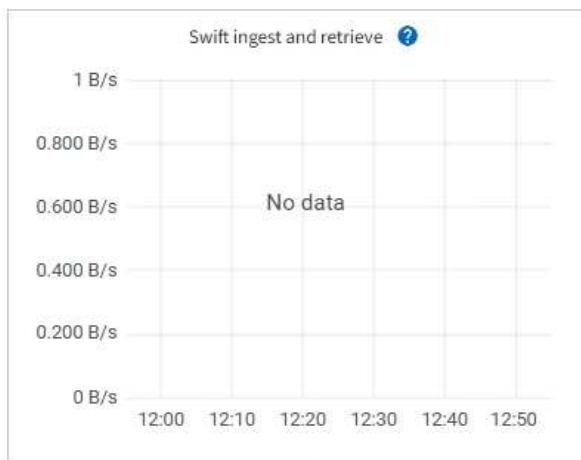
La scheda Oggetti viene visualizzata per ogni nodo di archiviazione, ogni sito e l'intera griglia. Per i nodi di archiviazione, la scheda Oggetti fornisce anche conteggi degli oggetti e informazioni sulle query dei metadati e sulla verifica in background.

DC1-S1 (Storage Node)



Overview Hardware Network Storage **Objects** ILM Tasks

1 hour 1 day 1 week 1 month Custom



Object counts

Total objects:  1,295

Lost objects:  0 

S3 buckets and Swift containers:  161

Metadata store queries

Average latency:  10.00 milliseconds

Queries - successful:  14,587 

Queries - failed (timed out):  0 

Queries - failed (consistency level unmet):  0 

Verification

Status:  No errors 

Percent complete:  47.14% 

Average stat time:  0.00 microseconds 

Objects verified:  0 

Object verification rate:  0.00 objects / second 

Data verified:  0 bytes 

Data verification rate:  0.00 bytes / second 

Missing objects:  0 

Corrupt objects:  0 

Corrupt objects unidentified:  0

Quarantined objects:  0 

Visualizza la scheda ILM

La scheda ILM fornisce informazioni sulle operazioni di gestione del ciclo di vita delle informazioni (ILM).

La scheda ILM viene visualizzata per ogni nodo di archiviazione, ogni 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 di archiviazione, la scheda ILM fornisce dettagli sulla valutazione ILM e sulla verifica in background per gli oggetti con codice di cancellazione.

DC2-S1 (Storage Node)

Overview Hardware Network Storage Objects **ILM** Tasks

Evaluation

Awaiting - all:  0	objects	
Awaiting - client:  0	objects	
Evaluation rate:  0.00	objects / second	
Scan rate:  0.00	objects / second	

Erasure coding verification

Status:  Idle	
Next scheduled:  2021-09-09 17:36:44 MDT	
Fragments verified:  0	
Data verified:  0 bytes	
Corrupt copies:  0	
Corrupt fragments:  0	
Missing fragments:  0	

Informazioni correlate

- "Monitorare la gestione del ciclo di vita delle informazioni"
- "Amministra StorageGRID"

Utilizzare la scheda Attività

La scheda Attività viene visualizzata per tutti i nodi. È possibile utilizzare questa scheda per rinominare o riavviare un nodo oppure per mettere un nodo appliance in modalità di manutenzione.

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

- "[Rinomina griglia, siti e nodi](#)"
- "[Riavvia il nodo della griglia](#)"
- "[Mettere l'apparecchio in modalità manutenzione](#)"

Visualizza la scheda Bilanciatore del carico

La scheda Load Balancer include grafici delle prestazioni e della diagnostica relativi al funzionamento del servizio Load Balancer.

La scheda Load Balancer viene visualizzata per i nodi di amministrazione e i nodi gateway, per ciascun sito e per l'intera griglia. Per ogni sito, la scheda Load Balancer fornisce un riepilogo aggregato delle statistiche per tutti i nodi di quel sito. Per l'intera griglia, la scheda Load Balancer fornisce un riepilogo aggregato delle statistiche per tutti i siti.

Se non viene eseguito alcun I/O tramite il servizio Load Balancer o non è configurato alcun load balancer, i grafici visualizzano "Nessun dato".

DC1-G1 (Gateway Node)

X

Overview Hardware Network Storage Load balancer Tasks

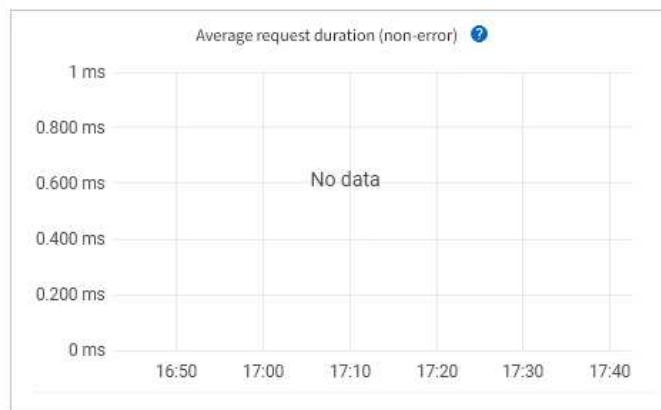
1 hour

1 day

1 week

1 month

Custom



Richiedi traffico

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



Questo valore viene aggiornato al completamento di ogni richiesta. Di conseguenza, questo valore potrebbe differire dalla produttività in tempo reale in caso di basse frequenze di richiesta o per richieste di durata molto lunga. È possibile consultare la scheda Rete per avere una visione più realistica del comportamento attuale della rete.

Tasso di richiesta in arrivo

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

Durata media della richiesta (senza errori)

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

client.

Tasso di risposta agli errori

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

Informazioni correlate

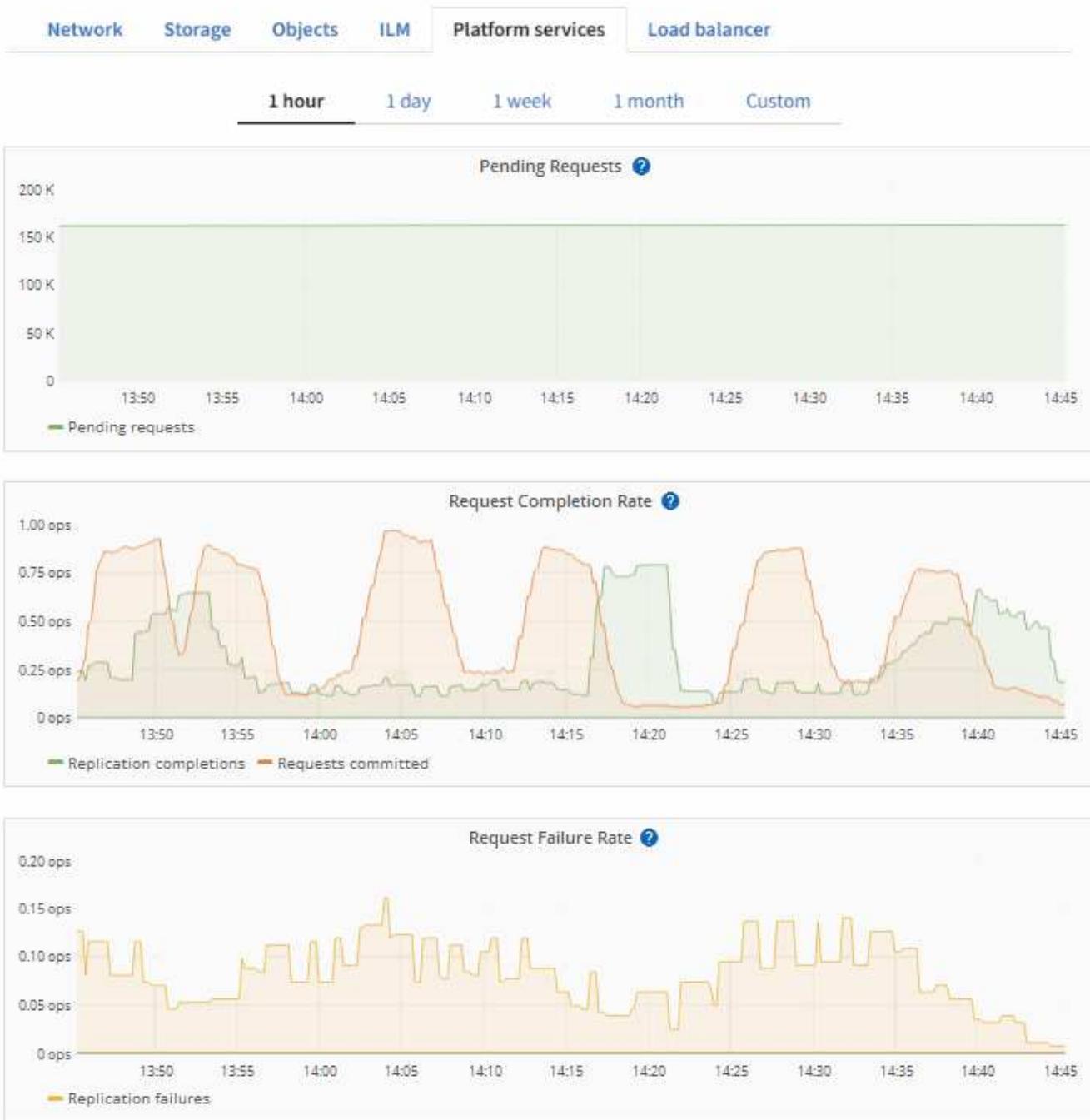
- ["Monitorare le operazioni di bilanciamento del carico"](#)
- ["Amministra StorageGRID"](#)

Visualizza la scheda Servizi della piattaforma

La scheda Servizi della piattaforma fornisce informazioni su tutte le operazioni dei servizi della piattaforma S3 in un sito.

Per ogni sito viene visualizzata la scheda Servizi della piattaforma. Questa scheda fornisce informazioni sui servizi della piattaforma S3, come la replica CloudMirror e il servizio di integrazione della ricerca. I grafici in questa scheda mostrano parametri quali il numero di richieste in sospeso, la percentuale di completamento delle richieste e la percentuale di errore delle richieste.

DC1 (Site)



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

Visualizza la scheda Gestisci unità

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

Utilizzando la scheda Gestisci unità, puoi effettuare le seguenti operazioni:

- Visualizza un layout delle unità di archiviazione dati nell'appliance
- Visualizza una tabella che elenca ciascuna posizione dell'unità, tipo, stato, versione del firmware e numero di serie
- Eseguire funzioni di risoluzione dei problemi e manutenzione su ciascuna unità

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

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 SANtricity System Manager consente di accedere a SANtricity System Manager senza dover configurare o connettere la porta di gestione dell'appliance di archiviazione. È possibile utilizzare questa scheda per esaminare le informazioni diagnostiche e ambientali dell'hardware, nonché i problemi relativi alle unità.

 L'accesso a SANtricity System Manager da Grid Manager è in genere destinato solo al monitoraggio dell'hardware dell'appliance e alla configurazione di E-Series AutoSupport. Molte funzionalità e operazioni di SANtricity System Manager, come l'aggiornamento del firmware, non sono applicabili al monitoraggio dell'appliance StorageGRID . Per evitare problemi, seguire sempre le istruzioni di manutenzione hardware del proprio elettrodomestico. Per aggiornare il firmware SANtricity , vedere "[Procedure di configurazione della manutenzione](#)" per il tuo dispositivo di archiviazione.

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

Utilizzando SANtricity System Manager, è possibile effettuare le seguenti operazioni:

- Visualizza i dati sulle prestazioni, come le prestazioni a livello di array di archiviazione, la latenza di I/O, l'utilizzo della CPU del controller di archiviazione e la velocità effettiva.
- 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 SANtricity System Manager per configurare un proxy per E-Series AutoSupport, vedere "[Inviare pacchetti E-Series AutoSupport tramite StorageGRID](#)" .

Per accedere a SANtricity System Manager tramite Grid Manager, è necessario disporre di "[Amministratore dell'appliance di archiviazione o autorizzazione di accesso root](#)" .



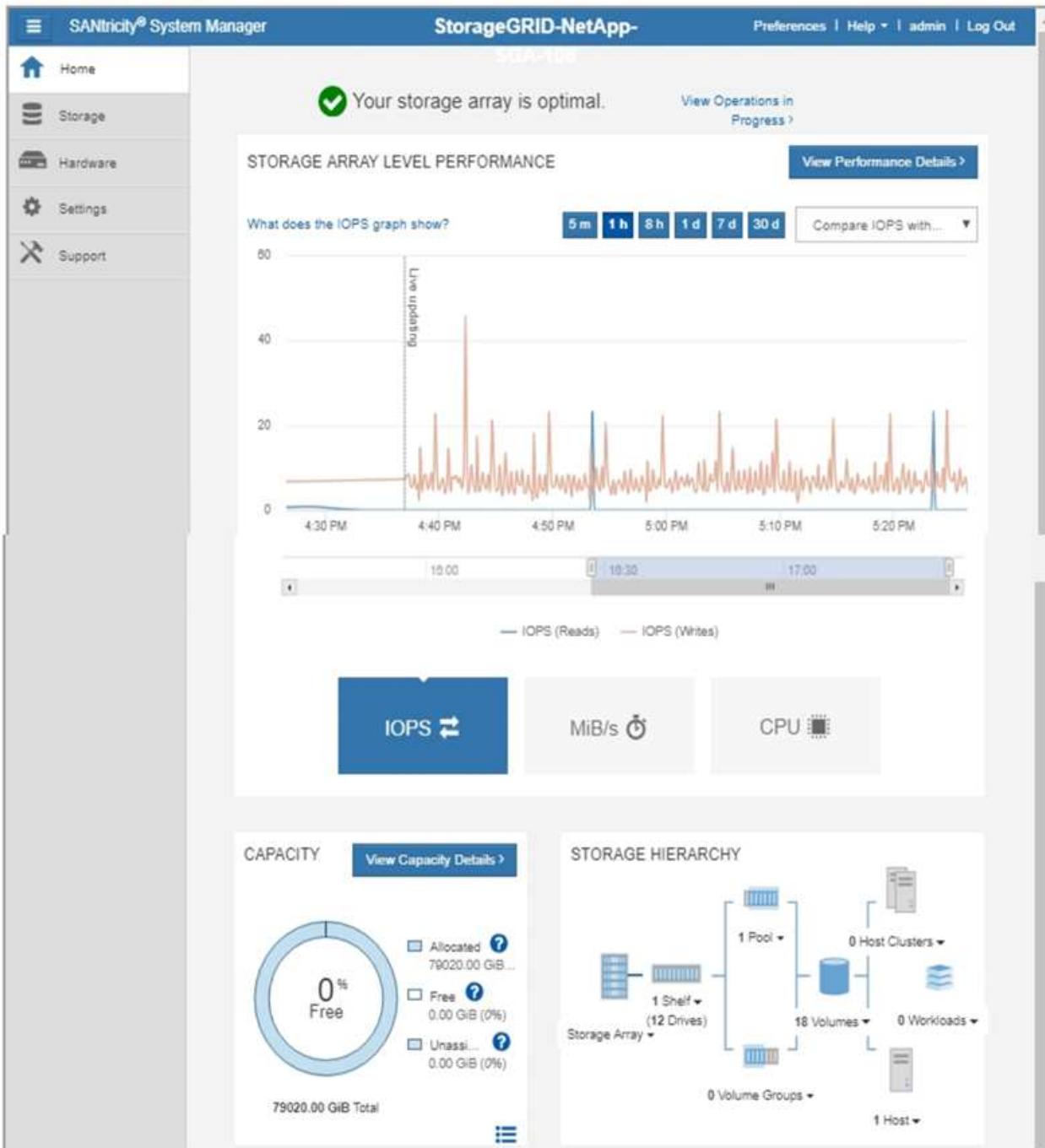
Per accedere a SANtricity System Manager tramite Grid Manager è necessario disporre del firmware SANtricity 8.70 o superiore.

La scheda visualizza la home page di SANtricity System Manager.

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 SANtricity System Manager per aprire SANtricity System Manager in una nuova finestra del browser per una visualizzazione più semplice.

Per visualizzare i dettagli sulle prestazioni a livello di array di archiviazione e sull'utilizzo della capacità,

posizionare il cursore su ciascun grafico.

Per maggiori dettagli sulla visualizzazione delle informazioni accessibili dalla scheda SANtricity System Manager, vedere "Documentazione 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 rete non sono disponibili, è opportuno monitorare e risolvere i potenziali problemi prima che influiscano sull'efficienza o sulla disponibilità della rete.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai ["autorizzazioni di accesso specifiche"](#).

Informazioni sulle attività di monitoraggio

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

Cosa monitorare	Frequenza
"Stato di salute del sistema"	Quotidiano
Tasso a cui " Capacità degli oggetti e dei metadati del nodo di archiviazione " viene consumato	Settimanale
"Operazioni di gestione del ciclo di vita delle informazioni"	Settimanale
"Risorse di rete e di sistema"	Settimanale
"Attività degli inquilini"	Settimanale
"Operazioni client S3"	Settimanale
"Operazioni di bilanciamento del carico"	Dopo la configurazione iniziale e dopo eventuali modifiche alla configurazione
"Connessioni di federazione della rete"	Settimanale

Monitorare lo stato di salute del sistema

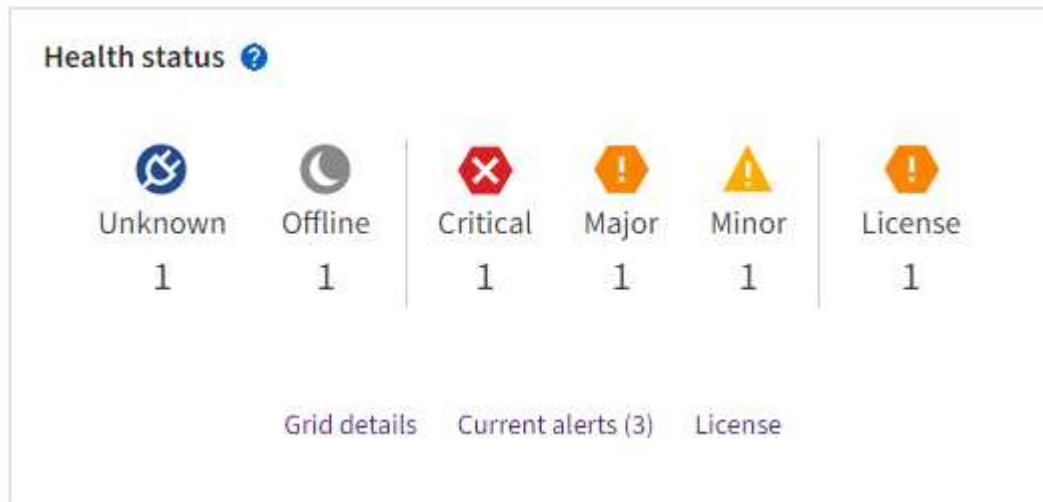
Monitora quotidianamente lo stato di salute generale del tuo sistema StorageGRID .

Informazioni su questo compito

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

Esaminare i problemi riepilogati nella scheda Stato di integrità della dashboard di Grid Manager.

Per essere avvisato degli avvisi non appena vengono attivati, puoi "[impostare notifiche e-mail per gli avvisi](#)" o "[configurare trappole SNMP](#)".



Quando si verificano problemi, vengono visualizzati dei link che consentono di visualizzare ulteriori dettagli:

Collegamento	Appare quando...
Dettagli della griglia	Alcuni nodi sono disconnessi (stato di connessione Sconosciuto o Amministrativamente inattivo).
Avvisi attuali (critici, gravi, minori)	Gli avvisi sono attualmente attivo .
Avvisi risolti di recente	Avvisi attivati nell'ultima settimana sono ora risolti .
Licenza	Si è verificato un problema con la licenza software per questo sistema StorageGRID. È possibile " aggiornare le informazioni sulla licenza secondo necessità ". Potrebbe

Monitorare gli stati di connessione dei nodi

Se uno o più nodi vengono disconnessi dalla rete, le operazioni critiche StorageGRID potrebbero essere compromesse. 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 è disconnesso oppure i servizi sul nodo sono inaspettatamente inattivi. Ad esempio, un servizio sul nodo potrebbe essere interrotto oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un'interruzione imprevista.</p> <p>Potrebbe anche essere attivato l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.</p>	<p>Richiede attenzione immediata. Seleziona ogni avviso e seguire le azioni consigliate.</p> <p>Ad esempio, potrebbe essere necessario riavviare un servizio che si è arrestato o riavviare l'host per il nodo.</p> <p>Nota: un nodo potrebbe apparire come Sconosciuto durante le operazioni di arresto gestito. In questi casi è possibile ignorare lo stato Sconosciuto.</p>
	<p>Non connesso - Amministrativamente inattivo</p> <p>Per un motivo prevedibile, il nodo non è connesso alla griglia.</p> <p>Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.</p> <p>In base al problema di fondo, questi nodi spesso tornano online senza alcun intervento.</p>	<p>Determina se ci sono avvisi che interessano questo nodo.</p> <p>Se uno o più avvisi sono attivi, seleziona ogni avviso e seguire le azioni consigliate.</p>
	<p>Collegato</p> <p>Il nodo è collegato alla rete.</p>	Nessuna azione richiesta.

Visualizza gli avvisi correnti e risolti

Avvisi attuali: quando viene attivato un avviso, sulla dashboard viene visualizzata un'icona di avviso. Nella pagina Nodi viene visualizzata anche un'icona di avviso per il nodo. Se "le notifiche e-mail di avviso sono configurate", verrà inviata anche una notifica via e-mail, a meno che l'avviso non sia stato disattivato.

Avvisi risolti: puoi cercare e visualizzare la cronologia degli avvisi che sono stati risolti.

Facoltativamente, hai guardato il video: "[Video: Panoramica degli avvisi](#)"



Nella tabella seguente vengono descritte 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 sua descrizione.
Gravità	<p>La gravità dell'allerta. Per gli avvisi correnti, se vengono raggruppati più avvisi, la riga del titolo mostra quante istanze di quell'avviso si verificano per ogni livello di gravità.</p> <p> Critico: si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID . Bisogna affrontare immediatamente il problema di fondo. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.</p> <p> Grave: Esiste una condizione anomala che sta influenzando le operazioni in corso o che si sta avvicinando alla soglia di un avviso critico. È necessario esaminare gli avvisi principali e risolvere eventuali problemi sottostanti per garantire che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID .</p> <p> Minore: Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe compromettere la capacità del sistema di funzionare se continua a verificarsi tale condizione. È opportuno monitorare e risolvere gli avvisi minori che non si risolvono da soli, per evitare che diano origine a problemi più seri.</p>
Tempo attivato	<p>Avvisi attuali: data e ora in cui è stato attivato l'avviso, in base all'ora locale e all'ora UTC. Se vengono raggruppati più avvisi, la riga del titolo mostra gli orari dell'istanza più recente dell'avviso (<i>newest</i>) e dell'istanza più vecchia dell'avviso (<i>oldest</i>).</p> <p>Avvisi risolti: da quanto tempo è stato attivato l'avviso.</p>
Sito/Nodo	Nome del sito e del nodo in cui si sta verificando o si è verificato l'avviso.

Intestazione di colonna	Descrizione
Stato	Se l'avviso è attivo, disattivato o risolto. Se vengono raggruppati più avvisi e nel menu a discesa è selezionato Tutti gli avvisi , la riga del titolo mostra quante istanze di quell'avviso sono attive e quante istanze sono state silenziate.
Tempo di risoluzione (solo avvisi risolti)	Da quanto tempo è stato risolto l'avviso.
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 per aiutarti a comprendere e analizzare l'avviso. Ad esempio, i valori mostrati per un avviso Archiviazione dati oggetto insufficiente 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 per aiutarti a comprendere e analizzare l'avviso. Ad esempio, i valori mostrati per un avviso Archiviazione dati oggetto insufficiente includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.

Passi

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

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

- Vengono mostrati per primi gli avvisi attivati più di recente.
- Più avvisi dello stesso tipo vengono visualizzati come gruppo.
- Gli avvisi disattivati non vengono visualizzati.
- Per un avviso specifico su un nodo specifico, se vengono raggiunte le soglie per più di una gravità, viene visualizzato solo l'avviso più grave. Ciò significa che se vengono raggiunte le soglie di allerta per le gravità minore, maggiore e critica, viene visualizzato solo l'avviso critico.

La pagina Avvisi correnti viene aggiornata ogni due minuti.

2. Per espandere i gruppi di avvisi, selezionare il cursore verso il basso . Per comprimere i singoli avvisi in un gruppo, selezionare il cursore verso l'alto oppure seleziona il nome del gruppo.
3. Per visualizzare avvisi individuali anziché gruppi di avvisi, deselectare la casella di controllo **Avvisi di gruppo**.
4. Per ordinare gli avvisi correnti o i gruppi di avvisi, selezionare le frecce su/giù in ogni intestazione di colonna.
 - Quando si seleziona **Avvisi di gruppo**, vengono ordinati sia i gruppi di avvisi sia i singoli avvisi all'interno di ciascun gruppo. Ad esempio, potresti voler ordinare gli avvisi in un gruppo in base all'**ora di attivazione** per trovare l'istanza più recente di un avviso specifico.

- Quando si cancella **Avvisi di gruppo**, viene ordinato l'intero elenco degli avvisi. Ad esempio, potresti voler ordinare tutti gli avvisi per **Nodo/Sito** per visualizzare tutti gli avvisi che interessano 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 "[Disattiva le notifiche di avviso](#)".

6. Per ordinare gli avvisi risolti:
- Selezionare un periodo di tempo dal menu a discesa **Quando attivato**.
 - Selezionare uno o più livelli di gravità dal menu a discesa **Gravità**.
 - 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, seleziona l'avviso. Una finestra di dialogo fornisce dettagli e azioni consigliate per l'avviso selezionato.
8. (Facoltativo) Per un avviso specifico, seleziona Disattiva questo avviso per disattivare la regola di avviso che ha causato l'attivazione dell'avviso.

Devi avere il "[Gestisci avvisi o autorizzazione di accesso root](#)" per silenziare una regola di avviso.



Prestare attenzione quando si decide di disattivare una regola di avviso. Se una regola di avviso viene disattivata, potresti non rilevare un problema di fondo finché non impedisce il completamento di un'operazione critica.

9. Per visualizzare le condizioni attuali per la regola di avviso:
- a. Dai dettagli dell'avviso, seleziona **Visualizza condizioni**.
Viene visualizzata una finestra pop-up che elenca l'espressione Prometheus per ogni gravità definita.
 - b. Per chiudere il pop-up, fare clic in un punto qualsiasi al di fuori del pop-up.
10. Facoltativamente, seleziona **Modifica regola** per modificare la regola di avviso che ha causato l'attivazione di questo avviso.

Devi avere il "[Gestisci avvisi o autorizzazione di accesso root](#)" per modificare una regola di avviso.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, è possibile che non venga rilevato un problema di fondo finché non si impedisce il completamento di un'operazione critica.

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

Monitorare la capacità di archiviazione

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

StorageGRID archivia separatamente i dati degli oggetti e i metadati degli oggetti e riserva una quantità specifica di spazio per un database Cassandra distribuito che contiene i metadati degli oggetti. Monitora la quantità totale di spazio occupato dagli oggetti e dai metadati degli oggetti, nonché le tendenze nella quantità di spazio occupato per ciascuno. Ciò ti consentirà di pianificare in anticipo l'aggiunta di nodi ed evitare eventuali interruzioni del servizio.

Puoi "[visualizza le informazioni sulla capacità di archiviazione](#)" per l'intera griglia, per ciascun sito e per ciascun nodo di archiviazione nel sistema StorageGRID .

Monitorare la capacità di archiviazione per l'intera rete

Monitora la capacità di archiviazione complessiva della tua griglia per assicurarti che rimanga spazio libero adeguato per i dati degli oggetti e i metadati degli oggetti. Comprendere come la capacità di archiviazione cambia nel tempo può aiutarti a pianificare l'aggiunta di nodi di archiviazione o volumi di archiviazione prima che la capacità di archiviazione utilizzabile della griglia venga esaurita.

La dashboard di Grid Manager consente di valutare rapidamente la quantità di spazio di archiviazione disponibile per l'intera griglia e per ciascun data center. La pagina Nodi fornisce valori più dettagliati per i dati degli oggetti e i metadati degli oggetti.

Passi

1. Valutare la quantità di spazio di archiviazione disponibile per l'intera rete e per ciascun data center.
 - a. Selezionare **Dashboard > Panoramica**.
 - b. Prendere nota dei valori nelle schede Ripartizione utilizzo spazio dati e Ripartizione utilizzo spazio metadati consentito. Ogni scheda elenca la percentuale di utilizzo dello spazio di archiviazione, la capacità dello spazio utilizzato e lo spazio totale disponibile o consentito dal sito.



Il riassunto non include supporti d'archivio.

Data space usage breakdown ?

1.97 MB (0%) of 3.09 TB used overall

Site name	Data storage usage	Used space	Total space
Data Center 3	0%	621.26 KB	926.62 GB
Data Center 1	0%	798.16 KB	1.24 TB
Data Center 2	0%	552.10 KB	926.62 GB

Metadata allowed space usage breakdown ?

2.44 MB (0%) of 19.32 GB used in Data Center 3

Data Center 3 has the highest metadata space usage and it determines the metadata space available in the grid.

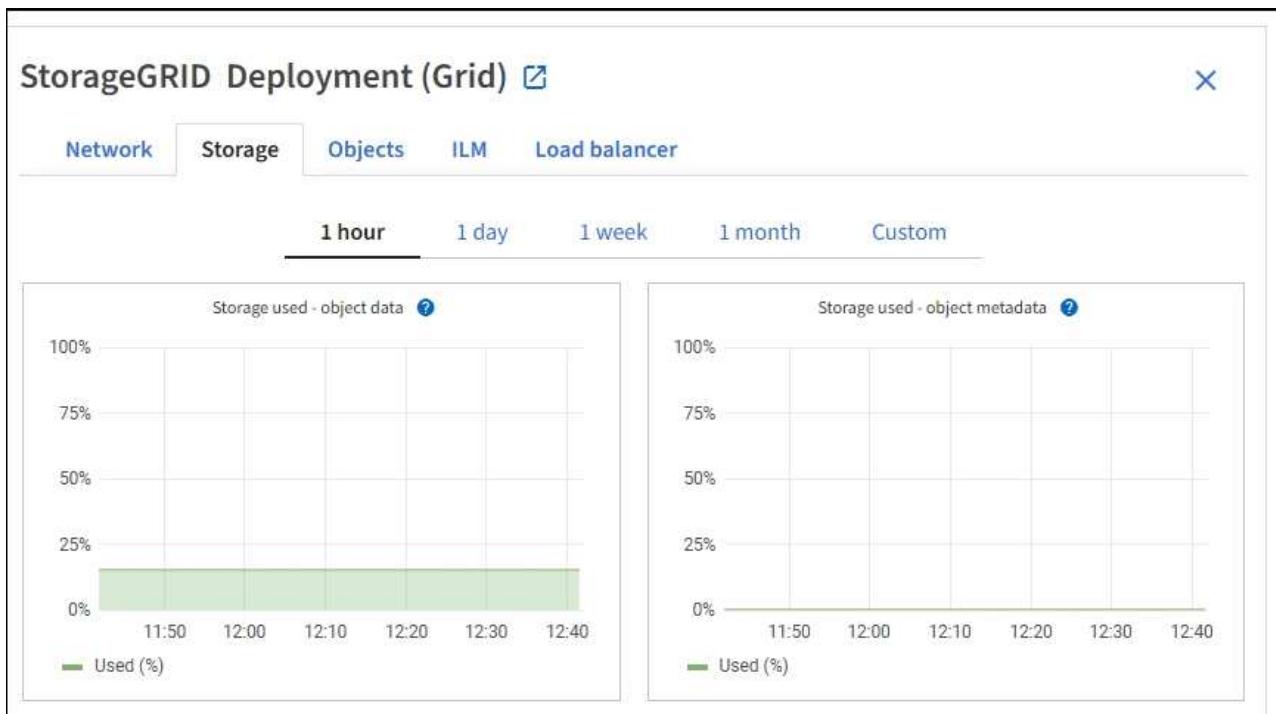
Site name	Metadata space usage	Metadata used space	Metadata allowed space
Data Center 3	0%	2.44 MB	19.32 GB

- a. Notare il grafico sulla scheda Conservazione nel tempo. Utilizza il menu a discesa del periodo di tempo per determinare la rapidità con cui viene consumato lo spazio di archiviazione.



2. Utilizzare la pagina Nodi per ulteriori dettagli sulla quantità di spazio di archiviazione utilizzata e su quanto spazio di archiviazione rimane disponibile sulla griglia per i dati degli oggetti e i metadati degli oggetti.

- Selezionare **NODES**.
- Selezionare **grid > Archiviazione**.



- c. Posiziona il cursore sui grafici **Spazio di archiviazione utilizzato - dati oggetto** e **Spazio di archiviazione utilizzato - metadati oggetto** per vedere quanto spazio di archiviazione oggetto e spazio di archiviazione metadati oggetto è disponibile per l'intera griglia e quanto è stato utilizzato nel tempo.



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

3. Pianificare l'esecuzione di un'espansione per aggiungere nodi di archiviazione o volumi di archiviazione prima che la capacità di archiviazione utilizzabile della griglia venga esaurita.

Quando si pianifica la tempistica di un'espansione, bisogna considerare quanto tempo ci vorrà per procurarsi e installare ulteriore spazio di archiviazione.



Se la policy ILM utilizza la codifica di cancellazione, potrebbe essere preferibile espandere quando i nodi di archiviazione esistenti sono pieni al 70% circa, per ridurre il numero di nodi da aggiungere.

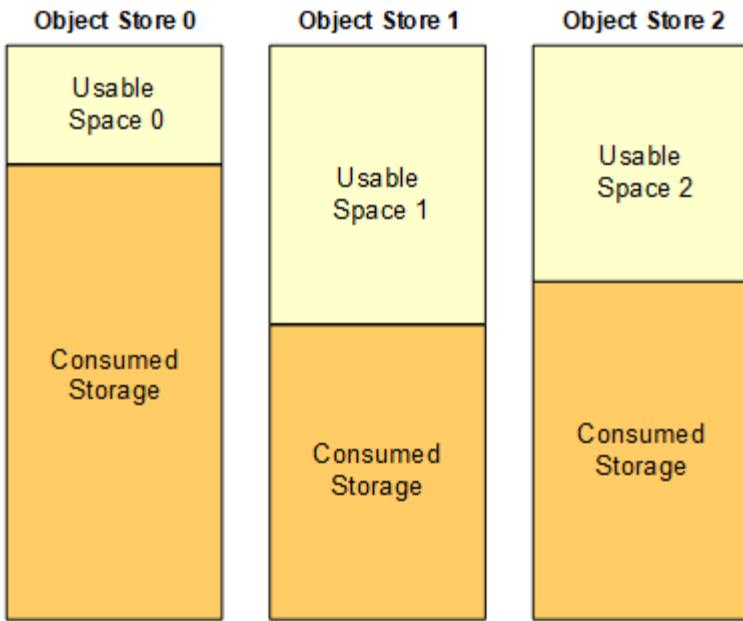
Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, vedere "[istruzioni per espandere StorageGRID](#)" .

Monitorare la capacità di archiviazione per ogni nodo di archiviazione

Monitorare lo spazio totale utilizzabile per ciascun nodo di archiviazione per garantire che il nodo disponga di spazio sufficiente per i nuovi dati degli oggetti.

Informazioni su questo compito

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



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

Passi

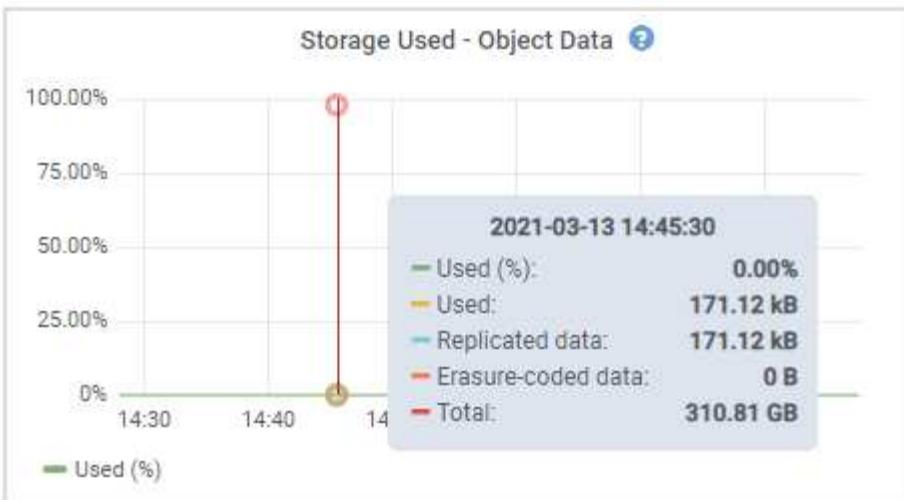
1. Selezionare **NODI > Nodo di archiviazione > Archiviazione**.

Vengono visualizzati i grafici e le tabelle per il nodo.

2. Posiziona il cursore sul grafico dei dati dell'oggetto Spazio di archiviazione utilizzato.

Vengono mostrati i seguenti valori:

- **Utilizzato (%)**: la percentuale dello spazio utilizzabile totale che è stata utilizzata per i dati dell'oggetto.
- **Utilizzato**: quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
- **Dati replicati**: una stima della quantità di dati di oggetti replicati su questo nodo, sito o griglia.
- **Dati con codice di cancellazione**: una stima della quantità di dati di oggetti con codice di cancellazione su questo nodo, sito o griglia.
- **Totale**: quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è il `storagegrid_storage_utilization_data_bytes` metrica.



3. Esaminare i valori disponibili nelle tabelle Volumi e Archivi 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 la velocità con cui viene consumato lo spazio di archiviazione utilizzabile.
- Per mantenere il normale funzionamento del sistema, aggiungere nodi di archiviazione, aggiungere volumi di archiviazione o archiviare i dati degli oggetti prima che lo spazio utilizzabile venga consumato.

Quando si pianifica la tempistica di un'espansione, bisogna considerare quanto tempo ci vorrà per procurarsi e installare ulteriore spazio di archiviazione.



Se la policy ILM utilizza la codifica di cancellazione, potrebbe essere preferibile espandere quando i nodi di archiviazione esistenti sono pieni al 70% circa, per ridurre il numero di nodi da aggiungere.

Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, vedere ["Istruzioni per](#)

[espandere StorageGRID](#)" .

IL "Bassa capacità di archiviazione dei dati degli oggetti" L'avviso viene attivato quando non rimane spazio sufficiente per archiviare i dati degli oggetti su un nodo di archiviazione.

Monitorare la capacità dei metadati degli oggetti per ogni nodo di archiviazione

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

Informazioni su questo compito

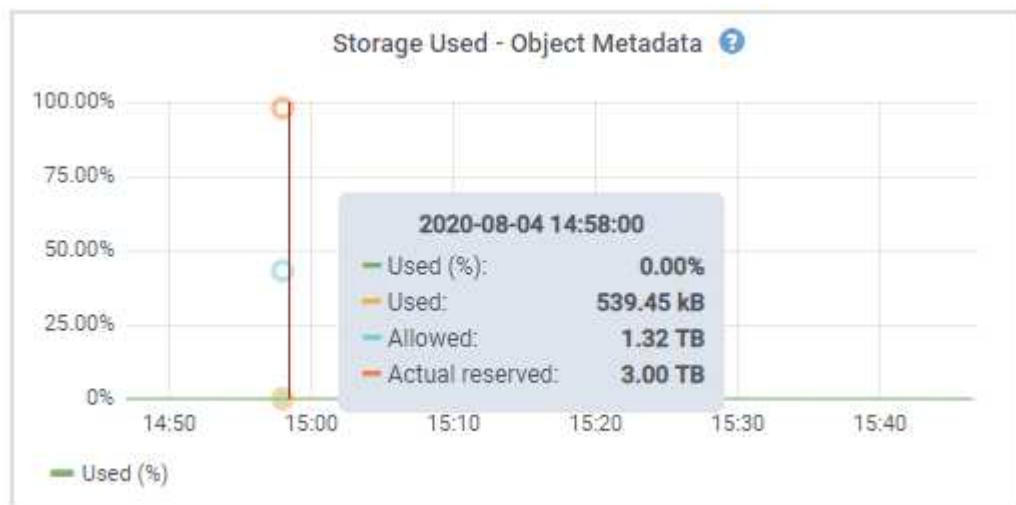
StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di archiviazione in ciascun sito, utilizzando lo spazio riservato ai metadati sul volume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

In alcuni casi, la capacità dei metadati degli oggetti della griglia potrebbe essere consumata più velocemente della sua capacità di archiviazione degli oggetti. Ad esempio, se in genere si acquisiscono grandi quantità di piccoli oggetti, potrebbe essere necessario aggiungere nodi di archiviazione per aumentare la capacità dei metadati, anche se rimane una capacità di archiviazione degli oggetti sufficiente.

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

Passi

1. Selezionare **NODI > Nodo di archiviazione > Archiviazione**.
2. Posiziona il cursore sul grafico dei metadati dell'oggetto Spazio di archiviazione utilizzato per visualizzare i valori per un periodo di tempo specifico.



Usato (%)

Percentuale dello spazio metadati consentito che è stato utilizzato su questo nodo di archiviazione.

Metriche di Prometheus: `storagegrid_storage_utilization_metadata_bytes` E `storagegrid_storage_utilization_metadata_allowed_bytes`

Usato

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

Metrica di Prometeo: storagegrid_storage_utilization_metadata_bytes

Consentito

Lo spazio consentito per i metadati degli oggetti su questo nodo di archiviazione. Per sapere come viene determinato questo valore per ogni nodo di archiviazione, vedere "[descrizione completa dello spazio metadati consentito](#)".

Metrica di Prometeo: storagegrid_storage_utilization_metadata_allowed_bytes

Effettivo riservato

Lo spazio effettivamente riservato ai metadati su questo nodo di archiviazione. Include lo spazio consentito e lo spazio richiesto per le operazioni essenziali sui metadati. Per sapere come viene calcolato questo valore per ogni nodo di archiviazione, vedere "[descrizione completa dello spazio effettivamente riservato per i metadati](#)".

La metrica Prometheus verrà aggiunta in una versione futura.



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

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



L'avviso **Archiviazione metadati insufficiente** viene attivato quando il valore **Utilizzato (%)** raggiunge determinate soglie. Se i metadati degli oggetti utilizzano più del 100% dello spazio consentito, si possono verificare risultati indesiderati.

Quando si aggiungono nuovi nodi, il sistema ribilancia automaticamente i metadati degli oggetti su tutti i nodi di archiviazione all'interno del sito. Vedi il "[istruzioni per espandere un sistema StorageGRID](#)".

Monitorare le previsioni di utilizzo dello spazio

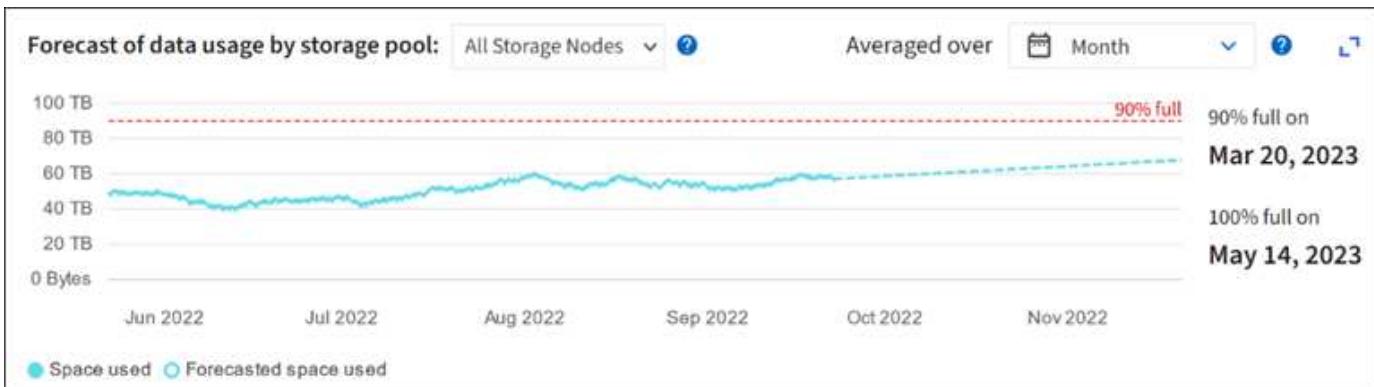
Monitorare le previsioni di utilizzo dello spazio per i dati utente e i metadati per stimare quando sarà necessario "[espandere una griglia](#)".

Se noti che il tasso di consumo cambia nel tempo, seleziona un intervallo più breve dal menu a discesa **Media su** per riflettere solo i modelli di consumo più recenti. Se noti modelli stagionali, seleziona 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.

Passi

1. Nella dashboard, seleziona **Archiviazione**.
2. Visualizza le schede della dashboard, Previsione dell'utilizzo dei dati per pool di archiviazione e Previsione dell'utilizzo dei metadati per sito.
3. Utilizzare questi valori per stimare quando sarà necessario aggiungere nuovi nodi di archiviazione per l'archiviazione di dati e metadati.



Monitorare la gestione del ciclo di vita delle informazioni

Il sistema di gestione del ciclo di vita delle informazioni (ILM) garantisce la gestione dei dati per tutti gli oggetti memorizzati nella griglia. È necessario monitorare le operazioni ILM per capire se la rete è in grado di gestire il carico attuale o se sono necessarie più risorse.

Informazioni su questo compito

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

L'acquisizione di oggetti e altre attività correlate agli oggetti possono superare la velocità con cui StorageGRID può valutare ILM, facendo sì che il sistema metta in coda oggetti le cui istruzioni di posizionamento ILM non possono essere soddisfatte quasi in tempo reale. È necessario monitorare se StorageGRID sta tenendo il passo con le azioni del client.

Utilizzare la scheda dashboard di Grid Manager

Passi

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

1. Sign in a Grid Manager.
2. Dalla dashboard, seleziona la scheda ILM e prendi nota dei valori nella scheda Coda ILM (Oggetti) e nella scheda Velocità di valutazione ILM.

Sono previsti picchi temporanei nella scheda Coda ILM (Oggetti) sulla dashboard. Ma se la coda continua ad aumentare e non diminuisce mai, la griglia ha bisogno di più risorse per funzionare in modo efficiente: più nodi di archiviazione oppure, se la politica ILM colloca gli oggetti in posizioni remote, più larghezza di banda di rete.

Utilizzare la pagina NODI

Passi

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



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

1. Selezionare **NODES**.
2. Selezionare **nome griglia > ILM**.
3. Posiziona il cursore sul grafico della coda ILM per visualizzare il valore dei seguenti attributi in un dato momento:
 - **Oggetti in coda (da operazioni client)**: numero totale di oggetti in attesa di valutazione ILM a causa di operazioni client (ad esempio, acquisizione).
 - **Oggetti in coda (da tutte le operazioni)**: numero totale di oggetti in attesa di valutazione ILM.
 - **Frequenza di scansione (oggetti/sec)**: la velocità con cui gli oggetti nella griglia vengono scansionati e messi in coda per ILM.
 - **Frequenza di valutazione (oggetti/sec)**: la frequenza attuale con cui gli oggetti vengono valutati in base alla policy ILM nella griglia.
4. Nella sezione Coda ILM, osservare i seguenti attributi.



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

- **Periodo di scansione - stimato**: tempo stimato per completare una scansione ILM completa di tutti gli oggetti.



Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti.

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



La riparazione dello stesso oggetto potrebbe incrementarsi nuovamente se la replica fallisce dopo la riparazione.

Questi attributi possono essere utili quando si monitora l'avanzamento del ripristino del volume del nodo di archiviazione. Se il numero di tentativi di riparazione ha smesso di aumentare ed è stata completata una scansione completa, è probabile che la riparazione sia 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 della griglia, sono fondamentali per l'efficienza delle operazioni.

Monitorare le connessioni e le prestazioni di rete

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

Utilizza Grid Manager per monitorare la connettività e le prestazioni della rete, in modo da poter risolvere

tempestivamente eventuali problemi.

Inoltre, considera "creazione di policy di classificazione del traffico di rete" in modo da poter monitorare il traffico correlato a tenant, bucket, subnet o endpoint del bilanciatore del carico specifici. È possibile impostare criteri di limitazione del traffico in base alle proprie esigenze.

Passi

1. Selezionare NODES.

Viene visualizzata la pagina Nodi. Ogni nodo nella griglia è elencato in formato tabella.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

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

Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo per la griglia nel suo complesso, per il sito del data center o per il nodo.



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

Network interfaces

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 **Comunicazione di rete** della pagina.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati su 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 tue policy di classificazione del traffico per monitorare il traffico di rete.

- a. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina 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.

Traffic Classification Policies			
Actions		Metrics	
Name	Description	ID	
ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574	
Fabric Pools	Monitor Fabric Pools	223b0ccb-6968-4646-b32d-7665bddc894b	

Displaying 2 traffic classification policies.

- a. Per visualizzare i grafici che mostrano le metriche di rete associate a una policy, selezionare il pulsante di opzione a sinistra della policy, quindi fare clic su **Metriche**.

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

Se una policy di classificazione del traffico è progettata per limitare il traffico di rete, analizza la

frequenza con cui il traffico viene limitato e decidi se la policy continua a soddisfare le tue esigenze. Di tanto in tanto, "adattare ogni politica di classificazione del traffico secondo necessità".

Informazioni correlate

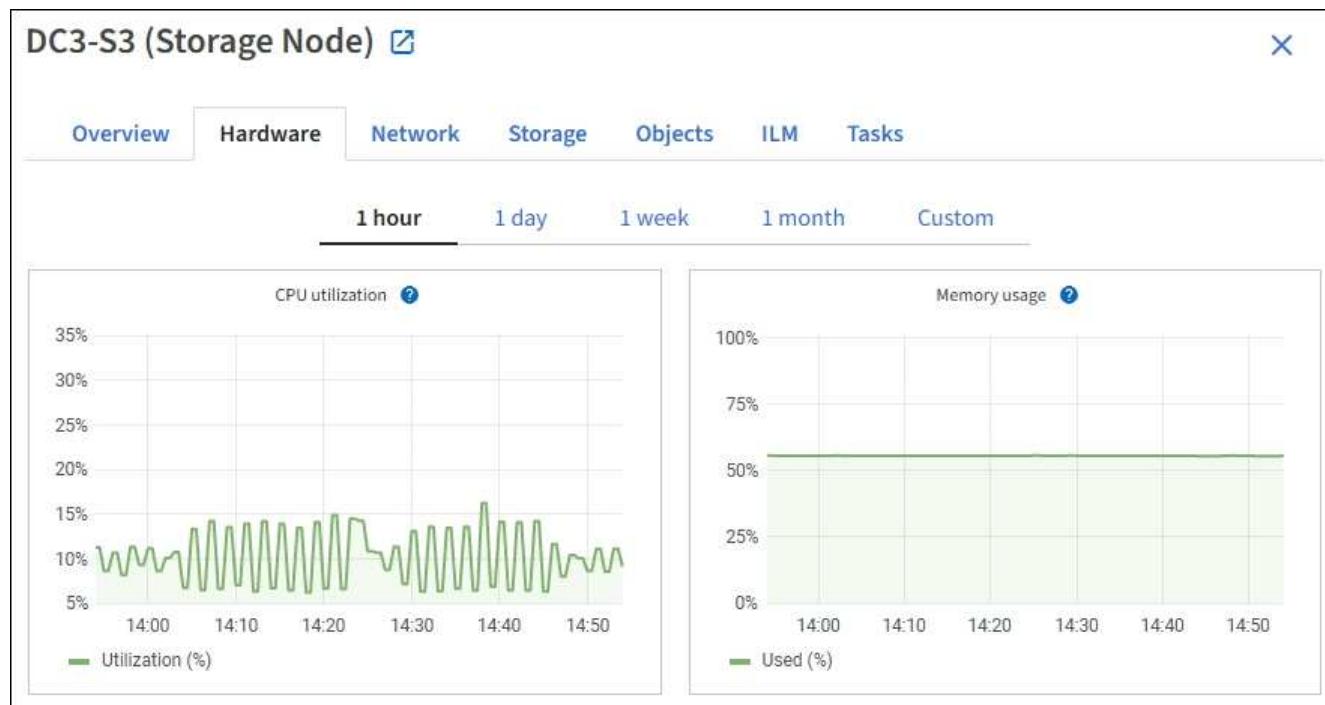
- "[Visualizza la scheda Rete](#)"
- "[Monitorare gli stati di connessione dei nodi](#)"

Monitorare le risorse a livello di nodo

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

Passi

1. Dalla pagina **NODI**, seleziona il nodo.
2. Selezionare la scheda **Hardware** per visualizzare i grafici dell'utilizzo della CPU e della memoria.



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

Informazioni correlate

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

Monitorare l'attività degli inquilini

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

possibile utilizzare Grid Manager per monitorare l'utilizzo dello storage o il traffico di rete per tutti i tenant o per un tenant specifico. È possibile utilizzare il registro di controllo o le dashboard di Grafana per raccogliere informazioni più dettagliate su come i tenant utilizzano StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Accesso root o autorizzazione account tenant](#)" .

Visualizza tutti gli inquilini

La pagina Inquilini mostra le informazioni di base per tutti gli account degli inquilini attuali.

Passi

1. Selezionare **INQUILINI**.
2. Esaminare le informazioni mostrate nelle pagine dedicate agli inquilini.

Per ogni tenant vengono elencati lo spazio logico utilizzato, l'utilizzo della quota, la quota e il conteggio degli oggetti. Se non è impostata una quota per un tenant, i campi Utilizzo quota e Quota contengono un trattino (—).



I valori dello spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo.

Tenants						
View information for each tenant account. Depending on the timing of ingest, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.						
	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%;">10%</div>	20.00 GB	100	
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%;">85%</div>	100.00 GB	500	
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%;">50%</div>	1.00 PB	10,000	
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%;">95%</div>	500.00 TB	50,000	
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	

3. Facoltativamente, accedi a un account tenant selezionando il collegamento di accesso nella colonna * Sign in/Copia URL*.
4. Facoltativamente, copia l'URL della pagina di accesso di un tenant selezionando il collegamento Copia URL nella colonna * Sign in/Copia URL*.
5. Facoltativamente, seleziona **Esporta in CSV** per visualizzare ed esportare un .csv file contenente i valori di utilizzo per tutti gli inquilini.

Ti verrà chiesto di aprire o salvare il .csv file.

Il contenuto del .csv il file appare come nell'esempio seguente:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	47500000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	50000000000	Infinity		500	S3

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

6. Se non è elencato alcun oggetto, facoltativamente, selezionare **Azioni > Elimina** per rimuovere uno o più tenant. Vedere "[Elimina account inquilino](#)".

Non è possibile rimuovere un account tenant se l'account include bucket o contenitori.

Visualizza un inquilino specifico

È possibile visualizzare i dettagli di un inquilino specifico.

Passi

1. Selezionare il nome dell'inquilino dalla pagina Inquilini.

Viene visualizzata la pagina dei dettagli dell'inquilino.

Tenant 02

Tenant ID: 4103 1879 2208 5551 2180 [Edit](#) 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%).

Bucket	Space used (GB)	Object count
bucket-01	40.00	250
bucket-02	30.00	200
bucket-03	15.00	50

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. Consulta la panoramica degli inquilini nella parte superiore della pagina.

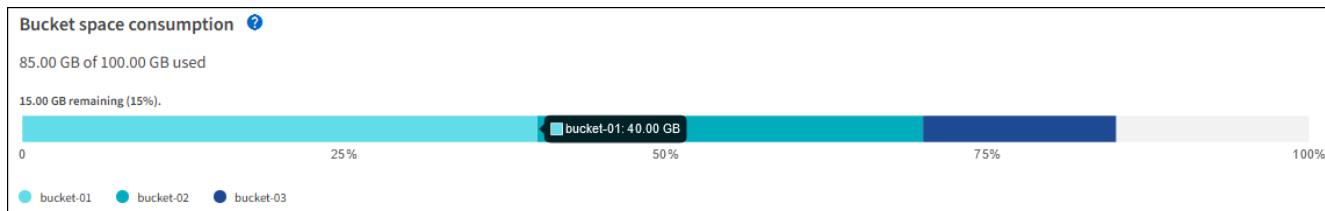
Questa sezione della pagina dei dettagli fornisce informazioni riepilogative per il tenant, tra cui il conteggio degli oggetti del tenant, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

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

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

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

È possibile posizionare il cursore sul grafico a barre per visualizzare lo spazio di archiviazione utilizzato da ciascun bucket o contenitore. È possibile posizionare il cursore sul segmento di spazio libero per visualizzare la quota di archiviazione 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 inizia a caricare oggetti e rifiuta nuovi ingest 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 finché non viene ricalcolato l'utilizzo della quota. I calcoli dell'utilizzo delle quote possono richiedere 10 minuti o più.



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



È possibile abilitare la regola di avviso **Utilizzo elevato della quota tenant** per determinare se i tenant stanno consumando le loro quote. Se abilitato, questo avviso viene attivato quando un tenant ha utilizzato il 90% della sua quota. Per le istruzioni, vedere "[Modifica le regole di avviso](#)".

4. Dalla scheda **Ripartizione dello spazio**, rivedere i **Dettagli del bucket**.

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

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

Il contenuto di un singolo tenant S3 .csv il file appare come nell'esempio seguente:

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

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

- Facoltativamente, seleziona la scheda **Funzionalità consentite** per visualizzare un elenco delle autorizzazioni e delle funzionalità abilitate per il tenant. Vedere "[Modifica account inquilino](#)" se è necessario modificare una di queste impostazioni.
- Se il tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, selezionare facoltativamente la scheda **Federazione griglia** per saperne di più sulla connessione.

Vedere "[Che cos'è la federazione di rete?](#)" E "[Gestire gli inquilini autorizzati per la federazione della rete](#)".

Visualizza il traffico di rete

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

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti sono elencati nella tabella.

2. Esaminare l'elenco delle policy per identificare quelle che si applicano a un inquilino specifico.
3. Per visualizzare le metriche associate a una policy, selezionare il pulsante di opzione a sinistra della policy e selezionare **Metriche**.
4. Analizza i grafici per determinare la frequenza con cui la policy limita il traffico e se è necessario modificarla.

Vedere "[Gestire le policy di classificazione del traffico](#)" per maggiori informazioni.

Utilizzare il registro di controllo

Facoltativamente, è possibile utilizzare il registro di controllo per un monitoraggio più dettagliato 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 client

I registri di controllo vengono scritti in file di testo che è possibile analizzare utilizzando lo strumento di analisi dei registri scelto. Ciò consente di comprendere meglio le attività dei clienti o di implementare modelli sofisticati di addebito e fatturazione.

Vedere "[Esaminare i registri di controllo](#)" per maggiori informazioni.

Utilizzare le metriche di Prometheus

Facoltativamente, utilizzare le metriche di Prometheus per generare report sull'attività dei tenant.

- Nel Grid Manager, seleziona **SUPPORTO > Strumenti > Metriche**. È possibile utilizzare dashboard esistenti, come S3 Overview, per esaminare le attività dei clienti.



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

- Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**. È possibile utilizzare le metriche nella sezione Metriche dell'API di gestione della griglia per creare regole di avviso e dashboard personalizzate per l'attività dei tenant.

Vedere "[Esaminare le metriche di supporto](#)" per maggiori informazioni.

Monitorare le operazioni del client S3

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

Prima di iniziare

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

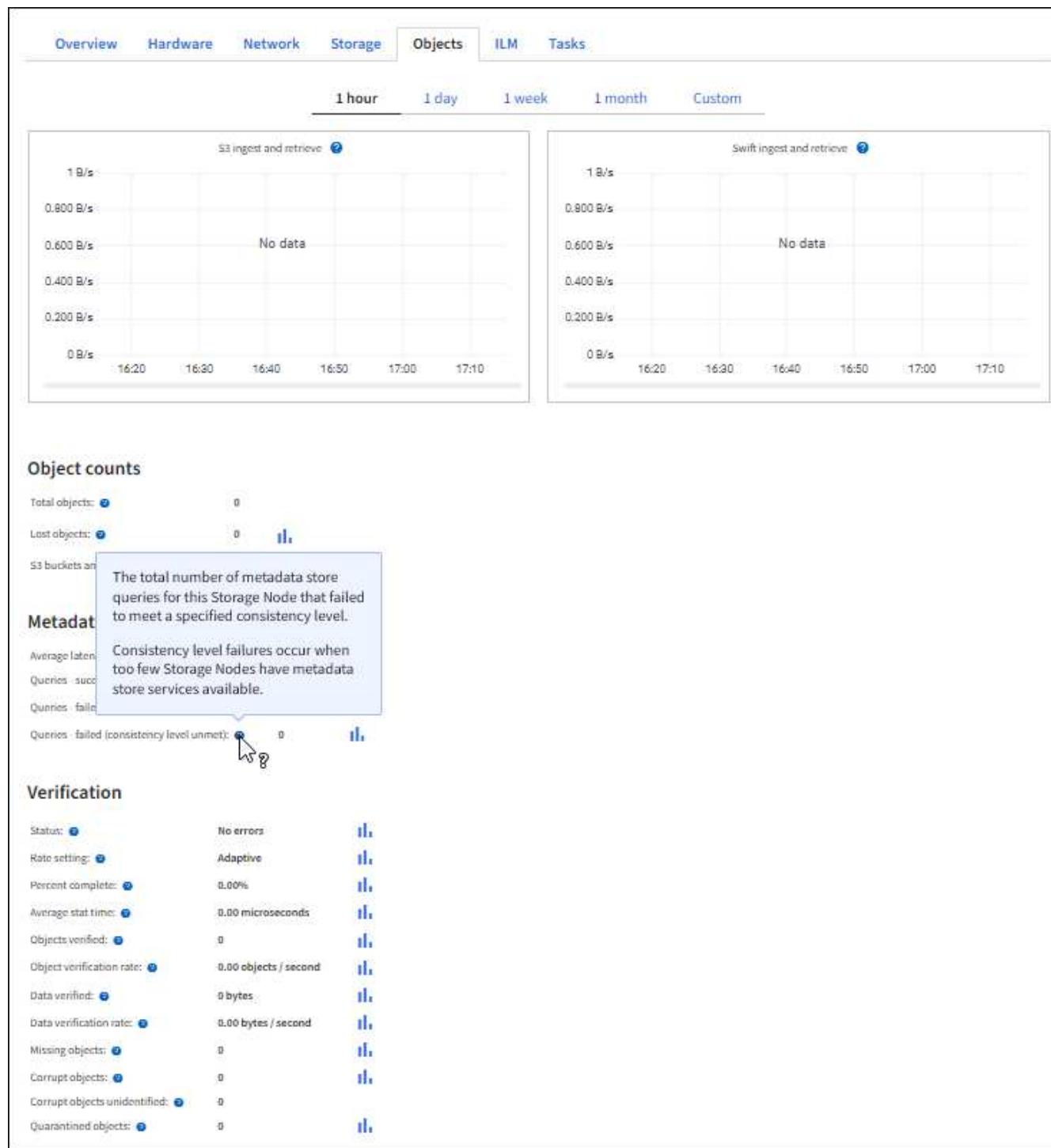
Passi

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

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

5. Per visualizzare le informazioni relative a un particolare nodo di archiviazione, seleziona il nodo dall'elenco a sinistra e seleziona la scheda **Oggetti**.

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



Monitorare le operazioni di bilanciamento del carico

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

Informazioni su questo compito

È possibile utilizzare il servizio Load Balancer sui nodi amministrativi o sui nodi gateway oppure un bilanciatore del carico esterno di terze parti per distribuire le richieste client su più nodi di archiviazione.

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

Se è stato configurato un gruppo ad alta disponibilità (HA) di nodi gateway o nodi amministrativi in modalità di backup attivo, solo un nodo nel gruppo distribuisce attivamente le richieste client.

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

Passi

1. Se i client S3 si connettono tramite il servizio Load Balancer, verificare che i nodi amministrativi o i nodi gateway distribuiscano attivamente il traffico come previsto:

- a. Selezionare **NODES**.
- b. Selezionare un nodo gateway o un nodo amministrativo.
- c. Nella scheda **Panoramica**, verificare se un'interfaccia nodo si trova in un gruppo HA e se l'interfaccia 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 dovrebbe distribuire attivamente le richieste dei client, selezionare "[Scheda Bilanciatore del carico](#)" .
- e. Esaminare il grafico del traffico delle richieste del Load Balancer dell'ultima settimana per assicurarsi che il nodo abbia distribuito attivamente le richieste.

I nodi in 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 della frequenza delle richieste in arrivo del Load Balancer dell'ultima settimana per esaminare la produttività degli oggetti del nodo.
 - g. Ripetere questi passaggi per ogni nodo amministrativo o nodo gateway nel sistema StorageGRID .
 - h. Facoltativamente, utilizzare i criteri di classificazione del traffico per visualizzare un'analisi più dettagliata del traffico servito dal servizio Load Balancer.
2. Verificare che queste richieste vengano distribuite uniformemente tra i nodi di archiviazione.

- a. Selezionare **Nodo di archiviazione > LDR > HTTP**.
- b. Esaminare il numero di **Sessioni in arrivo attualmente stabilite**.
- c. Ripetere l'operazione per ogni nodo di archiviazione nella griglia.

Il numero di sessioni dovrebbe essere più o meno uguale su tutti i nodi di archiviazione.

Monitorare le connessioni della federazione di rete

È possibile monitorare le informazioni di base su tutti "[connessioni della federazione di rete](#)", informazioni dettagliate su una connessione specifica o metriche Prometheus sulle operazioni di replicazione tra griglie. È possibile monitorare una connessione da entrambe le griglie.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su entrambe le griglie utilizzando un "browser web supportato".
- Tu hai il "[Permesso di accesso root](#)" per la griglia a cui hai effettuato l'accesso.

Visualizza tutte le connessioni

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

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.

Viene visualizzata la pagina Federazione Grid.

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

Da questa scheda puoi:

- "[Crea una nuova connessione](#)" .
- Seleziona una connessione esistente a "[modificare o testare](#)" .

The screenshot shows the 'Grid federation' page. At the top, there's a link to 'Learn more about grid federation'. Below that, a message states: '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.' There are two tabs at the top: 'Connections' (which is selected) and 'Permitted tenants'. Below the tabs are buttons for 'Add connection', 'Upload verification file', 'Actions', and a search bar. To the right, it says 'Displaying 1 connection'. A table lists one connection: 'Grid 1 - Grid 2' with 'Remote hostname' 10.96.130.76 and 'Connection status' as 'Connected' with a green checkmark.

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

Da questa scheda puoi:

- "[Visualizza la pagina dei dettagli per ogni inquilino autorizzato](#)" .
- Visualizza la pagina dei dettagli per ogni connessione. Vedere [Visualizza una connessione specifica](#) .
- Selezionare un inquilino autorizzato e "[rimuovere il permesso](#)" .
- Verificare la presenza di errori di replicazione tra griglie e cancellare l'ultimo errore, se presente. Vedere "[Risolvere gli 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.

The screenshot shows a user interface for managing grid federation connections. At the top, there are two tabs: 'Connections' and 'Permitted tenants'. The 'Permitted tenants' tab is currently selected and highlighted in yellow. Below the tabs is a row of buttons: 'Remove permission', 'Clear error', 'Search...', and a magnifying glass icon. To the right of the search bar, it says 'Displaying one result'. Underneath these are several filter dropdowns: 'Tenant name', 'Connection name', 'Connection status', 'Remote grid hostname', and 'Last error'. The main content area shows a single row of data: 'Tenant A' (with a blue circular icon), 'Grid 1 - Grid 2' (with a green checkmark icon), 'Connected' (with a green checkmark icon), '10.96.130.76', and a 'Check for errors' link.

Visualizza una connessione specifica

È possibile visualizzare i dettagli di una specifica connessione di federazione di rete.

Passi

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

Dalla pagina dei dettagli della connessione, puoi:

- Visualizza le informazioni di base sullo stato della connessione, inclusi i nomi host locali e remoti, la porta e lo stato della connessione.
- Seleziona una connessione a "[modificare, testare o rimuovere](#)" .

2. Quando si visualizza una connessione specifica, selezionare la scheda **Tenant consentiti** per visualizzare i dettagli sui tenant consentiti per la connessione.

Da questa scheda puoi:

- "[Visualizza la pagina dei dettagli per ogni inquilino autorizzato](#)" .
- "[Rimuovere l'autorizzazione di un inquilino](#)" per utilizzare la connessione.
- Verificare la presenza di errori di replicazione tra griglie e cancellare l'ultimo errore. Vedere "[Risolvere gli 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](#)

Search...



Displaying one result.

Tenant name 

Last error 



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 puoi:

- "Ruota i certificati di connessione".
- Selezionare **Server** o **Client** per visualizzare o scaricare il certificato associato o copiare il certificato PEM.

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-----  
MIIGdTCCBF2gAwIBAgIIMIG3a6yhgowDQYJKoZIhvvcNAQENBQAwdzELMAkGA1UE  
BhMCVVMxExARBgNVBAgIMkNhbg1mb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEU  
MRQFU15Ca1tV0o...Y4...A7...NVBAsMEk1dEF...CBX...Ag...Wd1R1...  
-----END CERTIFICATE-----
```

Esaminare le metriche di replicazione tra griglie

È possibile utilizzare la dashboard Cross-Grid Replication in Grafana per visualizzare le metriche di Prometheus sulle operazioni di replica cross-grid sulla propria griglia.

Passi

1. Da Grid Manager, seleziona **SUPPORTO > Strumenti > Metriche**.



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

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

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

3. Per riprovare la replica degli oggetti che non sono riusciti a replicare, vedere "Identificare e riprovare le operazioni di replicazione non riuscite".

Gestisci gli avvisi

Gestisci gli avvisi

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

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

- Un'icona di gravità dell'avviso viene visualizzata sulla dashboard di Grid Manager e il conteggio degli avvisi correnti viene incrementato.
- L'avviso viene visualizzato nella pagina di riepilogo **NODES** e nella scheda **NODES > node > Panoramica**.
- Verrà inviata una notifica via e-mail, presupponendo che sia stato configurato un server SMTP e siano stati forniti gli indirizzi e-mail dei destinatari.
- Viene inviata una notifica SNMP (Simple Network Management Protocol), presupponendo che sia stato configurato l'agente SNMP StorageGRID .

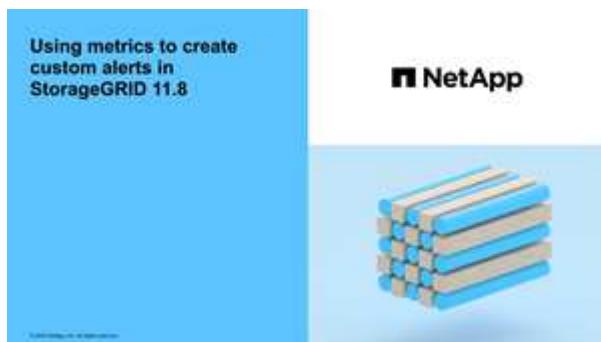
È possibile creare avvisi personalizzati, modificare o disattivare gli avvisi e gestire le notifiche degli avvisi.

Per saperne di più:

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



- Rivedi il video: "[Video: avvisi personalizzati](#)"



- Vedi il "[Riferimento avvisi](#)" .

Visualizza le regole di avviso

Le regole di avviso definiscono le condizioni che attivano "avvisi specifici". StorageGRID include un set di regole di avviso predefinite, che è possibile utilizzare così come sono 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 alcuni avvisi sono disabilitati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)".
- Facoltativamente, hai guardato il video: "[Video: Panoramica degli avvisi](#)"



Passi

1. Selezionare AVVISI > 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.

+ Create custom rule	Edit rule	Remove custom rule	Type	Status
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
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
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
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
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
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
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
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
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
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:

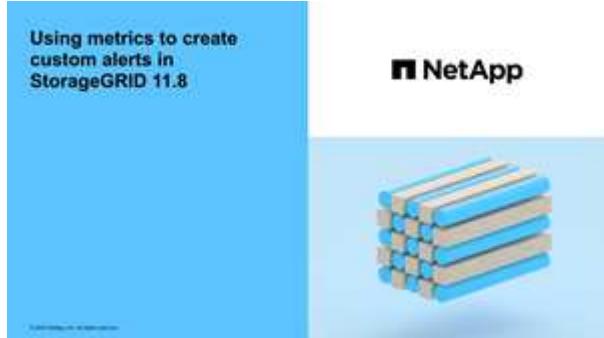
Intestazione di colonna	Descrizione
Nome	Nome e descrizione univoci della regola di avviso. Per prime vengono elencate le regole di avviso personalizzate, seguite dalle regole di avviso predefinite. Il nome della regola di avviso è l'oggetto delle notifiche e-mail.
Condizioni	<p>Le espressioni di Prometheus che determinano quando viene attivato questo avviso. Un avviso può essere attivato a uno o più dei seguenti livelli di gravità, ma non è richiesta una condizione per ciascun livello di gravità.</p> <ul style="list-style-type: none"> • *Critico*  : Si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID . Bisogna affrontare immediatamente il problema di fondo. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati. • *Maggiore*  : Esiste una condizione anomala che sta influenzando le operazioni in corso o che si sta avvicinando alla soglia di un avviso critico. È necessario esaminare gli avvisi principali e risolvere eventuali problemi sottostanti per garantire che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID . • *Minore*  : Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe compromettere la capacità del sistema di funzionare se continua così. È opportuno monitorare e risolvere gli avvisi minori che non si risolvono da soli, per evitare che diano origine a problemi più seri.
Tipo	<p>Tipo di regola di avviso:</p> <ul style="list-style-type: none"> • Predefinito: una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificarne le condizioni e la durata. Non è possibile rimuovere una regola di avviso predefinita. • Predefinito*: una regola di avviso predefinita che include una condizione o una durata modificata. Se necessario, è possibile ripristinare facilmente una condizione modificata riportandola al valore predefinito originale. • Personalizzato: una regola di avviso creata da te. È possibile disattivare, modificare e rimuovere le regole di avviso personalizzate.
Stato	Indica se questa regola di avviso è attualmente abilitata o disabilitata. Le condizioni per le regole di avviso disabilitate non vengono valutate, quindi non vengono attivati avvisi.

Crea regole di avviso personalizzate

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)" .
- Hai familiarità con il "[metriche Prometheus comunemente utilizzate](#)" .
- Tu capisci il "[sintassi delle query di Prometheus](#)" .
- Facoltativamente, hai guardato il video: "[Video: avvisi personalizzati](#)" .



Informazioni su questo compito

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

- Esamina le condizioni per le regole di avviso predefinite e usale come esempi per le tue 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 soglia per ogni condizione.
- Controllare attentamente ogni condizione per individuare eventuali errori di battitura e logici.
- Utilizzare solo le metriche elencate nell'API di gestione della griglia.
- Quando si testa un'espressione utilizzando l'API di gestione della griglia, tenere presente che una risposta "riuscita" potrebbe essere un corpo di risposta vuoto (nessun avviso attivato). Per verificare se l'avviso viene effettivamente attivato, puoi impostare temporaneamente una soglia su un valore che al momento ti aspetti sia vero.

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

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

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

2. Seleziona **Crea regola personalizzata**.

Viene visualizzata la finestra di dialogo 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 deselectare la casella di controllo **Abilitato** per determinare se questa regola di avviso è attualmente abilitata.

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

4. Inserisci le seguenti informazioni:

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi e costituisce anche l'oggetto delle notifiche e-mail. I nomi per le regole di avviso possono avere una lunghezza compresa tra 1 e 64 caratteri.

Campo	Descrizione
Descrizione	Una descrizione del problema che si sta verificando. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono contenere da 1 a 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Inserisci le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono avere una lunghezza compresa 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 solitamente della forma:

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

Le espressioni possono avere qualsiasi lunghezza, ma devono essere visualizzate su una singola riga nell'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 di byte (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

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

Il valore predefinito è 5 minuti.

7. Seleziona **Salva**.

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

Modifica le regole di avviso

È possibile modificare una regola di avviso per cambiare 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

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

- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)".

Informazioni su questo compito

Quando modifichi una regola di avviso predefinita, puoi cambiare le condizioni per gli avvisi minori, maggiori e critici, nonché la durata. Quando modifichi una regola di avviso personalizzata, puoi anche modificarne il nome, la descrizione e le azioni consigliate.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, è possibile che non venga rilevato un problema di fondo finché non si impedisce il completamento di un'operazione critica.

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

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

3. Seleziona **Modifica regola**.

Viene visualizzata la finestra di dialogo Modifica regola. Questo esempio mostra una regola di avviso predefinita: i campi Nome univoco, Descrizione e Azioni consigliate sono disabilitati e non possono essere modificati.

Edit Rule - Low installed node memory

Enabled	<input checked="" type="checkbox"/>
Unique Name	Low installed node memory
Description	The amount of installed memory on a node is low.
Recommended Actions (optional)	<p>Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.</p> <p>See the instructions for your platform:</p> <ul style="list-style-type: none">• VMware installation• Red Hat Enterprise Linux or CentOS installation• Ubuntu or Debian installation
Conditions ?	
Minor	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	node_memory_MemTotal_bytes <= 12000000000
Enter the amount of time a condition must continuously remain in effect before an alert is triggered.	
Duration	2 minutes ▾
Cancel Save	

4. Selezionare o deselectare la casella di controllo **Abilitato** per determinare se questa regola di avviso è attualmente abilitata.

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



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

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



Non è possibile 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 e costituisce anche l'oggetto delle notifiche e-mail. I nomi per le regole di avviso possono avere una lunghezza compresa tra 1 e 64 caratteri.
Descrizione	Una descrizione del problema che si sta verificando. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono contenere da 1 a 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Inserisci le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono avere una lunghezza compresa 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 una condizione per una regola di avviso predefinita modificata al suo valore originale, selezionare i tre punti a destra della condizione modificata.

Conditions

Minor	<input type="text"/>
Major	<input type="text"/> node_memory_MemTotal_bytes < 24000000000
Critical	<input type="text"/> node_memory_MemTotal_bytes <= 14000000000



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

Un'espressione di base è solitamente della forma:

[metric] [operator] [value]

Le espressioni possono avere qualsiasi lunghezza, ma devono essere visualizzate su una singola riga nell'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 di byte (24 GB).

node_memory_MemTotal_bytes < 24000000000

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

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

Il valore predefinito è 5 minuti.

8. Seleziona **Salva**.

Se hai modificato una regola di avviso predefinita, nella colonna **Tipo** verrà visualizzato **Predefinito***. Se hai disabilitato una regola di avviso predefinita o personalizzata, nella colonna **Stato** apparirà **Disabilitato**.

Disabilita le regole di avviso

È possibile modificare lo stato abilitato/disabilitato per una regola di avviso predefinita o personalizzata.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)" .

Informazioni su questo compito

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



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

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

2. Selezionare il pulsante di opzione per la regola di avviso che si desidera disabilitare o abilitare.

3. Seleziona **Modifica regola**.

Viene visualizzata la finestra di dialogo Modifica regola.

4. Selezionare o deselectrare la casella di controllo **Abilitato** per determinare se questa regola di avviso è attualmente abilitata.

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



Se 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. Seleziona **Salva**.

Nella colonna **Stato** appare **Disabilitato**.

Rimuovi regole di avviso personalizzate

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)" .

Passi

1. Selezionare **AVVISI > Regole**.

Viene visualizzata la pagina Regole di avviso.

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

Non è possibile rimuovere una regola di avviso predefinita.

3. Seleziona **Rimuovi regola personalizzata**.

Viene visualizzata una finestra di dialogo di conferma.

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

Eventuali istanze attive dell'avviso verranno risolte entro 10 minuti.

Gestisci le notifiche di avviso

Imposta le notifiche SNMP per gli avvisi

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

È possibile utilizzare l'opzione **CONFIGURAZIONE > Monitoraggio > Agente SNMP** in Grid Manager o gli endpoint SNMP per l'API di gestione della griglia per abilitare e configurare l'agente SNMP StorageGRID . L'agente SNMP supporta tutte e tre le versioni del protocollo SNMP.

Per informazioni su come configurare l'agente SNMP, vedere "[Utilizzare il monitoraggio SNMP](#)" .

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

- Le trappole sono notifiche inviate dall'agente SNMP che non richiedono la conferma da parte del sistema di gestione. Le trappole servono a notificare al sistema di gestione che si è verificato un evento all'interno StorageGRID, ad esempio l'attivazione di un avviso. Le trappole sono supportate in tutte e tre le versioni di SNMP.
- Le informazioni sono simili alle trappole, ma richiedono il riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un certo lasso di tempo, invia nuovamente l'informazione finché non riceve una conferma o finché non viene raggiunto il valore massimo di tentativi. Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche Trap and Inform vengono inviate quando viene attivato un avviso predefinito o personalizzato a

qualsiasi livello di gravità. Per sopprimere le notifiche SNMP per un avviso, è necessario configurare il silenzio per l'avviso. Vedere "[Disattiva le notifiche di avviso](#)" .

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

Imposta notifiche e-mail per gli avvisi

Se desideri che vengano inviate notifiche e-mail quando si verificano avvisi, devi fornire informazioni sul tuo server SMTP. È necessario immettere anche gli indirizzi e-mail dei destinatari delle notifiche di avviso.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)" .

Informazioni su questo compito

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

Passi

1. Selezionare **AVVISI > Configurazione e-mail**.

Viene visualizzata la pagina Configurazione e-mail.

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

Vengono visualizzate le sezioni Server di posta elettronica (SMTP), Transport Layer Security (TLS), Indirizzi di posta elettronica e Filtri.

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

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

Campo	Entra
Server di posta	Il nome di dominio completo (FQDN) o l'indirizzo IP del server SMTP.
Porta	La porta utilizzata per accedere al server SMTP. Deve essere compreso tra 1 e 65535.
Nome utente (facoltativo)	Se il server SMTP richiede l'autenticazione, inserisci il nome utente con cui effettuare l'autenticazione.

Campo	Entra
Password (facoltativa)	Se il server SMTP richiede l'autenticazione, immettere la password per l'autenticazione.

4. Nella sezione Indirizzi e-mail, inserisci gli indirizzi e-mail del mittente e di ciascun destinatario.
- Per **Indirizzo email del mittente**, specificare un indirizzo email valido da utilizzare come indirizzo del mittente per le notifiche di avviso.
Ad esempio: storagegrid-alerts@example.com
 - Nella sezione Destinatari, inserisci un indirizzo email per ogni elenco email o persona che deve ricevere un'email quando si verifica un avviso.
Selezione l'icona più+ per aggiungere destinatari.
5. Se per le comunicazioni con il server SMTP è richiesto Transport Layer Security (TLS), selezionare **Richiedi TLS** nella sezione Transport Layer Security (TLS).
- Nel campo **Certificato CA**, fornire il certificato CA che verrà utilizzato per verificare l'identità del server SMTP.
È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfoglia** e selezionare il file.
È necessario fornire un singolo file contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.
 - Seleziona la casella di controllo **Invia certificato client** se il tuo server di posta elettronica SMTP richiede ai mittenti di posta elettronica di fornire certificati client per l'autenticazione.
 - Nel campo **Certificato client**, fornire il certificato client codificato PEM da inviare al server SMTP.
È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfoglia** e selezionare il file.
 - Nel campo **Chiave privata**, immettere la chiave privata per il certificato client nella codifica PEM non crittografata.
È possibile copiare e incollare il contenuto in questo campo oppure selezionare **Sfoglia** e selezionare il file.
-  Se devi modificare la configurazione dell'email, seleziona l'icona della matita per aggiornare questo campo.
6. Nella sezione Filtri, seleziona i livelli di gravità degli avvisi che devono generare notifiche e-mail, a meno che la regola per un avviso specifico non sia stata disattivata.

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

Gravità	Descrizione
Maggiore, critico	Una notifica via e-mail viene inviata quando viene soddisfatta la condizione principale o critica per una regola di avviso. Le notifiche non vengono inviate per gli avvisi minori.
Solo critico	Una notifica via e-mail 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 sei pronto a testare le impostazioni della tua email, procedi come segue:

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

Viene visualizzato un messaggio di conferma che indica che è stata inviata un'e-mail di prova.

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



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

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



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

8. Seleziona **Salva**.

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

Le impostazioni e-mail vengono salvate.

Informazioni incluse nelle notifiche e-mail di avviso

Dopo aver configurato il server di posta elettronica 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 "[Disattiva le notifiche di avviso](#)" .

Le notifiche e-mail includono le seguenti informazioni:

Low object data storage (6 alerts) 1The 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

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

Come vengono raggruppati gli avvisi

Per evitare che venga inviato 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 esempi di come StorageGRID raggruppa più avvisi nelle notifiche e-mail.

Comportamento	Esempio
Ogni notifica di avviso si applica solo agli avvisi che hanno lo stesso nome. Se vengono attivati contemporaneamente due avvisi con nomi diversi, vengono inviate due notifiche e-mail.	<ul style="list-style-type: none"> L'avviso A viene attivato contemporaneamente su due nodi. Viene inviata una sola notifica. L'avviso A viene attivato sul nodo 1 e contemporaneamente l'avviso B viene attivato sul nodo 2. Vengono inviate due notifiche: una per ogni avviso.
Per un avviso specifico su un nodo specifico, se vengono raggiunte le soglie per più di una gravità, viene inviata una notifica solo per l'avviso più grave.	<ul style="list-style-type: none"> Viene attivato l'avviso A e vengono raggiunte le soglie di avviso minore, maggiore e critico. Per l'avviso critico viene inviata una notifica.
La prima volta che viene attivato un avviso, StorageGRID attende 2 minuti prima di inviare una notifica. Se durante tale periodo vengono attivati altri avvisi con lo stesso nome, StorageGRID raggruppa tutti gli avvisi nella notifica iniziale.	<ol style="list-style-type: none"> L'avviso A viene attivato sul nodo 1 alle 08:00. Non viene inviata alcuna notifica. L'avviso A viene attivato sul nodo 2 alle 08:01. Non viene inviata alcuna notifica. Alle 08:02 viene inviata una notifica per segnalare entrambe le istanze dell'avviso.
Se viene attivato un altro avviso con lo stesso nome, StorageGRID attende 10 minuti prima di inviare una nuova notifica. La nuova notifica segnala tutti gli avvisi attivi (avvisi correnti che non sono stati disattivati), anche se segnalati in precedenza.	<ol style="list-style-type: none"> L'avviso A viene attivato sul nodo 1 alle 08:00. Una notifica viene inviata alle 08:02. L'avviso A viene attivato sul nodo 2 alle 08:05. Una seconda notifica viene inviata alle 08:15 (10 minuti dopo). Entrambi i nodi sono segnalati.
Se sono presenti più avvisi correnti con lo stesso nome e uno di questi avvisi viene risolto, non verrà inviata una nuova notifica se l'avviso si ripresenta sul nodo per il quale è stato risolto.	<ol style="list-style-type: none"> L'avviso A viene attivato per il nodo 1. Viene inviata una notifica. L'avviso A viene attivato per il nodo 2. Viene inviata una seconda notifica. L'avviso A è stato risolto per il nodo 2, ma rimane attivo per il nodo 1. 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.
StorageGRID continua a inviare notifiche e-mail una volta ogni 7 giorni finché tutte le istanze dell'avviso non vengono risolte o la regola di avviso non viene disattivata.	<ol style="list-style-type: none"> L'avviso A viene attivato per il nodo 1 l'8 marzo. Viene inviata una notifica. L'avviso A non è stato risolto o silenziato. Ulteriori notifiche vengono inviate il 15 marzo, il 22 marzo, il 29 marzo e così via.

Risoluzione dei problemi relativi alle notifiche e-mail di avviso

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)" .

Passi

1. Verifica le tue impostazioni.
 - a. Selezionare **AVVISI > Configurazione e-mail**.
 - b. Verificare che le impostazioni del server di posta elettronica (SMTP) siano corrette.
 - c. Verifica di aver specificato indirizzi email validi per i destinatari.
2. Controlla il filtro antispam e assicurati che l'e-mail non sia stata inviata nella cartella posta indesiderata.
3. Chiedi all'amministratore della tua posta elettronica di confermare che le email provenienti dall'indirizzo del mittente non siano bloccate.
4. Raccogli un file di registro per il nodo di amministrazione, quindi contatta l'assistenza tecnica.

L'assistenza tecnica può utilizzare le informazioni contenute nei registri per determinare cosa è andato storto. Ad esempio, il file `prometheus.log` potrebbe mostrare un errore durante la connessione al server specificato.

Vedere "[Raccogli file di registro e dati di sistema](#)" .

Disattiva le notifiche di avviso

Facoltativamente, è possibile configurare dei silenzi per sopprimere temporaneamente le notifiche di avviso.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Gestisci avvisi o autorizzazione di accesso root](#)" .

Informazioni su questo compito

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

Se è stato abilitato l'agente SNMP, i silenziamenti sopprimono anche le trappole e le informazioni SNMP.



Prestare attenzione quando si decide di disattivare una regola di avviso. Se si disattiva un avviso, è possibile che non venga rilevato un problema di fondo finché non si impedisce il completamento di un'operazione critica.

Passi

1. Selezionare **AVVISI > Silenzi**.

Viene visualizzata la pagina Silenzi.

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.

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. Seleziona 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. Seleziona o inserisci le seguenti informazioni:

Campo	Descrizione
Regola di avviso	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 disabilitata. Nota: selezionare Tutte le regole se si desidera disattivare tutte le regole di avviso utilizzando i criteri specificati in questa finestra di dialogo.

Campo	Descrizione
Descrizione	Facoltativamente, una descrizione del silenzio. Descrivi, ad esempio, lo scopo di questo silenzio.
Durata	<p>Per quanto tempo desideri che questo silenzio rimanga in vigore, in minuti, ore o giorni. Il silenzio può avere una durata che va da 5 minuti a 1.825 giorni (5 anni).</p> <p>Nota: non dovresti disattivare una regola di avviso per un periodo di tempo prolungato. Se una regola di avviso viene disattivata, potresti non rilevare un problema di fondo finché non impedisce il completamento di un'operazione critica. Tuttavia, potrebbe essere necessario utilizzare un silenzio prolungato se un avviso viene attivato da una configurazione specifica e intenzionale, come potrebbe essere il caso degli avvisi Collegamento appliance servizi inattivo e degli avvisi Collegamento appliance di archiviazione inattivo.</p>
Gravità	Quale livello di gravità dell'avviso deve essere silenziato. Se l'avviso viene attivato a uno dei livelli di gravità selezionati, non vengono inviate notifiche.
Nodi	<p>A quale nodo o nodi vuoi che venga applicato questo silenzio. È possibile sopprimere una regola di avviso o tutte le regole sull'intera griglia, su un singolo sito o su un singolo nodo. Se si seleziona l'intera griglia, il silenzio si applica a tutti i siti e a tutti i nodi. Se si seleziona un sito, il silenzio si applica solo ai nodi di quel sito.</p> <p>Nota: non è possibile selezionare più di un nodo o più di un sito per ogni silenzio. È necessario creare silenzi aggiuntivi se si desidera sopprimere la stessa regola di avviso su più nodi o più siti contemporaneamente.</p>

4. Seleziona **Salva**.

5. Se vuoi modificare o terminare un silenzio prima che scada, puoi modificarlo o rimuoverlo.

Opzione	Descrizione
Modifica un silenzio	<ol style="list-style-type: none"> Selezionare AVVISI > Silenzi. Nella tabella, seleziona il pulsante di opzione relativo al silenzio che desideri modificare. Selezionare Modifica. Modifica la descrizione, il tempo rimanente, i livelli di gravità selezionati o il nodo interessato. Seleziona Salva.

Opzione	Descrizione
Rimuovere un silenzio	<p>a. Selezionare AVVISI > Silenzi.</p> <p>b. Nella tabella, seleziona il pulsante di opzione relativo al silenzio che desideri rimuovere.</p> <p>c. Seleziona 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 vengano sopprese da un altro silenzio). Se questo avviso è già attivato, potrebbero essere necessari alcuni minuti prima che le notifiche via e-mail o SNMP vengano inviate e che la pagina Avvisi venga aggiornata.</p>

Informazioni correlate

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

Riferimento avvisi

In questo riferimento sono elencati gli avvisi predefiniti visualizzati in Grid Manager. Le azioni consigliate sono riportate nel messaggio di avviso ricevuto.

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

Alcuni degli avvisi predefiniti utilizzano "[Metriche di Prometeo](#)" .

Avvisi sugli elettrodomestici

Nome dell'avviso	Descrizione
Batteria dell'apparecchio scaduta	La batteria nel controller di accumulo dell'apparecchio è scaduta.
Batteria dell'apparecchio guasta	La batteria nel controller di accumulo dell'apparecchio è guasta.
La batteria dell'apparecchio ha una capacità di apprendimento insufficiente	La batteria nel controller di accumulo dell'apparecchio non ha una capacità di apprendimento sufficiente.
Batteria dell'apparecchio prossima alla scadenza	La batteria nel controller di accumulo dell'apparecchio sta per esaurirsi.
Batteria dell'apparecchio rimossa	Manca la batteria nel controller di accumulo dell'apparecchio.
Batteria dell'apparecchio troppo calda	La batteria nel controller di accumulo dell'apparecchio è surriscaldata.

Nome dell'avviso	Descrizione
Errore di comunicazione BMC dell'apparecchio	La comunicazione con il controller di gestione della scheda madre (BMC) è stata interrotta.
Rilevato errore del dispositivo di avvio dell'appliance	È stato rilevato un problema con il dispositivo di avvio nell'appliance.
Errore del dispositivo di backup della cache dell'appliance	Un dispositivo di backup della cache persistente non è riuscito.
Capacità insufficiente del dispositivo di backup della cache dell'appliance	La capacità del dispositivo di backup della cache è insufficiente.
Dispositivo di backup della cache dell'appliance protetto da scrittura	Un dispositivo di backup della cache è protetto da scrittura.
Mancata corrispondenza delle dimensioni della memoria cache dell'appliance	I due controller nell'appliance hanno dimensioni di 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 elaborazione dell'appliance troppo alta	La temperatura del controller di elaborazione in un dispositivo StorageGRID ha superato una soglia nominale.
Temperatura della CPU del controller di elaborazione dell'appliance troppo alta	La temperatura della CPU nel controller di elaborazione di un dispositivo StorageGRID ha superato una soglia nominale.
Il controller di elaborazione dell'appliance necessita di attenzione	È stato rilevato un guasto hardware nel controller di elaborazione di un dispositivo StorageGRID .
L'alimentatore A del controller di elaborazione dell'apparecchio presenta un problema	L'alimentatore A nel controller di elaborazione presenta un problema.
L'alimentatore B del controller di elaborazione dell'apparecchio presenta un problema	L'alimentatore B nel controller di elaborazione presenta un problema.
Servizio di monitoraggio dell'hardware di elaborazione dell'appliance bloccato	Il servizio che monitora lo stato dell'hardware di archiviazione è bloccato.

Nome dell'avviso	Descrizione
L'unità DAS dell'appliance supera il limite di dati scritti al giorno	Ogni giorno viene scritta una quantità eccessiva di dati su un'unità, il che potrebbe invalidarne la garanzia.
Rilevato guasto dell'unità DAS dell'apparecchio	È stato rilevato un problema con un'unità di archiviazione collegata direttamente (DAS) nell'appliance.
Spia di localizzazione dell'unità DAS dell'apparecchio accesa	La spia di individuazione dell'unità per una o più unità di archiviazione collegate direttamente (DAS) in un nodo di archiviazione dell'appliance è accesa.
Ricostruzione dell'unità DAS dell'appliance	Un'unità di archiviazione collegata direttamente (DAS) è in fase di ricostruzione. Ciò è previsto se è stato sostituito o rimosso/reinserito di recente.
Rilevato guasto alla ventola dell'apparecchio	È stato rilevato un problema con un'unità ventola nell'apparecchio.
Rilevato guasto Fibre Channel dell'appliance	È stato rilevato un problema di collegamento Fibre Channel tra il controller di archiviazione dell'appliance e il controller di elaborazione
Errore della porta HBA Fibre Channel dell'appliance	Una porta HBA Fibre Channel è guasta o è guasta.
Unità cache flash dell'appliance non ottimali	Le unità utilizzate per la cache SSD non sono ottimali.
Interconnessione dell'apparecchio/contenitore della batteria rimosso	Manca il contenitore di interconnessione/batteria.
Porta LACP dell'appliance mancante	Una porta su un dispositivo StorageGRID non partecipa al bond LACP.
Rilevato guasto della scheda di rete dell'apparecchio	È stato rilevato un problema con una scheda di interfaccia di rete (NIC) nell'appliance.
Alimentazione elettrica complessiva dell'apparecchio degradata	La potenza di un dispositivo StorageGRID si è discostata dalla tensione operativa consigliata.
Avviso critico SSD dell'appliance	Un SSD dell'apparecchio segnala un avviso critico.
Errore del controller di archiviazione dell'apparecchio A	Il controller di archiviazione A in un dispositivo StorageGRID non funziona.

Nome dell'avviso	Descrizione
Guasto del controller di archiviazione dell'apparecchio B	Il controller di archiviazione B in un dispositivo StorageGRID non funziona.
Guasto dell'unità del controller di archiviazione dell'appliance	Una o più unità in un dispositivo StorageGRID sono guaste o non sono ottimali.
Problema hardware del controller di archiviazione dell'appliance	Il software SANtricity segnala "Richiede attenzione" per un componente in un dispositivo StorageGRID .
Guasto dell'alimentatore del controller di archiviazione dell'apparecchio A	L'alimentatore A in un dispositivo StorageGRID si è discostato dalla tensione di esercizio consigliata.
Guasto all'alimentatore B del controller di archiviazione dell'apparecchio	L'alimentatore B in un dispositivo StorageGRID si è discostato dalla tensione di esercizio consigliata.
Servizio di monitoraggio dell'hardware di archiviazione degli elettrodomestici bloccato	Il servizio che monitora lo stato dell'hardware di archiviazione è bloccato.
Ripiani di stoccaggio degli elettrodomestici degradati	Lo stato di uno dei componenti nello scaffale di archiviazione di un dispositivo di archiviazione è degradato.
Temperatura dell'apparecchio superata	È stata superata la temperatura nominale o massima del regolatore di accumulo dell'apparecchio.
Sensore di temperatura dell'apparecchio rimosso	È stato rimosso un sensore di temperatura.
Errore di avvio sicuro UEFI dell'appliance	Un dispositivo non è stato avviato in modo sicuro.
L'I/O del disco è molto lento	Un I/O del disco molto lento potrebbe influire sulle prestazioni della griglia.
Rilevato guasto della ventola dell'apparecchio di archiviazione	È stato rilevato un problema con un'unità ventola nel controller di archiviazione di un dispositivo.
Connettività di archiviazione dell'appliance di archiviazione degradata	Si è verificato un problema con una o più connessioni tra il controller di elaborazione e il controller di archiviazione.
Dispositivo di archiviazione inaccessibile	Non è possibile accedere a un dispositivo di archiviazione.

Avvisi di audit e syslog

Nome dell'avviso	Descrizione
I registri di controllo vengono aggiunti alla coda in memoria	Il nodo non riesce a inviare log al server syslog locale e la coda in memoria si sta riempiendo.
Errore di inoltro del server syslog esterno	Il nodo non può inoltrare i log al server syslog esterno.
Ampia coda di controllo	La coda del disco 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 riesce a 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 Available o Strong-site, che non è supportato.
Il bucket FabricPool ha un'impostazione di controllo delle versioni non supportata	Un bucket FabricPool ha abilitato il controllo delle versioni o il blocco degli oggetti S3, che non sono supportati.

Avvisi di Cassandra

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

Nome dell'avviso	Descrizione
Le metriche di riparazione di Cassandra sono obsolete	Le metriche che descrivono i lavori di riparazione di Cassandra non sono aggiornate.
I progressi nella riparazione di Cassandra sono lenti	I progressi nelle riparazioni del database Cassandra sono lenti.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione Cassandra non è disponibile.
Corruzione della tabella Cassandra	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva un danneggiamento della tabella.

Avvisi di Cloud Storage Pool

Nome dell'avviso	Descrizione
Errore di connettività del pool di archiviazione cloud	Il controllo dello stato di Cloud Storage Pool ha rilevato uno o più nuovi errori.
Scadenza della certificazione dell'entità finale di IAM Roles Anywhere	Il certificato dell'entità finale di IAM Roles Anywhere sta per scadere.

Avvisi di replicazione tra griglie

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

Avvisi DHCP

Nome dell'avviso	Descrizione
Contratto di locazione DHCP scaduto	Il lease DHCP su un'interfaccia di rete è scaduto.
La scadenza del contratto di locazione DHCP è imminente	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 sulle prestazioni di debug	Quando la modalità debug è abilitata, le prestazioni del sistema potrebbero essere influenzate negativamente.
Configurazione della traccia abilitata	Quando la configurazione della traccia è abilitata, le prestazioni del sistema potrebbero subire un impatto negativo.

Avvisi via e-mail e AutoSupport

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

Avvisi di codifica di cancellazione (EC)

Nome dell'avviso	Descrizione
Errore di ribilanciamento della CE	La procedura di riequilibrio della CE è fallita o è stata interrotta.
Guasto alla riparazione della CE	Un processo di riparazione dei dati EC non è riuscito o è stato interrotto.
Riparazione EC bloccata	Un lavoro di riparazione dei dati EC è bloccato.
Errore di verifica del frammento codificato tramite cancellazione	I frammenti con codice di cancellazione non possono più essere verificati. I frammenti danneggiati potrebbero non essere riparati.

Avvisi di scadenza dei certificati

Nome dell'avviso	Descrizione
Scadenza del certificato CA del proxy di amministrazione	Uno o più certificati nel bundle CA del server proxy di amministrazione stanno per scadere.

Nome dell'avviso	Descrizione
Scadenza del certificato client	Uno o più certificati client stanno per scadere.
Scadenza del certificato server globale per S3 e Swift	Il certificato server globale per S3 e Swift sta per scadere.
Scadenza del certificato dell'endpoint del bilanciatore del carico	Uno o più certificati dell'endpoint del bilanciatore 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 di rete

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

Avvisi sulla federazione della griglia

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

Avvisi di utilizzo elevato o di latenza elevata

Nome dell'avviso	Descrizione
Utilizzo elevato dell'heap Java	Viene utilizzata un'elevata percentuale di spazio heap Java.
Elevata latenza per le query sui metadati	Il tempo medio per le query sui metadati di Cassandra è troppo lungo.

Avvisi di federazione delle identità

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

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

Nome dell'avviso	Descrizione
Posizionamento ILM non realizzabile	Per determinati oggetti non è possibile ottenere un'istruzione di posizionamento in una regola ILM.
Bassa frequenza di scansione ILM	La velocità di scansione ILM è impostata su meno di 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 stata caricata.
Errore di connettività KMS	Un nodo appliance non è riuscito a connettersi al server di gestione delle chiavi per il proprio sito.
Nome della 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 decrittografati correttamente, ma uno o più volumi non sono riusciti a ruotare alla chiave più recente.
KMS non è configurato	Per questo sito non esiste alcun server di gestione delle chiavi.
La chiave KMS non è riuscita a decrittografare un volume dell'appliance	Uno o più volumi su un dispositivo con crittografia dei nodi abilitata non possono essere decrittografati 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 riuscito a connettersi a uno o più server nel cluster del server di gestione delle chiavi per il suo sito.

Avvisi del bilanciatore del carico

Nome dell'avviso	Descrizione
Connessioni di bilanciamento del carico con richiesta zero elevate	Una percentuale elevata di connessioni agli endpoint del bilanciatore del carico si è interrotta senza eseguire richieste.

Avvisi di scostamento dell'orologio locale

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

Avvisi di memoria o spazio insufficienti

Nome dell'avviso	Descrizione
Bassa capacità del disco del registro di controllo	Lo spazio disponibile per i registri di controllo è limitato. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
Memoria del nodo disponibile insufficiente	La quantità di RAM disponibile su un nodo è bassa.
Spazio libero insufficiente per il pool di archiviazione	Lo spazio disponibile per l'archiviazione dei dati degli oggetti nel nodo di archiviazione è limitato.
Bassa memoria del nodo installata	La quantità di memoria installata su un nodo è bassa.
Basso spazio di archiviazione dei metadati	Lo spazio disponibile per l'archiviazione dei metadati degli oggetti è limitato.
Bassa capacità del disco metrico	Lo spazio disponibile per il database delle metriche è limitato.
Bassa capacità di archiviazione dei dati degli oggetti	Lo spazio disponibile per l'archiviazione dei dati degli oggetti è limitato.

Nome dell'avviso	Descrizione
Sovrascrittura della filigrana di sola lettura bassa	L'override della filigrana di sola lettura software del volume di archiviazione è inferiore alla filigrana minima ottimizzata per un nodo di archiviazione.
Bassa capacità del disco radice	Lo spazio disponibile sul disco radice è basso.
Bassa capacità di dati del 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 basso.

Avvisi di nodo o di rete di nodi

Nome dell'avviso	Descrizione
Utilizzo della rete di amministrazione ricevuto	L'utilizzo della ricezione sulla rete di amministrazione è elevato.
Utilizzo della trasmissione della rete amministrativa	L'utilizzo della trasmissione sulla rete di amministrazione è elevato.
Errore di configurazione del firewall	Impossibile applicare la configurazione del firewall.
Endpoint dell'interfaccia di gestione in modalità fallback	Per troppo tempo tutti gli endpoint dell'interfaccia di gestione sono tornati alle porte predefinite.
Errore di connettività della rete del nodo	Si sono verificati errori durante il trasferimento dei dati tra i nodi.
Errore di ricezione del frame della rete del nodo	Un'alta percentuale di frame di rete ricevuti da un nodo presentava errori.
Nodo non sincronizzato con il server NTP	Il nodo non è sincronizzato con il server NTP (Network Time Protocol).
Nodo non bloccato con il server NTP	Il nodo non è bloccato su un server NTP (Network Time Protocol).
Rete di nodi non elettrodomestici inattiva	Uno o più dispositivi di rete sono inattivi o disconnessi.
Collegamento dell'appliance dei servizi non attivo sulla rete di amministrazione	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.

Nome dell'avviso	Descrizione
Collegamento dell'appliance dei servizi non attivo sulla porta 1 della rete di amministrazione	La porta di rete amministrativa 1 sull'appliance è inattiva o disconnessa.
Collegamento dell'appliance dei servizi non attivo sulla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 2	La porta di rete 2 dell'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 3	La porta di rete 3 dell'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di servizi non attivo sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla rete di amministrazione	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta 1 della rete di amministrazione	La porta di rete amministrativa 1 sull'appliance è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non funzionante sulla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta di rete 2	La porta di rete 2 dell'apparecchio è inattiva o disconnessa.
Collegamento dell'appliance di archiviazione non attivo sulla porta di rete 3	La porta di rete 3 dell'apparecchio è inattiva o disconnessa.

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

Avvisi sugli oggetti

Nome dell'avviso	Descrizione
Controllo esistenza oggetto fallito	Il processo di controllo dell'esistenza dell'oggetto non è riuscito.
Controllo dell'esistenza dell'oggetto bloccato	Il processo di controllo dell'esistenza dell'oggetto si è bloccato.
Oggetti persi	Uno o più oggetti sono stati persi dalla griglia.
S3 PUT dimensione dell'oggetto troppo grande	Un client sta tentando un'operazione PUT Object che supera i limiti di dimensione S3.
Rilevato oggetto corrotto non identificato	È stato trovato un file nell'archivio oggetti replicati che non è stato possibile identificare come oggetto replicato.

Avvisi sui servizi della piattaforma

Nome dell'avviso	Descrizione
Capacità richiesta in sospeso dei servizi della piattaforma bassa	Il numero di richieste in sospeso dei Servizi della piattaforma sta per raggiungere la capacità massima.
Servizi della piattaforma non disponibili	In un sito sono in esecuzione o disponibili troppi nodi di archiviazione con il servizio RSM.

Avvisi sul volume di archiviazione

Nome dell'avviso	Descrizione
Il volume di archiviazione richiede attenzione	Un volume di archiviazione è offline e necessita di attenzione.
Il volume di archiviazione deve essere ripristinato	Un volume di archiviazione è stato recuperato e deve essere ripristinato.
Volume di archiviazione offline	Un volume di archiviazione è stato offline per più di 5 minuti.
Tentativo di rimontaggio del volume di archiviazione	Un volume di archiviazione era offline e ha attivato un rimontaggio automatico. Ciò potrebbe indicare un problema dell'unità o errori del file system.
Il ripristino del volume non è riuscito ad avviare la riparazione dei dati replicati	Non è stato possibile avviare automaticamente la riparazione dei dati replicati per un volume riparato.

Avvisi dei servizi StorageGRID

Nome dell'avviso	Descrizione
servizio nginx che utilizza la configurazione di backup	La configurazione del servizio nginx non è valida. Ora viene utilizzata la configurazione precedente.
servizio nginx-gw che utilizza la configurazione di backup	La configurazione del servizio nginx-gw non è valida. Ora viene utilizzata la configurazione precedente.
Riavvio richiesto per disabilitare FIPS	La policy di sicurezza non richiede la modalità FIPS, ma il modulo di sicurezza crittografica NetApp è abilitato.
Riavvio richiesto per abilitare FIPS	La policy di sicurezza richiede la modalità FIPS, ma il modulo di sicurezza crittografica NetApp è disabilitato.
Servizio SSH che utilizza la configurazione di backup	La configurazione del servizio SSH non è valida. Ora viene utilizzata la configurazione precedente.

Avvisi agli inquilini

Nome dell'avviso	Descrizione
Elevato utilizzo della quota degli inquilini	Viene utilizzata un'elevata percentuale di spazio quota. Questa regola è disabilitata per impostazione predefinita perché potrebbe causare troppe notifiche.

Metriche di 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.

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

Per i dettagli sulla sintassi delle query di Prometheus, vedere "[Interrogando Prometeo](#)".

Cosa sono le metriche di Prometheus?

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

Dove vengono utilizzate le metriche di Prometheus?

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

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



- **Avvisi:** gli avvisi vengono attivati a livelli di gravità specifici quando le condizioni delle regole di avviso che utilizzano le metriche Prometheus vengono valutate come vere.
- **API di gestione della griglia:** puoi utilizzare le metriche di Prometheus nelle regole di avviso personalizzate o con strumenti di automazione esterni per monitorare il tuo sistema StorageGRID. Un elenco completo delle metriche di Prometheus è disponibile nella Grid Management API. (Dalla parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API > metriche**.) Sebbene siano disponibili più di mille metriche, per monitorare le operazioni StorageGRID più critiche ne basta un numero relativamente piccolo.



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

- La pagina **SUPPORTO > Strumenti > Diagnostica** e la pagina **SUPPORTO > Strumenti > Metriche**: queste pagine, destinate principalmente all'assistenza tecnica, forniscono diversi strumenti e grafici che utilizzano i valori delle metriche di Prometheus.



Alcune funzionalità e voci di menu nella pagina Metriche sono intenzionalmente non funzionali e sono soggette a modifiche.

Elenco delle metriche più comuni

L'elenco seguente contiene le metriche Prometheus più comunemente utilizzate.



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

alertmanager_notifiche_fallite_totale

Numero totale di notifiche di avviso non riuscite.

node_filesystem_disponibilità_byte

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

node_memory_MemAvailable_bytes

Campo informativo sulla memoria MemAvailable_bytes.

nodo_operatore_di_rete

Valore del vettore di /sys/class/net/iface .

node_network_receive_errs_total

Statistica del dispositivo di rete receive_errs .

errori_di_trasmissione_della_rete_del_nodo_totale

Statistica del dispositivo di rete transmit_errs .

storagegrid_amministrativamente_inattivo

Il nodo non è connesso alla rete per un motivo prevedibile. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando o il software è in fase di aggiornamento.

storagegrid_appliance_compute_controller_hardware_status

Lo stato dell'hardware del controller di elaborazione in un dispositivo.

storagegrid_appliance_failed_disks

Per il controller di archiviazione di un dispositivo, il numero di unità che non sono ottimali.

storagegrid_appliance_storage_controller_hardware_status

Stato generale dell'hardware del controller di archiviazione in un dispositivo.

storagegrid_content_buckets_and_containers

Numero totale di bucket S3 e container Swift noti a questo nodo di archiviazione.

oggetti_contenuto_di_archiviazione

Numero totale di oggetti dati S3 e Swift noti a questo nodo di archiviazione. Il conteggio è valido solo per gli oggetti dati creati dalle applicazioni client che interagiscono con il sistema tramite S3.

oggetti_contenuto_di_archiviazione_persi

Numero totale di oggetti che questo servizio rileva come mancanti dal sistema StorageGRID . È necessario

intervenire per determinare la causa della perdita e se è possibile un recupero.

"Risolvere i problemi relativi ai dati degli oggetti persi e mancanti"

storagegrid_http_sessions_incoming_attempted

Numero totale di sessioni HTTP tentate su un nodo di archiviazione.

storagegrid_http_sessions_incoming_currently_established

Numero di sessioni HTTP attualmente attive (aperte) sul nodo di archiviazione.

storagegrid_http_sessions_incoming_failed

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

storagegrid_http_sessions_incoming_successful

Numero totale di sessioni HTTP completate correttamente.

storagegrid_ilm_in_attesa_di_oggetti_di_sfondo

Numero totale di oggetti su questo nodo in attesa della valutazione ILM dalla scansione.

storagegrid_ilm_in_attesa_di_oggetti_di_valutazione_client_al_secondo

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

storagegrid_ilm_in_attesa_di_oggetti_client

Numero totale di oggetti su questo nodo in attesa di valutazione ILM da parte delle operazioni client (ad esempio, acquisizione).

storagegrid_ilm_in_attesa_di_oggetti_totali

Numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_oggetti_al_secondo

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

storagegrid_ilm_scan_period_estimated_minutes

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_scadenza_tempo

Tempo di scadenza del certificato dell'endpoint del bilanciatore del carico in secondi dall'epoca.

storagegrid_metadata_queries_latenza_media_millisecondi

Tempo medio necessario per eseguire una query sull'archivio metadati tramite questo servizio.

storagegrid_network_bytes_ricevuti

Quantità totale di dati ricevuti dall'installazione.

storagegrid_network_bytes_trasmessi

Quantità totale di dati inviati dall'installazione.

percentuale_utilizzo_cpu_node_storagegrid

Percentuale di tempo CPU disponibile attualmente utilizzata da questo servizio. Indica il livello di attività del servizio. La quantità di tempo CPU disponibile dipende dal numero di CPU del server.

storagegrid_ntp_chosen_time_source_offset_millisecondi

Offset sistematico del tempo fornito da una sorgente temporale scelta. L'offset viene introdotto quando il ritardo per raggiungere una sorgente temporale non è uguale al tempo necessario alla sorgente temporale per raggiungere il client NTP.

storagegrid_ntp_bloccato

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

storagegrid_s3_data_transfers_bytes_ingested

Quantità totale di dati acquisiti dai client S3 in questo nodo di archiviazione dall'ultima reimpostazione dell'attributo.

storagegrid_s3_data_transfers_bytes_retrieved

Quantità totale di dati recuperati dai client S3 da questo nodo di archiviazione dall'ultima reimpostazione dell'attributo.

storagegrid_s3_operations_failed

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

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_unauthorized

Numero totale di operazioni S3 non riuscite dovute a un errore di autorizzazione.

giorni_di_scadenza_del_certificato_dell'interfaccia_di_gestione_del_certificato_del_server_di_storagegrid

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

giorni_di_scadenza_del_certificato_degli_endpoint_dell'api_di_archiviazione_del_certificato_del_server_di_storagegrid

Numero di giorni prima della scadenza del certificato Object Storage API.

storagegrid_service_cpu_seconds

Quantità cumulativa di tempo in cui la CPU è stata utilizzata da questo servizio dall'installazione.

storagegrid_service_memory_usage_bytes

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

storagegrid_service_network_bytes_ricevuti

Quantità totale di dati ricevuti da questo servizio dall'installazione.

storagegrid_service_network_bytes_trasmessi

La quantità totale di dati inviati da questo servizio.

storagegrid_service_restarts

Numero totale di volte in cui il servizio è stato riavviato.

secondi di esecuzione del servizio storagegrid

Tempo totale di esecuzione del servizio dall'installazione.

secondi di attività del servizio storagegrid

Tempo totale di esecuzione del servizio dall'ultimo riavvio.

storagegrid_stato_di_archiviazione_corrente

Lo stato attuale dei servizi di archiviazione. I valori degli attributi sono:

- 10 = Non in linea
- 15 = Manutenzione
- 20 = Sola lettura
- 30 = In linea

storagegrid_stato_archiviazione

Lo stato attuale dei servizi di archiviazione. I valori degli attributi sono:

- 0 = Nessun errore
- 10 = In transizione
- 20 = Spazio libero insufficiente
- 30 = Volume/i non disponibile/i
- 40 = Errore

storagegrid_byte_dati_di_utilizzo_archiviazione

Una stima della dimensione totale dei dati degli oggetti replicati e codificati per la cancellazione sul nodo di archiviazione.

storagegrid_metadati_utilizzo_archiviazione_byte_consentiti

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

storagegrid_metadati_utilizzo_archiviazione_byte

Quantità di metadati dell'oggetto sul volume di archiviazione 0, in byte.

storagegrid_utilizzo_archiviazione_spazio_totale_byte

Quantità totale di spazio di archiviazione assegnato a tutti gli archivi di oggetti.

storagegrid_storage_utilization_space_usable_bytes

Quantità totale di spazio di archiviazione degli oggetti rimanente. Calcolato sommando la quantità di spazio disponibile per tutti gli archivi di oggetti sul nodo di archiviazione.

storagegrid_swift_data_transfers_bytes_ingested

Quantità totale di dati acquisiti dai client Swift in questo nodo di archiviazione dall'ultima reimpostazione

dell'attributo.

storagegrid_swift_data_transfers_bytes_recuperati

Quantità totale di dati recuperati dai client Swift da questo nodo di archiviazione dall'ultima reimpostazione dell'attributo.

operazioni_swift_di_archiviazione_fallite

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

operazioni_rapide_di_archiviazione_riuscite

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

operazioni_rapide_di_archiviazione_non_autorizzate

Numero totale di operazioni Swift non riuscite dovute a 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.

conteggio_oggetti_utilizzo_tenant_storagegrid

Numero di oggetti per l'inquilino.

storagegrid_tenant_quota_utilizzo_byte

Quantità massima di spazio logico disponibile per gli oggetti del tenant. Se non viene specificata una metrica di quota, lo spazio disponibile è illimitato.

Ottieni un elenco di tutte le metriche

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

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

Riferimento ai file di registro

Riferimento ai file di registro

StorageGRID fornisce registri utilizzati per acquisire eventi, messaggi diagnostici e condizioni di errore. Potrebbe esserti richiesto di raccogliere i file di registro e di inoltrarli al supporto tecnico per aiutarti a risolvere i problemi.

I registri sono classificati come segue:

- "[Registri del software StorageGRID](#)"
- "[Registri di distribuzione e manutenzione](#)"
- "[Informazioni su bycast.log](#)"



I dettagli forniti per ciascun tipo di registro sono solo a scopo di riferimento. I registri sono destinati alla risoluzione avanzata dei problemi da parte del supporto tecnico. Le tecniche avanzate che comportano la ricostruzione della cronologia dei problemi utilizzando i log di controllo e i file di log delle applicazioni esulano dallo scopo di queste istruzioni.

Accedi ai registri

Per accedere ai registri, puoi "[raccogliere file di registro e dati di sistema](#)" da uno o più nodi come un singolo archivio di file di registro. In alternativa, se il nodo di amministrazione primario non è disponibile o non riesce a 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. Inserisci la password elencata nel `Passwords.txt` file.
3. Immettere il seguente comando per passare alla root: `su -`
4. Inserisci la password elencata nel `Passwords.txt` file.

Esportare i registri sul server syslog

L'esportazione dei log sul 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 sulle richieste S3 che restituiscono errori, senza l'impatto sulle prestazioni causato dai metodi di registrazione degli audit.
- Accesso alle richieste di livello HTTP e ai codici di errore facili da analizzare.
- Migliore visibilità sulle richieste bloccate dai classificatori del traffico nel bilanciatore del carico.

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

Categorie dei file di registro

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

Posizione dell'archivio	Descrizione
revisione contabile	Messaggi di controllo generati durante il normale funzionamento del sistema.
base-os-logs	Informazioni di base sul sistema operativo, incluse le versioni delle immagini StorageGRID .
fasci	Informazioni di configurazione globali (bundle).
Cassandra	Informazioni sul database di Cassandra e registri di riparazione di Reaper.
ec	Informazioni VCS sul nodo corrente e informazioni sul gruppo EC in base all'ID del profilo.

Posizione dell'archivio	Descrizione
griglia	Registri generali della griglia, incluso il debug(bycast.log) E servermanager registri.
griglia.json	File di configurazione della griglia condiviso tra tutti i nodi. Inoltre, node.json è specifico del nodo corrente.
hagruppi	Metriche e log dei gruppi ad alta disponibilità.
installare	`Gdu-server`e installare i registri.
Lambda-arbitro	Registri relativi alla richiesta proxy S3 Select.
boscaiolo.log	Messaggi di debug relativi alla raccolta dei log.
Metrica	Registri di servizio per Grafana, Jaeger, node exporter e Prometheus.
miscd	Registri di accesso ed errori vari.
MySQL	Configurazione del database mariaDB e relativi log.
netto	Registri generati da script correlati alla rete e dal servizio Dynip.
nginx	File e registri di configurazione del bilanciatore del carico e della federazione della griglia. Include anche i registri del traffico di Grid Manager e Tenant Manager.

Posizione dell'archivio	Descrizione
nginx-gw	<ul style="list-style-type: none"> • access.log: Messaggi di registro delle richieste del Grid Manager e del Tenant Manager. <ul style="list-style-type: none"> ◦ Questi messaggi sono preceduti da mgmt: quando esportato tramite syslog. ◦ 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> • cgr-access.log.gz: Richieste di replicazione cross-grid in entrata. <ul style="list-style-type: none"> ◦ Questi messaggi sono preceduti da cgr: quando esportato tramite syslog. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • endpoint-access.log.gz: Richieste S3 e Swift agli endpoint del bilanciatore del carico. <ul style="list-style-type: none"> ◦ Questi messaggi sono preceduti da endpoint: quando esportato tramite syslog. ◦ Il formato di questi messaggi di registro è <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • nginx-gw-dns-check.log: Correlato al nuovo avviso di controllo DNS.
ntp	File di configurazione e registri NTP.
Oggetti orfani	Registri relativi agli oggetti orfani.
sistema operativo	File di stato del nodo e della griglia, inclusi i servizi pid .
altro	File di registro sotto /var/local/log che non vengono raccolti in altre cartelle.
perf	Informazioni sulle prestazioni di CPU, rete e I/O del disco.
dati di Prometheus	Metriche Prometheus correnti, se la raccolta di log include dati Prometheus.
approvvigionamento	Registri relativi al processo di provisioning della rete.
zattera	Registri del cluster Raft utilizzati nei servizi della piattaforma.
ssh	Registri relativi alla configurazione e al servizio SSH.

Posizione dell'archivio	Descrizione
SNMP	Configurazione dell'agente SNMP utilizzata per l'invio di notifiche SNMP.
socket-dati	Dati socket per il debug di rete.
comandi-di-sistema.txt	Output dei comandi del contenitore StorageGRID . Contiene informazioni di sistema, come la rete e l'utilizzo del disco.
pacchetto di recupero sincronizzato	Correlato al mantenimento della coerenza dell'ultimo pacchetto di ripristino su tutti i nodi di amministrazione e di archiviazione che ospitano il servizio ADC.

Registri del software StorageGRID

È possibile utilizzare i log StorageGRID per risolvere i problemi.



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

Registri generali di StorageGRID

Nome del file	Note	Trovato su
/var/local/log/broadcast.log	Il file principale per la risoluzione dei problemi StorageGRID . Selezionare SUPPORTO > Strumenti > Topologia griglia . Quindi seleziona Sito > Nodo > SSM > Eventi .	Tutti i nodi
/var/local/log/broadcast-err.log	Contiene un sottoinsieme di <code>broadcast.log</code> (messaggi con gravità ERROR e CRITICAL). Nel sistema vengono visualizzati anche i messaggi CRITICI . Selezionare SUPPORTO > Strumenti > Topologia griglia . Quindi seleziona Sito > Nodo > SSM > Eventi .	Tutti i nodi
/var/local/core/	Contiene tutti i file core dump creati se il programma termina in modo anomalo. Le possibili cause includono errori di asserzione, violazioni o timeout dei thread. Nota: Il file <code>"/var/local/core/kexec_cmd"</code> di solito è presente sui nodi dell'appliance e non indica un errore.	Tutti i nodi

Registri relativi alla cifratura

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

Registri della federazione della griglia

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

Registri NMS

Nome del file	Note	Trovato su
/var/local/log/nms.log	<ul style="list-style-type: none"> • Acquisisce notifiche dal Grid Manager e dal Tenant Manager. • Cattura gli eventi relativi al funzionamento del servizio NMS. Ad esempio, notifiche e-mail e modifiche alla configurazione. • Contiene gli aggiornamenti del bundle XML derivanti dalle modifiche di configurazione apportate al 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 della pagina ed errori HTTP Status 500. 	Nodi amministrativi
/var/local/log/nms.errlog	<p>Contiene messaggi di errore relativi agli aggiornamenti del database MySQL.</p> <p>Contiene il flusso di errore standard (stderr) dei servizi corrispondenti. Esiste un file di registro per servizio. Questi file sono generalmente vuoti, a meno che non ci siano problemi con il servizio.</p>	Nodi amministrativi
/var/local/log/nms.requestlog	Contiene informazioni sulle connessioni in uscita dall'API di gestione ai servizi StorageGRID interni.	Nodi amministrativi

Registri di Server Manager

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

Registri dei servizi StorageGRID

Nome del file	Note	Trovato su
/var/local/log/acct.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/adc.errlog	Contiene il flusso di errore standard (stderr) dei servizi corrispondenti. Esiste un file di registro per servizio. Questi file sono generalmente vuoti, a meno che non ci siano problemi con il servizio.	Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/ams.errlog		Nodi amministrativi
/var/local/log/cassandra/system.log	Informazioni per l'archivio metadati (database Cassandra) che possono essere utilizzate se si verificano problemi durante l'aggiunta di nuovi nodi di archiviazione o se l'attività di riparazione di nodetool si blocca.	Nodi di archiviazione
/var/local/log/cassandra-reaper.log	Informazioni per il servizio Cassandra Reaper, che esegue riparazioni dei dati nel database Cassandra.	Nodi di archiviazione
/var/local/log/cassandra-reaper.errlog	Informazioni di errore per il servizio Cassandra Reaper.	Nodi di archiviazione
/var/local/log/chunk.errlog		Nodi di archiviazione
/var/local/log/cmn.errlog		Nodi amministrativi
/var/local/log/cms.errlog	Questo file di registro potrebbe essere presente nei sistemi che sono stati aggiornati da una versione precedente di StorageGRID. Contiene informazioni legacy.	Nodi di archiviazione
/var/local/log/dds.errlog		Nodi di archiviazione
/var/local/log/dmv.errlog		Nodi di archiviazione
/var/local/log/dynip*	Contiene i registri relativi al servizio dynip, che monitora la griglia per rilevare modifiche IP dinamiche e aggiorna la configurazione locale.	Tutti i nodi
/var/local/log/grafana.log	Il registro associato al servizio Grafana, utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi amministrativi

Nome del file	Note	Trovato su
/var/local/log/hagroups.log	Il registro associato ai gruppi ad alta disponibilità.	Nodi amministrativi e nodi gateway
/var/local/log/hagroups_events.log	Tiene traccia dei cambiamenti di stato, come la transizione da BACKUP a MASTER o FAULT.	Nodi amministrativi e nodi gateway
/var/local/log/idnt.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/jaeger.log	Il registro associato al servizio Jaeger, utilizzato per la raccolta delle tracce.	Tutti i nodi
/var/local/log/kstn.errlog		Nodi di archiviazione che eseguono il servizio ADC
/var/local/log/lambda*	Contiene i registri per il servizio S3 Select.	Nodi di amministrazione e gateway Solo alcuni nodi Admin e Gateway contengono questo registro. Vedi il " Requisiti e limitazioni di S3 Select per i nodi Admin e Gateway ".
/var/local/log/ldr.errlog		Nodi di archiviazione
/var/local/log/miscd/*.log	Contiene i registri per il servizio MISCD (Information Service Control Daemon), che fornisce un'interfaccia per interrogare e gestire i servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio interrogando lo 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 vari servizi di griglia (come Prometheus e Dynip) per poter comunicare con i servizi su altri nodi tramite API HTTPS.	Tutti i nodi

Nome del file	Note	Trovato su
/var/local/log/nginx-gw/*.log	Contiene registri generali relativi al servizio nginx-gw, inclusi i registri degli errori e i registri per le porte amministrative riservate sui nodi amministrativi.	Nodi amministrativi e nodi gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene i registri di accesso relativi al traffico di replicazione tra griglie.	Nodi amministrativi, nodi gateway o entrambi, in base alla configurazione della federazione della griglia. Presente solo sulla griglia di destinazione per la replica tra griglie.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene i registri di accesso per il servizio Load Balancer, che fornisce il bilanciamento del carico del traffico S3 dai client ai nodi di archiviazione.	Nodi amministrativi e nodi gateway
/var/local/log/persistence*	Contiene i registri per il servizio di persistenza, che gestisce i file sul disco radice che devono essere mantenuti anche dopo un riavvio.	Tutti i nodi
/var/local/log/prometheus.log	<p>Per tutti i nodi, contiene il registro del servizio di esportazione dei nodi e il registro del servizio delle metriche di esportazione ade.</p> <p>Per i nodi amministrativi, contiene anche i registri per i servizi Prometheus e Alert Manager.</p>	Tutti i nodi
/var/local/log/raft.log	Contiene l'output della libreria utilizzata dal servizio RSM per il protocollo Raft.	Nodi di archiviazione con servizio RSM
/var/local/log/rms.errlog	Contiene i registri per il servizio Replicated State Machine Service (RSM), utilizzato per i servizi della piattaforma S3.	Nodi di archiviazione con servizio RSM
/var/local/log/ssm.errlog		Tutti i nodi

Nome del file	Note	Trovato su
/var/local/log/update-s3vs-domains.log	Contiene i registri relativi all'elaborazione degli aggiornamenti per la configurazione dei nomi di dominio ospitati virtuali S3. Consultare le istruzioni per l'implementazione delle applicazioni client S3.	Nodi di amministrazione e gateway
/var/local/log/update-snmp-firewall.*	Contiene i registri relativi alle porte del firewall gestite per SNMP.	Tutti i nodi
/var/local/log/update-sysl.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 di amministrazione 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

- "[Informazioni su bycast.log](#)"
- "[Utilizzare l'API REST S3](#)"

Registri di distribuzione e manutenzione

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

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

Nome del file	Note	Trovato su
/var/local/log/pa-move-old_pa.log	Creato durante l'esecuzione del pa-move.sh sceneggiatura.	Nodo di amministrazione primario
/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 di amministrazione 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

Informazioni su bycast.log

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

Il file /var/local/log/broadcast-err.log è un sottoinsieme di broadcast.log . Contiene messaggi di gravità ERRORE e CRITICO.

Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno. Vedere " [Configurare i messaggi di controllo e le destinazioni dei registri](#)" .

Rotazione dei file per broadcast.log

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

Il file salvato viene rinominato broadcast.log.1 e il nuovo file è denominato broadcast.log . Quando il nuovo broadcast.log raggiunge 1 GB, broadcast.log.1 viene rinominato e compresso per diventare broadcast.log.2.gz , E broadcast.log è rinominato broadcast.log.1 .

Il limite di rotazione per broadcast.log è di 21 file. Quando la 22a versione del broadcast.log viene creato un file, il file più vecchio viene eliminato.

Il limite di rotazione per broadcast-err.log è composto da sette file.



Se un file di registro è stato compresso, non è possibile decomprimere nella stessa posizione in cui è stato scritto. La decompressione del file nella stessa posizione può interferire con gli script di rotazione del registro.

Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati

quando viene configurato un server syslog esterno. Vedere "Configurare i messaggi di controllo e le destinazioni dei registri".

Informazioni correlate

"Raccogli file di registro e dati di sistema"

Messaggi in `broadcast.log`

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

Esempio di messaggio ADE:

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

I messaggi ADE contengono le seguenti informazioni:

Segmento del messaggio	Valore nell'esempio
Nodo ID	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-GGTHH:MM:SS.uuuuuu)
Livello di gravità	ERRORE
Numero di tracciamento interno	0906
Messaggio	SVMR: Il controllo dello stato di salute del volume 3 è fallito con il motivo 'TOUT'

Gravità dei messaggi in `broadcast.log`

I messaggi in `broadcast.log` vengono assegnati livelli di gravità.

Per esempio:

- **AVVISO** — Si è verificato un evento che dovrebbe essere registrato. La maggior parte dei messaggi di registro si trova a questo livello.
- **ATTENZIONE** — Si è verificata una condizione imprevista.
- **ERRORE** — Si è verificato un errore grave che avrà ripercussioni sulle operazioni.

- **CRITICO** — Si è verificata una condizione anomala che ha interrotto le normali operazioni. È necessario intervenire immediatamente sulla condizione di base.

Codici di errore in `broadcast.log`

La maggior parte dei messaggi di errore in `broadcast.log` contengono codici di errore.

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

Codice di errore	Senso
SUCS	Nessun errore
GERR	Sconosciuto
CANC	Annullato
ABRT	Abortito
TUTTO	Tempo scaduto
INVL	Non valido
NFND	Non trovato
VERSO	Versione
CONF	Configurazione
FALLIRE	Fallito
ICPL	Incompleto
FATTO	Fatto
SUNV	Servizio non disponibile

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

Numero di errore	Codice di errore	Senso
001	EPERM	Operazione non consentita
002	ENOENTE	Nessun file o directory con questo nome

Numero di errore	Codice di errore	Senso
003	ESRCH	Nessun processo del genere
004	EINTR	Chiamata di sistema interrotta
005	EIO	errore di I/O
006	ENXIO	Nessun dispositivo o indirizzo del genere
007	E2BIG	Elenco argomenti troppo lungo
008	ENOEXEC	Errore di formato Exec
009	EBADF	Numero di file errato
010	BAMBINO	Nessun processo figlio
011	DI NUOVO	Riprova
012	ENOMEM	Memoria esaurita
013	EACCES	Permesso negato
014	ERRORE	Indirizzo errato
015	ENOTBLK	Dispositivo di blocco richiesto
016	EBUSY	Dispositivo o risorsa occupati
017	EESI	Il file esiste
018	EXDEV	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo del genere
020	ENOTDIR	Non una directory
021	EISDIR	È una directory
022	EINVAL	Argomento non valido
023	ENFILE	Overflow della tabella dei file

Numero di errore	Codice di errore	Senso
024	EMFILE	Troppi file aperti
025	ENOTTY	Non una macchina da scrivere
026	ETXTBSY	File di testo occupato
027	EFBIG	File troppo grande
028	ENOSPC	Nessuno spazio rimasto sul dispositivo
029	ESPIARE	Ricerca illegale
030	EROFS	File system di sola lettura
031	EMLINK	Troppi link
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dal dominio della funzione
034	GAMMA	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un blocco delle risorse
036	Smaltolungo	Nome del file troppo lungo
037	ENOLCK	Nessun blocco record disponibile
038	ENOSYS	Funzione non implementata
039	ENOTEMPTY	Directory non vuota
040	ELOOP	Sono stati riscontrati troppi link simbolici
041		
042	ENOMSG	Nessun messaggio del tipo desiderato
043	EIDRM	Identificatore rimosso
044	ECHRNG	Numero di canale fuori intervallo

Numero di errore	Codice di errore	Senso
045	EL2NSYNC	Livello 2 non sincronizzato
046	EL3HLT	Livello 3 interrotto
047	EL3RST	Ripristino di 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 interrotto
052	EBADE	Scambio non valido
053	EBADR	Descrittore di richiesta non valido
054	EXFULL	Scambio completo
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato file font non valido
060	ENOSTR	Dispositivo non in streaming
061	ENODATI	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse fuori flusso
064	ENONET	La macchina non è in rete
065	ENOPKG	Pacchetto non installato

Numero di errore	Codice di errore	Senso
066	EREMOTE	L'oggetto è remoto
067	ENOLINK	Il collegamento è stato interrotto
068	EADV	Errore di pubblicità
069	ESRMNT	Errore di srmount
070	ECOMM	Errore di comunicazione durante l'invio
071	EPROTO	Errore di protocollo
072	EMULTIHOP	Tentativo multihop
073	EDOTDOT	Errore specifico RFS
074	EBADMSG	Non è un messaggio di dati
075	EOVERFLOW	Valore troppo grande per il tipo di dati definito
076	ENOTUNIQ	Nome non univoco sulla rete
077	EBADFD	Descrittore di 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 collegare troppe librerie condivise
083	ELIBEXEC	Impossibile eseguire direttamente una libreria condivisa
084	EILSEQ	Sequenza di byte non valida
085	RIAVVIARE	La chiamata di sistema interrotta deve essere riavviata

Numero di errore	Codice di errore	Senso
086	ESTRPIPE	Errore del tubo di flusso
087	EUSERS	Troppi utenti
088	ENOTSOCK	Funzionamento della presa su non presa
089	EDESTADDRREQ	Indirizzo di destinazione richiesto
090	EMSGSIZE	Messaggio troppo lungo
091	EPROTOTIPO	Tipo di protocollo errato per il socket
092	ENOPROTOOPT	Protocollo non disponibile
093	EPROTONOSUPPORT	Protocollo non supportato
094	ESOCKTNOSUPPORT	Tipo di socket non supportato
095	EOPNOTSUPP	Operazione non supportata sull'endpoint di trasporto
096	EPFNOSUPPORT	Famiglia di protocolli non supportata
097	EAFNOSUPPORT	Indirizzo famiglia non supportato dal protocollo
098	EADDRINUSE	Indirizzo già in uso
099	EADDRNOTAVAIL	Impossibile assegnare l'indirizzo richiesto
100	ENETDOWN	La rete è inattiva
101	ENETUNREACH	La rete non è raggiungibile
102	ENETRESET	Connessione di rete interrotta a causa del ripristino
103	ECONNABORTED	Il software ha causato la terminazione della connessione
104	ECONNRESET	Connessione ripristinata dal peer
105	ENOBUFS	Nessuno spazio buffer disponibile
106	EISCONN	L'endpoint di trasporto è già connesso

Numero di errore	Codice di errore	Senso
107	ENOTCONN	L'endpoint di trasporto non è connesso
108	SPEGNIMENTO	Impossibile inviare dopo l'arresto dell'endpoint di trasporto
109	ETOOMANYREFS	Troppi riferimenti: impossibile unire
110	ETIMEDOUT	Connessione scaduta
111	ECONNRFIUTATO	Connessione rifiutata
112	EHOSTDOWN	L'host è inattivo
113	EHOSTUNREACH	Nessun percorso per l'host
114	GIÀ	Operazione già in corso
115	EINPROGRESS	Operazione in corso
116		
117	EUCLEAN	La struttura necessita di pulizia
118	ENOTNAM	Non è un file di tipo denominato XENIX
119	DISPONIBILE	Nessun semaforo XENIX disponibile
120	EISNAM	È un file di tipo denominato
121	EREMOTEIO	Errore di I/O remoto
122	EDQUOT	Quota superata
123	ENOMEDIO	Nessun mezzo trovato
124	TIPOMEDIO	Tipo di mezzo sbagliato
125	ECANCELED	Operazione annullata
126	ENOKEY	Chiave richiesta non disponibile
127	EKEYEXPIRED	La chiave è scaduta

Numero di errore	Codice di errore	Senso
128	EKEYREVOKED	La chiave è stata revocata
129	EKEYREJECTED	La chiave è stata rifiutata dal servizio
130	PROPRIETARIOMORTO	Per mutex robusti: il proprietario è morto
131	NON RECUPERABILI	Per mutex robusti: Stato non recuperabile

Configurare le destinazioni dei messaggi di controllo e dei registri

Considerazioni sull'utilizzo di un server syslog esterno

Un server syslog esterno è un server esterno a StorageGRID che puoi utilizzare per raccogliere informazioni di controllo del sistema in un'unica posizione. Utilizzando un server syslog esterno è possibile ridurre il traffico di rete sui nodi amministrativi e gestire le informazioni in modo più efficiente. Per StorageGRID, il formato del pacchetto dei messaggi syslog in uscita è conforme a RFC 3164.

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

- Registri di controllo contenenti i messaggi di controllo generati durante il normale funzionamento del sistema
- Eventi relativi alla sicurezza come accessi ed escalation alla radice
- Registri 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 una griglia di grandi dimensioni, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit. L'invio di informazioni di audit a un server syslog esterno consente di:

- Raccogli e gestisci 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 tuoi nodi amministrativi poiché le informazioni di controllo vengono trasferite direttamente dai vari nodi di archiviazione al server syslog esterno, senza dover passare attraverso un nodo amministrativo.



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



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

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 prevede di 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:** il 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. Non vi è alcun vantaggio significativo in termini di sicurezza nell'utilizzare una chiave privata crittografata, poiché sia la chiave che la passphrase devono essere memorizzate; per semplicità, si consiglia di utilizzare una chiave privata non crittografata, se disponibile.

Come stimare la dimensione del server syslog esterno

Normalmente, la griglia viene dimensionata per raggiungere la produttività richiesta, definita in termini di operazioni S3 al secondo o byte al secondo. Ad esempio, potresti avere il requisito che la tua griglia gestisca 1.000 operazioni S3 al secondo, o 2.000 MB al secondo, di inserimenti e recuperi di oggetti. Dovresti dimensionare il tuo server syslog esterno in base ai requisiti di dati della tua griglia.

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

Utilizzare S3 operazioni al secondo nelle formule di stima

Se la griglia è stata dimensionata per una velocità espressa in byte al secondo, è necessario convertire questa dimensione in operazioni S3 al secondo per utilizzare le formule di stima. Per convertire la velocità effettiva della griglia, è necessario innanzitutto determinare la dimensione media dell'oggetto, operazione che è possibile effettuare utilizzando le informazioni presenti nei registri di controllo e nelle metriche esistenti (se presenti) oppure sfruttando la conoscenza delle applicazioni che utilizzeranno StorageGRID. Ad esempio, se la griglia è stata dimensionata per raggiungere una velocità di elaborazione di 2.000 MB/secondo e la dimensione media degli oggetti è di 2 MB, la griglia è stata dimensionata per poter gestire 1.000 operazioni S3 al secondo ($2.000 \text{ MB} / 2 \text{ MB}$).



Le formule per il dimensionamento del server syslog esterno nelle sezioni seguenti forniscono stime del caso comune (piuttosto che stime del caso peggiore). A seconda della configurazione e del carico di lavoro, potresti riscontrare una frequenza di messaggi syslog o un volume di dati syslog maggiore o minore rispetto a quanto previsto dalle formule. Le formule sono da intendersi solo come linee guida.

Formule di stima per i registri di controllo

Se non si hanno informazioni sul carico di lavoro S3, a parte il numero di operazioni S3 al secondo che la griglia dovrebbe supportare, è possibile stimare il volume di log di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, partendo dal presupposto che i Livelli di controllo vengano lasciati impostati sui valori predefiniti (tutte le categorie impostate su Normale, eccetto Archiviazione, che è impostata

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 dovrebbe essere dimensionato per supportare 2.000 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere archiviare) i dati del registro di controllo a una velocità di 1,6 MB al secondo.

Se si conoscono meglio i propri carichi di lavoro, è possibile ottenere stime più precise. Per i registri di controllo, le variabili aggiuntive più importanti sono la percentuale di operazioni S3 che sono PUT (rispetto a GETS) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni di 4 caratteri utilizzate nella tabella sono nomi di campi del registro di controllo):

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

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

Utilizziamo K per rappresentare la dimensione media della somma dei nomi degli account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi di lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi di lunghezza fissa come 5733a5d7-f069-41ef-8fdb-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 log di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, partendo dal presupposto che i Livelli di controllo vengano lasciati impostati sui valori predefiniti (tutte le categorie impostate su Normale, tranne Archiviazione, che è impostata su Errore):

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

Ad esempio, se la griglia è dimensionata per 1.000 operazioni S3 al secondo, il carico di lavoro è costituito al 50% da PUT e i nomi degli account S3, dei bucket e degli oggetti sono in media pari a 90 byte, il server syslog esterno dovrebbe essere dimensionato per supportare 1.500 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere archiviare) 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 impostate su Normale, tranne Archiviazione, che è impostata su Errore). Non sono disponibili formule dettagliate per stimare la frequenza e la dimensione media dei messaggi di controllo per impostazioni di livello di controllo non predefinite. Tuttavia, la tabella seguente può essere utilizzata per effettuare una stima approssimativa della frequenza; è possibile utilizzare la formula per la dimensione media fornita per i registri di controllo, ma è importante tenere presente che è probabile che si ottenga 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 impostati su Debug o Normale	Tasso di controllo log = 8 x tasso di operazioni S3
Codifica di cancellazione: livelli di controllo tutti impostati su Debug o Normale	Utilizzare la stessa formula delle impostazioni predefinite

Formule di stima per eventi di sicurezza

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

Formule di stima per i registri delle applicazioni

Se non si hanno informazioni sul carico di lavoro S3, a parte il numero di operazioni S3 al secondo che la griglia dovrebbe supportare, è possibile stimare il volume dei registri 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 la griglia è dimensionata per 1.000 operazioni S3 al secondo, il server syslog esterno dovrebbe essere dimensionato per supportare 3.300 log delle applicazioni al secondo ed essere in grado di ricevere (e archiviare) i dati dei log delle applicazioni a una velocità di circa 1,2 MB al secondo.

Se si conoscono meglio i propri carichi di lavoro, è possibile ottenere stime più precise. Per i registri delle applicazioni, le variabili aggiuntive più importanti sono la strategia di protezione dei dati (replicazione vs. codifica di cancellazione), la percentuale di operazioni S3 che sono PUT (vs. GET/altro) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni di 4 caratteri utilizzate nella tabella sono nomi di campi del registro di controllo):

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

Esempi di stime dimensionali

In questa sezione vengono illustrati alcuni casi esemplificativi su come utilizzare le formule di stima per le griglie con i seguenti metodi di protezione dei dati:

- Replicazione
- Codifica di cancellazione

Se si utilizza la replica per la protezione dei dati

Sia P la percentuale di operazioni S3 che sono PUT, 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 nomi degli account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi di lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi di lunghezza fissa come 5733a5d7-f069-41ef-8fdb-13247494c69c (36 byte). Allora K ha un valore di 90 (13+13+28+36).

Se riesci a determinare i valori per P e K , puoi stimare il volume dei log delle applicazioni che il tuo server syslog esterno dovrà essere in grado di 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
```

Quindi, ad esempio, se la griglia è dimensionata per 1.000 operazioni S3 al secondo, il carico di lavoro è costituito al 50% da PUT e i nomi degli account S3, dei bucket e degli oggetti sono in media pari a 90 byte, il server syslog esterno dovrebbe essere dimensionato per supportare 1.800 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 la codifica di cancellazione per la protezione dei dati

Sia P la percentuale di operazioni S3 che sono PUT, 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 nomi degli account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi di lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi di lunghezza fissa come 5733a5d7-f069-41ef-8fdb-13247494c69c (36 byte). Allora K ha un valore di 90 (13+13+28+36).

Se riesci a determinare i valori per P e K, puoi stimare il volume dei log delle applicazioni che il tuo server syslog esterno dovrà essere in grado di 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
```

Quindi, ad esempio, se la griglia è dimensionata per 1.000 operazioni S3 al secondo, il carico di lavoro è costituito al 50% da PUT e i nomi degli account S3, dei bucket e degli oggetti sono in media pari a 90 byte, il server syslog esterno dovrebbe essere dimensionato per supportare 2.250 log delle applicazioni al secondo e dovrebbe essere in grado di ricevere (e in genere archiviare) i 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 le intestazioni delle richieste HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client, configurare un server syslog esterno e specificare dove inviare i registri di controllo, i registri degli eventi di sicurezza e i registri del software StorageGRID .

I messaggi e i registri di controllo 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 controllo e registri per monitorare l'attività e gli eventi del sistema.

Facoltativamente, è possibile configurare un server syslog esterno per salvare le informazioni di audit in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto sulle 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 una griglia di grandi dimensioni, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit. Vedere "[Configurare i messaggi di controllo e il server syslog esterno](#)" per i dettagli.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Autorizzazione di accesso alla manutenzione o alla root](#)".
- Se si prevede di configurare un server syslog esterno, è necessario aver esaminato il "[considerazioni sull'utilizzo di un server syslog esterno](#)" e ha garantito che il server avesse capacità sufficiente per ricevere e archiviare i file di registro.
- Se si prevede di configurare un server syslog esterno utilizzando il protocollo TLS o RELP/TLS, è necessario disporre dei certificati CA e client del server richiesti e della chiave privata del client.

Modifica i livelli dei messaggi di controllo

È possibile impostare un livello di controllo diverso per ciascuna delle seguenti categorie di messaggi nel registro di controllo:

Categoria di revisione	Impostazione predefinita	Ulteriori informazioni
Sistema	Normale	"Messaggi di controllo del sistema"
Magazzinaggio	Errore	"Messaggi di controllo dell'archiviazione degli oggetti"
Gestione	Normale	"Messaggio di controllo di gestione"
Il cliente legge	Normale	"Il cliente ha letto i messaggi di controllo"
Il cliente scrive	Normale	"Il cliente scrive messaggi di audit"
ILM	Normale	"Messaggi di controllo ILM"
Replicazione cross-grid	Errore	"CGRR: richiesta di replicazione tra griglie"



Queste impostazioni predefinite si applicano se StorageGRID è stato inizialmente installato utilizzando la versione 10.3 o successiva. Se inizialmente hai utilizzato 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 immediatamente effettive.

Passi

1. Selezionare **CONFIGURAZIONE > Monitoraggio > Server di audit e syslog**.
2. Per ogni categoria di messaggio di controllo, selezionare un livello di controllo dall'elenco a discesa:

Livello di audit	Descrizione
Spento	Nessun messaggio di controllo della categoria viene registrato.
Errore	Vengono registrati solo i messaggi di errore, ovvero i messaggi di controllo per i quali il codice risultato non è stato "riuscito" (SUCS).
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 controllo Normale.

I messaggi inclusi per ogni livello specifico includono quelli che verrebbero registrati ai livelli superiori. Ad

esempio, il livello Normale include tutti i messaggi di errore.



Se non è necessario un registro dettagliato delle operazioni di lettura client per le applicazioni S3, è possibile modificare facoltativamente l'impostazione **Lettura client** in **Errore** per ridurre il numero di messaggi di controllo registrati nel registro di controllo.

3. Seleziona **Salva**.

Un banner verde indica che la configurazione è stata salvata.

Definisci le intestazioni delle richieste HTTP

Facoltivamente, 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.

Passi

1. Nella sezione **Intestazioni protocollo di controllo**, definisci le intestazioni delle richieste HTTP che desideri includere nei messaggi di controllo di lettura e scrittura del client.

Utilizzare un asterisco (*) come carattere jolly per trovare la corrispondenza con zero o più caratteri.
Utilizzare la sequenza di escape (*) per trovare la corrispondenza con un asterisco letterale.

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

Quando in una richiesta vengono trovate intestazioni HTTP, queste vengono incluse nel messaggio di controllo nel campo HTRH.



Le intestazioni delle richieste del protocollo di controllo vengono registrate solo se il livello di controllo per **Lettura client** o **Scrittura client** non è **Disattivato**.

3. Seleziona **Salva**

Un banner verde indica che la configurazione è stata salvata.

Utilizza un server syslog esterno

Facoltivamente, è possibile configurare un server syslog esterno per salvare i log di controllo, i log delle applicazioni e i log degli eventi di sicurezza in una posizione esterna alla griglia.



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



Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili per soddisfare le vostre esigenze, è possibile applicare opzioni di configurazione aggiuntive utilizzando audit-destinations endpoint, che si trovano nella sezione API privata dell'["API di gestione della griglia"](#). Ad esempio, è possibile utilizzare l'API se si desidera utilizzare server syslog diversi per gruppi diversi di nodi.

Inserisci le informazioni syslog

Accedere alla procedura guidata Configura server syslog esterno e fornire le informazioni necessarie a StorageGRID per accedere al server syslog esterno.

Passi

1. Dalla pagina Server di controllo e syslog, selezionare **Configura server syslog esterno**. Oppure, se in precedenza hai configurato un server syslog esterno, seleziona **Modifica server syslog esterno**.
Viene visualizzata la procedura guidata Configura server syslog esterno.
2. Per il passaggio **Inserisci 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. Immettere 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 aiuta a proteggere le connessioni tra la griglia e il server syslog esterno. Per ulteriori informazioni, consultare "[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 la funzionalità del protocollo syslog per garantire una consegna affidabile dei messaggi di evento. L'utilizzo di RELP può aiutare a prevenire la perdita di informazioni di audit se il server syslog esterno deve essere riavviato.

5. Selezionare **Continua**.
6. Se hai selezionato **TLS** o **RELP/TLS**, carica 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 chiave.
 - c. Selezionare **Apri** per caricare il file.

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

7. Selezionare **Continua**.

Gestisci il contenuto syslog

È possibile selezionare quali informazioni inviare al server syslog esterno.

Passi

1. Per il passaggio **Gestisci contenuto syslog** della procedura guidata, seleziona ogni tipo di informazione di controllo che desideri inviare al server syslog esterno.
 - **Invia registri di controllo**: invia eventi StorageGRID e attività di sistema
 - **Invia eventi di sicurezza**: invia eventi di sicurezza, ad esempio quando un utente non autorizzato

tenta di accedere o un utente accede come root

- **Invia registri applicazione:** Invia "File di registro del software StorageGRID" utile 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 registri di accesso:** invia registri di accesso HTTP per richieste esterne a Grid Manager, Tenant Manager, endpoint del bilanciatore del carico configurati e richieste di federazione della griglia da sistemi remoti.

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

Impostando i valori di gravità e di funzionalità è possibile aggregare i registri in modi personalizzabili per un'analisi più semplice.

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

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

Gravità	Descrizione
Passaggio	Ogni messaggio inviato al syslog esterno deve 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 vengono generati dalla distribuzione Linux sui nodi.• Per i registri delle applicazioni, la gravità varia tra "info" e "notice", a seconda del problema. Ad esempio, l'aggiunta di un server NTP e la configurazione di un gruppo HA forniscono il valore "info", mentre l'arresto intenzionale del servizio SSM o RSM fornisce il valore "notice".• Per i registri di accesso, la gravità è "info".
0	Emergenza: il sistema è inutilizzabile
1	Attenzione: è necessario intervenire immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore

Gravità	Descrizione
4	Attenzione: Condizioni di avviso
5	Avviso: condizione normale ma significativa
6	Informativo: Messaggi informativi
7	Debug: messaggi a livello di debug

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

Se selezioni un valore, questo verrà applicato a tutti i messaggi di questo tipo. Se si sovrascrive una struttura con un valore fisso, le informazioni sulle diverse strutture andranno perse.

Facilità	Descrizione
Passaggio	<p>Ogni messaggio inviato al syslog esterno deve avere lo stesso valore di funzionalità di quando è stato registrato localmente sul nodo:</p> <ul style="list-style-type: none"> • Per i registri di controllo, la funzione 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 hanno i seguenti valori di funzionalità: <ul style="list-style-type: none"> ◦ bycast.log: utente o demone ◦ bycast-err.log: utente, demone, local3 o local4 ◦ jaeger.log: locale2 ◦ nms.log: locale3 ◦ prometheus.log: locale4 ◦ raft.log: locale5 ◦ hagroups.log: locale6 • Per i registri di accesso, la funzione inviata al server syslog esterno è "local0".
0	kern (messaggi del kernel)
1	utente (messaggi a livello utente)
2	posta
3	demone (demoni di sistema)

Facilità	Descrizione
4	auth (messaggi di sicurezza/autorizzazione)
5	syslog (messaggi generati internamente da syslogd)
6	lpr (sottosistema della stampante di linea)
7	notizie (sottosistema di notizie di rete)
8	UUCP
9	cron (demone dell'orologio)
10	sicurezza (messaggi di sicurezza/autorizzazione)
11	FTP
12	NTP
13	logaudit (revisione dei registri)
14	logalert (avviso di registro)
15	orologio (demone dell'orologio)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selezionare **Continua**.

Invia messaggi di prova

Prima di iniziare a utilizzare un server syslog esterno, è necessario richiedere a tutti i nodi della griglia di inviare messaggi di prova al server syslog esterno. Dovresti utilizzare questi messaggi di prova per convalidare l'intera infrastruttura di raccolta dei log prima di impegnarti a inviare dati al server syslog esterno.



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

Passi

- Se non si desidera inviare messaggi di prova perché si è certi che il server syslog esterno sia configurato correttamente e possa ricevere informazioni di audit da tutti i nodi della griglia, selezionare **Salta e termina**.

Un banner verde indica che la configurazione è stata salvata.

- Altrimenti, seleziona **Invia messaggi di prova** (consigliato).

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

- Se si verificano errori durante la configurazione del server syslog o in fase di esecuzione, correggerli e selezionare nuovamente **Invia messaggi di prova**.

Vedere "[Risolvere i problemi di un server syslog esterno](#)" per aiutarti a risolvere eventuali errori.

- Attendi finché non vedi un banner verde che indica che tutti i nodi hanno superato il test.
- Controllare il server syslog per verificare se i messaggi di prova 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 altrettanto rigoroso come gli altri protocolli.

- Seleziona **Interrompi e termina**.

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



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

Selezione le destinazioni delle informazioni di audit

È possibile specificare dove salvare i registri di controllo, i registri degli eventi di sicurezza e "[Registri del software StorageGRID](#)" vengono inviati.

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 trovare quale nodo ha le voci più recenti utilizzando `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.

Passi

1. Nella pagina Server di controllo e syslog, selezionare la destinazione per le informazioni di controllo.



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

Opzione	Descrizione
Solo nodi locali (predefinito)	I messaggi di controllo, i registri degli eventi di sicurezza e i registri delle applicazioni non vengono inviati ai nodi di amministrazione. Vengono invece salvati solo sui nodi che li hanno generati ("nodo locale"). Le informazioni di audit generate su ogni nodo locale vengono memorizzate in <code>/var/local/log/localaudit.log</code> . Nota: StorageGRID rimuove periodicamente i registri locali a rotazione per liberare spazio. Quando il file di registro di un nodo raggiunge 1 GB, il file esistente viene salvato e ne viene avviato uno nuovo. Il limite di rotazione per il registro è di 21 file. Quando viene creata la 22a versione del file di registro, il file di registro più vecchio viene eliminato. In media, su ogni nodo vengono archiviati circa 20 GB di dati di registro.
Nodi amministrativi/nodi locali	I messaggi di controllo vengono inviati al registro di controllo sui nodi di amministrazione, mentre i registri degli eventi di sicurezza e i registri delle applicazioni vengono archiviati sui nodi che li hanno generati. Le informazioni di audit sono archiviate nei seguenti file: <ul style="list-style-type: none">• Nodi amministrativi (primari e non primari): <code>/var/local/audit/export/audit.log</code>• Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> il file è solitamente vuoto o mancante. Potrebbe contenere informazioni secondarie, come una copia aggiuntiva di alcuni messaggi.
Server syslog esterno	Le informazioni di audit 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 è abilitata solo dopo aver configurato un server syslog esterno.

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 di amministrazione 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 è abilitata solo dopo aver configurato un server syslog esterno.

2. Seleziona **Salva**.

Viene visualizzato un messaggio di avviso.

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

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

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

Utilizzare il monitoraggio SNMP

Utilizzare il monitoraggio SNMP

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

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

Capacità

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



Vedere "[Accedi ai file MIB](#)" se vuoi scaricare i file MIB sui nodi della tua griglia.

Inizialmente, SNMP è disabilitato 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 in sola lettura per le query e può inviare due tipi di notifiche basate su eventi a un sistema di gestione:

Trappole

Le trappole sono notifiche inviate dall'agente SNMP che non richiedono la conferma da parte del sistema di gestione. Le trappole servono a notificare al sistema di gestione che si è verificato un evento all'interno StorageGRID, ad esempio l'attivazione di un avviso.

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

Informa

Le informazioni sono simili alle trappole, ma richiedono il riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un certo lasso di tempo, invia nuovamente l'informazione finché non riceve una conferma o finché 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:

- A qualsiasi livello di gravità viene attivato un avviso predefinito o personalizzato. Per sopprimere le notifiche SNMP per un avviso, è necessario "[configurare un silenzio](#)" per l'avviso. Le notifiche di avviso vengono inviate da "[mittente preferito Nodo amministratore](#)".

Ogni avviso viene mappato su uno dei tre tipi di trap in base al livello di gravità dell'avviso: activeMinorAlert, activeMajorAlert e activeCriticalAlert. Per un elenco degli avvisi che possono attivare queste trappole, vedere "[Riferimento avvisi](#)".

Supporto della versione SNMP

La tabella fornisce un riepilogo di alto livello di ciò che è supportato 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
Autenticazion e delle query	Stringa della comunità	Stringa della comunità	Modello di sicurezza basato sull'utente (USM) utente
Notifiche (TRAPPOLA e INFORMA)	Solo trappole	Intrappola e informa	Intrappola e informa
Autenticazion e delle notifiche	Comunità trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Comunità trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Utente USM per ogni destinazione trap

Limitazioni

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Permesso di accesso root](#)" .

Informazioni su questo compito

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

Tutti i nodi della griglia utilizzano la stessa configurazione SNMP.

Specificare la configurazione di base

Come primo passo, abilitare l'agente SMNP StorageGRID e fornire informazioni di base.

Passi

1. Selezionare **CONFIGURAZIONE > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina dell'agente SNMP.

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

Campo	Descrizione
Contatto di sistema	<p>Opzionale. Contatto primario per il sistema StorageGRID , restituito nei messaggi SNMP come sysContact.</p> <p>Il contatto di sistema è in genere un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID . Contatto di sistema può contenere al massimo 255 caratteri.</p>
Posizione del sistema	<p>Opzionale. Posizione del sistema StorageGRID , restituita nei messaggi SNMP come sysLocation.</p> <p>La posizione del sistema può essere qualsiasi informazione utile per identificare dove si trova il sistema StorageGRID . Ad esempio, potresti utilizzare l'indirizzo di una struttura. Questo valore si applica a tutti i nodi nel sistema StorageGRID . Posizione del sistema può contenere al massimo 255 caratteri.</p>
Abilita le notifiche dell'agente SNMP	<ul style="list-style-type: none">• Se selezionato, l'agente SNMP StorageGRID invia notifiche trap e inform.• Se non selezionato, l'agente SNMP supporta l'accesso MIB in sola lettura, ma non invia alcuna notifica SNMP.

Campo	Descrizione
Abilita trappole di autenticazione	Se selezionata, l'agente SNMP StorageGRID invia trap di autenticazione se riceve messaggi di protocollo autenticati in modo non corretto.

Inserisci stringhe di comunità

Se si utilizza SNMPv1 o SNMPv2c, compilare la sezione Stringhe della community.

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

Passi

1. Per **Community di sola lettura**, immettere facoltativamente una stringa di community per consentire l'accesso MIB di sola lettura sugli indirizzi agente IPv4 e IPv6.



Per garantire la sicurezza del tuo sistema StorageGRID , non utilizzare "public" come stringa della community. Se si lascia vuoto questo campo, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa della community.

Ogni stringa di comunità può contenere al massimo 32 caratteri e non può contenere spazi.

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

Sono consentite fino a cinque stringhe.

Crea destinazioni trappola

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

Passi

1. Nel campo **Community trap predefinita**, immettere facoltativamente la stringa della community predefinita che si desidera utilizzare per le destinazioni trap SNMPv1 o SNMPv2.

Se necessario, è possibile fornire una stringa di community diversa ("personalizzata") quando si definisce una destinazione trap specifica.

La comunità trap predefinita può contenere al massimo 32 caratteri e non può contenere spazi.

2. Per aggiungere una destinazione trap, selezionare **Crea**.
3. Selezionare la versione SNMP che verrà utilizzata per questa destinazione trap.
4. Compila il modulo Crea destinazione trappola per la versione selezionata.

SNMPv1

Se hai selezionato SNMPv1 come versione, compila questi campi.

Campo	Descrizione
Tipo	Deve essere Trap per SNMPv1.
Ospite	Un indirizzo IPv4 o IPv6 oppure un nome di dominio completo (FQDN) per ricevere la trap.
Porta	Utilizzare 162, che è la porta standard per le 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 della comunità	<p>Utilizzare la community trap predefinita, se ne è stata specificata una, oppure immettere una stringa community personalizzata per questa destinazione trap.</p> <p>La stringa community personalizzata può contenere al massimo 32 caratteri e non può contenere spazi.</p>

SNMPv2c

Se hai selezionato SNMPv2c come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trappole o informazioni.
Ospite	Un indirizzo IPv4 o IPv6 o FQDN per ricevere la trap.
Porta	Utilizzare 162, che è la porta standard per le 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 della comunità	<p>Utilizzare la community trap predefinita, se ne è stata specificata una, oppure immettere una stringa community personalizzata per questa destinazione trap.</p> <p>La stringa community personalizzata può contenere al massimo 32 caratteri e non può contenere spazi.</p>

SNMPv3

Se hai selezionato SNMPv3 come versione, compila questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trappole o informazioni.
Ospite	Un indirizzo IPv4 o IPv6 o FQDN per ricevere la trap.
Porta	Utilizzare 162, che è la porta standard per le 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 hai selezionato Trappola, verranno visualizzati solo gli utenti USM senza ID motore autorevoli. • Se hai selezionato Informa, verranno visualizzati solo gli utenti USM con ID motore autorevoli. • Se non vengono visualizzati utenti: <ol style="list-style-type: none"> i. Creare e salvare la destinazione della trappola. ii. Vai a Crea 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. Seleziona **Crea**.

La destinazione della trappola viene creata e aggiunta alla tabella.

Crea indirizzi di agenti

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

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

Passi

1. Seleziona **Crea**.
2. Inserisci 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	<p>Se questo indirizzo utilizzerà UDP o TCP.</p> <p>Per impostazione predefinita, SNMP utilizza UDP.</p>
Rete StorageGRID	<p>Su quale rete StorageGRID l'agente ascolterà.</p> <ul style="list-style-type: none"> • Reti Grid, Admin e Client: l'agente SNMP ascolterà le query su tutte e tre le reti. • Rete a griglia • Rete di amministrazione • Rete clienti <p>Nota: se si utilizza la rete client per dati non sicuri e si crea un indirizzo agente per la rete client, tenere presente che anche il traffico SNMP non sarà sicuro.</p>
Porta	<p>Facoltativamente, il numero di porta su cui l'agente SNMP deve essere in ascolto.</p> <p>La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta non utilizzato.</p> <p>Nota: quando si salva l'agente SNMP, StorageGRID apre automaticamente le porte degli indirizzi dell'agente sul firewall interno. È necessario assicurarsi che eventuali firewall esterni consentano l'accesso a queste porte.</p>

3. Seleziona **Crea**.

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

Crea 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.



Le destinazioni SNMPv3 *inform* devono avere utenti con ID motore. La destinazione SNMPv3 *trap* non può avere utenti con ID motore.

Questi passaggi non sono validi se si utilizza solo SNMPv1 o SNMPv2c.

Passi

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

Campo	Descrizione
Nome utente	<p>Un nome univoco per questo utente USM.</p> <p>I nomi utente possono contenere un massimo di 32 caratteri e non possono contenere spazi. Dopo la creazione dell'utente, non è possibile modificare il nome utente.</p>
Accesso MIB di sola lettura	Se selezionata, l'utente avrà accesso in sola lettura al MIB.
ID motore autorevole	<p>Se questo utente verrà utilizzato in una destinazione informata, l'ID motore autorevole per questo utente.</p> <p>Inserire da 10 a 64 caratteri esadecimale (da 5 a 32 byte) senza spazi. Questo valore è obbligatorio per gli utenti USM che verranno selezionati nelle destinazioni trap per le informazioni. Questo valore non è consentito per gli utenti USM che verranno selezionati nelle destinazioni delle trappole.</p> <p>Nota: questo campo non viene visualizzato se è stato selezionato Accesso MIB di sola lettura perché gli utenti USM con accesso MIB di sola lettura non possono avere ID motore.</p>
Livello di sicurezza	<p>Livello di sicurezza per l'utente USM:</p> <ul style="list-style-type: none"> • authPriv: Questo utente comunica con autenticazione e privacy (crittografia). È necessario specificare un protocollo di autenticazione e una password, nonché un protocollo di privacy e una password. • authNoPriv: Questo utente comunica con autenticazione e senza privacy (nessuna crittografia). È necessario 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 questo utente utilizzerà per l'autenticazione.
Protocollo sulla privacy	Visualizzato solo se hai selezionato authPriv e impostato sempre su AES, che è l'unico protocollo di privacy supportato.
Password	Visualizzato solo se hai selezionato authPriv . La password che questo utente utilizzerà per la privacy.

3. Seleziona **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.

Aggiorna l'agente SNMP

È possibile disattivare le notifiche SNMP, aggiornare le stringhe della community oppure aggiungere o rimuovere indirizzi degli agenti, utenti USM e destinazioni trap.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Permesso di accesso root](#)" .

Informazioni su questo compito

Vedere "[Configurare l'agente SNMP](#)" per i dettagli su ciascun campo nella pagina dell'agente SNMP. Per salvare le modifiche apportate in ogni scheda, è necessario selezionare **Salva** in fondo alla pagina.

Passi

1. Selezionare **CONFIGURAZIONE > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina dell'agente SNMP.

2. Per disabilitare l'agente SNMP su tutti i nodi della griglia, deselectare la casella di controllo **Abilita SNMP** e selezionare **Salva**.

Se si riabilita l'agente SNMP, tutte le impostazioni di configurazione SNMP precedenti verranno mantenute.

3. Facoltativamente, aggiorna le informazioni nella sezione Configurazione di base:

- a. Se necessario, aggiornare **Contatto di sistema** e **Posizione di sistema**.
- b. Facoltativamente, selezionare o deselectare la casella di controllo **Abilita notifiche agente SNMP** per controllare se l'agente SNMP StorageGRID invia notifiche trap e inform.

Se questa casella di controllo è deselectata, l'agente SNMP supporta l'accesso MIB in sola lettura, ma non invia notifiche SNMP.

- c. Facoltativamente, selezionare o deselectare la casella di controllo **Abilita trap di autenticazione** per controllare se l'agente SNMP StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo autenticati in modo non corretto.

4. Se si utilizza SNMPv1 o SNMPv2c, è possibile aggiornare o aggiungere una **community di sola lettura** nella sezione Stringhe della community.

5. Per aggiornare le destinazioni delle trappole, selezionare la scheda Destinazioni delle trappole nella sezione Altre configurazioni.

Utilizzare questa scheda per definire una o più destinazioni per le notifiche trap o informative StorageGRID . Quando si abilita l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Le notifiche standard vengono inviate anche per le entità MIB-II supportate (ad esempio, ifDown e coldStart).

Per i dettagli su cosa inserire, vedere "[Creare destinazioni trappola](#)" .

- Facoltativamente, aggiorna o rimuovi la community trap predefinita.

Se si rimuove la community trap predefinita, è necessario innanzitutto assicurarsi che tutte le destinazioni trap esistenti utilizzino una stringa community personalizzata.

- Per aggiungere una destinazione trap, selezionare **Crea**.

- Per modificare la destinazione di una trappola, selezionare il pulsante di opzione e selezionare **Modifica**.
 - Per rimuovere una destinazione trap, selezionare il pulsante di opzione e scegliere **Rimuovi**.
 - Per salvare le modifiche, seleziona **Salva** in fondo alla pagina.
6. Per aggiornare gli indirizzi degli agenti, selezionare la scheda Indirizzi degli agenti nella sezione Altre configurazioni.

Utilizzare questa scheda per specificare uno o più "indirizzi di ascolto". Questi sono gli indirizzi StorageGRID sui quali l'agente SNMP può ricevere query.

Per i dettagli su cosa inserire, vedere "[Crea indirizzi di agenti](#)" .

- Per aggiungere l'indirizzo di un agente, seleziona **Crea**.
 - Per modificare l'indirizzo di un agente, seleziona il pulsante di opzione e seleziona **Modifica**.
 - Per rimuovere l'indirizzo di un agente, seleziona il pulsante di opzione e seleziona **Rimuovi**.
 - Per salvare le modifiche, seleziona **Salva** in fondo alla 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 i dettagli su cosa inserire, vedere "[Crea utenti USM](#)" .

- Per aggiungere un utente USM, seleziona **Crea**.
- Per modificare un utente USM, selezionare il pulsante di opzione e scegliere **Modifica**.

Il nome utente di un utente USM esistente non può essere modificato. Se devi cambiare un nome utente, devi rimuovere l'utente e crearne uno nuovo.



Se aggiungi o rimuovi l'ID motore autorevole di un utente e quell'utente è attualmente selezionato per una destinazione, devi modificare o rimuovere la destinazione. 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 scegliere **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 salvare le modifiche, seleziona **Salva** in fondo alla pagina.

8. Dopo aver aggiornato la configurazione dell'agente SNMP, selezionare **Salva**.

Accedi 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 monitorare la tua rete.

Vedere "Utilizzare il monitoraggio SNMP" per ulteriori informazioni sui file SNMP e MIB.

Accedi ai file MIB

Per accedere ai file MIB, seguire questi passaggi.

Passi

1. Selezionare **CONFIGURAZIONE > Monitoraggio > Agente SNMP**.
2. Nella pagina dell'agente SNMP, seleziona il file che desideri scaricare:
 - **NETAPP-STORAGEGRID-MIB.txt**: definisce la tabella degli avvisi e le notifiche (trap) accessibili su tutti i nodi di amministrazione.
 - **ES-NETAPP-06-MIB.mib**: definisce oggetti e notifiche per appliance basate su E-Series.
 - **MIB_1_10.zip**: definisce oggetti e notifiche per appliance con 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. Ottieni l'OID della radice 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 (utilizzando paste per unire le linee):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " -- | grep 28669
```



Il `snmptranslate` comando ha molte opzioni utili per esplorare il MIB. Questo comando è disponibile su qualsiasi nodo StorageGRID .

Contenuto del file MIB

Tutti gli oggetti sono sotto l'OID StorageGRID .

Nome dell'oggetto	ID oggetto (OID)	Descrizione
		Modulo MIB per entità NetApp StorageGRID .

oggetti MIB

Nome dell'oggetto	ID oggetto (OID)	Descrizione
activeAlertCount		Numero di avvisi attivi in activeAlertTable.
TabellaAvvisiAttivi		Una tabella degli avvisi attivi in StorageGRID.

Nome dell'oggetto	ID oggetto (OID)	Descrizione
activeAlertId		L'ID dell'avviso. Unico nel set attuale di avvisi attivi.
NomeAvvisoAttivo		Il nome dell'avviso.
activeAlertInstance		Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
activeAlertSeverity		La gravità dell'allerta.
activeAlertStartTime		Data e ora in cui è stato attivato l'avviso.

Tipi di notifica (Trappole)

Tutte le notifiche includono le seguenti variabili come varbind:

- activeAlertId
- NomeAvvisoAttivo
- activeAlertInstance
- activeAlertSeverity
- activeAlertStartTime

Tipo di notifica	ID oggetto (OID)	Descrizione
activeMinorAlert		Un avviso di gravità minore
activeMajorAlert		Un avviso di grave gravità
Avviso critico attivo		Un avviso con gravità critica

Raccogli dati StorageGRID aggiuntivi

Utilizzare diagrammi 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 agli screenshot di esempio presenti in questa pagina.

Tipi di grafici

I grafici e i diagrammi riepilogano i valori di specifiche metriche e attributi StorageGRID .

La dashboard di Grid Manager include schede che riepilogano lo spazio di archiviazione disponibile per la griglia e per ciascun sito.

Data space usage breakdown

1.97 MB (0%) of 3.09 TB used overall

Site name	Data storage usage	Used space	Total space
Data Center 3	0%	621.26 KB	926.62 GB
Data Center 1	0%	798.16 KB	1.24 TB
Data Center 2	0%	552.10 KB	926.62 GB

Metadata allowed space usage breakdown

2.44 MB (0%) of 19.32 GB used in Data Center 3

Data Center 3 has the highest metadata space usage and it determines the metadata space available in the grid.

Site name	Metadata space usage	Metadata used space	Metadata allowed space
Data Center 3	0%	2.44 MB	19.32 GB

Il pannello Utilizzo dello storage nella dashboard di Tenant Manager mostra quanto segue:

- Un elenco dei bucket (S3) o dei contenitori (Swift) più grandi per il tenant
- Un grafico a barre che rappresenta le dimensioni relative dei contenitori o dei bucket più grandi
- La quantità totale di spazio utilizzato e, se è impostata una quota, la quantità e la percentuale di spazio rimanente

Dashboard

16 Buckets
[View buckets](#)

2 Platform services endpoints
[View endpoints](#)

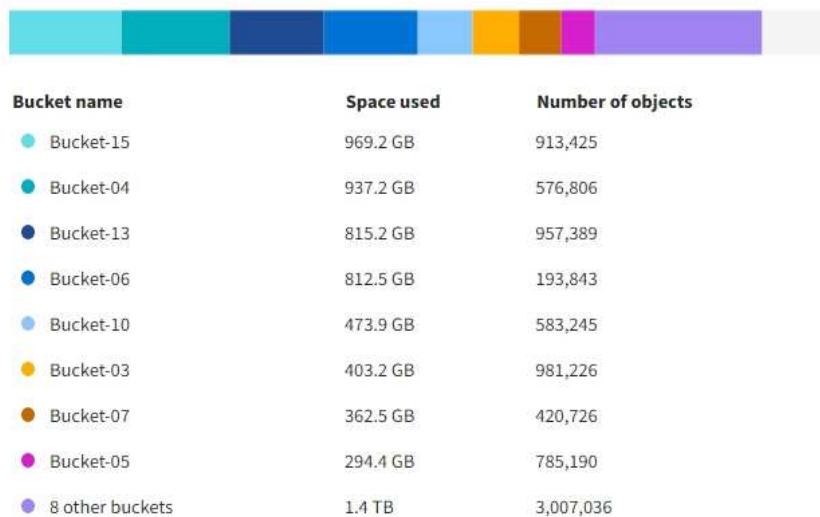
0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

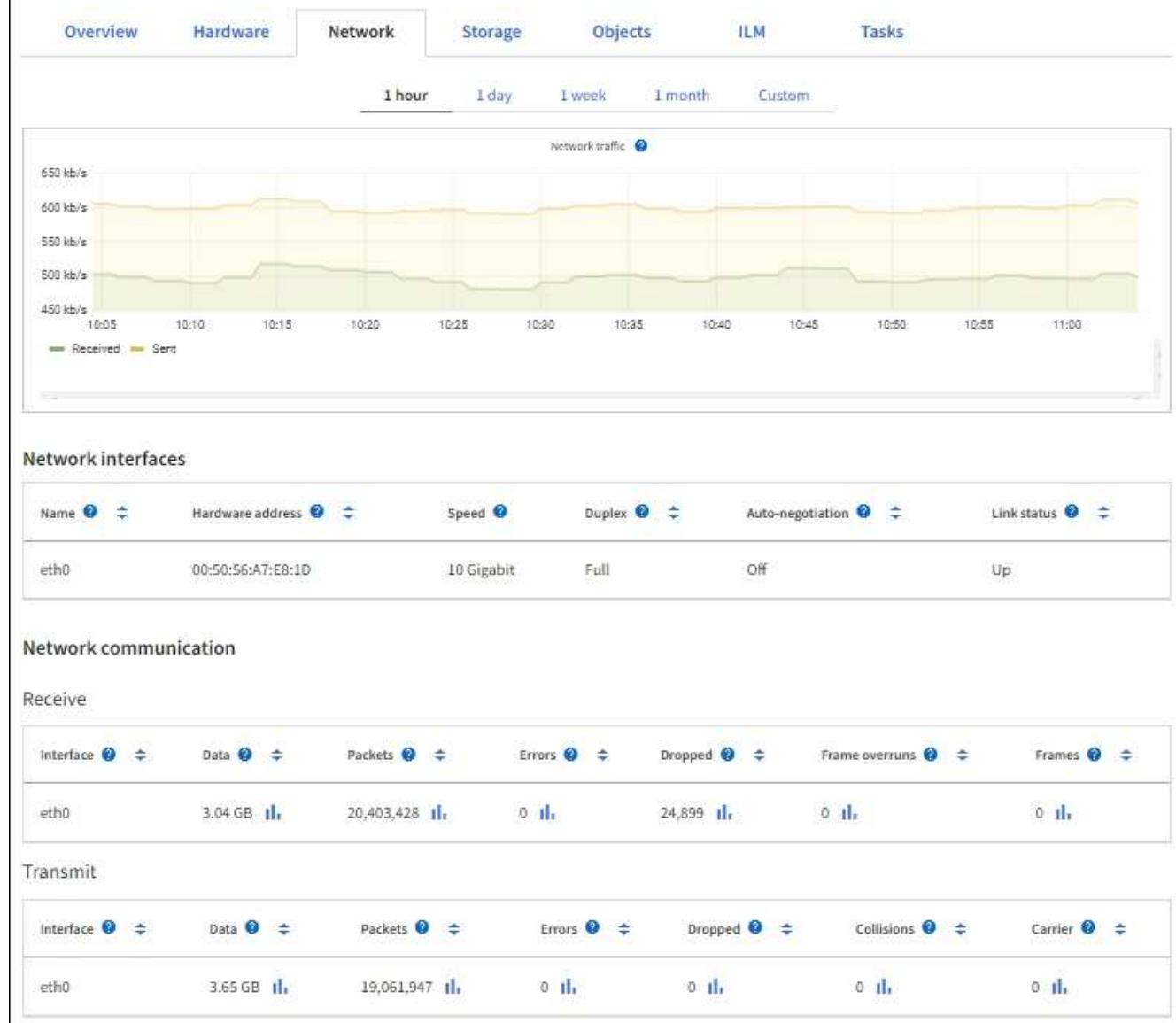
Name:	Tenant02
ID:	3341 1240 0546 8283 2208
<input checked="" type="checkbox"/> Platform services enabled	
<input checked="" type="checkbox"/> Can use own identity source	
<input checked="" type="checkbox"/> S3 Select enabled	

Inoltre, nella pagina Nodi e nella pagina **SUPPORTO > Strumenti > Topologia griglia** sono disponibili grafici che mostrano come le metriche e gli attributi StorageGRID cambiano nel tempo.

Esistono quattro tipi di grafici:

- **Grafici Grafana:** mostrati nella pagina Nodi, i grafici Grafana vengono utilizzati per tracciare i valori delle metriche di Prometheus nel tempo. Ad esempio, la scheda **NODI > Rete** per un nodo di archiviazione include un grafico Grafana per il traffico di rete.

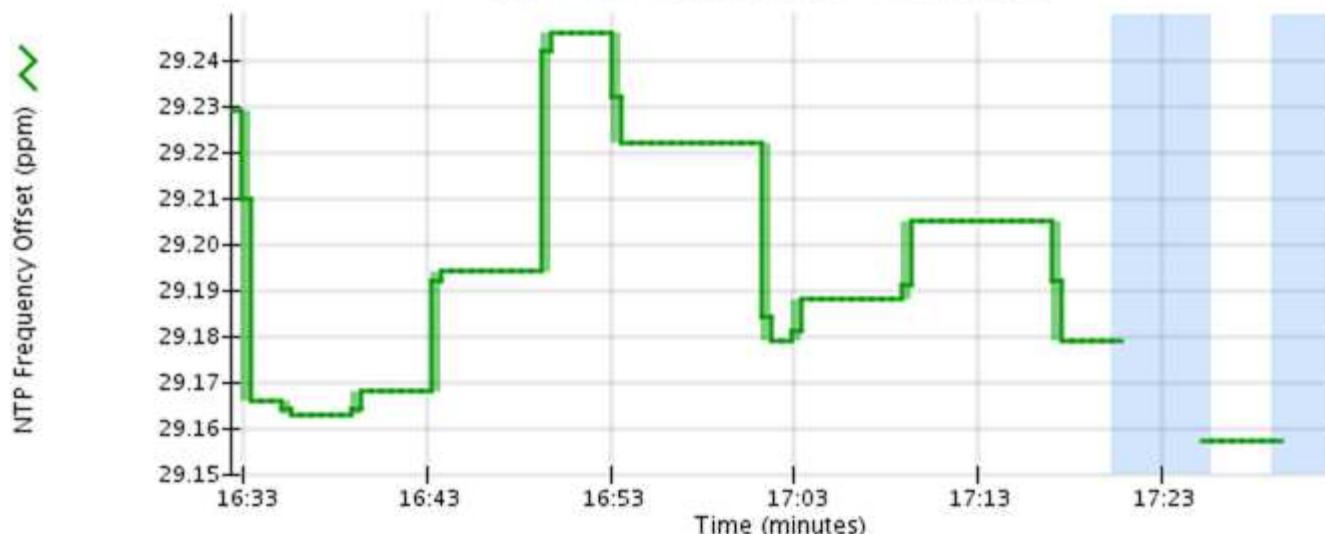
DC1-S2 (Storage Node)



I grafici Grafana sono inclusi anche nei dashboard predefiniti disponibili nella pagina **SUPPORTO > Strumenti > Metriche**.

- **Grafici lineari:** disponibili dalla pagina Nodi e dalla pagina **SUPPORTO > Strumenti > Topologia griglia** (selezionare l'icona del grafico  dopo un valore di dati), i grafici lineari vengono utilizzati per tracciare i valori degli attributi StorageGRID che hanno un valore unitario (ad esempio l'offset di frequenza NTP, in ppm). Le variazioni del valore vengono rappresentate graficamente in intervalli di dati regolari (bin) nel tempo.

NTP Frequency Offset (ppm) vs Time
2010-07-18 16:32:15 PDT to 2010-07-18 17:32:15 PDT

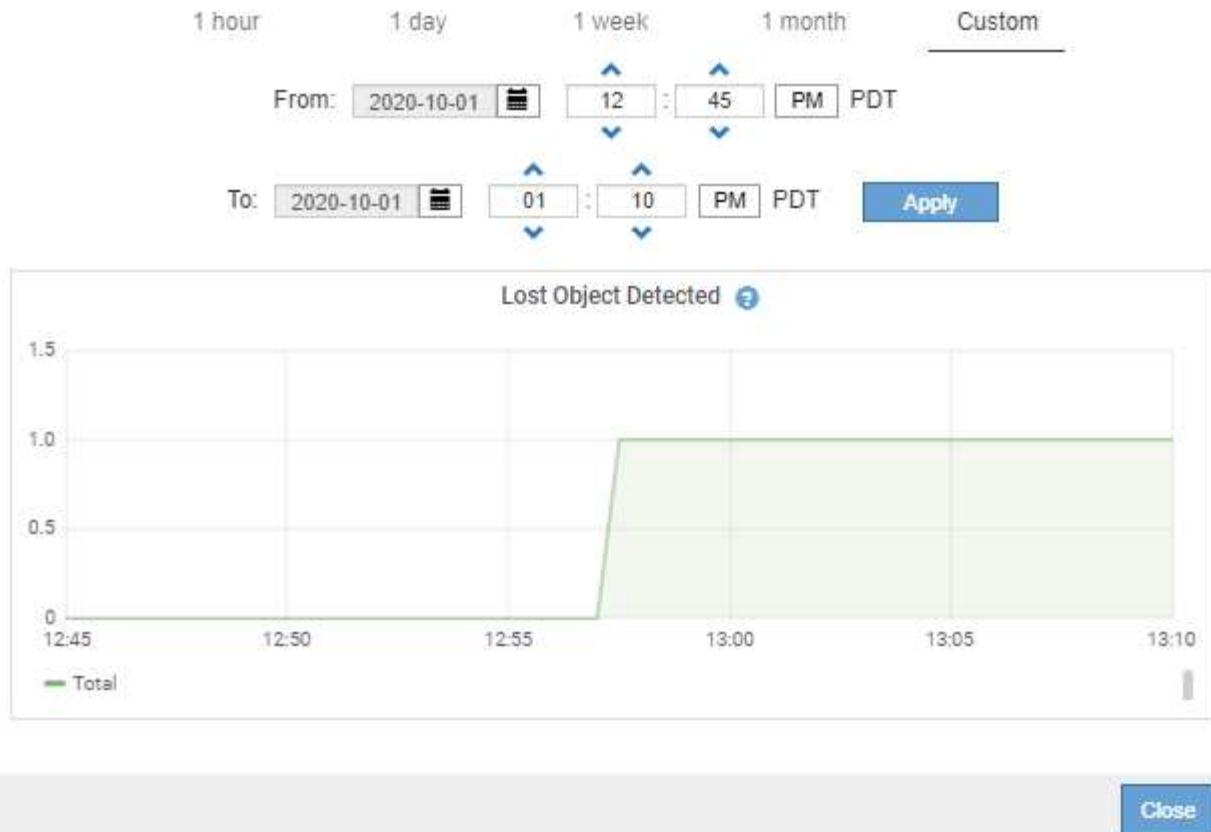


- **Grafici ad area:** disponibili dalla pagina Nodi e dalla pagina **SUPPORTO > Strumenti > Topologia griglia** (selezionare l'icona del grafico dopo un valore di dati), i grafici ad area vengono utilizzati per tracciare quantità di attributi volumetrici, come conteggi di oggetti o valori di carico del servizio. I grafici ad area sono simili ai grafici a linee, ma presentano una leggera ombreggiatura marrone sotto la linea. Le variazioni del valore vengono rappresentate graficamente in intervalli di dati regolari (bin) nel tempo.

Service Load @@ vs Time
2010-07-19 14:05:02 PDT to 2010-07-19 15:30:02 PDT

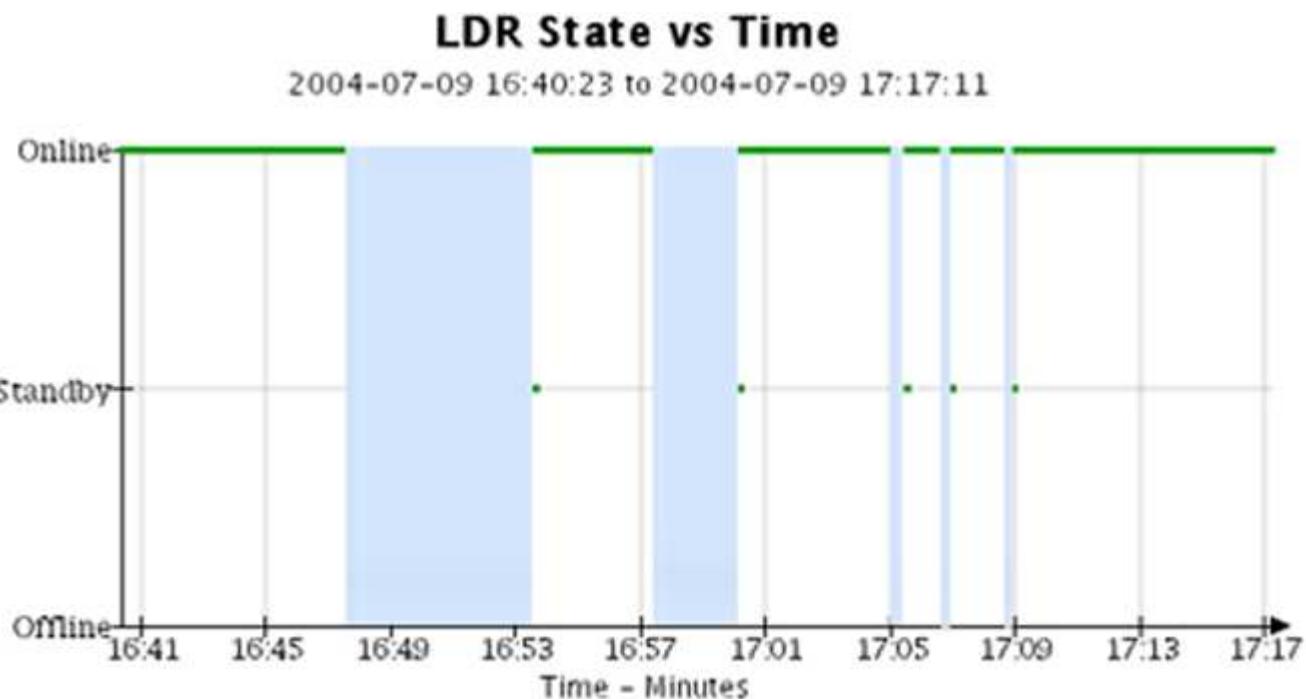


- Alcuni grafici sono contrassegnati da un diverso tipo di icona del grafico e hanno un formato diverso:



Close

- **Grafico di stato:** disponibile dalla pagina **SUPPORTO > Strumenti > Topologia griglia** (selezionare l'icona del grafico dopo un valore di dati), i grafici di stato vengono utilizzati per tracciare i valori degli attributi che rappresentano stati distinti, ad esempio uno stato di servizio che può essere online, in standby o offline. I grafici di stato sono simili ai grafici lineari, ma la transizione è discontinua, ovvero il valore salta da un valore di stato a un altro.



Informazioni correlate

- "Visualizza la pagina Nodi"
- "Visualizza l'albero della topologia della griglia"
- "Esaminare le metriche di supporto"

Legenda del grafico

Le linee e i colori utilizzati per disegnare i grafici hanno un significato specifico.

Esempio	Senso
	I valori degli attributi segnalati vengono tracciati utilizzando linee verde scuro.
	L'ombreggiatura verde chiaro attorno alle linee verde scuro indica che i valori effettivi in quell'intervallo di tempo variano e sono stati "classificati" per una rappresentazione grafica più rapida. La linea scura rappresenta la media ponderata. L'intervallo in verde chiaro indica i valori massimo e minimo all'interno del contenitore. Nei grafici ad area viene utilizzata l'ombreggiatura marrone chiaro per indicare i dati volumetrici.
	Le aree vuote (nessun dato tracciato) 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 azzurra chiara indica che alcuni o tutti i valori degli attributi in quel momento erano indeterminati; l'attributo non segnalava valori perché il servizio era in uno stato sconosciuto.
	L'ombreggiatura grigia indica che alcuni o tutti i valori degli attributi in quel momento non erano noti perché il servizio che segnalava gli attributi era amministrativamente inattivo.
	Una combinazione di ombreggiature grigie e blu indica che alcuni valori degli attributi in quel momento erano indeterminati (perché il servizio era in uno stato sconosciuto), mentre altri non erano noti perché il servizio che segnalava gli attributi era amministrativamente inattivo.

Visualizzare grafici e diagrammi

La pagina Nodi contiene i grafici e i diagrammi a cui dovresti accedere regolarmente per monitorare attributi quali capacità di archiviazione e produttività. In alcuni casi, soprattutto quando si lavora con l'assistenza tecnica, è possibile utilizzare la pagina **SUPPORTO > Strumenti > Topologia griglia** per accedere a grafici aggiuntivi.

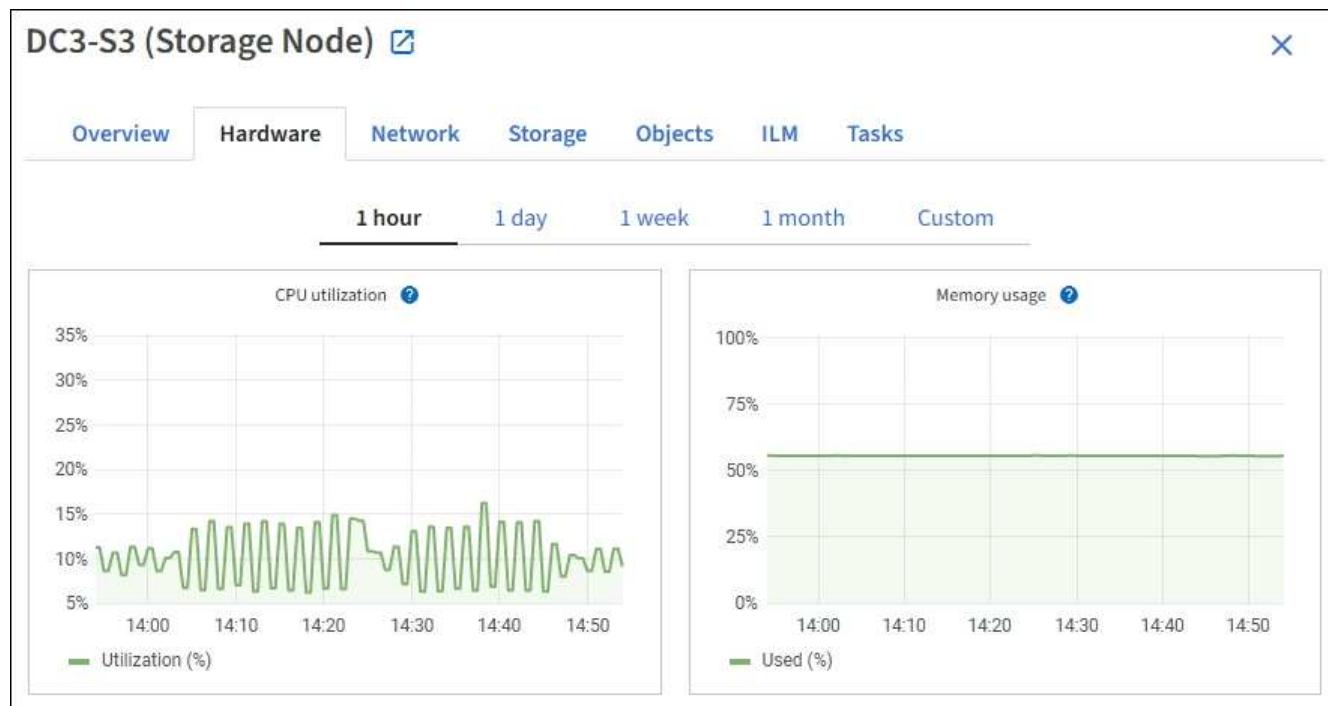
Prima di iniziare

Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .

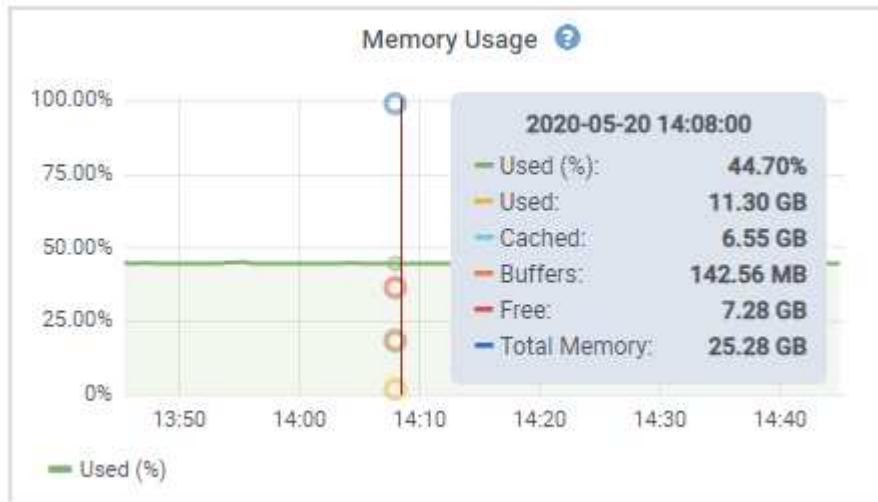
Passi

1. Selezionare **NODES**. Quindi, seleziona un nodo, un sito o l'intera griglia.
2. Seleziona la scheda di cui desideri visualizzare le informazioni.

Alcune schede includono uno o più grafici Grafana, utilizzati per tracciare i valori delle metriche di Prometheus nel tempo. Ad esempio, la scheda **NODI > Hardware** per un nodo include due grafici Grafana.



3. Facoltativamente, posiziona il cursore sul grafico per visualizzare valori più dettagliati per un determinato momento.

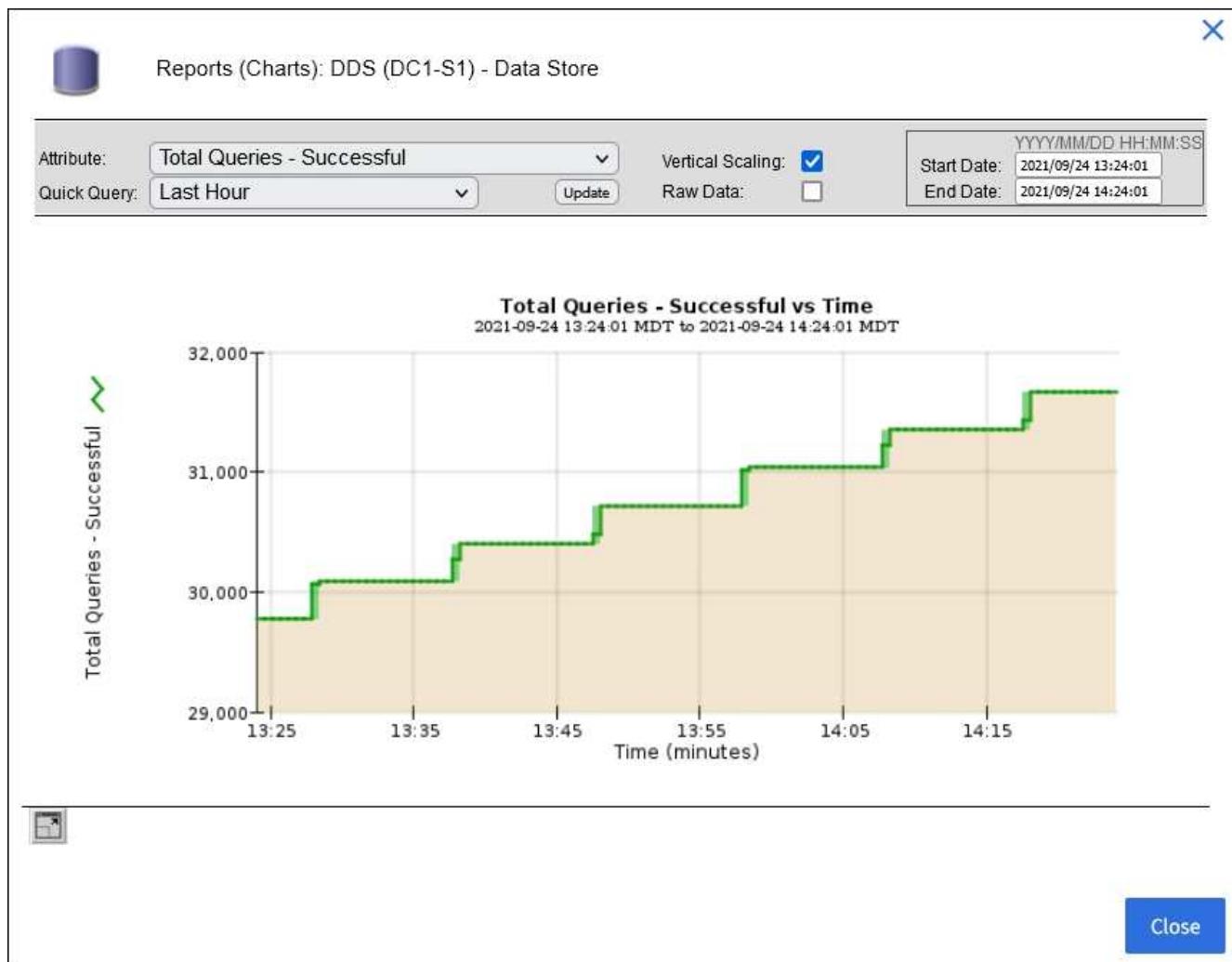


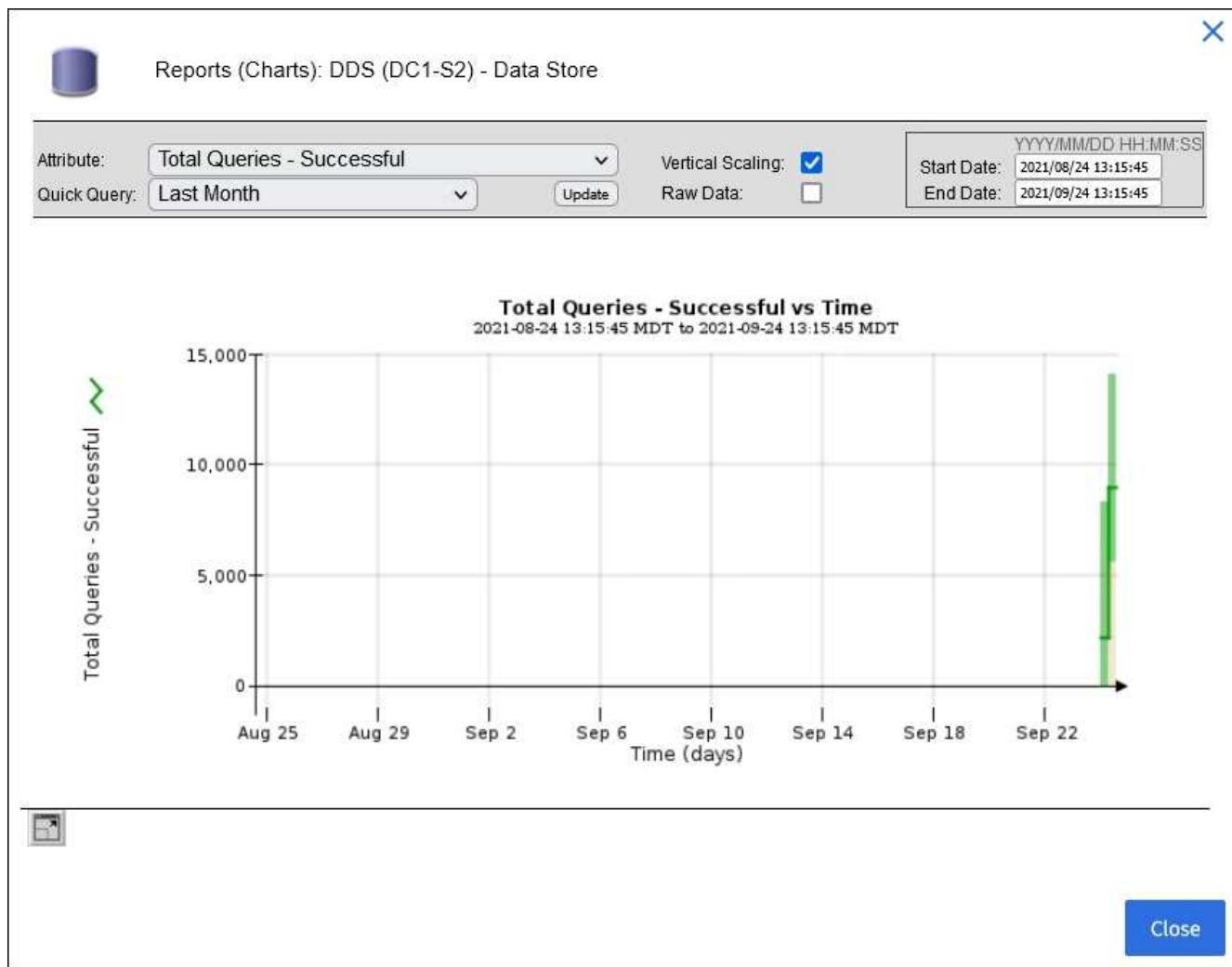
4. A seconda delle necessità, spesso è possibile visualizzare un grafico per un attributo o una metrica specifici. Dalla tabella nella pagina Nodi, seleziona l'icona del grafico a destra del nome dell'attributo.



I grafici non sono disponibili per tutte le metriche e tutti gli attributi.

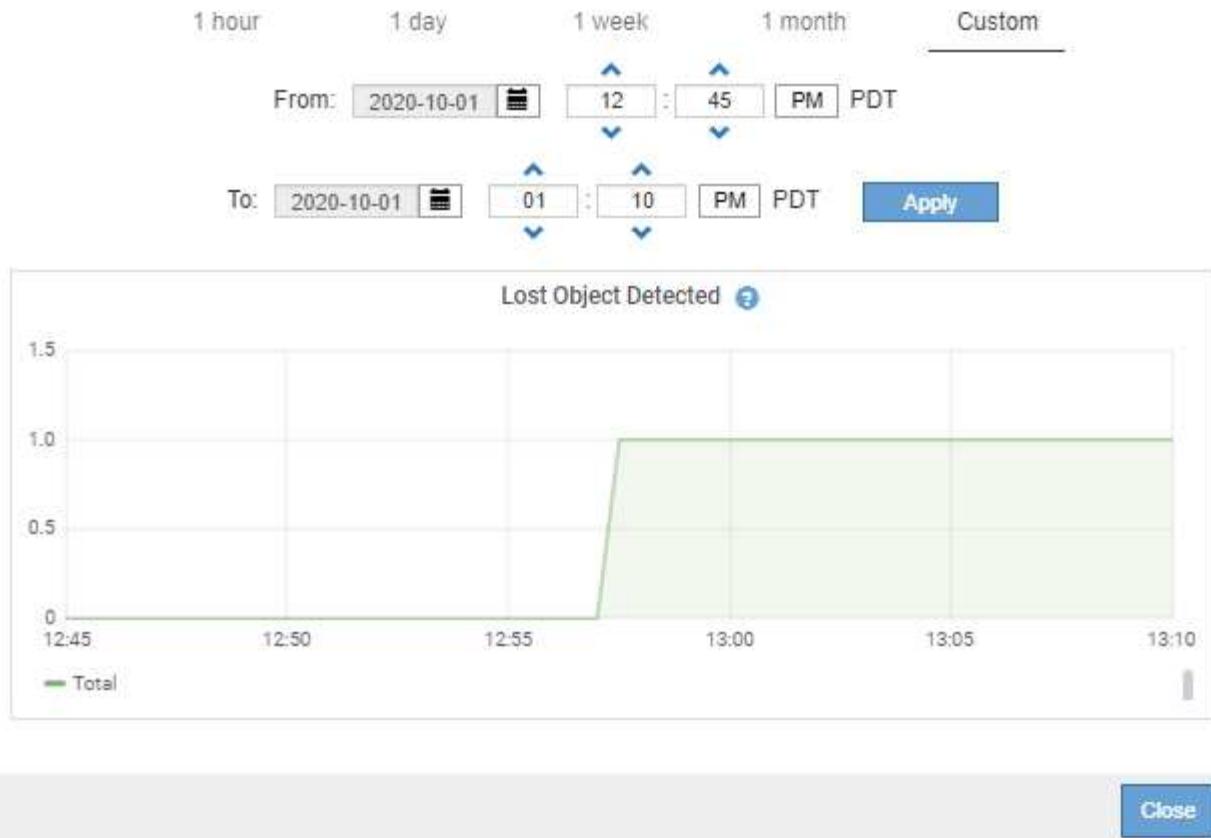
Esempio 1: dalla scheda Oggetti per un nodo di archiviazione, è possibile selezionare l'icona del grafico per visualizzare il numero totale di query di archiviazione metadati riuscite per il nodo di archiviazione.





Esempio 2: Dalla scheda Oggetti per un nodo di archiviazione, è possibile selezionare l'icona del grafico per vedere 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 per gli attributi non mostrati nella pagina Nodo, selezionare **SUPPORTO > Strumenti > Topologia griglia**.
6. Selezionare **nodo griglia > componente o servizio > Panoramica > Principale**.

The screenshot shows the 'Overview' tab selected in the top navigation bar. Below it, a 'Main' link is visible. The main content area displays 'Computational Resources' with a table showing service restarts, runtime, uptime, CPU seconds, and load. It also shows 'Memory' usage with installed and available memory. A 'Processors' table lists eight Intel Xeon E5-2630 v0 processors. On the right, there are three small status icons.

Computational Resources

Service Restarts:	1	<input checked="" type="checkbox"/>
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	<input checked="" type="checkbox"/>

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 v0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 v0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 v0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 v0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 v0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 v0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 v0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 v0 @ 2.30GHz	15 MiB

7. Seleziona l'icona del grafico accanto all'attributo.

La visualizzazione passa automaticamente alla pagina **Report > Grafici**. Il grafico mostra i dati dell'attributo nel giorno precedente.

Genera grafici

I grafici mostrano una rappresentazione grafica dei valori dei dati degli attributi. È possibile creare report su un sito di data center, un nodo di griglia, un componente o un servizio.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **nodo griglia > componente o servizio > Report > Grafici**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **Attributo**.
4. Per forzare l'asse Y a partire da zero, deselect the checkbox **Scala verticale**.
5. Per visualizzare i valori con la massima precisione, select the checkbox **Dati grezzi** oppure,

per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselectare la casella di controllo **Dati grezzi**.

6. Selezionare il periodo di tempo su cui effettuare il report dall'elenco a discesa **Query rapida**.

Selezionare l'opzione Query personalizzata per selezionare un intervallo di tempo specifico.

Il grafico appare dopo qualche istante. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni minuti.

7. Se hai selezionato Query personalizzata, personalizza il periodo di tempo per il grafico inserendo **Data di inizio e Data di fine**.

Utilizzare il formato *YYYY/MM/DDHH:MM:SS* nell'ora locale. Per rispettare il formato è necessario utilizzare gli zeri iniziali. 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 pochi secondi viene generato un grafico. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni minuti. A seconda della durata impostata per la query, viene visualizzato un report di testo grezzo o un report di testo aggregato.

Utilizzare report di testo

I report di testo mostrano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. A seconda del periodo di tempo su cui si sta effettuando il report, vengono generati due tipi di report: report di testo grezzo per periodi inferiori a una settimana e report di testo aggregato per periodi superiori a una settimana.

Rapporti di testo grezzo

Un report di testo grezzo visualizza i dettagli sull'attributo selezionato:

- Ora di ricezione: data e ora locali in cui un valore campione dei dati di un attributo è stato elaborato dal servizio NMS.
- Ora di campionamento: data e ora locali in cui un valore di attributo è stato campionato o modificato all'origine.
- 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 %

Rapporti di testo aggregati

Un report di testo aggregato visualizza i dati per un periodo di tempo più lungo (solitamente una settimana) rispetto a un report di testo grezzo. Ogni voce è il risultato della sintesi di più valori di attributi (un aggregato di valori di attributi) da parte del servizio NMS nel tempo in un'unica voce con valori medi, massimi e minimi derivati dall'aggregazione.

Ogni voce visualizza le seguenti informazioni:

- Ora aggregata: ultima data e ora locale in cui il servizio NMS ha aggregato (raccolto) un set di valori di attributi modificati.
- Valore medio: la media del valore dell'attributo nel periodo di tempo aggregato.
- Valore minimo: il valore minimo nel periodo di tempo aggregato.
- 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

Genera report di testo

I report di testo mostrano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. È possibile creare report su un sito di data center, un nodo di griglia, un componente o un servizio.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .

Informazioni su questo compito

Per i dati degli attributi che si prevede cambino continuamente, questi dati vengono campionati dal servizio NMS (alla fonte) a intervalli regolari. Per i dati degli attributi che cambiano raramente (ad esempio, dati basati su eventi quali cambiamenti di stato o di stato), un valore dell'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 era amministrativamente inattivo durante il periodo in cui è stato effettuato il campionamento. Il testo blu indica che il servizio era in uno stato sconosciuto.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **nodo griglia > componente o servizio > 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), deselect the checkbox **Dati grezzi**.
6. Selezionare il periodo di tempo su cui effettuare il report dall'elenco a discesa **Query rapida**.

Selezionare l'opzione Query personalizzata per selezionare un intervallo di tempo specifico.

Il rapporto appare dopo qualche istante. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni

minuti.

7. Se hai selezionato Query personalizzata, devi personalizzare il periodo di tempo su cui effettuare il report inserendo la **Data di inizio** e la **Data di fine**.

Utilizzare il formato YYYY/MM/DDHH:MM:SS nell'ora locale. Per rispettare il formato è necessario utilizzare gli zeri iniziali. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

8. Fare clic su **Aggiorna**.

Dopo qualche istante viene generato un report di testo. Per la tabulazione di intervalli di tempo lunghi, attendere alcuni minuti. A seconda della durata impostata per la query, viene visualizzato un report di testo grezzo o un report di testo aggregato.

Esporta report di testo

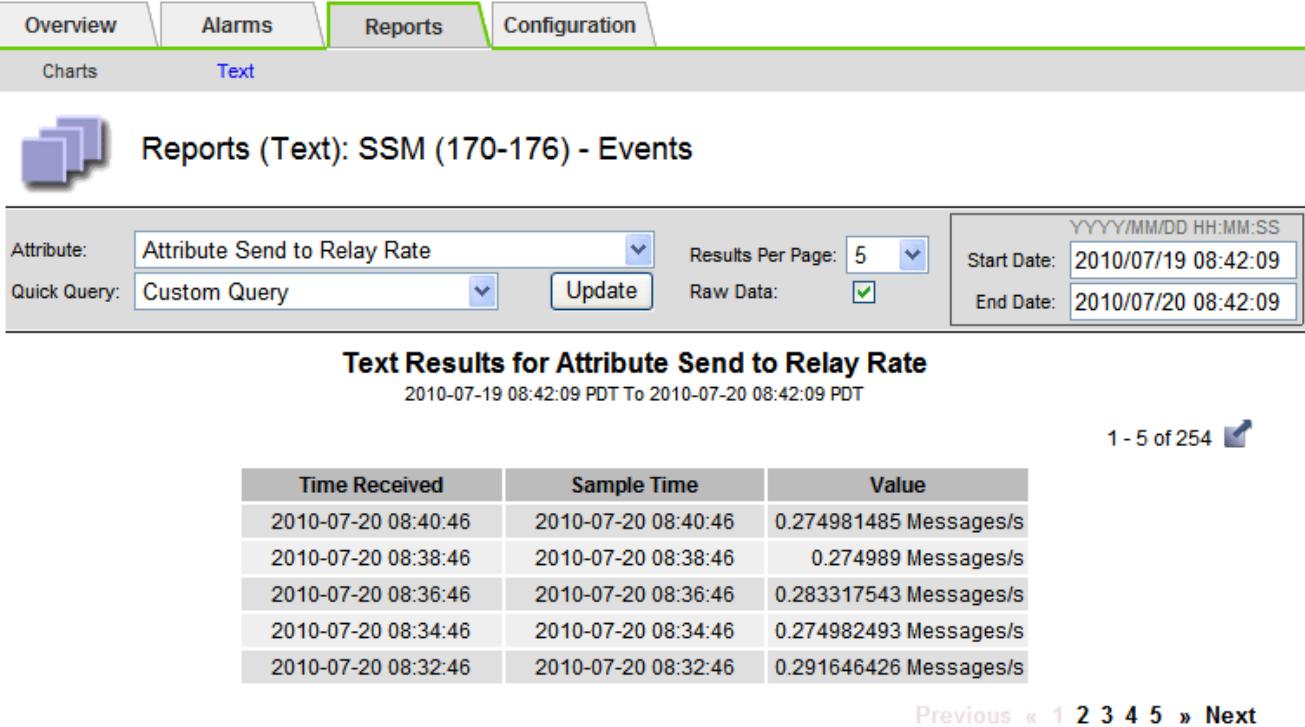
I report di testo esportati aprono una nuova scheda del browser, che consente di selezionare e copiare i dati.

Informazioni su questo compito

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 .

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Crea un report di testo.
3. Fare clic su ***Esporta*** 



The screenshot shows the StorageGRID interface with the 'Reports' tab selected. The main title is 'Reports (Text): SSM (170-176) - Events'. The left sidebar has icons for Overview, Alarms, Reports (selected), and Configuration. The top navigation bar includes 'Overview', 'Alarms', 'Reports', 'Configuration', 'Charts', and 'Text'. The report parameters are set to Attribute Send to Relay Rate, Custom Query, 5 results per page, and raw data checked. The date range is from 2010-07-19 08:42:09 PDT to 2010-07-20 08:42:09 PDT. The results table is titled 'Text Results for Attribute Send to Relay Rate' and shows the following data:

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

Pagination controls at the bottom show '1 - 5 of 254' with a link to the export icon.

Si apre la finestra Esporta report di testo che visualizza il report.

Grid ID: 000 000
 OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
 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 le prestazioni PUT e GET

È possibile monitorare le prestazioni di determinate operazioni, come l'archiviazione e il recupero di oggetti, per identificare modifiche che potrebbero richiedere ulteriori indagini.

Informazioni su questo compito

Per monitorare le prestazioni PUT e GET, è possibile eseguire i comandi S3 direttamente da una workstation oppure utilizzando l'applicazione open source S3tester. Utilizzando questi metodi è possibile valutare le prestazioni indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o problemi con una rete esterna.

Quando si eseguono test sulle operazioni PUT e GET, attenersi alle seguenti linee guida:

- Utilizza dimensioni degli oggetti paragonabili a quelle degli oggetti che solitamente inserisci nella tua griglia.
- Eseguire operazioni sia su siti locali che remoti.

Messaggi nel "[registro di controllo](#)" 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 controllo SGET. È inoltre possibile trovare l'attributo TIME nei messaggi di controllo per le seguenti operazioni S3: DELETE, GET, HEAD, Metadati aggiornati, POST, PUT

Quando si analizzano i risultati, bisogna considerare il tempo medio necessario per soddisfare una richiesta, nonché la produttività complessiva che è possibile ottenere. Ripeti regolarmente gli stessi test e registra i risultati, in modo da poter identificare le tendenze che potrebbero richiedere indagini.

- Puoi ["scarica S3tester da github"](#).

Monitorare le operazioni di verifica degli oggetti

Il sistema StorageGRID può verificare l'integrità dei dati degli oggetti sui nodi di archiviazione, controllando sia gli oggetti danneggiati che quelli mancanti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Autorizzazione di accesso alla manutenzione o alla root](#)" .

Informazioni su questo compito

Due "[processi di verifica](#)" collaborare per garantire l'integrità dei dati:

- **La verifica degli sfondi** viene eseguita automaticamente, verificando costantemente la correttezza dei dati dell'oggetto.

La verifica in background controlla automaticamente e costantemente tutti i nodi di archiviazione per determinare se sono presenti copie danneggiate di dati di oggetti replicati e codificati per la cancellazione. Se vengono rilevati problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati degli oggetti danneggiati dalle copie archiviate altrove nel sistema. La verifica in background non viene eseguita sugli oggetti in un Cloud Storage Pool.



L'avviso **Oggetto danneggiato non identificato rilevato** viene attivato se il sistema rileva un oggetto danneggiato che non può essere corretto automaticamente.

- **Il controllo dell'esistenza dell'oggetto** 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 dell'oggetto verifica se tutte le copie replicate previste degli oggetti e dei frammenti con codice di cancellazione sono presenti su un nodo di archiviazione. Il controllo dell'esistenza degli oggetti consente di verificare l'integrità dei dispositivi di archiviazione, soprattutto se un recente problema hardware potrebbe aver influito sull'integrità dei dati.

Dovresti rivedere regolarmente i risultati delle verifiche dei precedenti e dei controlli dell'esistenza degli oggetti. Indagare immediatamente su eventuali casi di dati di oggetti danneggiati o mancanti per determinarne la causa principale.

Passi

1. Esaminare i risultati delle verifiche dei precedenti:
 - a. Selezionare **NODI > Nodo di archiviazione > Oggetti**.
 - b. Controlla i risultati della verifica:
 - Per verificare la verifica dei dati degli oggetti replicati, consultare 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 verificare la verifica dei frammenti con codice di cancellazione, selezionare **Storage Node > ILM** e osservare gli attributi nella sezione Verifica del codice di cancellazione.

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

Seleziona il punto interrogativo accanto al nome di un attributo per visualizzare il testo della guida.

2. Esaminare i risultati dei processi di controllo dell'esistenza degli oggetti:
 - a. Selezionare **MANUTENZIONE > Controllo esistenza oggetto > Cronologia lavori**.
 - b. Esaminare la colonna Copie di oggetti mancanti rilevate. Se durante un processo mancano 100 o più copie di oggetti e viene attivato l'avviso **Oggetti persi**, contattare l'assistenza tecnica.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify objects defined by your ILM policy, still exist on the volumes.

The screenshot shows a user interface for performing an object existence check. At the top, there are two tabs: "Active job" (selected) and "Job history". Below the tabs is a search bar with a "Delete" button and a magnifying glass icon. The main area displays a table of completed jobs:

<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 della griglia, inclusi gli eventi personalizzati creati per tenere traccia degli eventi registrati sul server syslog. Il messaggio Ultimo evento visualizzato in Grid Manager fornisce maggiori informazioni sull'evento più recente.

I messaggi di evento sono elencati anche in `/var/local/log/bycast-err.log` file di registro. Vedi il "[Riferimento ai file di registro](#)" .

L'allarme SMTT (eventi totali) può essere attivato ripetutamente da problemi quali problemi di rete, interruzioni di corrente o aggiornamenti. Questa sezione contiene informazioni su come indagare sugli 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 reimpostare i contatori degli eventi.

Passi

1. Esaminare gli eventi di sistema per ciascun nodo della griglia:
 - a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Seleziona **site > grid node > SSM > Eventi > Panoramica > Principale**.
2. Genera un elenco di messaggi di eventi precedenti per aiutare a isolare i problemi verificatisi in passato:

a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.

b. Selezionare **site > grid node > SSM > Eventi > Report**.

c. Seleziona **Testo**.

L'attributo **Ultimo evento** non viene visualizzato in "[visualizzazione dei grafici](#)". Per visualizzarlo:

d. Cambia **Attributo** in **Ultimo evento**.

e. Facoltativamente, seleziona un periodo di tempo per **Query rapida**.

f. Selezionare **Aggiorna**.

The screenshot shows the 'Reports' tab selected in a navigation bar. Below it, a 'Text' tab is highlighted. The main area displays a title 'Reports (Text): SSM (170-41) - Events' next to a document icon. A search bar at the top includes fields for 'Attribute' (set to 'Last Event'), 'Quick Query' (set to 'Last 5 Minutes'), 'Results Per Page' (set to 20), 'Raw Data' (checkbox checked), and date/time inputs for 'Start Date' (2009/04/15 15:19:53) and 'End Date' (2009/04/15 15:24:53). Below this is a section titled 'Text Results for Last Event' with a timestamp range from 2009-04-15 15:19:53 PDT to 2009-04-15 15:24:53 PDT. A table follows, showing two rows of event data:

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)

A page number '1 - 2 of 2' and a small icon are visible at the bottom right of the table.

Crea eventi syslog personalizzati

Gli eventi personalizzati consentono di tenere traccia di tutti gli eventi utente di livello kernel, daemon, errore e critico registrati sul server syslog. Un evento personalizzato può essere utile per monitorare il verificarsi di messaggi di registro di sistema (e quindi eventi di sicurezza di rete e guasti hardware).

Informazioni su questo compito

Prendi in considerazione la creazione di eventi personalizzati per monitorare i problemi ricorrenti. Le seguenti considerazioni si applicano agli eventi personalizzati.

- Dopo aver creato un evento personalizzato, ogni sua occorrenza viene monitorata.
- Per creare un evento personalizzato basato sulle parole chiave nel /var/local/log/messages file, i registri in quei file devono essere:
 - Generato dal kernel
 - Generato dal demone o dal programma utente a livello di errore o critico

Nota: Non tutte le voci nel /var/local/log/messages file verranno abbinati a meno che non soddisfino i requisiti sopra indicati.

Passi

1. Selezionare **SUPPORTO > Allarmi (legacy) > Eventi personalizzati**.
2. Fai clic su ***Modifica*** (o ***Inserisci*** se questo non è il primo evento).

3. Inserisci una stringa di evento personalizzata, ad esempio, arresto

The screenshot shows a web-based application titled 'Events'. At the top left is a blue square icon with a white grid pattern. To its right is the word 'Events' and below it, 'Updated: 2021-10-22 11:15:34 MDT'. A horizontal line separates this from the main content area. The main area is titled 'Custom Events (1 - 1 of 1)'. It contains a table with one row. The first column is labeled 'Event' and contains the value 'shutdown'. The second column is labeled 'Actions' and contains four icons: a pencil, a plus sign, a minus sign, and a refresh symbol. Below the table are buttons for 'Show 10 ▾ Records Per Page', 'Refresh', 'Previous', '1', 'Next', and 'Apply Changes' with a blue arrow icon.

4. Selezionare **Applica modifiche**.
5. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
6. Selezionare **nodo griglia > SSM > Eventi**.
7. Individuare la voce Eventi personalizzati nella tabella Eventi e monitorare il valore per **Conteggio**.

Se il conteggio aumenta, significa che su quel nodo della griglia viene attivato un evento personalizzato che stai monitorando.

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	
Chunk Service Events	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	

Reimposta a zero il conteggio degli eventi personalizzati

Se si desidera reimpostare il contatore solo per gli eventi personalizzati, è necessario utilizzare la pagina Topologia griglia nel menu Supporto.

L'azzeramento di un contatore fa sì che l'allarme venga attivato dall'evento successivo. Al contrario, quando si riconosce un allarme, l'allarme viene riattivato solo se viene raggiunto il livello di soglia successivo.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **grid node > SSM > Eventi > Configurazione > Principale**.
3. Selezionare la casella di controllo **Reimposta** per Eventi personalizzati.

The screenshot shows the StorageGRID Management UI with the 'Configuration' tab selected. In the top navigation bar, 'Main' is highlighted under 'Alarms'. Below the navigation, there's a section titled 'Configuration: SSM (DC2-ADM1) - Events' with a last updated timestamp of '2018-04-11 10:35:44 MDT'. A purple icon representing events is visible. The main content is a table listing various event types with their counts and a 'Reset' link:

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**.

Rivedi i messaggi di audit

I messaggi di controllo possono aiutarti a comprendere meglio le operazioni dettagliate del tuo sistema StorageGRID . È possibile utilizzare i registri di controllo per risolvere i problemi e valutare le prestazioni.

Durante il normale funzionamento del sistema, tutti i servizi StorageGRID generano messaggi di controllo, come segue:

- I messaggi di controllo del sistema sono correlati al sistema di controllo 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 controllo dell'archiviazione degli oggetti sono correlati all'archiviazione e alla gestione degli oggetti all'interno StorageGRID, inclusi l'archiviazione e il recupero degli oggetti, i trasferimenti da un nodo della griglia all'altro e le verifiche.
- I messaggi di controllo di lettura e scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare, modificare o recuperare un oggetto.
- I messaggi di controllo di gestione registrano le richieste degli utenti nell'API di gestione.

Ogni nodo amministrativo memorizza i messaggi di audit in file di testo. La condivisione di controllo contiene il file attivo (audit.log) e i registri di controllo 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 registro di controllo direttamente dalla riga di comando del nodo di amministrazione.

StorageGRID può inviare informazioni di audit per impostazione predefinita, ma è possibile modificare la destinazione:

- StorageGRID utilizza per impostazione predefinita le destinazioni di controllo dei nodi locali.

- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione.
- Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno.
- ["Scopri come configurare i messaggi di controllo e le destinazioni dei log"](#) .

Per i dettagli sul file di registro di controllo, il formato dei messaggi di controllo, i tipi di messaggi di controllo e gli strumenti disponibili per analizzare i messaggi di controllo, vedere "[Esaminare i registri di controllo](#)" .

Raccogli file di registro e dati di sistema

È possibile utilizzare Grid Manager per recuperare file di registro e dati di sistema (inclusi i dati di configurazione) per il sistema StorageGRID .

Prima di iniziare

- È necessario aver effettuato l'accesso a Grid Manager sul nodo di amministrazione primario utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .
- È necessario disporre della passphrase di provisioning.

Informazioni su questo compito

Puoi usare Grid Manager per raccogliere "[file di registro](#)" , 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 puoi poi scaricare sul tuo computer locale.

Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno. Vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)" .

Passi

1. Selezionare **SUPPORTO > Strumenti > Registri**.

The screenshot shows the StorageGRID log collection interface. On the left, a tree view lists nodes under StorageGRID, specifically DC1 and DC2, with their respective sub-nodes. To the right, various parameters are set for log collection:

- Log Start Time:** 2021-12-03 06:31 AM MST
- Log End Time:** 2021-12-03 10:31 AM MST
- Log Types:**
 - Application Logs
 - Audit Logs
 - Network Trace
 - Prometheus Database
- Notes:** An empty text area.
- Provisioning Passphrase:** A yellow masked input field showing '*****'.

A large blue button labeled "Collect Logs" is located at the bottom right.

2. Selezionare i nodi della griglia per i quali si desidera raccogliere i file di registro.

A seconda delle necessità, è possibile raccogliere file di registro per l'intera griglia o per un intero sito di data center.

3. Selezionare un'**Ora di inizio** e un'**Ora di fine** per impostare l'intervallo di tempo dei dati da includere nei file di registro.

Se si seleziona un periodo di tempo molto lungo o si raccolgono i log da tutti i nodi in una griglia di grandi dimensioni, l'archivio dei log potrebbe diventare troppo grande per essere archiviato su un nodo o troppo grande per essere raccolto nel nodo di amministrazione primario per il download. In tal caso, è necessario riavviare la raccolta dei registri con un set di dati più piccolo.

4. Seleziona i tipi di log che vuoi 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 delle applicazioni disponibili.
- **Registri di controllo:** registri contenenti i messaggi di controllo generati durante il normale funzionamento del sistema.
- **Traccia di rete:** registri utilizzati per il debug di rete.
- **Database Prometheus:** Metriche delle serie temporali dai servizi su tutti i nodi.

5. Facoltativamente, inserisci delle note sui file di registro che stai raccogliendo nella casella di testo **Note**.

È possibile utilizzare queste note per fornire al supporto tecnico informazioni sul problema che ha spinto a raccogliere i file di registro. Le tue note vengono aggiunte a un file denominato `info.txt`, insieme ad

altre informazioni sulla raccolta dei file di registro. Il `info.txt` il file viene salvato nel pacchetto di archivio dei file di registro.

6. Immettere la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.
7. Seleziona **Raccogli registri**.

Quando si invia una nuova richiesta, la precedente raccolta di file di registro viene eliminata.

È possibile utilizzare la pagina Registri per monitorare l'avanzamento della raccolta dei file di registro per ciascun nodo della griglia.

Se ricevi un messaggio di errore relativo alle dimensioni del registro, prova a raccogliere i registri per un periodo di tempo più breve o per un numero inferiore di nodi.

8. Selezionare **Scarica** una volta completata la raccolta dei file di registro.

Il file `.tar.gz` contiene tutti i file di registro di tutti i nodi della griglia in cui la raccolta dei registri è riuscita. All'interno del file `.tar.gz` combinato, è presente un archivio di file di registro per ciascun nodo della griglia.

Dopo aver finito

Se necessario, puoi scaricare nuovamente il pacchetto di archiviazione del file di registro in un secondo momento.

Facoltativamente, è possibile selezionare **Elimina** per rimuovere il pacchetto di archivio del file di registro e liberare spazio su disco. Il pacchetto di archivio dei file di registro corrente verrà rimosso automaticamente la prossima volta che si raccolgono i file di registro.

Attivare manualmente un pacchetto AutoSupport

Per aiutare il supporto tecnico a risolvere i problemi del sistema StorageGRID , è possibile attivare manualmente l'invio di un pacchetto AutoSupport .

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- È necessario disporre dell'autorizzazione di accesso Root o di un'altra configurazione della griglia.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport***.
2. Nella scheda **Azioni**, seleziona **Invia AutoSupport attivato dall'utente**.

StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp . Se il tentativo ha esito positivo, i valori **Risultato più recente** e **Ultima volta riuscita** nella scheda **Risultati** vengono aggiornati. Se si verifica un problema, il valore **Risultato più recente** viene aggiornato in "Non riuscito" e StorageGRID non tenta più di inviare il pacchetto AutoSupport .

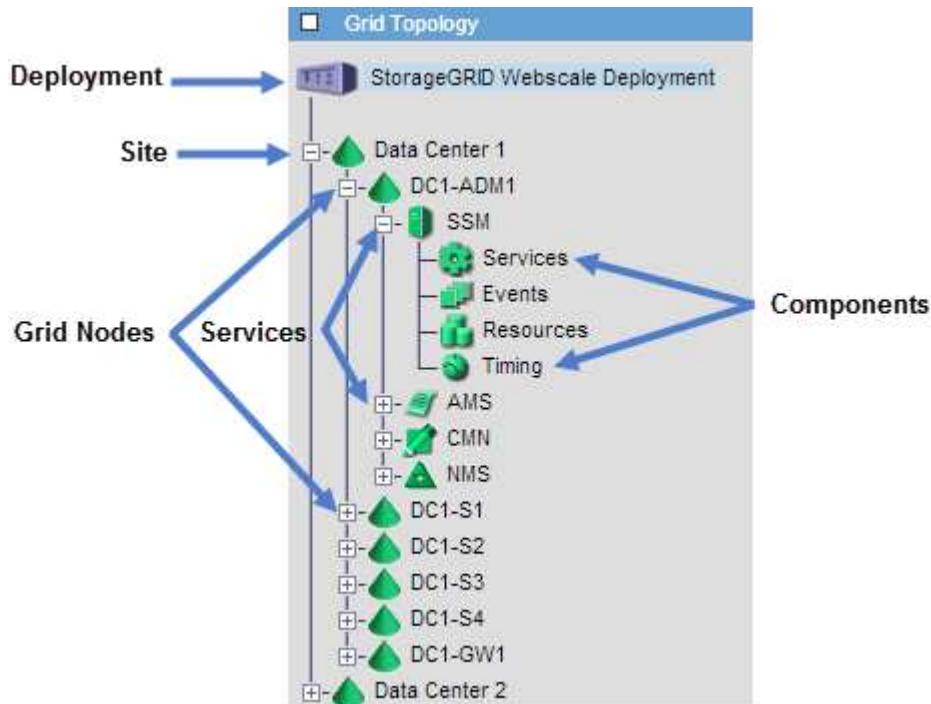


Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiorna la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Visualizza l'albero della topologia della griglia

L'albero della topologia della griglia fornisce accesso a informazioni dettagliate sugli elementi del sistema StorageGRID , inclusi siti, nodi della griglia, servizi e componenti. Nella maggior parte dei casi, è necessario accedere all'albero della topologia della griglia solo quando indicato nella documentazione o quando si lavora con il supporto tecnico.

Per accedere all'albero della topologia della griglia, selezionare **SUPPORTO > Strumenti > Topologia della griglia**.



Per espandere o comprimere l'albero della topologia della griglia, fare clic su o a livello di sito, nodo o servizio. Per espandere o comprimere tutti gli elementi nell'intero sito o in ciascun nodo, tenere premuto il tasto **<Ctrl>** e fare clic.

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, ciascun sito e l'intera griglia.

Gli attributi StorageGRID vengono utilizzati in diversi punti di Grid Manager:

- **Pagina Nodi:** molti dei valori mostrati nella pagina Nodi sono attributi StorageGRID . (Le metriche di Prometheus sono mostrate anche nelle pagine Nodi.)
- **Albero della topologia della griglia:** i valori degli attributi vengono visualizzati nell'albero della topologia della griglia (**SUPPORTO > Strumenti > Topologia della griglia**).
- **Eventi:** gli eventi di sistema si verificano quando determinati attributi registrano un errore o una condizione di guasto per un nodo, inclusi errori quali errori di rete.

Valori degli attributi

Gli attributi vengono riportati con la massima cura e sono approssimativamente corretti. In alcune circostanze, gli aggiornamenti degli attributi possono andare persi, ad esempio in caso di crash di un servizio o di errore e

ricostruzione di un nodo della griglia.

Inoltre, i ritardi di propagazione potrebbero rallentare la segnalazione degli attributi. I valori aggiornati per la maggior parte degli attributi vengono inviati al sistema StorageGRID a intervalli fissi. Possono volerci diversi minuti prima che un aggiornamento sia visibile nel sistema e due attributi che cambiano più o meno simultaneamente possono essere segnalati in momenti leggermente diversi.

Esaminare le metriche di supporto

Durante la risoluzione di un problema, puoi collaborare con il supporto tecnico per esaminare metriche e grafici dettagliati per il tuo sistema StorageGRID .

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .

Informazioni su questo compito

La pagina Metriche consente di accedere alle interfacce utente di 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'uso da parte del supporto tecnico. Alcune funzionalità e voci di menu all'interno di questi strumenti sono intenzionalmente non funzionali e sono soggette a modifiche. Vedi l'elenco di "[metriche Prometheus comunemente utilizzate](#)" .

Passi

1. Come indicato dal supporto tecnico, seleziona **SUPPORTO > Strumenti > Metriche**.

Di seguito è riportato un esempio della pagina 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://> [REDACTED]

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.

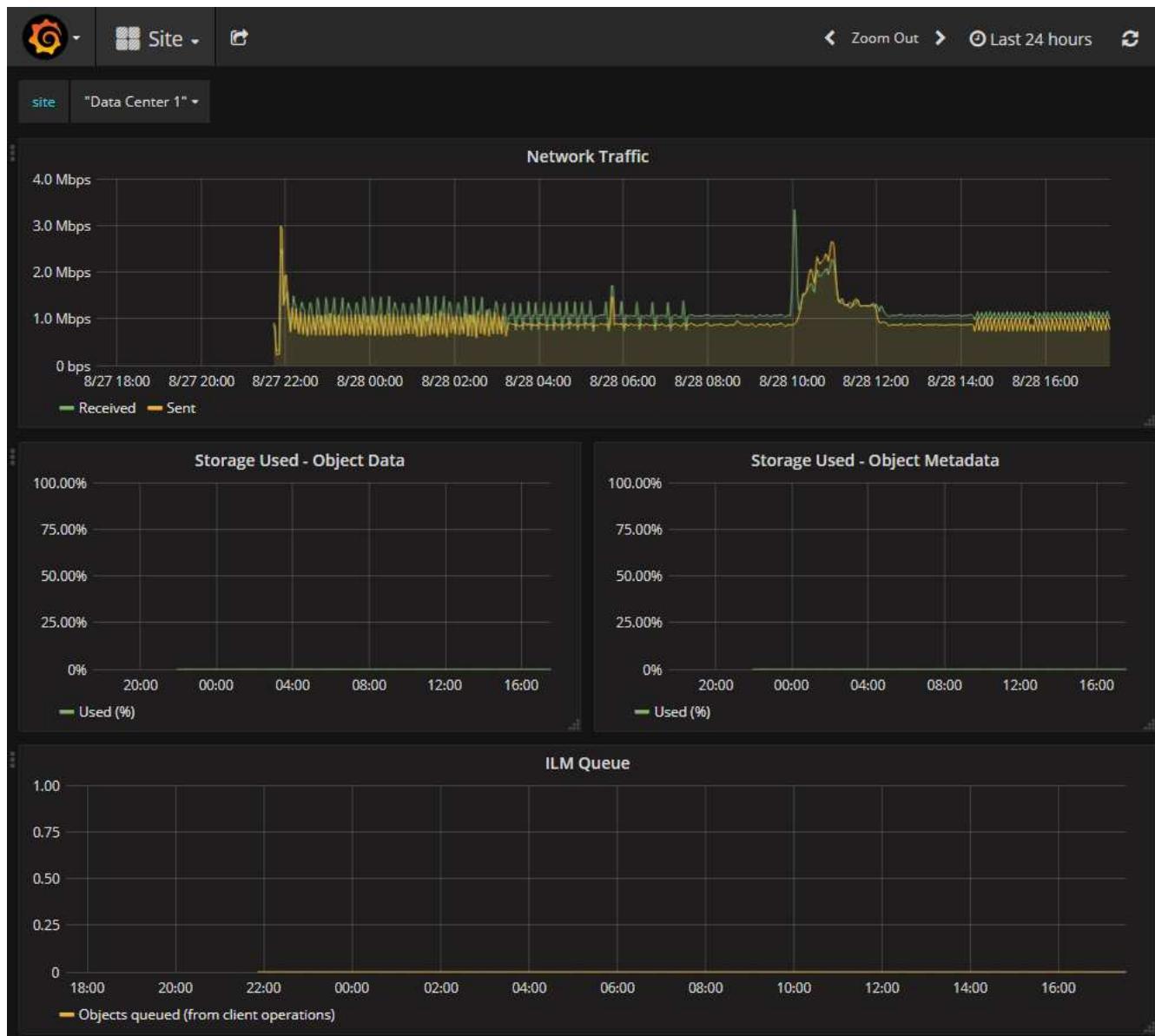
Viene visualizzata l'interfaccia di Prometheus. È possibile utilizzare questa interfaccia per eseguire query sulle metriche StorageGRID disponibili e per rappresentare graficamente le metriche StorageGRID nel tempo.



Le metriche che includono *private* nei loro nomi sono destinate esclusivamente all'uso interno e sono soggette a modifiche tra le versioni 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.



Eseguire la diagnostica

Durante la risoluzione di un problema, puoi collaborare con il supporto tecnico per eseguire la diagnostica sul tuo sistema StorageGRID e analizzare i risultati.

- ["Esaminare le metriche di supporto"](#)
- ["Metriche di Prometheus comunemente utilizzate"](#)

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai ["autorizzazioni di accesso specifiche"](#) .

Informazioni su questo compito

La pagina Diagnostica esegue una serie di controlli diagnostici sullo stato attuale della griglia. Ogni controllo diagnostico può avere uno dei tre stati:

-

- **Normale:** Tutti i valori rientrano nell'intervallo normale.
- **Attenzione:** uno o più valori sono al di fuori dell'intervallo normale.
- **Attenzione:** uno o più valori sono significativamente al di fuori dell'intervallo normale.

Gli stati diagnostici sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la rete. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato Attenzione anche se non è stato attivato alcun avviso.

Passi

1. Selezionare **SUPPORTO > Strumenti > Diagnostica**.

Viene visualizzata la pagina Diagnostica, in cui sono elencati i risultati di ciascun controllo diagnostico. I risultati sono ordinati in base alla gravità (Attenzione, Attenzione e Normale). All'interno di ogni gravità, i risultati sono ordinati alfabeticamente.

In questo esempio, tutte le diagnosi hanno uno stato Normale.

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- 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.

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.

Run Diagnostics

Cassandra automatic restarts	▼
Cassandra blocked task queue too large	▼
Cassandra commit log latency	▼
Cassandra commit log queue depth	▼

2. Per saperne di più su una diagnosi specifica, fare clic in un punto qualsiasi della riga.

Vengono visualizzati i dettagli sulla diagnosi e i suoi risultati attuali. Sono elencati i seguenti dettagli:

- **Stato:** lo stato attuale di questa diagnosi: Normale, Attenzione o Attenzione.
- **Query Prometheus:** se utilizzata per la diagnostica, l'espressione Prometheus utilizzata per generare i valori di stato. (L'espressione di Prometheus non viene utilizzata per tutte le diagnosi.)

- **Soglie:** se disponibili per la diagnosi, le soglie definite dal sistema per ogni stato diagnostico anomalo. (I valori soglia non vengono utilizzati per tutte le diagnosi.)



Non è possibile modificare queste soglie.

- **Valori di stato:** una tabella che mostra lo stato e il valore della diagnostica nell'intero sistema StorageGRID . In questo esempio viene mostrato l'utilizzo attuale 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 diagnosi 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%																																				
<table border="1"> <thead> <tr> <th>Status</th><th>Instance</th><th>CPU Utilization</th></tr> </thead> <tbody> <tr><td>✓</td><td>DC1-ADM1</td><td>2.598%</td></tr> <tr><td>✓</td><td>DC1-ARC1</td><td>0.937%</td></tr> <tr><td>✓</td><td>DC1-G1</td><td>2.119%</td></tr> <tr><td>✓</td><td>DC1-S1</td><td>8.708%</td></tr> <tr><td>✓</td><td>DC1-S2</td><td>8.142%</td></tr> <tr><td>✓</td><td>DC1-S3</td><td>9.669%</td></tr> <tr><td>✓</td><td>DC2-ADM1</td><td>2.515%</td></tr> <tr><td>✓</td><td>DC2-ARC1</td><td>1.152%</td></tr> <tr><td>✓</td><td>DC2-S1</td><td>8.204%</td></tr> <tr><td>✓</td><td>DC2-S2</td><td>5.000%</td></tr> <tr><td>✓</td><td>DC2-S3</td><td>10.469%</td></tr> </tbody> </table>		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%
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. **Facoltativo:** Per visualizzare i grafici Grafana correlati a questa diagnosi, fare clic sul collegamento **Dashboard Grafana**.

Questo collegamento non viene visualizzato per tutte le diagnosi.

Viene visualizzata la dashboard Grafana correlata. In questo esempio, viene visualizzata la dashboard del nodo che mostra l'utilizzo della CPU nel tempo per questo nodo, nonché altri grafici Grafana per il nodo.



È anche possibile accedere alle dashboard Grafana predefinite dalla sezione Grafana della pagina **SUPPORTO > Strumenti > Metriche**.



4. **Facoltativo:** Per visualizzare un grafico dell'espressione di Prometheus nel tempo, fare clic su **Visualizza in Prometheus**.

Appare un grafico di Prometeo dell'espressione utilizzata nella diagnosi.

Enable query history

```
sum by (instance) (sum by (instance, mode) (rate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

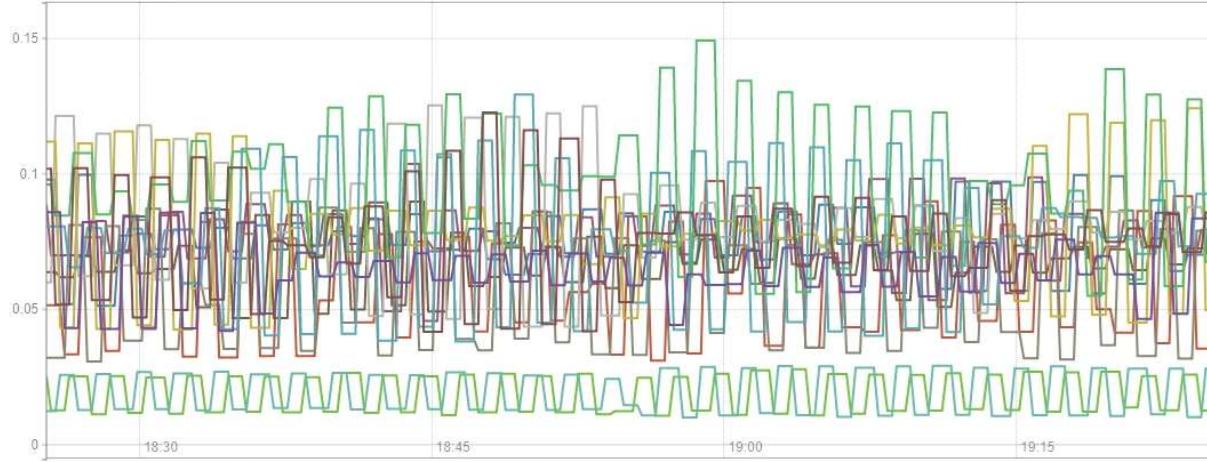
Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor -

Graph

Console

- 1h + ◀ Until ▶ Res. (s) stacked


- {instance="DC3-S3"}
- {instance="DC3-S2"}
- {instance="DC3-S1"}
- {instance="DC2-S3"}
- {instance="DC2-S2"}
- {instance="DC2-S1"}
- {instance="DC2-ADM1"}
- {instance="DC1-S3"}
- {instance="DC1-S2"}
- {instance="DC1-S1"}
- {instance="DC1-G1"}
- {instance="DC1-ARC1"}
- {instance="DC1-ADM1"}

Remove Graph

Add Graph

Crea applicazioni di monitoraggio personalizzate

È possibile creare applicazioni di monitoraggio e dashboard personalizzate utilizzando le metriche StorageGRID disponibili nell'API Grid Management.

Se si desidera monitorare metriche non visualizzate in una pagina esistente di Grid Manager o se si desidera creare dashboard personalizzate per StorageGRID, è possibile utilizzare l'API Grid Management per interrogare le metriche StorageGRID .

È anche possibile accedere direttamente alle metriche di Prometheus tramite uno strumento di monitoraggio esterno, come Grafana. Per utilizzare uno strumento esterno è necessario caricare o generare un certificato client amministrativo per consentire a StorageGRID di autenticare lo strumento per motivi di sicurezza. Vedi il "["Istruzioni per l'amministrazione StorageGRID"](#)" .

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, vai a Grid Manager. Nella parte superiore della pagina, seleziona l'icona della guida e seleziona **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 dallo scopo di questa documentazione.

Risoluzione dei problemi del sistema StorageGRID

Risoluzione dei problemi di un sistema StorageGRID

Se si verifica un problema durante l'utilizzo di un sistema StorageGRID , fare riferimento ai suggerimenti e alle linee guida in questa sezione per individuare e risolvere il problema.

Spesso è possibile risolvere i problemi autonomamente; tuttavia, potrebbe essere necessario segnalare alcuni problemi al supporto tecnico.

Definisci il problema

Il primo passo per risolvere un problema è definirlo chiaramente.

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

Domanda	Esempio di risposta
Cosa fa o non fa il sistema StorageGRID ? Quali sono i suoi sintomi?	Le applicazioni client segnalano che gli oggetti non possono essere acquisiti in StorageGRID.
Quando è iniziato il problema?	L'acquisizione di oggetti è stata negata per la prima volta intorno alle 14:50 dell'8 gennaio 2020.
Come hai notato per la prima volta il problema?	Notificato dall'applicazione client. Ho ricevuto anche notifiche di avviso via email.
Il problema si verifica regolarmente o solo a volte?	Il problema persiste.
Se il problema si verifica regolarmente, quali passaggi lo causano?	Il problema si verifica ogni volta che un client tenta di acquisire un oggetto.

Domanda	Esempio di risposta
Se il problema si verifica in modo intermittente, quando si verifica? Annota gli orari di ogni incidente di cui sei a conoscenza.	Il problema non è intermittente.
Hai già riscontrato questo problema? Con quale frequenza hai avuto questo problema in passato?	È la prima volta che vedo questo problema.

Valutare il rischio e l'impatto sul sistema

Dopo aver 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 erogando servizi essenziali.

Questa tabella riassume l'impatto che il problema di esempio sta avendo sulle operazioni del sistema:

Domanda	Esempio di risposta
Il sistema StorageGRID può acquisire contenuti?	NO.
Le applicazioni client possono recuperare contenuti?	Alcuni oggetti possono essere recuperati, altri no.
I dati sono a rischio?	NO.
La capacità di svolgere attività imprenditoriale è gravemente compromessa?	Sì, perché le applicazioni client non possono archiviare oggetti nel sistema StorageGRID e i dati non possono essere recuperati in modo coerente.

Raccogliere dati

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

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Crea una cronologia delle modifiche recenti	Le modifiche apportate al sistema StorageGRID , alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	<ul style="list-style-type: none"> • Crea una cronologia delle modifiche recenti

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Avvisi di revisione	<p>Gli avvisi possono aiutarti a determinare rapidamente la causa principale di un problema, fornendo indizi importanti sui problemi sottostanti che potrebbero esserne la causa.</p> <p>Esamina l'elenco degli avvisi correnti per verificare se StorageGRID ha identificato la causa principale di un problema.</p> <p>Per ulteriori informazioni, consultare gli avvisi attivati in passato.</p>	<ul style="list-style-type: none"> "Visualizza gli avvisi correnti e risolti"
Monitorare gli eventi	Gli eventi includono qualsiasi errore di sistema o evento di guasto per un nodo, compresi errori come gli errori di rete. Monitora gli eventi per saperne di più sui problemi o per trovare aiuto nella risoluzione dei problemi.	<ul style="list-style-type: none"> "Monitorare gli eventi"
Identificare le tendenze utilizzando grafici e report di testo	Le tendenze possono fornire indizi preziosi su quando si sono manifestati i primi problemi e possono aiutarti a capire con quale rapidità le cose stanno cambiando.	<ul style="list-style-type: none"> "Utilizzare diagrammi e grafici" "Utilizzare report di testo"
Stabilire le linee di base	Raccogliere informazioni sui livelli normali dei vari valori operativi. Questi valori di base e le deviazioni da essi possono fornire indizi preziosi.	<ul style="list-style-type: none"> "Stabilire le linee di base"
Eseguire test di ingestione e recupero	Per risolvere i problemi di prestazioni relativi all'acquisizione e al recupero, utilizzare una workstation per archiviare e recuperare gli oggetti. Confronta i risultati con quelli ottenuti utilizzando l'applicazione client.	<ul style="list-style-type: none"> "Monitorare le prestazioni PUT e GET"
Rivedi i messaggi di audit	Esaminare i messaggi di controllo per seguire in dettaglio le operazioni StorageGRID . I dettagli nei messaggi di controllo possono essere utili per risolvere molti tipi di problemi, compresi quelli relativi alle prestazioni.	<ul style="list-style-type: none"> "Rivedi i messaggi di audit"
Controllare le posizioni degli oggetti e l'integrità dell'archiviazione	Se riscontri problemi di stoccaggio, verifica che gli oggetti siano posizionati dove previsto. Verificare l'integrità dei dati degli oggetti su un nodo di archiviazione.	<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"

Tipologia di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Raccogliere dati per il supporto tecnico	L'assistenza tecnica potrebbe chiederti di raccogliere dati o di esaminare informazioni specifiche per aiutarti a risolvere i problemi.	<ul style="list-style-type: none"> • ""Raccogli file di registro e dati di sistema" • ""Attivare manualmente un pacchetto AutoSupport" • ""Esaminare le metriche di supporto"

Crea una cronologia delle modifiche recenti

Quando si verifica un problema, è opportuno considerare cosa è cambiato di recente e quando si sono verificati tali cambiamenti.

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

Crea una tabella delle modifiche recenti apportate al tuo sistema che includa informazioni su quando si è verificata ciascuna modifica e tutti i dettagli rilevanti sulla modifica, come informazioni su cos'altro stava accadendo mentre la modifica era in corso:

Tempo di cambiamento	Tipo di modifica	Dettagli
Per esempio: <ul style="list-style-type: none"> • Quando hai iniziato il ripristino del nodo? • Quando è stato completato l'aggiornamento del software? • Hai interrotto il processo? 	Quello che è successo? Che cosa hai fatto?	Documentare tutti i dettagli rilevanti relativi alla modifica. Per esempio: <ul style="list-style-type: none"> • Dettagli delle modifiche alla rete. • Quale hotfix è stato installato. • Come sono cambiati i carichi di lavoro dei clienti. Assicurati di annotare se si verificano più modifiche contemporaneamente. Ad esempio, questa modifica è stata apportata mentre era in corso un aggiornamento?

Esempi di cambiamenti significativi recenti

Ecco alcuni esempi di cambiamenti potenzialmente significativi:

- Il sistema StorageGRID è stato installato, ampliato o ripristinato di recente?
- Il sistema è stato aggiornato di recente? È stato applicato un hotfix?
- Di recente è stato riparato o cambiato qualche componente hardware?
- La politica ILM è stata aggiornata?

- Il carico di lavoro del cliente è cambiato?
- L'applicazione client o il suo comportamento sono cambiati?
- Hai modificato i bilanciatori del carico oppure aggiunto o rimosso un gruppo ad alta disponibilità di nodi amministrativi o nodi gateway?
- Sono stati avviati dei compiti che potrebbero richiedere molto tempo per essere completati? Alcuni esempi:
 - Ripristino di un nodo di archiviazione non riuscito
 - Dismissione del nodo di archiviazione
- Sono state apportate modifiche all'autenticazione utente, ad esempio l'aggiunta di un tenant o la modifica della configurazione LDAP?
- È in corso la migrazione dei dati?
- I servizi della piattaforma sono stati abilitati o modificati di recente?
- La conformità è stata abilitata di recente?
- Sono stati aggiunti o rimossi pool di archiviazione cloud?
- Sono state apportate modifiche alla compressione o alla crittografia dell'archiviazione?
- Ci sono state modifiche all'infrastruttura di rete? Ad esempio, VLAN, router o DNS.
- Sono state apportate modifiche alle fonti 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 i valori di base per il sistema registrando i livelli normali di vari valori operativi. In futuro, sarà possibile confrontare i valori attuali con questi valori di base per individuare e risolvere i valori anomali.

Proprietà	Valore	Come ottenere
Consumo medio di spazio di archiviazione	GB consumati/giorno Percentuale consumata/giorno	Vai al Grid Manager. Nella pagina Nodi, seleziona l'intera griglia o un sito e vai alla scheda Archiviazione. Nel grafico Spazio di archiviazione utilizzato - Dati oggetto, individuare un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare la quantità di spazio di archiviazione 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/giorno Percentuale consumata/giorno	Vai al Grid Manager. Nella pagina Nodi, seleziona l'intera griglia o un sito e vai alla scheda Archiviazione. Nel grafico Spazio di archiviazione utilizzato - Metadati oggetto, individuare un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare la quantità di spazio di archiviazione 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, seleziona Prestazioni > Operazioni S3 oppure Prestazioni > Operazioni Swift . Per visualizzare le velocità e i conteggi di acquisizione e recupero per un sito o un nodo specifico, selezionare NODI > sito o Nodo di archiviazione > Oggetti . Posiziona il cursore sul grafico Ingest and Retrieve per S3.
Operazioni S3/Swift non riuscite	Operazioni	Selezionare SUPPORTO > Strumenti > Topologia griglia . Nella scheda Panoramica nella sezione Operazioni API, visualizza il valore per Operazioni S3 - Non riuscite o Operazioni Swift - Non riuscite.
Tasso di valutazione ILM	Oggetti/secondo	Dalla pagina Nodi, seleziona grid > ILM . Nel grafico della coda ILM, trova un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di base per il tasso di valutazione del tuo sistema.
Frequenza di scansione ILM	Oggetti/secondo	Selezionare NODI > griglia > ILM . Nel grafico della coda ILM, trova un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di base per la velocità di scansione del tuo sistema.
Oggetti in coda dalle operazioni client	Oggetti/secondo	Selezionare NODI > griglia > ILM . Nel grafico della coda ILM, trova un periodo in cui la linea è abbastanza stabile. Posiziona il cursore sul grafico per stimare un valore di base per gli Oggetti in coda (dalle operazioni client) per il tuo sistema.

Proprietà	Valore	Come ottenere
Latenza media delle query	Millisecondi	Selezionare NODI > Nodo di archiviazione > Oggetti . Nella tabella Query, visualizza il valore per Latenza media.

Analizzare i dati

Utilizza le informazioni raccolte per determinare la causa del problema e le possibili soluzioni.

L'analisi dipende dal problema, ma in generale:

- Individua i punti di errore e i colli di bottiglia utilizzando gli avvisi.
- Ricostruire la cronologia dei problemi utilizzando la cronologia degli avvisi e i grafici.
- Utilizzare i grafici per individuare anomalie e confrontare la situazione problematica con il normale funzionamento.

Lista di controllo delle informazioni di escalation

Se non riesci a risolvere il problema da solo, contatta l'assistenza tecnica. Prima di contattare l'assistenza tecnica, raccogliere le informazioni elencate nella tabella seguente per facilitare la risoluzione dei problemi.

✓	Articolo	Note
	Enunciato del problema	<p>Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo costante o intermittente? Se si verifica in modo intermittente, in quali momenti?</p> <p>Definisci il problema</p>
	Valutazione dell'impatto	<p>Qual è la gravità del problema? Qual è l'impatto sull'applicazione client?</p> <ul style="list-style-type: none"> • Il client si è già connesso correttamente in precedenza? • Il client può acquisire, recuperare ed eliminare dati?
	ID di sistema StorageGRID	Selezionare MANUTENZIONE > Sistema > Licenza . L'ID del sistema StorageGRID viene visualizzato come parte della licenza corrente.
	Versione del software	Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona Informazioni per visualizzare la versione StorageGRID .

	Articolo	Note
	Personalizzazione	<p>Riassumi la configurazione del tuo sistema StorageGRID . Ad esempio, elenca quanto segue:</p> <ul style="list-style-type: none"> • La griglia utilizza la compressione dell'archiviazione, la crittografia dell'archiviazione o la conformità? • ILM realizza oggetti replicati o con codice di cancellazione? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano i comportamenti di ingestione Balanced, Strict o Dual Commit?
	File di registro e dati di sistema	<p>Raccogli file di registro e dati di sistema per il tuo sistema. Selezionare SUPPORTO > Strumenti > Registri.</p> <p>È possibile raccogliere i log per l'intera griglia o per nodi selezionati.</p> <p>Se si raccolgono i log solo per nodi selezionati, assicurarsi di includere almeno un nodo di archiviazione che disponga del servizio ADC. (I primi tre nodi di archiviazione in un sito includono il servizio ADC.)</p> <p>"Raccogli file di registro e dati di sistema"</p>
	Informazioni di base	<p>Raccogliere informazioni di base sulle operazioni di acquisizione, sulle operazioni di recupero e sul consumo di spazio di archiviazione.</p> <p>Stabilire le linee di base</p>
	Cronologia delle modifiche recenti	<p>Crea una cronologia che riepiloghi tutte le modifiche recenti apportate al sistema o al suo ambiente.</p> <p>Crea una cronologia delle modifiche recenti</p>
	Cronologia degli sforzi per diagnosticare il problema	<p>Se hai adottato misure per diagnosticare o risolvere autonomamente il problema, assicurati di annotare i passaggi eseguiti e il risultato.</p>

Risolvere i problemi relativi agli oggetti e all'archiviazione

Confermare le posizioni dei dati degli oggetti

A seconda del problema, potresti voler "[confermare dove vengono archiviati i dati dell'oggetto](#)" . Ad esempio, potresti voler verificare che la policy ILM funzioni come previsto e che i dati degli oggetti vengano archiviati dove previsto.

Prima di iniziare

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:

- **UUID:** Identificatore univoco universale dell'oggetto. Inserire il UUID in maiuscolo.
- **CBID:** Identificatore univoco dell'oggetto all'interno StorageGRID . È possibile ottenere il CBID di un oggetto dal registro di controllo. Inserire il CBID in maiuscolo.
- **Chiave oggetto e bucket S3:** quando un oggetto viene ingerito tramite "Interfaccia S3" , l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto.

Passi

1. Selezionare **ILM > Ricerca metadati oggetto**.
2. Digitare l'identificatore dell'oggetto nel campo **Identificatore**.

È possibile immettere un UUID, CBID, bucket S3/chiave oggetto o contenitore Swift/nome oggetto.

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

4. Seleziona **Cerca**.

IL "[risultati della ricerca dei metadati degli oggetti](#)" apparire. In questa pagina sono elencati i seguenti tipi di informazioni:

- Metadati di sistema, tra cui l'ID dell'oggetto (UUID), l'ID della 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 in cui l'oggetto è stato creato per la prima volta e la data e l'ora in cui l'oggetto è stato modificato per l'ultima volta.
- Qualsiasi coppia chiave-valore di metadati utente personalizzati associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore del tag oggetto associata all'oggetto.
- Per le copie di oggetti replicati, la posizione di archiviazione corrente di ciascuna copia.
- Per le copie di oggetti con codice di cancellazione, la posizione di archiviazione corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
- Per oggetti segmentati e oggetti multipart, un elenco di segmenti di oggetti, inclusi gli identificatori di segmento e le dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono mostrati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di archiviazione interna non elaborato. Questi metadati grezzi includono metadati di sistema interni la cui persistenza da una versione all'altra non è garantita.

L'esempio seguente mostra i risultati della ricerca dei metadati dell'oggetto per un oggetto di test S3

archiviato come due copie replicate.

System Metadata

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

Replicated Copies

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

Raw Metadata

Errori dell'archivio oggetti (volume di archiviazione)

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

È possibile visualizzare le informazioni sull'archivio oggetti per ciascun nodo di archiviazione. Gli archivi degli oggetti vengono visualizzati nella parte inferiore della pagina **NODI > Nodo di archiviazione_ > Archiviazione**.

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 vedere di più "dettagli su ciascun nodo di archiviazione", segui questi passaggi:

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **site > Storage Node > LDR > Storage > Panoramica > Principale**.

The screenshot shows the StorageGRID Management UI with the following sections:

- Storage State:** 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:** A table showing three 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 con un volume di archiviazione potrebbero riflettersi in "[avvisi sul volume di archiviazione](#)". Se un volume di archiviazione si guasta, è necessario ripararlo per ripristinare la piena funzionalità del nodo di archiviazione il prima possibile. Se necessario, puoi andare alla scheda **Configurazione** e "[posizionare il nodo di archiviazione in uno stato di sola lettura](#)" in modo che il sistema StorageGRID possa utilizzarlo per il recupero dei dati mentre ci 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 archiviazione, controllando sia gli oggetti danneggiati che quelli mancanti.

Esistono due processi di verifica: la verifica in background e il controllo dell'esistenza dell'oggetto (in precedenza denominato verifica in foreground). Lavorano insieme per garantire l'integrità dei dati. La verifica in background viene eseguita automaticamente e contantemente 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 cosa è la verifica dei precedenti?

Il processo di verifica in background controlla automaticamente e costantemente i nodi di archiviazione per individuare copie danneggiate dei dati degli oggetti e tenta automaticamente di riparare eventuali problemi

rilevati.

La verifica degli sfondi verifica l'integrità degli oggetti replicati e degli oggetti con codice di cancellazione, come segue:

- **Oggetti replicati:** se il processo di verifica in background rileva un oggetto replicato danneggiato, la copia danneggiata viene rimossa dalla sua posizione e messa in quarantena altrove nel nodo di archiviazione. Quindi, viene generata una nuova copia non danneggiata e posizionata per soddisfare i criteri ILM attivi. La nuova copia potrebbe non essere posizionata sul nodo di archiviazione utilizzato per la copia originale.



I dati degli oggetti danneggiati vengono messi in quarantena anziché essere eliminati dal sistema, in modo che sia ancora possibile accedervi. Per ulteriori informazioni sull'accesso ai dati degli oggetti in quarantena, contattare l'assistenza tecnica.

- **Oggetti con codice di cancellazione:** se il processo di verifica in background rileva che un frammento di un oggetto con codice di cancellazione è danneggiato, StorageGRID tenta automaticamente di ricostruire il frammento mancante sul posto sullo stesso nodo di archiviazione, utilizzando i dati rimanenti e i frammenti di parità. Se il frammento danneggiato non può essere ricostruito, viene effettuato 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 archiviazione. Non controlla gli oggetti in un Cloud Storage Pool. Per poter essere sottoposti alla verifica dei precedenti, gli oggetti devono avere più di quattro giorni.

La verifica degli sfondi avviene a una velocità continua, studiata per non interferire con le normali attività del sistema. La verifica dei precedenti non può essere interrotta. Tuttavia, è possibile aumentare la frequenza di verifica in background per verificare più rapidamente il contenuto di un nodo di archiviazione se si sospetta un problema.

Avvisi relativi alla verifica dei precedenti

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

Se la verifica in background non riesce a sostituire un oggetto danneggiato perché non riesce a individuarne un'altra copia, viene attivato l'avviso **Oggetti persi**.

Modificare il tasso di verifica in background

È possibile modificare la frequenza con cui la verifica in background controlla i dati degli oggetti replicati su un nodo di archiviazione se si hanno dubbi sull'integrità dei dati.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".

Informazioni su questo compito

È possibile modificare la frequenza di verifica per la verifica in background su un nodo di archiviazione:

- Adattivo: impostazione predefinita. L'attività è progettata per verificare un massimo di 4 MB/s o 10 oggetti/s (a seconda di quale valore venga superato per primo).

- Alto: la verifica dell'archiviazione procede rapidamente, a una velocità che può rallentare le normali attività del sistema.

Utilizzare il tasso di verifica elevato solo quando si sospetta che un errore hardware o software possa aver danneggiato i dati dell'oggetto. Una volta completata la verifica in background ad alta priorità, la frequenza di verifica viene automaticamente reimpostata su Adattiva.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **Nodo di archiviazione > LDR > Verifica**.
3. Selezionare **Configurazione > Principale**.
4. Vai a **LDR > Verifica > Configurazione > Principale**.
5. In Verifica in background, seleziona **Tasso di verifica > Alto o Tasso di verifica > Adatto**.

The screenshot shows the StorageGRID configuration interface. At the top, there are tabs: Overview, Alarms, Reports, and Configuration, with Configuration being the active tab. Below the tabs, a sub-menu 'Main' is visible. The main content area has a title 'Configuration: LDR (REDACTED) - Verification' with a last updated timestamp 'Updated: 2021-11-11 07:13:00 MST'. There are several configuration sections: 'Reset Missing Objects Count' with a checkbox, 'Background Verification' with a 'Verification Rate' dropdown set to 'Adaptive' (which is highlighted with a green border), 'Reset Corrupt Objects Count' with a checkbox, and 'Quarantined Objects' with a 'Delete Quarantined Objects' checkbox. At the bottom right of the configuration area is a blue 'Apply Changes' button with a circular arrow icon.

6. Fare clic su **Applica modifiche**.
7. Monitorare i risultati della verifica in background per gli oggetti replicati.
 - a. Vai a **NODI > Nodo di archiviazione > Oggetti**.
 - b. Nella sezione Verifica, monitorare i valori per **Oggetti corrotti** e **Oggetti corrotti non identificati**.

Se la verifica in background rileva dati di oggetti replicati corrotti, la metrica **Oggetti corrotti** viene incrementata e StorageGRID tenta di estrarre l'identificatore dell'oggetto dai dati, come segue:

- Se è possibile estrarre l'identificatore dell'oggetto, StorageGRID crea automaticamente una nuova copia dei dati dell'oggetto. La nuova copia può essere creata in qualsiasi punto del sistema StorageGRID che soddisfi i criteri ILM attivi.
- Se non è possibile estrarre l'identificatore dell'oggetto (perché è danneggiato), la metrica **Oggetti danneggiati non identificati** viene incrementata e viene attivato l'avviso **Oggetto danneggiato non identificato rilevato**.

- c. Se vengono rilevati dati di oggetti replicati danneggiati, contattare l'assistenza tecnica per determinare la causa principale del danneggiamento.
8. Monitorare i risultati della verifica in background per gli oggetti con codice di cancellazione.

Se la verifica in background rileva frammenti danneggiati di dati di oggetti con codice di cancellazione, l'attributo Frammenti danneggiati rilevati viene incrementato. StorageGRID esegue il ripristino ricostruendo il frammento danneggiato sul posto, sullo stesso nodo di archiviazione.

- a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **Nodo di archiviazione > LDR > Codifica di cancellazione**.
 - c. Nella tabella Risultati di verifica, monitorare l'attributo Frammenti corrotti rilevati (ECCD).
9. Dopo che gli oggetti danneggiati sono stati ripristinati automaticamente dal sistema StorageGRID , reimpostare il conteggio degli oggetti danneggiati.
- a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
 - b. Selezionare **Nodo di archiviazione > LDR > Verifica > Configurazione**.
 - c. Selezionare **Reimposta conteggio oggetti danneggiati**.
 - d. Fare clic su **Applica modifiche**.
10. Se sei sicuro che gli oggetti in quarantena non siano necessari, puoi eliminarli.



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

- a. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
- b. Selezionare **Nodo di archiviazione > LDR > Verifica > Configurazione**.
- c. Selezionare **Elimina oggetti in quarantena**.
- d. Selezionare **Applica modifiche**.

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

Il controllo dell'esistenza dell'oggetto verifica se tutte le copie replicate previste degli oggetti e dei frammenti con codice di cancellazione sono presenti su un nodo di archiviazione. Il controllo dell'esistenza dell'oggetto non verifica i dati dell'oggetto stesso (lo fa la verifica in background); fornisce invece un modo per verificare l'integrità dei dispositivi di archiviazione, soprattutto se un recente problema hardware potrebbe aver influito sull'integrità dei dati.

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

Il controllo dell'esistenza degli oggetti legge i metadati di ogni oggetto archiviato in StorageGRID e verifica l'esistenza sia delle copie replicate degli oggetti sia dei frammenti degli oggetti con codice di cancellazione. Eventuali dati mancanti vengono gestiti come segue:

- **Copie replicate:** se manca una copia dei dati dell'oggetto replicato, StorageGRID tenta automaticamente di sostituire la copia con una copia archiviata altrove nel sistema. Il nodo di archiviazione esegue una copia esistente tramite una valutazione ILM, che determinerà che l'attuale criterio ILM non viene più rispettato per questo oggetto perché manca un'altra copia. Viene generata e posizionata una nuova copia per soddisfare le policy ILM attive del sistema. Questa nuova copia potrebbe non essere collocata nella stessa posizione in cui era archiviata la copia mancante.

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

Esegui il controllo dell'esistenza dell'oggetto

È possibile creare ed eseguire un processo di controllo dell'esistenza di un oggetto alla volta. Quando si crea un processo, si selezionano i nodi di archiviazione e i volumi che si desidera verificare. Seleziona anche la coerenza del lavoro.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Autorizzazione di accesso alla manutenzione o alla root](#)" .
- Hai verificato che i nodi di archiviazione che desideri controllare siano online. Selezionare **NODI** per visualizzare la tabella dei nodi. Assicurarsi che non vengano visualizzate icone di avviso accanto al nome del nodo per i nodi che si desidera controllare.
- Hai verificato che le seguenti procedure **non** siano in esecuzione sui nodi che vuoi controllare:
 - Espansione della griglia per aggiungere un nodo di archiviazione
 - Disattivazione del nodo di archiviazione
 - Recupero di un volume di archiviazione non riuscito
 - Ripristino di un nodo di archiviazione con un'unità di sistema guasta
 - Riequilibrio della CE
 - Clonazione del nodo dell'appliance

Il controllo dell'esistenza dell'oggetto non fornisce informazioni utili mentre queste procedure sono in corso.

Informazioni su questo compito

Il completamento di un processo di controllo dell'esistenza di un oggetto può richiedere giorni o settimane, a seconda del numero di oggetti nella griglia, dei nodi e dei volumi di archiviazione selezionati e della coerenza selezionata. È possibile eseguire un solo processo alla volta, ma è possibile selezionare più nodi di archiviazione e volumi contemporaneamente.

Passi

1. Selezionare **MANUTENZIONE > Attività > Controllo esistenza oggetto**.
2. Seleziona **Crea lavoro**. Viene visualizzata la procedura guidata Crea un processo di controllo 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 **Nome nodo** nell'intestazione della colonna.
4. Selezionare **Continua**.
5. Selezionare uno o più volumi per ciascun nodo nell'elenco. È possibile cercare volumi utilizzando il numero del volume di archiviazione o il nome del nodo.

È possibile effettuare la ricerca per nome del nodo o per sito.

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

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

6. Selezionare **Continua**.
7. Selezionare la coerenza per il lavoro.

La coerenza determina quante copie dei metadati dell'oggetto vengono utilizzate per il controllo dell'esistenza dell'oggetto.

- **Strong-site**: due copie di metadati in un unico sito.
- **Strong-global**: due copie di metadati in ogni sito.
- **Tutti** (predefinito): tutte e tre le copie dei metadati in ciascun sito.

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

8. Selezionare **Continua**.
9. Rivedi e verifica le tue selezioni. È possibile selezionare **Precedente** per tornare a un passaggio precedente della procedura guidata e aggiornare le selezioni.

Viene generato un processo di controllo dell'esistenza dell'oggetto che viene eseguito finché non si verifica una delle seguenti situazioni:

- Il lavoro è completato.
- Metti in pausa o annulla il lavoro. Puoi riprendere un lavoro che hai messo in pausa, ma non puoi riprendere un lavoro che hai annullato.
- Il lavoro si blocca. Viene attivato l'avviso **Controllo esistenza oggetto bloccato**. Seguire le azioni correttive specificate per l'avviso.
- Il lavoro fallisce. Viene attivato l'avviso **Controllo esistenza oggetto fallito**. Seguire le azioni correttive specificate per l'avviso.
- Viene visualizzato il messaggio "Servizio non disponibile" o "Errore interno del server". Dopo un minuto, aggiorna la pagina per continuare a monitorare il lavoro.



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

10. Durante l'esecuzione del processo, visualizzare la scheda **Processo attivo** e annotare il valore di Copie di oggetti mancanti rilevate.

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

Se il numero di copie di oggetti mancanti rilevate è maggiore di 100, potrebbe esserci un problema con l'archiviazione del nodo di archiviazione.

Object existence check

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

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

The screenshot shows the 'Job history' tab selected in the top navigation bar. The job status is 'Accepted' with ID 2334602652907829302. A message box highlights 'Missing object copies detected 0'. The progress bar is at 0%. The consistency control is set to 'All'. The start time is 2021-11-10 14:43:02 MST. The table below lists selected nodes and their corresponding storage volumes and sites.

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 il valore di Copie di oggetti mancanti rilevate è pari a zero, non sono stati rilevati problemi. Non è richiesta alcuna azione.
- Se il valore Copie di oggetti mancanti rilevate è maggiore di zero e non è stato attivato l'avviso **Oggetti persi**, 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 il valore Copie di oggetti mancanti rilevate è maggiore di zero e viene attivato l'avviso **Oggetti persi**, l'integrità dei dati potrebbe essere compromessa. Contattare l'assistenza tecnica.
- È possibile esaminare le copie degli oggetti persi utilizzando grep per estrarre i messaggi di controllo LLST: grep LLST audit_file_name .

Questa procedura è simile a quella per "[investigare oggetti smarriti](#)" , sebbene per le copie degli oggetti si cerchi LLST invece di OLST .

12. Se per il processo è stata selezionata la coerenza strong-site o strong-global, attendere circa tre settimane per la coerenza dei metadati, quindi eseguire nuovamente il processo sugli stessi volumi.

Quando StorageGRID ha avuto il tempo di raggiungere la coerenza dei metadati per i nodi e i volumi inclusi nel processo, la riesecuzione del processo potrebbe cancellare le copie di oggetti mancanti segnalate erroneamente o determinare il controllo di copie di oggetti aggiuntive, se mancanti.

- Selezionare **MANUTENZIONE > Controllo esistenza oggetto > Cronologia lavori**.
- Determina quali lavori sono pronti per essere rieseguiti:

- i. Consultare la colonna **Ora di fine** per determinare quali lavori sono stati eseguiti più di tre settimane fa.
 - ii. Per tali lavori, scansionare la colonna Controllo coerenza per strong-site o strong-global.
- c. Selezionare la casella di controllo per ogni processo che si desidera rieseguire, quindi selezionare **Riesegui**.

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.

Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
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 (3 weeks ago)	2021-11-10 14:43:06 MST
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 (17 minutes ago)	2021-11-10 14:42:11 MST

- d. Nella procedura guidata Riesegui processi, rivedere i nodi e i volumi selezionati e la coerenza.
- e. Quando sei pronto a rieseguire i processi, seleziona **Riesegui**.

Viene visualizzata la scheda Lavoro attivo. Tutti i lavori selezionati vengono rieseguiti come un unico lavoro con la coerenza di strong-site. Nel campo **Lavori correlati** nella sezione Dettagli sono elencati gli ID dei lavori originali.

Dopo aver finito

Se hai ancora dubbi sull'integrità dei dati, vai su **SUPPORTO > Strumenti > Topologia griglia > sito > Nodo di archiviazione > LDR > Verifica > Configurazione > Principale** e aumenta la frequenza di verifica in background. La verifica in background verifica la correttezza di tutti i dati degli oggetti memorizzati e ripara eventuali problemi rilevati. Individuare e riparare i potenziali problemi il più rapidamente possibile riduce il rischio di perdita di dati.

Risoluzione dei problemi S3 PUT Avviso di dimensione dell'oggetto troppo grande

L'avviso "Dimensione oggetto S3 PUT troppo grande" viene attivato se un tenant tenta un'operazione PutObject non multipart che supera il limite di dimensione S3 di 5 GiB.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .

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

Passi

1. Vai a **CONFIGURAZIONE > Monitoraggio > Server di audit e syslog**.

2. Se le scritture client sono normali, accedere al registro di controllo:

- Entra `ssh admin@primary_Admin_Node_IP`
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: `su -`
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$ A #` .

e. Passare alla directory in cui si trovano i registri di controllo.

La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni di destinazione del controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	<code>/var/local/log/localaudit.log</code>
Nodi amministrativi/nodi locali	<ul style="list-style-type: none"> Nodi amministrativi (primari e non primari): <code>/var/local/audit/export/audit.log</code> Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> in questa modalità il file è solitamente vuoto o mancante.
Server syslog esterno	<code>/var/local/log/localaudit.log</code>

A seconda delle impostazioni di destinazione dell'audit, immettere: `cd /var/local/log O /var/local/audit/export/`

Per saperne di più, fare riferimento a "[Seleziona le destinazioni delle informazioni di audit](#)" .

f. Identificare quali tenant utilizzano oggetti di dimensioni superiori a 5 GiB.

- Entra `zgrep SPUT * | egrep "CSIZ\(\UI64\):([5-9]|1-9)[0-9]+)[0-9]{9}"`
- Per ogni messaggio di controllo nei risultati, guarda `S3AI` campo per determinare l'ID dell'account tenant. Utilizzare gli altri campi nel messaggio per determinare quale indirizzo IP è stato utilizzato dal client, dal bucket e dall'oggetto:

Codice	Descrizione
SAIP	IP sorgente

Codice	Descrizione
S3AI	ID inquilino
S3BK	Secchio
S3KY	Oggetto
CSIZ	Dimensione (byte)

Esempi 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):"060X85M40Q90Y280B7YT"][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 client non sono normali, utilizzare l'ID tenant dall'avviso per identificare il tenant:

- Vai su **SUPPORTO > Strumenti > Registri**. Raccogliere i registri delle applicazioni per il nodo di archiviazione nell'avviso. Specificare 15 minuti prima e dopo l'avviso.
- Estrarre il file e andare su `broadcast.log`:

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

- Cerca nel registro `method=PUT` e identificare il cliente nel `clientIP` campo.

Esempio broadcast.log

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

- Informare gli inquilini che la dimensione massima di PutObject è di 5 GiB e di utilizzare carichi multipart per oggetti di dimensioni superiori a 5 GiB.
- 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 richieste di lettura da un'applicazione client, verifiche in background dei dati degli oggetti replicati, rivalutazioni ILM e ripristino dei dati degli oggetti durante il ripristino di un nodo di archiviazione.

Il sistema StorageGRID utilizza le informazioni sulla posizione contenute nei metadati di un oggetto per determinare da quale posizione recuperare l'oggetto. Se non viene trovata una copia dell'oggetto nella posizione prevista, il sistema tenta di recuperare un'altra copia dell'oggetto da un'altra posizione nel sistema, presupponendo che la policy ILM contenga una regola per creare due o più copie dell'oggetto.

Se il recupero ha esito positivo, il sistema StorageGRID sostituisce la copia mancante dell'oggetto. In caso contrario, viene attivato l'avviso **Oggetti persi**, come segue:

- Per le copie replicate, se non è possibile recuperarne un'altra copia, l'oggetto viene considerato perso e viene attivato l'avviso.
- Per le copie con codice di cancellazione, se non è possibile recuperare una copia dalla posizione prevista, l'attributo ECOR (Corrupt Copies Detected) viene incrementato di uno prima che venga effettuato un tentativo di recuperare una copia da un'altra posizione. Se non viene trovata nessun'altra copia, viene attivato l'avviso.

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

Nel caso in cui i dati degli oggetti senza copie vengano persi, non esiste alcuna soluzione di recupero. Tuttavia, è necessario reimpostare il contatore degli oggetti persi per evitare che gli oggetti persi noti mascherino nuovi oggetti persi. Vedere "[Reimposta il conteggio degli oggetti persi e mancanti](#)".

Indagare sugli oggetti smarriti

Quando viene attivato l'avviso **Oggetti smarriti**, è necessario indagare immediatamente. Raccogliere informazioni sugli oggetti interessati e contattare l'assistenza tecnica.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".
- Devi avere il Passwords.txt file.

Informazioni su questo compito

L'avviso **Oggetti persi** indica che StorageGRID ritiene che non vi siano copie di un oggetto nella griglia. I dati potrebbero essere andati persi definitivamente.

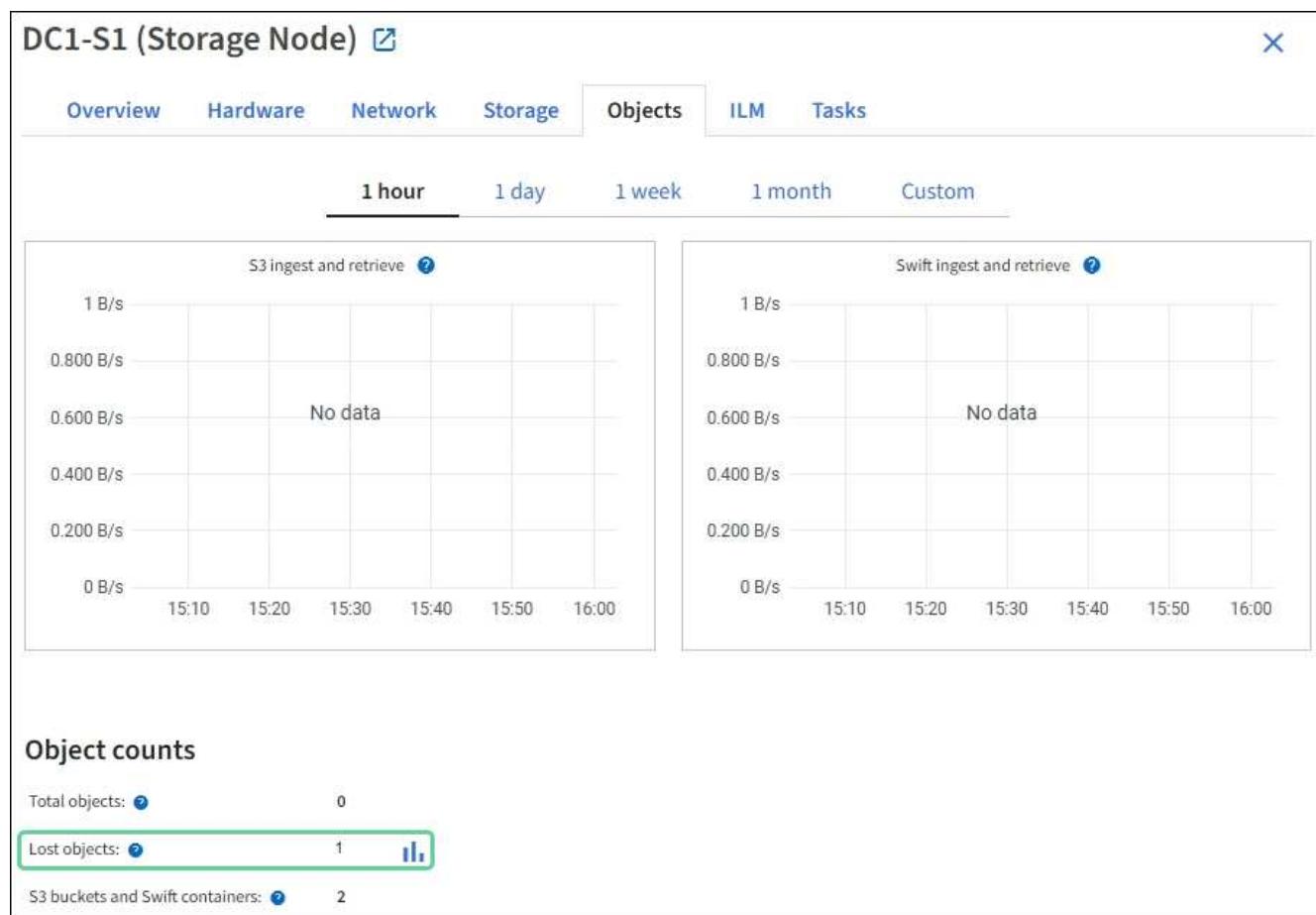
Indagare immediatamente sugli avvisi di oggetti smarriti. Potrebbe essere necessario adottare misure per evitare ulteriori perdite di dati. In alcuni casi, potresti riuscire a recuperare un oggetto smarrito se intervieni tempestivamente.

Passi

1. Selezionare **NODES**.

2. Selezionare **Nodo di archiviazione > Oggetti**.
3. Esamina il numero di oggetti smarriti mostrato nella tabella Conteggio oggetti.

Questo numero indica il numero totale di oggetti che questo nodo della griglia rileva come mancanti dall'intero sistema StorageGRID . Il valore è la somma dei contatori degli oggetti persi del componente Archivio dati all'interno dei servizi LDR e DDS.



4. Da un nodo di amministrazione, "[accedere al registro di controllo](#)" per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **Oggetti persi**:
 - a. Accedi al nodo della griglia:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Inserisci la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla root: `su -`
 - iv. Inserisci la password elencata nel `Passwords.txt` file. Quando si accede come root, il prompt cambia da `$ A #` .
 - b. Passare alla directory in cui si trovano i registri di controllo.

La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni di destinazione del controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	/var/local/log/localaudit.log
Nodi amministrativi/nodi locali	<ul style="list-style-type: none"> Nodi amministrativi (primari e non primari): /var/local/audit/export/audit.log Tutti i nodi: Il /var/local/log/localaudit.log in questa modalità il file è solitamente vuoto o mancante.
Server syslog esterno	/var/local/log/localaudit.log

A seconda delle impostazioni di destinazione dell'audit, immettere: cd /var/local/log O /var/local/audit/export/

Per saperne di più, fare riferimento a "[Seleziona le destinazioni delle informazioni di audit](#)" .

- Utilizzare grep per estrarre i messaggi di controllo Object Lost (OLST). Inserisci: grep OLST audit_file_name
- Prendere nota del valore UUID incluso nel messaggio.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5] [UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"] [NOID(UI32):12288733] [VOLI(UI64):3222345986
] [RSLT(FC32):NONE] [AVER(UI32):10]
[ATIM(UI64):1581535134780426] [ATYP(FC32):OLST] [ANID(UI32):12448208] [A
MID(FC32):ILMX] [ATID(UI64):7729403978647354233]]
```

5. Cerca i metadati dell'oggetto smarrito utilizzando l'UUID:

- Selezionare **ILM > Ricerca metadati oggetto**.
- Inserisci l'UUID e seleziona **Cerca**.
- Esaminare le posizioni nei metadati e adottare le misure appropriate:

Metadati	Conclusioni
Oggetto <identificatore_oggetto> non trovato	<p>Se l'oggetto non viene trovato, viene restituito il messaggio "ERROR""".</p> <p>Se l'oggetto non viene trovato, è possibile reimpostare il conteggio degli Oggetti persi per cancellare l'avviso. La mancanza di un oggetto indica che l'oggetto è stato eliminato intenzionalmente.</p>

Metadati	Conclusioni
Posizioni > 0	<p>Se nell'output sono elencate delle posizioni, l'avviso Oggetti persi potrebbe essere un falso positivo.</p> <p>Conferma che gli oggetti esistono. Utilizzare l'ID nodo e il percorso file elencati nell'output per confermare che il file oggetto 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 esistono, puoi reimpostare il conteggio degli Oggetti persi per cancellare l'avviso.</p>
Posizioni = 0	<p>Se nell'output non sono elencate posizioni, l'oggetto potrebbe essere mancante. Puoi provare a "cercare e ripristinare l'oggetto" oppure puoi contattare l'assistenza tecnica.</p> <p>L'assistenza tecnica potrebbe chiederti di verificare se è in corso una procedura di ripristino dell'archiviazione. Vedi le informazioni su "ripristino dei dati degli oggetti tramite Grid Manager" E "ripristino dei dati dell'oggetto su un volume di archiviazione".</p>

Cercare e ripristinare oggetti potenzialmente persi

Potrebbe essere possibile trovare e ripristinare gli oggetti che hanno attivato un avviso di **Oggetto smarrito** e un allarme legacy di Oggetti smarriti (LOST) e che hai identificato come potenzialmente smarriti.

Prima di iniziare

- Hai l'UUID di qualsiasi oggetto smarrito, come identificato in "[Indagare sugli oggetti smarriti](#)".
- Tu hai il `Passwords.txt` file.

Informazioni su questo compito

È possibile seguire questa procedura per cercare copie replicate dell'oggetto smarrito in altre parti della griglia. Nella maggior parte dei casi, l'oggetto smarrito non verrà ritrovato. Tuttavia, in alcuni casi, potresti riuscire a trovare e ripristinare un oggetto replicato perso se intervieni tempestivamente.



Per ricevere assistenza su questa procedura, contattare l'assistenza tecnica.

Passi

- Da un nodo di amministrazione, cerca nei registri di controllo le possibili posizioni degli oggetti:
 - Accedi al nodo della griglia:
 - Immettere il seguente comando: `ssh admin@grid_node_IP`
 - Inserisci la password elencata nel `Passwords.txt` file.
 - Immettere il seguente comando per passare alla root: `su -`

- iv. Inserisci la password elencata nel `Passwords.txt` file. Quando si accede come root, il prompt cambia da `$ A #`.
- b. Passare alla directory in cui si trovano i registri di controllo.

La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni di destinazione del controllo.

Opzione	Destinazione
Nodi locali (predefiniti)	<code>/var/local/log/localaudit.log</code>
Nodi amministrativi/nodi locali	<ul style="list-style-type: none"> Nodi amministrativi (primari e non primari): <code>/var/local/audit/export/audit.log</code> Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> in questa modalità il file è solitamente vuoto o mancante.
Server syslog esterno	<code>/var/local/log/localaudit.log</code>

A seconda delle impostazioni di destinazione dell'audit, immettere: `cd /var/local/log O /var/local/audit/export/`

Per saperne di più, fare riferimento a "[Seleziona le destinazioni delle informazioni di audit](#)" .

- c. Utilizzare grep per estrarre il "[messaggi di controllo associati all'oggetto potenzialmente perso](#)" e inviarli a un file di output. Inserisci: `grep uuid-value audit_file_name > output_file_name`

Per esempio:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

- d. Utilizzare grep per estrarre i messaggi di controllo LLST (Location Lost) da questo file di output. Inserisci: `grep LLST output_file_name`

Per esempio:

```
Admin: # grep LLST /var/local/tmp/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) :15815351
34379225]
[ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CLSM] [ATID (UI64) :70
86871083190743409]]
```

- e. Trovare il campo PCLD e il campo NOID nel messaggio LLST.

Se presente, il valore di PCLD è il percorso completo su disco alla copia dell'oggetto replicato mancante. Il valore di NOID è l'ID del nodo dell'LDR in cui potrebbe essere trovata una copia dell'oggetto.

Se trovi la posizione di un oggetto, potresti riuscire a ripristinarlo.

- a. Trova il nodo di archiviazione associato a questo ID nodo LDR. In Grid Manager, seleziona **SUPPORTO > Strumenti > Topologia griglia**. Quindi selezionare **Data Center > Storage Node > LDR**.

L'ID nodo per il servizio LDR si trova nella tabella Informazioni nodo. Esaminare le informazioni per ciascun nodo di archiviazione fino a trovare quello che ospita questo LDR.

2. Determinare se l'oggetto esiste sul nodo di archiviazione indicato nel messaggio di controllo:

- a. Accedi al nodo della griglia:

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

Quando si accede come root, il prompt cambia da \$ A # .

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

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

Ad esempio, inserisci:

```
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 evitare caratteri speciali.

- Se il percorso dell'oggetto non viene trovato, l'oggetto viene perso e non può essere ripristinato utilizzando questa procedura. Contattare l'assistenza tecnica.
- Se il percorso dell'oggetto viene trovato, procedere con il passaggio successivo. È possibile

provare a ripristinare l'oggetto trovato in StorageGRID.

3. Se il percorso dell'oggetto è stato trovato, provare a ripristinare l'oggetto in StorageGRID:
 - a. Dallo stesso nodo di archiviazione, modificare la proprietà del file oggetto in modo che possa essere gestito da StorageGRID. Inserisci: `chown ldr-user:bcast 'file_path_of_object'`
 - b. Per accedere alla console LDR, effettuare il login tramite Telnet a localhost 1402. Inserisci: `telnet 0 1402`
 - c. Inserisci: `cd /proc/STOR`
 - d. Inserisci: `Object_Found 'file_path_of_object'`

Ad esempio, inserisci:

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

Emissione del `Object_Found` Il comando notifica alla griglia la posizione dell'oggetto. Attiva inoltre le policy ILM attive, che creano copie aggiuntive come specificato in ciascuna policy.



Se il nodo di archiviazione in cui hai trovato l'oggetto è offline, puoi copiare l'oggetto in qualsiasi nodo di archiviazione online. Posizionare l'oggetto in una qualsiasi directory `/var/local/rangedb` del nodo di archiviazione online. Quindi, emettere il `Object_Found` comando utilizzando quel percorso file all'oggetto.

- Se l'oggetto non può essere ripristinato, il `Object_Found` il comando fallisce. Contattare l'assistenza tecnica.
- Se l'oggetto è stato ripristinato correttamente su StorageGRID, viene visualizzato un messaggio di conferma. Per 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'
```

Proseguì con il passaggio successivo.

4. Se l'oggetto è stato ripristinato correttamente in StorageGRID, verificare che siano state create le nuove posizioni:
 - a. Sign in a Grid Manager utilizzando un "[browser web supportato](#)".
 - b. Selezionare **ILM > Ricerca metadati oggetto**.
 - c. Inserisci l'UUID e seleziona **Cerca**.
 - d. Esaminare i metadati e verificare le nuove posizioni.
5. Da un nodo di amministrazione, cercare nei registri di controllo il messaggio di controllo ORLM per questo oggetto per confermare che la gestione del ciclo di vita delle informazioni (ILM) abbia inserito le copie

come richiesto.

- a. Accedi al nodo della griglia:
 - i. Immettere il seguente comando: ssh admin@grid_node_IP
 - ii. Inserisci la password elencata nel Passwords.txt file.
 - iii. Immettere il seguente comando per passare alla root: su -
 - iv. Inserisci la password elencata nel Passwords.txt file. Quando si accede come root, il prompt cambia da \$ A # .
- b. Passare alla directory in cui si trovano i registri di controllo. Fare riferimento a [sottofase 1. b](#) .
- c. Utilizzare grep per estrarre i messaggi di controllo associati all'oggetto in un file di output. Inserisci:
grep uuid-value audit_file_name > output_file_name

Per esempio:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >  
/var/local/tmp/messages_about_restored_object.txt
```

- d. Utilizzare grep per estrarre i messaggi di controllo Object Rules Met (ORLM) da questo file di output. Inserisci: grep ORLM output_file_name

Per esempio:

```
Admin: # grep ORLM /var/local/tmp/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. Trova il campo LOCS nel messaggio di controllo.

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 dell'oggetto in due posizioni nella griglia.

6. "["Azzera il conteggio degli oggetti persi e mancanti"](#) nel Grid Manager.

Reimposta il conteggio degli oggetti persi e mancanti

Dopo aver esaminato il sistema StorageGRID e verificato che tutti gli oggetti persi registrati sono andati persi definitivamente o che si tratta di un falso allarme, è possibile reimpostare il valore dell'attributo Oggetti persi su zero.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questo compito

È possibile azzerare il contatore degli oggetti smarriti 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 reimpostare il contatore dalla pagina **LDR > Data Store**.

Passi

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **Sito > Nodo di archiviazione > LDR > Archivio dati > Configurazione** per il nodo di archiviazione che presenta l'avviso **Oggetti persi** o l'allarme PERSO.
3. Seleziona **Reimposta conteggio oggetti smarriti**.

The screenshot shows the StorageGRID Grid Manager configuration interface for an LDR node. The top navigation bar has tabs: Overview, Alarms, Reports, and Configuration, with Configuration being the active tab. Below the tabs, there are two sub-tabs: Main and Alarms. The main content area displays the title 'Configuration: LDR (99-94) - Data Store' and the last updated date 'Updated: 2017-05-11 14:56:13 PDT'. There is a 'Reset Lost Objects Count' button with a small icon and an 'Apply Changes' button with a blue arrow icon.

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

L'attributo Oggetti smarriti viene reimpostato su 0 e l'avviso **Oggetti smarriti** e l'allarme SMARRITO vengono cancellati, operazione che può richiedere alcuni minuti.

5. Facoltativamente, reimpostare altri valori di attributi correlati che potrebbero essere stati incrementati durante il processo di identificazione dell'oggetto smarrito.
 - a. Selezionare **Sito > Nodo di archiviazione > LDR > Codifica di cancellazione > Configurazione**.
 - b. Selezionare **Reimposta conteggio errori di lettura** e **Reimposta conteggio copie danneggiate rilevate**.
 - c. Fare clic su **Applica modifiche**.

- d. Selezionare **Sito > Nodo di archiviazione > LDR > Verifica > Configurazione.**
- e. Selezionare **Reimposta conteggio oggetti mancanti e Reimposta conteggio oggetti danneggiati.**
- f. Se sei sicuro che gli oggetti in quarantena non siano necessari, puoi selezionare **Elimina oggetti in quarantena.**

Gli oggetti in quarantena vengono creati quando la verifica in background identifica una copia di un oggetto replicato corrotta. Nella maggior parte dei casi StorageGRID sostituisce automaticamente l'oggetto danneggiato ed è possibile eliminare in sicurezza gli oggetti in quarantena. Tuttavia, se viene attivato l'avviso **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 **Applica modifiche**, potrebbero essere necessari alcuni istanti prima che gli attributi vengano reimpostati.

Risoluzione dei problemi relativi all'avviso di spazio di archiviazione dati dell'oggetto insufficiente

L'avviso **Archiviazione dati oggetto insufficiente** monitora la quantità di spazio disponibile per l'archiviazione dei dati oggetto su ciascun nodo di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .

Informazioni su questo compito

L'avviso **Archiviazione dati oggetto insufficiente** viene attivato quando la quantità totale di dati oggetto replicati e codificati per la cancellazione 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 vera:

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

In questa condizione:

- `storagegrid_storage_utilization_data_bytes` è una stima della dimensione totale dei dati degli oggetti replicati e codificati per la cancellazione per un nodo di archiviazione.
- `storagegrid_storage_utilization_usable_space_bytes` è la quantità totale di spazio di archiviazione degli oggetti rimanente per un nodo di archiviazione.

Se viene attivato un avviso di **Archiviazione dati oggetto insufficiente**, importante o minore, è necessario eseguire una procedura di espansione il prima possibile.

Passi

1. Selezionare **AVVISI > Correnti.**

Viene visualizzata la pagina Avvisi.

2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Archiviazione dati oggetto insufficiente**, 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 notare quanto segue:

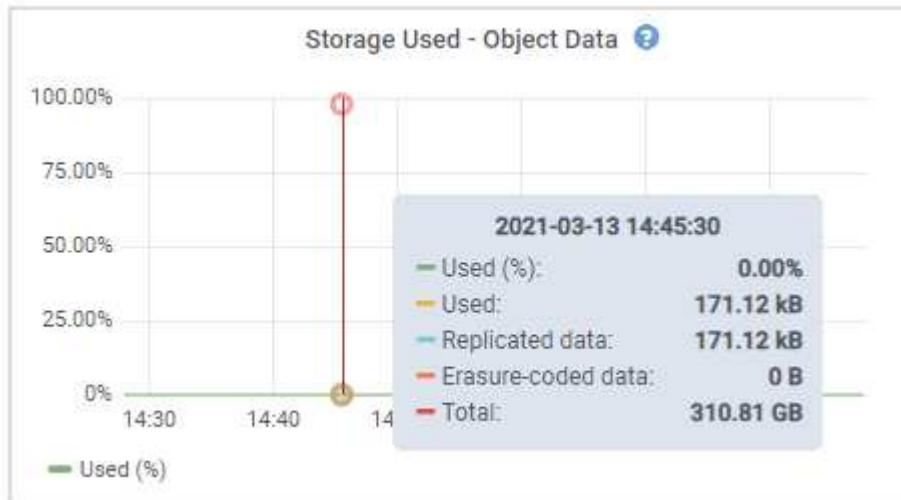
- Tempo attivato
- Il nome del sito e del nodo
- I valori correnti delle metriche per questo avviso

4. Selezionare **NODI > Nodo o sito di archiviazione_ > Archiviazione**.

5. Posiziona il cursore sul grafico Spazio di archiviazione utilizzato - Dati oggetto.

Vengono mostrati i seguenti valori:

- **Utilizzato (%)**: la percentuale dello spazio utilizzabile totale che è stata utilizzata per i dati dell'oggetto.
- **Utilizzato**: quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
- **Dati replicati**: una stima della quantità di dati di oggetti replicati su questo nodo, sito o griglia.
- **Dati con codice di cancellazione**: una stima della quantità di dati di oggetti con codice di cancellazione su questo nodo, sito o griglia.
- **Totale**: quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è il storagegrid_storage_utilization_data_bytes metrica.



6. Selezionare i controlli temporali sopra il grafico per visualizzare l'utilizzo dello spazio di archiviazione in diversi periodi di tempo.

Esaminare l'utilizzo dello spazio di archiviazione nel tempo può aiutare a capire quanto spazio di archiviazione è stato utilizzato prima e dopo l'attivazione dell'avviso e può aiutare a stimare quanto tempo potrebbe essere necessario affinché lo spazio rimanente del nodo si riempia.

7. Appena possibile, ["aggiungere capacità di archiviazione"](#) alla tua griglia.

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



Per ulteriori informazioni, consultare "Gestisci nodi di archiviazione completi".

Risoluzione dei problemi relativi agli avvisi di override della filigrana di sola lettura bassa

Se si utilizzano valori personalizzati per le filigrane del volume di archiviazione, potrebbe essere necessario risolvere l'avviso **Sostituzione filigrana di sola lettura bassa**. Se possibile, dovresti aggiornare il tuo sistema per iniziare a utilizzare i valori ottimizzati.

Nelle versioni precedenti, i tre "filigrane del volume di archiviazione" erano impostazioni globali, ovvero gli stessi valori applicati a ogni volume di archiviazione su ogni nodo di archiviazione. A partire da StorageGRID 11.6, il software è in grado di ottimizzare queste filigrane per ciascun volume di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

Quando si esegue l'aggiornamento a StorageGRID 11.6 o versione successiva, le filigrane ottimizzate di sola lettura e di lettura-scrittura vengono applicate automaticamente a tutti i volumi di archiviazione, a meno che non si verifichi una delle seguenti condizioni:

- Il sistema è prossimo alla capacità massima e non sarebbe in grado di accettare nuovi dati se fossero applicate filigrane ottimizzate. In questo caso StorageGRID non modificherà le impostazioni della filigrana.
- In precedenza hai impostato una qualsiasi delle filigrane del volume di archiviazione su un valore personalizzato. StorageGRID non sovrascriverà le impostazioni personalizzate della filigrana con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso **Sostituzione filigrana di sola lettura bassa** se il valore personalizzato per la filigrana di sola lettura software del volume di archiviazione è troppo piccolo.

Comprendere l'avviso

Se si utilizzano valori personalizzati per le filigrane del volume di archiviazione, potrebbe essere attivato l'avviso **Sostituzione filigrana di sola lettura bassa** per uno o più nodi di archiviazione.

Ogni istanza dell'avviso indica che il valore personalizzato della filigrana di sola lettura software 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 disponibile sul nodo di archiviazione potrebbe esaurirsi prima di poter passare in sicurezza allo stato di sola lettura. Alcuni volumi di archiviazione potrebbero diventare inaccessibili (smontati automaticamente) quando il nodo raggiunge la capacità massima.

Ad esempio, supponiamo di aver precedentemente impostato la filigrana di sola lettura software del volume di archiviazione su 5 GB. Supponiamo ora che StorageGRID abbia calcolato i seguenti valori ottimizzati per i quattro volumi di archiviazione nel nodo di archiviazione A:

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

L'avviso **Sostituzione filigrana di sola lettura bassa** viene attivato per il nodo di archiviazione A perché la filigrana personalizzata (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 disponibile sul nodo potrebbe esaurirsi prima di poter passare in sicurezza allo stato di sola lettura.

Risolvi l'avviso

Seguire questi passaggi se sono stati attivati uno o più avvisi di **sostituzione della filigrana di sola lettura bassa**. Puoi utilizzare queste istruzioni anche se attualmente utilizzi impostazioni di filigrana personalizzate e desideri iniziare a utilizzare impostazioni ottimizzate anche se non sono stati attivati avvisi.

Prima di iniziare

- Hai completato l'aggiornamento a StorageGRID 11.6 o versione successiva.
- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Permesso di accesso root](#)" .

Informazioni su questo compito

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

Valutare l'utilizzo dei dati degli oggetti per l'intera griglia

Passi

1. Selezionare **NODES**.
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 archiviazione 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 il passaggio appropriato:

- Se nessuno dei nodi di archiviazione è quasi pieno (ad esempio, tutti i valori dei **dati oggetto utilizzati** sono inferiori all'80%), è possibile iniziare a utilizzare le impostazioni di override. Vai a [Utilizza filigrane ottimizzate](#).
- Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se specifici pool di archiviazione sono quasi pieni, eseguire i passaggi in [Visualizza le filigrane di archiviazione ottimizzate](#) E [Determina se puoi utilizzare filigrane ottimizzate](#).

Visualizza le filigrane di archiviazione ottimizzate

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

Passi

- Selezionare **SUPPORTO > Strumenti > Metriche**.
- Nella sezione Prometheus, seleziona il collegamento per accedere all'interfaccia utente di Prometheus.
- Per visualizzare il watermark minimo consigliato per la sola lettura software, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_minimum_optimized_soft_READONLY_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato della filigrana di sola lettura software per tutti i volumi

di archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per la filigrana di sola lettura software del volume di archiviazione, viene attivato l'avviso **Sostituzione filigrana di sola lettura insufficiente** per il nodo di archiviazione.

4. Per visualizzare il limite massimo consigliato per la sola lettura software, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore massimo ottimizzato della filigrana di sola lettura software per tutti i volumi di archiviazione su ciascun nodo di archiviazione.

5. Nota il valore massimo ottimizzato per ogni nodo di archiviazione.

Determina se puoi utilizzare watermark ottimizzati

Passi

1. Selezionare **NODES**.
2. Ripetere questi passaggi per ogni nodo di archiviazione online:
 - a. Selezionare **Nodo di archiviazione > Archiviazione**.
 - b. Scorrere verso il basso fino alla tabella Archivi oggetti.
 - c. Confronta il valore **Disponibile** per ciascun archivio oggetti (volume) con il limite massimo ottimizzato annotato per quel nodo di archiviazione.
3. Se almeno un volume su ogni nodo di archiviazione online ha più spazio disponibile rispetto al limite massimo ottimizzato per quel nodo, vai a [Utilizza filigrane ottimizzate](#) per iniziare a utilizzare le filigrane ottimizzate.
Altrimenti, espandi la griglia il prima possibile. O "[aggiungere volumi di archiviazione](#)" a un nodo esistente o "[aggiungere nuovi nodi di archiviazione](#)". Poi vai a [Utilizza filigrane ottimizzate](#) per aggiornare le impostazioni della filigrana.
4. Se è necessario continuare a utilizzare valori personalizzati per le filigrane del volume di archiviazione, "[silenzio](#)" O "[disabilitare](#)" l'avviso **Sostituzione filigrana di sola lettura bassa**.



Gli stessi valori di filigrana personalizzati vengono applicati a ogni volume di archiviazione su ogni nodo di archiviazione. L'utilizzo di valori inferiori a quelli consigliati per le filigrane del volume di archiviazione potrebbe causare l'inaccessibilità di alcuni volumi di archiviazione (smontaggio automatico) quando il nodo raggiunge la capacità massima.

Usa filigrane ottimizzate

Passi

1. Vai a **SUPPORTO > Altro > Filigrane di archiviazione**.
2. Selezionare la casella di controllo **Usa valori ottimizzati**.
3. Seleziona **Salva**.

Le impostazioni ottimizzate della filigrana del volume di archiviazione sono ora attive per ogni volume di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

Risolvere i problemi relativi ai metadati

Se si verificano problemi con i metadati, gli avvisi ti informeranno sulla fonte dei problemi e sulle azioni consigliate da intraprendere. In particolare, è necessario aggiungere nuovi nodi di archiviazione se viene attivato l'avviso di spazio di archiviazione dei metadati insufficiente.

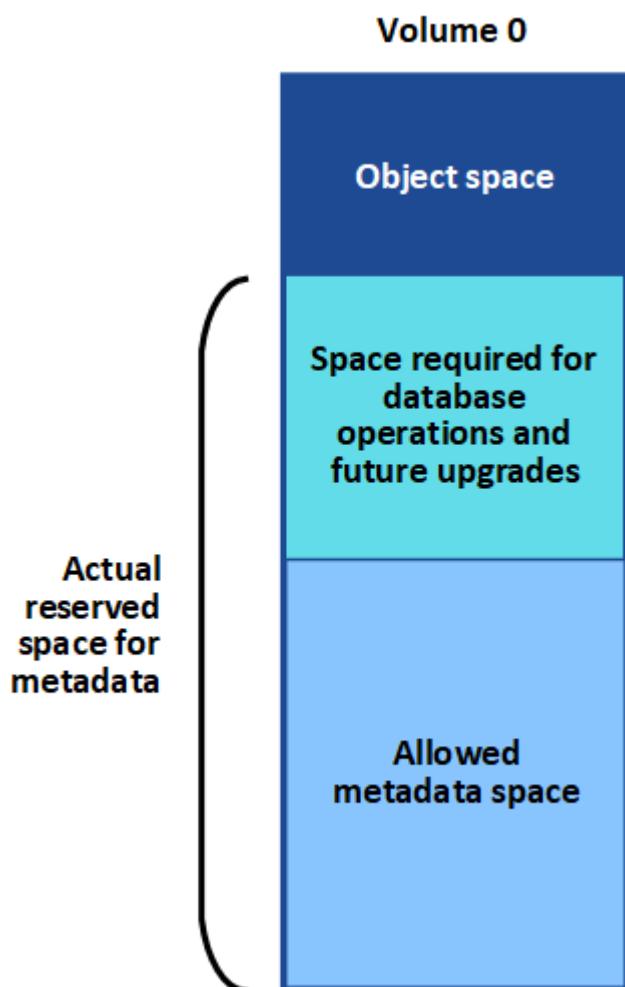
Prima di iniziare

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

Informazioni su questo compito

Seguire le azioni consigliate per ogni avviso correlato ai metadati attivato. Se viene attivato l'avviso **Archiviazione metadati insufficiente**, è necessario aggiungere nuovi nodi di archiviazione.

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



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

Puoi "monitorare la capacità dei metadati degli oggetti per ogni nodo di archiviazione" per aiutarti ad anticipare gli errori e correggerli prima che si verifichino.

StorageGRID utilizza la seguente metrica Prometheus per misurare il livello di riempimento dello spazio metadati consentito:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Quando questa espressione di Prometheus raggiunge determinate soglie, viene attivato l'avviso **Archiviazione metadati insufficiente**.

- **Minore**: i metadati dell'oggetto utilizzano il 70% o più dello spazio metadati consentito. Dovresti aggiungere nuovi nodi di archiviazione il prima possibile.
- **Maggiore**: i metadati dell'oggetto utilizzano il 90% o più dello spazio metadati consentito. È necessario aggiungere immediatamente nuovi nodi di archiviazione.



Quando i metadati degli oggetti utilizzano il 90% o più dello spazio metadati consentito, nella dashboard viene visualizzato un avviso. Se viene visualizzato questo avviso, è necessario aggiungere immediatamente nuovi nodi di archiviazione. Non devi mai consentire che i metadati degli oggetti utilizzino più del 100% dello spazio consentito.

- **Critico**: i metadati degli oggetti utilizzano il 100% o più dello spazio metadati 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 archiviazione.



Se la dimensione del volume 0 è inferiore all'opzione di archiviazione Spazio riservato ai metadati (ad esempio, in un ambiente non di produzione), il calcolo per l'avviso **Archiviazione metadati insufficiente** potrebbe essere impreciso.

Passi

1. Selezionare **AVVISI > Correnti**.
2. Dalla tabella degli avvisi, espandi il gruppo di avvisi **Archiviazione metadati insufficiente**, se necessario, e seleziona l'avviso specifico che desideri visualizzare.
3. Esaminare i dettagli nella finestra di dialogo di avviso.
4. Se è stato attivato un avviso importante o critico di **Archiviazione metadati insufficiente**, eseguire immediatamente un'espansione per aggiungere nodi di archiviazione.



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 hai bisogno di aggiungere capacità di metadati a un sito, dovresti anche "[espandere altri siti](#)" dallo stesso numero di nodi di archiviazione.

Dopo aver eseguito l'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti ai nuovi nodi, aumentando così la capacità complessiva dei metadati della griglia. Non è richiesta alcuna azione da parte dell'utente. L'avviso **Spazio di archiviazione metadati insufficiente** è stato cancellato.

Risolvere gli errori del certificato

Se riscontri un problema di sicurezza o di certificato quando provi a connetterti a StorageGRID tramite un browser Web, un client S3 o uno strumento di monitoraggio esterno, dovresti controllare il certificato.

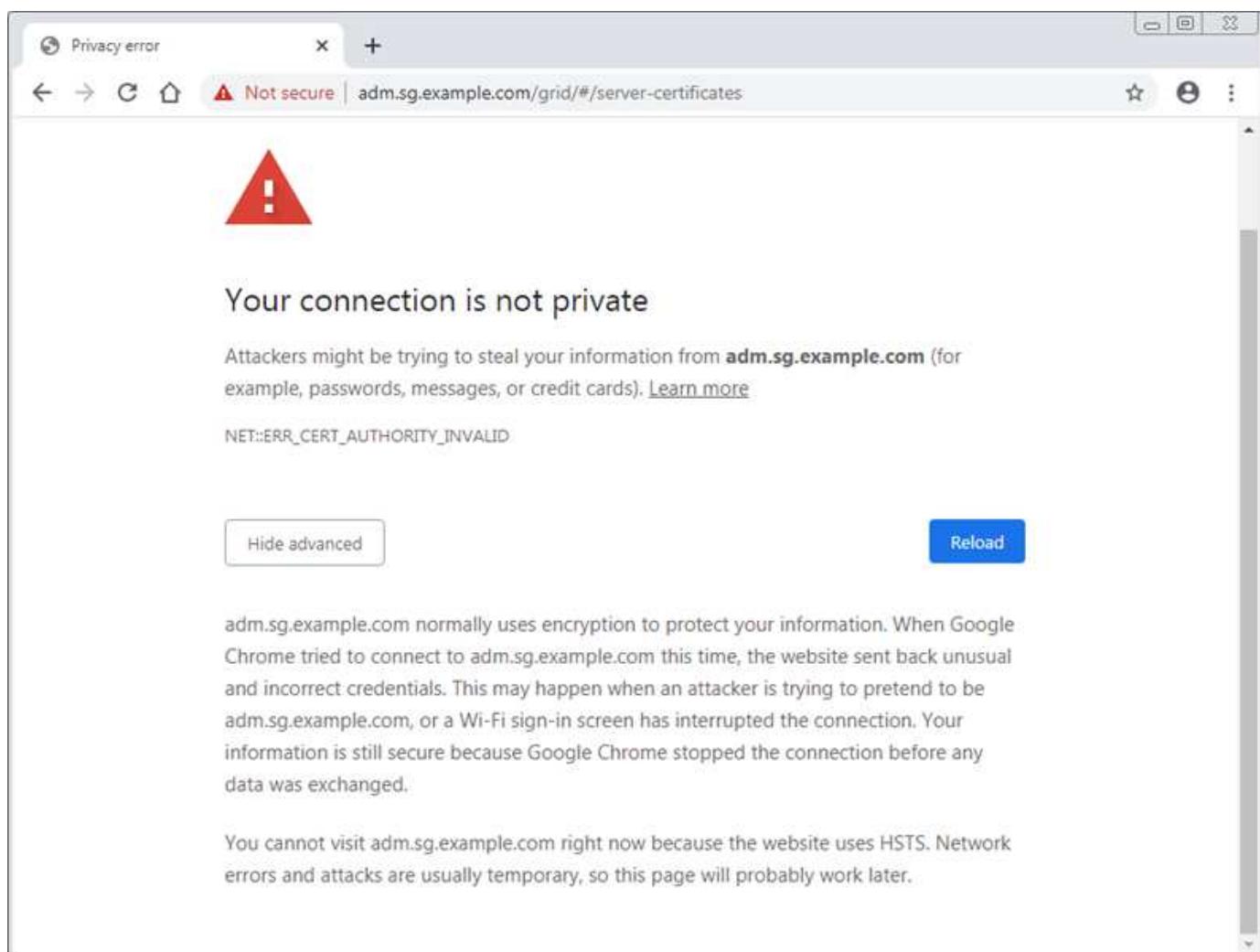
Informazioni su questo compito

Gli errori del certificato possono causare problemi quando si tenta di connettersi a StorageGRID tramite Grid Manager, Grid Management API, Tenant Manager o Tenant Management API. Gli errori del certificato 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 anziché un indirizzo IP, il browser visualizza un errore di certificato senza un'opzione per ignorarlo se si verifica una delle seguenti situazioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Si passa da un certificato di interfaccia di gestione personalizzato al certificato del server predefinito.

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



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza**

del certificato server per l'interfaccia di gestione viene attivato quando il certificato 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 StorageGRID o dai certificati client. L'avviso **Scadenza dei certificati client configurati nella pagina Certificati** viene attivato quando un certificato client sta per scadere.

Passi

Se hai ricevuto una notifica di avviso relativa a un certificato scaduto, accedi ai dettagli del certificato: . Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi "[seleziona la scheda del certificato appropriata](#)" .

1. Verificare 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, carica o genera un nuovo certificato.
 - Per un certificato del server, vedere i passaggi per "[configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager](#)" .
 - Per un certificato client, vedere i passaggi per "[configurazione di un certificato client](#)" .
3. Per gli errori del certificato del server, provare una o entrambe le seguenti opzioni:
 - Assicurarsi che il nome alternativo del soggetto (SAN) del certificato sia compilato e che il SAN corrisponda all'indirizzo IP o al nome host del nodo a cui ci si sta connettendo.
 - Se si tenta di connettersi a StorageGRID utilizzando un nome di dominio:
 - i. Immettere l'indirizzo IP del nodo di amministrazione anziché il nome di dominio per aggirare l'errore di connessione e accedere a Grid Manager.
 - ii. Da Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e poi "[seleziona la scheda del certificato appropriata](#)" per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
 - iii. Nelle istruzioni per l'amministrazione StorageGRID, vedere i passaggi 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 di amministrazione e all'interfaccia utente StorageGRID .

Errori di accesso al nodo di amministrazione

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il `Passwords.txt` file.
- Hai "[autorizzazioni di accesso specifiche](#)" .

Informazioni su questo compito

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 di amministrazione:

- 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...

Passi

1. Attendi 10 minuti e prova ad accedere nuovamente.

Se l'errore non viene risolto automaticamente, passare al passaggio successivo.

2. Se il sistema StorageGRID dispone di più di un nodo amministrativo, provare ad accedere a Grid Manager da un altro nodo amministrativo per verificare lo stato di un nodo amministrativo non disponibile.

- Se riesci ad accedere, puoi utilizzare le opzioni **Dashboard**, **NODI**, **Avvisi** e **SUPPORTO** per determinare la causa dell'errore.
- Se hai un solo nodo di amministrazione o non riesci ancora ad accedere, vai al passaggio successivo.

3. Determina se l'hardware del nodo è offline.

4. Se l'accesso singolo (SSO) è abilitato per il sistema StorageGRID , fare riferimento ai passaggi per "[configurazione dell'accesso singolo](#)" .

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



Se l'SSO è abilitato, non è possibile effettuare l'accesso utilizzando una porta con restrizioni. È necessario utilizzare la porta 443.

5. Verifica se l'account che stai utilizzando appartiene a un utente federato.

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

- Se l'utente locale può accedere:
 - i. Rivedi gli avvisi.
 - ii. Selezionare **CONFIGURAZIONE > Controllo accessi > Federazione identità**.
 - iii. Fare clic su **Test connessione** per convalidare le impostazioni di connessione per il server LDAP.
 - iv. Se il test fallisce, correggere eventuali errori di configurazione.
- Se l'utente locale non riesce ad accedere e sei sicuro che le credenziali siano corrette, vai al passaggio successivo.

6. Utilizzare Secure Shell (ssh) per accedere al nodo di amministrazione:

- a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$ A #`.

7. Visualizza lo stato di tutti i servizi in esecuzione sul nodo della 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. Conferma che il servizio nginx-gw è in esecuzione # `service nginx-gw status`

9. Usa Lumberjack per raccogliere i tronchi: # `/usr/local/sbin/lumberjack.rb`

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

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

10. Esamina i seguenti log:
 - /var/local/log/bycast.log
 - /var/local/log/bycast-err.log
 - /var/local/log/nms.log
 - **/*commands.txt
11. Se non è stato possibile identificare alcun problema con il nodo di amministrazione, eseguire uno dei seguenti comandi per determinare gli indirizzi IP dei tre nodi di archiviazione che eseguono il servizio ADC nel sito. In genere, si tratta dei primi tre nodi di archiviazione installati nel sito.

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

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

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

12. Dal nodo di amministrazione, utilizzare ssh per accedere a ciascuno dei nodi di archiviazione ADC, utilizzando gli indirizzi IP identificati.
13. Visualizza lo stato di tutti i servizi in esecuzione sul nodo della griglia: storagegrid-status
Assicurarsi che i servizi idnt, acct, nginx e cassandra siano tutti in esecuzione.
14. Ripeti i passaggi [Usa Lumberjack per raccogliere i tronchi](#) [ERegistri di revisione](#) per rivedere i registri sui nodi di archiviazione.
15. Se non riesci a risolvere il problema, contatta l'assistenza tecnica.

Fornisci i registri raccolti al supporto tecnico. Vedere anche ["Riferimento ai file di registro"](#).

Problemi dell'interfaccia utente

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

Passi

1. Assicurati di utilizzare un "[browser web supportato](#)" .
2. Svuota la cache del tuo browser web.

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

Risolvi i problemi di rete, hardware e piattaforma

Esistono diverse attività che è possibile svolgere per determinare l'origine dei problemi

relativi alla rete, all'hardware e alla piattaforma StorageGRID .

Errori "422: Entità non elaborabile"

L'errore 422: Entità non elaborabile può verificarsi per diversi motivi. Controlla 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 tramite Windows Active Directory (AD).</p> <p>L'utilizzo dell'opzione Non utilizzare TLS non è supportato per i server AD che applicano la firma LDAP. È necessario selezionare l'opzione Usa STARTTLS o l'opzione Usa LDAPS per TLS.</p>

Messaggio di errore	Causa principale e azione correttiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	<p>Questo messaggio viene visualizzato se si tenta di utilizzare una crittografia non supportata per stabilire una connessione Transport Layer Security (TLS) da StorageGRID a un sistema esterno utilizzato per identificare la federazione o i pool di archiviazione cloud.</p> <p>Controllare i cifrari offerti dal sistema esterno. Il sistema deve utilizzare uno dei "cifrari supportati da StorageGRID" per le connessioni TLS in uscita, come mostrato nelle istruzioni per l'amministrazione StorageGRID.</p>

Avviso di mancata corrispondenza MTU della rete di rete

L'avviso **Mancata corrispondenza MTU della rete di griglia** viene attivato quando l'impostazione dell'unità di trasmissione massima (MTU) per l'interfaccia della rete di griglia (eth0) differisce in modo significativo tra i nodi della griglia.

Informazioni su questo compito

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

Passi

1. Elenca le impostazioni MTU per eth0 su tutti i nodi.
 - Utilizzare la query fornita in Grid Manager.
 - Vai a *primary Admin Node IP address/metrics/graph* e inserisci la seguente query:
`node_network_mtu_bytes{device="eth0"}`
2. "[Modificare le impostazioni MTU](#)" se necessario per garantire che siano gli stessi per l'interfaccia Grid Network (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: sui nodi basati su Linux, se il valore MTU desiderato per la rete nel contenitore supera il valore già configurato sull'interfaccia host, è necessario prima configurare l'interfaccia host in modo che abbia il valore MTU desiderato, quindi utilizzare `change-ip.py` script per modificare il valore MTU della rete nel contenitore.

Utilizzare i seguenti argomenti per modificare l'MTU sui nodi basati su Linux o VMware.

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

+

Argomenti facoltativi	Descrizione
-h, - help	Mostra il messaggio di aiuto ed esci.
-n node, --node node	Il nodo. L'impostazione predefinita è il nodo locale.

Avviso di errore del frame di ricezione della rete del nodo

Gli avvisi di **errore frame di ricezione della rete del nodo** possono essere causati da problemi di connettività tra StorageGRID e l'hardware di rete. Questo avviso scompare da solo una volta risolto il problema sottostante.

Informazioni su questo compito

Gli avvisi di **errore frame di ricezione della rete del nodo** possono essere causati dai seguenti problemi con l'hardware di rete che si connette a StorageGRID:

- La correzione degli errori in avanti (FEC) è richiesta e non è in uso
- Mancata corrispondenza tra porta switch e MTU NIC
- Elevati tassi di errore nei collegamenti
- Sovraccarico del buffer ad anello della NIC

Passi

1. Seguire i passaggi per la risoluzione dei problemi per tutte le potenziali cause di questo avviso in base alla configurazione della rete.
2. Eseguire i seguenti passaggi a seconda della causa dell'errore:

Disallineamento FEC



Questi passaggi sono applicabili solo per gli avvisi di **Errore frame di ricezione della rete del nodo** causati dalla mancata corrispondenza FEC sugli appliance StorageGRID .

- a. Controllare lo stato FEC della porta nello switch collegato al dispositivo StorageGRID .
- b. Controllare l'integrità fisica dei cavi dall'apparecchio all'interruttore.
- c. Se si desidera modificare le impostazioni FEC per provare a risolvere l'avviso, assicurarsi innanzitutto che l'appliance sia configurata per la modalità **Auto** nella pagina Configurazione collegamento del programma di installazione dell'appliance StorageGRID (vedere le istruzioni per l'appliance:
 - ["SG6160"](#)
 - ["SGF6112"](#)
 - ["SG6000"](#)
 - ["SG5800"](#)
 - ["SG5700"](#)
 - ["SG110 e SG1100"](#)
 - ["SG100 e SG1000"](#)
- d. Modificare le impostazioni FEC sulle porte dello switch. Se possibile, le porte dell'appliance StorageGRID regoleranno le proprie impostazioni FEC per adattarle.

Non è possibile configurare le impostazioni FEC sugli appliance StorageGRID . Al contrario, gli apparecchi tentano di scoprire e rispecchiare le impostazioni FEC sulle porte dello switch a cui sono collegati. Se i collegamenti vengono forzati a velocità di rete pari a 25 GbE o 100 GbE, lo switch e la scheda di rete potrebbero non riuscire a negoziare un'impostazione FEC comune. Senza un'impostazione FEC comune, la rete tornerà alla modalità "no-FEC". Quando la funzione FEC non è abilitata, le connessioni sono più soggette a errori causati da disturbi elettrici.



Gli apparecchi StorageGRID supportano Firecode (FC) e Reed Solomon (RS) FEC, ma anche nessun FEC.

Mancata corrispondenza tra porta switch e MTU NIC

Se l'avviso è causato da una mancata corrispondenza tra la porta dello switch e l'MTU della scheda di rete, verificare che la dimensione dell'MTU configurata sul nodo sia la stessa dell'impostazione MTU per la porta dello switch.

La dimensione MTU configurata sul nodo potrebbe essere inferiore all'impostazione sulla porta dello switch a cui è connesso il nodo. Se un nodo StorageGRID riceve un frame Ethernet più grande del suo MTU, cosa possibile con questa configurazione, potrebbe essere segnalato l'avviso **Errore frame ricezione rete nodo**. Se ritieni che questo sia ciò che sta accadendo, modifica l'MTU della porta dello switch in modo che corrisponda all'MTU dell'interfaccia di rete StorageGRID oppure modifica l'MTU dell'interfaccia di rete StorageGRID in modo che corrisponda alla porta dello switch, a seconda degli obiettivi o dei requisiti MTU end-to-end.



Per ottenere le migliori prestazioni di rete, tutti i nodi devono essere configurati con valori MTU simili sulle loro interfacce Grid Network. L'avviso **Mancata corrispondenza MTU della rete Grid** viene attivato se si verifica una differenza significativa nelle impostazioni MTU per la rete Grid sui singoli nodi. I valori MTU non devono essere gli stessi per tutti i tipi di rete. Vedere [Risoluzione dei problemi relativi all'avviso di mancata corrispondenza dell'MTU della rete Grid](#) per maggiori informazioni.



Vedi anche ["Cambia l'impostazione MTU"](#).

Elevati tassi di errore nei collegamenti

- a. Abilitare FEC, se non è già abilitato.
- 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 la causa del problema, contattare l'assistenza tecnica.



In un ambiente con un elevato rumore elettrico, è possibile che si riscontrino alti tassi di errore.

Sovraccarico del buffer ad anello della NIC

Se l'errore è un sovraccarico del buffer ad anello della NIC, contattare l'assistenza tecnica.

Il buffer ad anello può essere superato quando il sistema StorageGRID è sovraccarico e non è in grado di elaborare tempestivamente gli eventi di rete.

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

Errori di sincronizzazione dell'ora

Potresti riscontrare problemi con la sincronizzazione oraria nella tua griglia.

Se si verificano problemi di sincronizzazione temporale, verificare di aver specificato almeno quattro sorgenti NTP esterne, ciascuna delle quali fornisca un riferimento Stratum 3 o superiore, e che tutte le sorgenti NTP esterne funzionino normalmente e siano accessibili dai nodi StorageGRID.



Quando ["specificando la sorgente NTP esterna"](#) per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Ora di Windows (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio orario delle versioni precedenti di Windows non è sufficientemente preciso e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, come StorageGRID.

Linux: problemi di connettività di rete

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

Clonazione dell'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 delle reti su "true" nel file di configurazione del nodo. Questa impostazione fa sì che l'indirizzo MAC del contenitore StorageGRID utilizzi l'indirizzo MAC dell'host. Per creare file di configurazione del nodo, vedere le istruzioni

per "Red Hat Enterprise Linux" O "Ubuntu o Debian".



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

Per ulteriori informazioni sull'abilitazione della clonazione MAC, vedere le istruzioni per "Red Hat Enterprise Linux" O "Ubuntu o Debian".

Modalità promiscua

Se non si desidera utilizzare la clonazione degli indirizzi MAC e si preferisce 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 **Accetta** per Modalità promiscua, Modifiche indirizzo MAC e Trasmissioni contraffatte. 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 entrambi i punti.

Per ulteriori informazioni sull'utilizzo della modalità promiscua, consultare le istruzioni per "Red Hat Enterprise Linux" O "Ubuntu o Debian".

Linux: lo stato del nodo è "orfano"

Un nodo Linux in stato orfano indica solitamente che il servizio StorageGRID o il demone del nodo StorageGRID che controlla il contenitore del nodo è morto inaspettatamente.

Informazioni su questo compito

Se un nodo Linux segnala di trovarsi in uno stato orfano, è necessario:

- Controllare i registri per errori e messaggi.
- Provare a riavviare il nodo.
- Se necessario, utilizzare i comandi del motore del contenitore per arrestare il contenitore del nodo esistente.
- Riavviare il nodo.

Passi

1. Controllare i registri sia del demone di servizio che del nodo orfano per individuare errori evidenti o messaggi relativi a un'uscita imprevista.
2. Accedi all'host come root o utilizzando un account con autorizzazione sudo.
3. Provare a 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 del contenitore e tutti i processi di controllo storagegrid-node. Ad esempio:
sudo docker stop --time secondscontainer-name

Per seconds , immettere il numero di secondi che si desidera attendere affinché il contenitore si arresti (in genere 15 minuti o meno). Per 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 di 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 dei nodi come previsto.

Informazioni su questo compito

Per visualizzare l'indirizzo IPv6 assegnato a un nodo della 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 questi passaggi per abilitare il supporto IPv6 nel kernel.

Passi

1. Accedi 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 dovrebbe essere 0.

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



Se il risultato non è 0, consultare la documentazione del sistema operativo per la modifica sysctl impostazioni. Quindi, prima di continuare, modifica il valore in 0.

3. Accedere al 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 dovrebbe essere 1.

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



Se il risultato è diverso da 1, questa procedura non si applica. Contattare l'assistenza tecnica.

5. Esci dal contenitore: exit

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

6. Come root, modifica 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, salva e chiudi il file.

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

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

8. Eseguire questi comandi per riavviare il contenitore StorageGRID :

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

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

Risolvere i problemi di un server syslog esterno

Nella tabella seguente vengono descritti i messaggi di errore che potrebbero essere correlati all'utilizzo di un server syslog esterno e vengono elencate le azioni correttive.

Questi errori vengono visualizzati dalla procedura guidata Configura server syslog esterno se si verificano problemi durante l'invio di messaggi di prova per convalidare la corretta configurazione del server syslog esterno.

Problemi in fase di esecuzione potrebbero essere segnalati dall'["Errore di inoltro del server syslog esterno"](#) allerta. Se ricevi questo avviso, segui le istruzioni contenute nell'avviso per inviare nuovamente i messaggi di prova e ottenere messaggi di errore dettagliati.

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

- ["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
Non è possibile risolvere un indirizzo su un nome host	<p>Il nome di dominio completo immesso per il server syslog non può essere risolto in un indirizzo IP.</p> <ol style="list-style-type: none"> 1. Controlla il nome host inserito. Se hai inserito un indirizzo IP, assicurati che sia un indirizzo IP valido in notazione WXYZ ("decimale puntato"). 2. Verificare che i server DNS siano configurati correttamente. 3. Verificare che ciascun nodo possa accedere agli indirizzi IP del server DNS.
Connessione rifiutata	<p>Una connessione TCP o TLS al server syslog è stata rifiutata. Potrebbe non esserci alcun servizio in ascolto sulla porta TCP o TLS per l'host oppure un firewall potrebbe bloccare l'accesso.</p> <ol style="list-style-type: none"> 1. Verificare di aver inserito il nome di dominio completo (FQDN) o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Verificare che l'host per il servizio syslog stia eseguendo un demone syslog in ascolto sulla porta specificata. 3. Verificare che un firewall non stia bloccando l'accesso alle connessioni TCP/TLS dai nodi all'IP e alla porta del server syslog.
Rete irraggiungibile	<p>Il server syslog non si trova su una subnet direttamente collegata. Un router ha restituito un messaggio di errore ICMP per indicare che non è riuscito a inoltrare i messaggi di prova dai nodi elencati al server syslog.</p> <ol style="list-style-type: none"> 1. Verificare di aver inserito il nome di dominio completo o l'indirizzo IP corretto per il server syslog. 2. Per ogni nodo elencato, controllare l'elenco delle subnet della rete Grid, gli elenchi delle subnet delle reti amministrative e i gateway della rete client. Verificare che siano configurati per instradare il traffico verso il server syslog tramite l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host non raggiungibile	<p>Il server syslog si trova su una subnet direttamente collegata (subnet utilizzata dai nodi elencati per i loro indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di prova, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del server syslog.</p> <ol style="list-style-type: none"> 1. Verificare di aver inserito il nome di dominio completo o l'indirizzo IP corretto per il server syslog. 2. Verificare che l'host che esegue il servizio syslog sia attivo.

Messaggio di errore	Descrizione e azioni consigliate
Connessione scaduta	<p>È stato effettuato un tentativo di connessione TCP/TLS, ma per molto tempo non è stata ricevuta alcuna risposta dal server syslog. Potrebbe esserci un errore di configurazione del routing oppure un firewall potrebbe interrompere il traffico senza inviare alcuna risposta (una configurazione comune).</p> <ol style="list-style-type: none"> 1. Verificare di aver inserito il nome di dominio completo o l'indirizzo IP corretto per il server syslog. 2. Per ogni nodo elencato, controllare l'elenco delle subnet della rete Grid, gli elenchi delle subnet delle reti amministrative e i gateway della rete client. Verificare che siano configurati per instradare il traffico verso il server syslog utilizzando l'interfaccia di rete e il gateway (Grid, Admin o Client) tramite i quali si prevede di raggiungere il server syslog. 3. Verificare che un firewall non stia bloccando 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 è stata successivamente chiusa. Le ragioni potrebbero essere:</p> <ul style="list-style-type: none"> • Il server syslog potrebbe essere stato 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 inserito il nome di dominio completo (FQDN) o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Se si utilizza TLS, verificare che anche il server syslog utilizzi TLS. Se si utilizza TCP, verificare che anche il server syslog utilizzi TCP. 3. Verificare che non sia configurato un firewall intermedio per chiudere le connessioni TCP inattive.
Errore del certificato TLS	<p>Il certificato del server ricevuto dal server syslog non era compatibile con il bundle di certificati CA e 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 del 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 rilevarne il motivo.</p> <p>Esaminare i log di debug forniti con questo errore per tentare di determinarne 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 rilevarne il motivo.</p> <ol style="list-style-type: none"> 1. Esaminare i log di debug forniti con questo errore per tentare di determinarne la causa principale. 2. Verificare di aver inserito il nome di dominio completo (FQDN) o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 3. Se si utilizza TLS, verificare che anche il server syslog utilizzi TLS. Se si utilizza TCP, verificare che anche il server syslog utilizzi TCP. 4. Verificare che il pacchetto di certificati CA e il certificato client (se presente) siano compatibili con il certificato del 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 dei test dai nodi elencati. Uno o più nodi potrebbero essere inattivi.</p> <ol style="list-style-type: none"> 1. Seguire i passaggi 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 controllo

Messaggi e registri di controllo

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di controllo e dei registri di controllo StorageGRID . È possibile utilizzare queste informazioni per leggere e analizzare la traccia di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli amministratori responsabili della produzione di report sull'attività e l'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID .

Per utilizzare il file di registro di testo, è necessario avere accesso alla condivisione di controllo configurata sul 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 controllo e le destinazioni dei registri"](#)" .

Flusso e conservazione dei messaggi di audit

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. Dovresti capire come questi messaggi di controllo si spostano attraverso il sistema StorageGRID verso audit.log file.

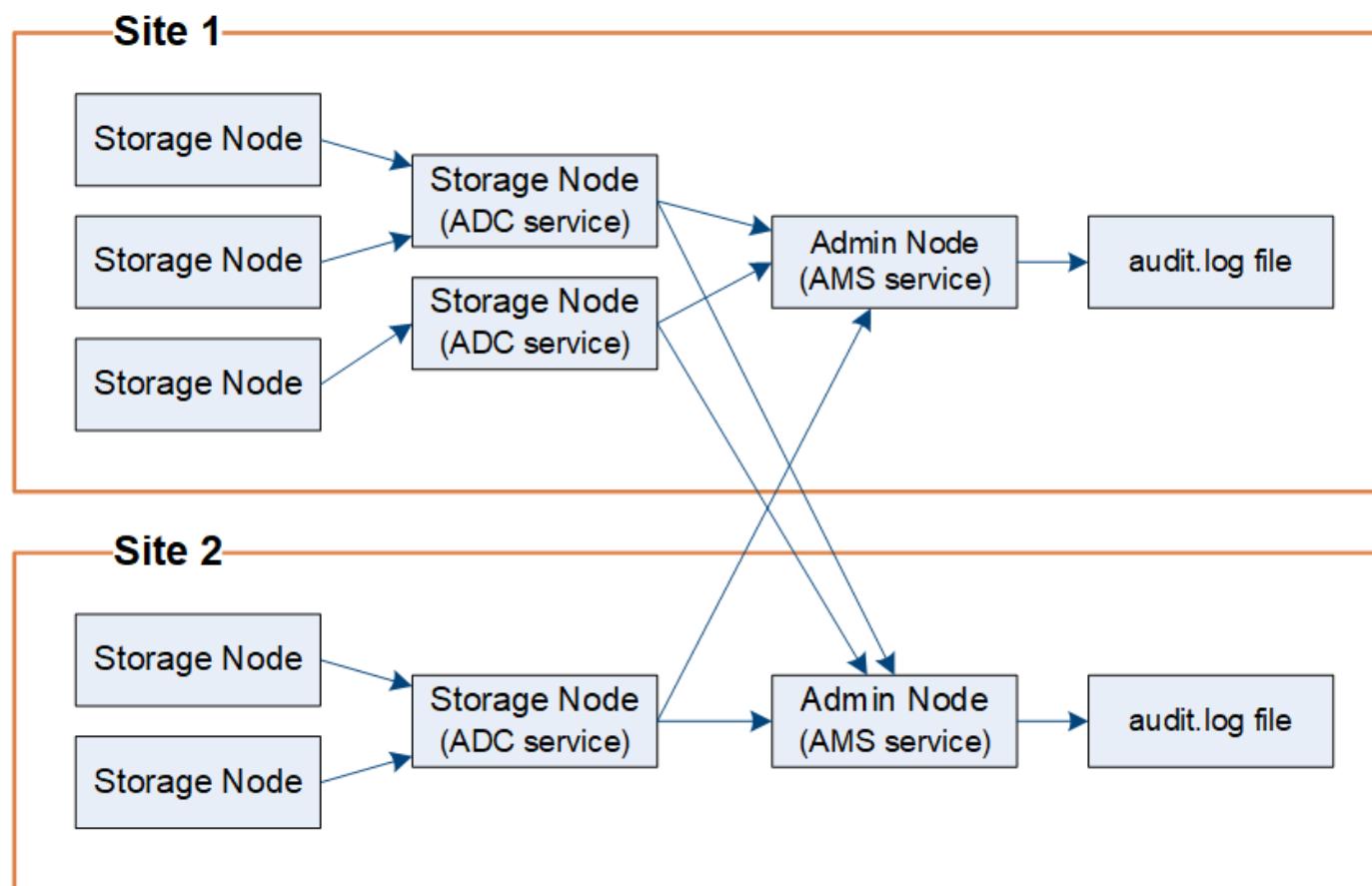
Flusso dei messaggi di audit

I messaggi di controllo vengono elaborati dai nodi di amministrazione e dai nodi di archiviazione che dispongono di un servizio di controller di dominio amministrativo (ADC).

Come mostrato nel diagramma del flusso dei messaggi di controllo, ogni nodo StorageGRID invia i propri messaggi di controllo a uno dei servizi ADC presso il sito del data center. Il servizio ADC viene abilitato automaticamente per i primi tre nodi di archiviazione installati in ciascun sito.

A sua volta, ogni servizio ADC funge da relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID , il che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

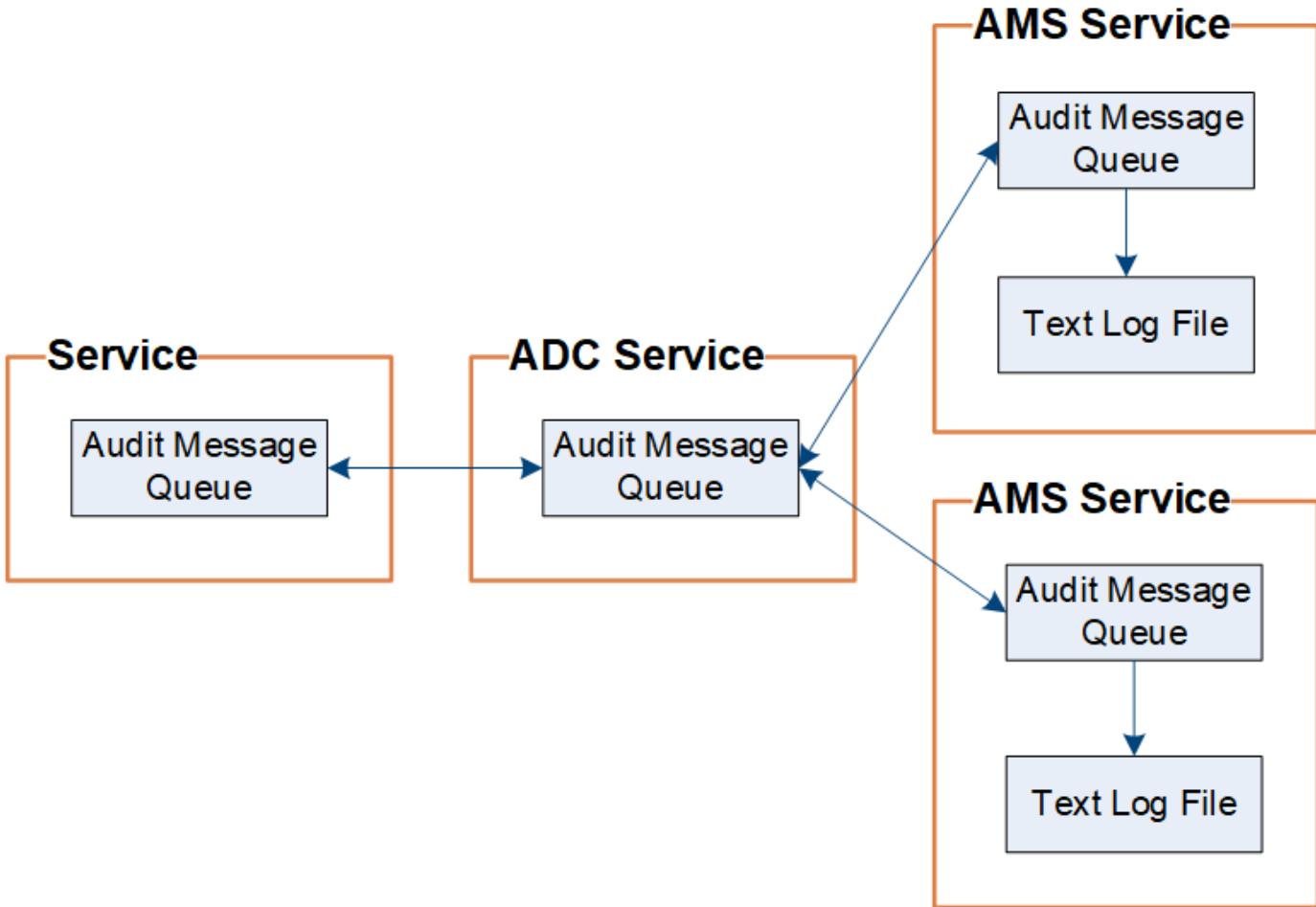
Ogni nodo di amministrazione memorizza i messaggi di controllo in file di registro di testo; il file di registro attivo è denominato `audit.log`.



Conservazione dei messaggi di controllo

StorageGRID utilizza un processo di copia ed eliminazione per garantire che nessun messaggio di controllo venga perso prima che possa essere scritto nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di controllo, il messaggio viene memorizzato in una coda di messaggi di controllo sul disco di sistema del nodo della griglia. 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 nel nodo di amministrazione `/var/local/log` elenco. Ciò aiuta a prevenire la perdita di un messaggio di controllo durante il trasporto.



La coda dei messaggi di controllo può aumentare temporaneamente a causa di problemi di connettività di rete o di capacità di controllo insufficiente. Man mano che le code aumentano, consumano più spazio disponibile in ciascun nodo /var/local/ elenco. Se il problema persiste e la directory dei messaggi di controllo di un nodo diventa troppo piena, i singoli nodi daranno priorità all'elaborazione del loro arretrato e diventeranno temporaneamente non disponibili per nuovi messaggi.

Nello specifico, potresti riscontrare i seguenti comportamenti:

- Se il /var/local/log Se la directory utilizzata da un nodo di amministrazione diventa piena, il nodo di amministrazione verrà contrassegnato come non disponibile per nuovi messaggi di controllo finché la directory non sarà più piena. Le richieste del client S3 non sono interessate. L'allarme XAMS (Unreachable Audit Repositories) viene attivato quando un repository di audit non è raggiungibile.
- Se il /var/local/ Quando la directory utilizzata da un nodo di archiviazione con il servizio ADC è piena al 92%, il nodo verrà contrassegnato come non disponibile per i messaggi di controllo finché la directory non sarà piena solo all'87%. Le richieste del client S3 ad altri nodi non sono interessate. L'allarme NRY (Available Audit Relays) viene attivato quando i relay di audit non sono raggiungibili.



Se non sono disponibili nodi di archiviazione con il servizio ADC, i nodi di archiviazione archiviano i messaggi di controllo localmente nel /var/local/log/localaudit.log file.

- Se il /var/local/ la directory utilizzata da un nodo di archiviazione diventa piena all'85%, il nodo inizierà a rifiutare le richieste del client S3 con 503 Service Unavailable .

I seguenti tipi di problemi possono causare un aumento notevole delle dimensioni delle code dei messaggi di controllo:

- Interruzione di un nodo di amministrazione o di un nodo di archiviazione con il servizio ADC. Se uno dei nodi del sistema è inattivo, i nodi rimanenti potrebbero accumulare arretrati.
- Un tasso di attività sostenuto che supera la capacità di audit del sistema.
- Il /var/local/ spazio su un nodo di archiviazione ADC che si riempie per motivi non correlati ai messaggi di controllo. Quando ciò accade, il nodo smette di accettare nuovi messaggi di audit e dà priorità al suo arretrato attuale, il che può causare arretrati su altri nodi.

Avviso di coda di controllo di grandi dimensioni e allarme di messaggi di controllo in coda (AMQS)

Per aiutarti a monitorare le dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Coda di controllo di grandi dimensioni** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda del nodo di archiviazione o in una coda del nodo di amministrazione raggiunge determinate soglie.

Se viene attivato l'avviso **Coda di controllo di grandi dimensioni** 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 dovrebbero risolversi nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di gravità, visualizza un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, è probabile che il carico di controllo abbia superato la capacità di controllo del sistema. Ridurre la frequenza operativa del client o diminuire il numero di messaggi di controllo registrati modificando il livello di controllo per Scritture client e Letture client su Errore o Disattivato. Vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)".

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto della rete o del nodo. Per questo motivo potrebbero esserci messaggi duplicati nel registro di controllo.

Accedi al file di registro di controllo

La condivisione di controllo contiene l'attivo audit.log file e tutti i file di registro di controllo compressi. È possibile accedere ai file di registro di controllo direttamente dalla riga di comando del nodo di amministrazione.

Prima di iniziare

- Hai "[autorizzazioni di accesso specifiche](#)".
- Devi avere il Passwords.txt file.
- È necessario conoscere l'indirizzo IP di un nodo di amministrazione.

Passi

1. Accedi a un nodo di amministrazione:
 - a. Immettere il seguente comando: ssh admin@primary_Admin_Node_IP
 - b. Inserisci la password elencata nel Passwords.txt file.
 - c. Immettere il seguente comando per passare alla root: su -
 - d. Inserisci la password elencata nel Passwords.txt file.

Quando si accede come root, il prompt cambia da \$ A # .

2. Andare alla directory contenente i file di registro di controllo:

```
cd /var/local/log
```

3. Visualizzare il file di registro di controllo corrente o salvato, a seconda delle necessità.

Rotazione del file di registro di controllo

I file dei registri di controllo vengono salvati nel nodo di amministrazione /var/local/log elenco. I file di registro di controllo attivi sono denominati audit.log



Facoltativamente, è possibile modificare la destinazione dei log 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 archiviati quando viene configurato un server syslog esterno. Vedere "["Configurare i messaggi di controllo e le destinazioni dei registri"](#)" .

Una volta al giorno, l'attivo audit.log il file viene salvato e ne viene creato uno nuovo audit.log il file è avviato. Il nome del file salvato indica quando è stato salvato, nel formato yyyy-mm-dd.txt . Se in un singolo giorno viene creato più di un registro di controllo, i nomi dei file utilizzano la data di salvataggio del file, seguita da un numero, nel formato yyyy-mm-dd.txt.n . Per esempio, 2018-04-15.txt È 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. Nel tempo, ciò si traduce nel consumo dello spazio di archiviazione allocato per i log di controllo sul nodo di amministrazione. Uno script monitora il consumo di spazio del registro di controllo ed elimina i file di registro se necessario per liberare spazio nel /var/local/log elenco. I registri di controllo vengono eliminati in base alla data di creazione, partendo da quelli più vecchi. È possibile monitorare le azioni dello script nel seguente file: /var/local/log/manage-audit.log .

Questo esempio mostra l'attivo audit.log file, il file del giorno precedente(2018-04-15.txt), e il file compresso del giorno precedente(2018-04-14.txt.gz).

```
audit.log  
2018-04-15.txt  
2018-04-14.txt.gz
```

Formato del file di registro di controllo

Formato del file di registro di controllo

I file di registro di controllo si trovano su ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di controllo.

Ogni messaggio di controllo contiene quanto segue:

- Il tempo coordinato universale (UTC) dell'evento che ha attivato il messaggio di controllo (ATIM) nel formato ISO 8601, seguito da uno spazio:

YYYY-MM-DDTHH:MM:SS.UUUUUU, Dove *UUUUUU* sono microsecondi.

- Il messaggio di controllo stesso, racchiuso tra parentesi quadre e che inizia con AUDT .

L'esempio seguente mostra tre messaggi di controllo in un file di registro di controllo (interruzioni di riga aggiunte per migliorare la leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e ha 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):PUT][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):PUT][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):PUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Nel loro formato predefinito, i messaggi di controllo nei file di registro di controllo non sono facili da leggere o

interpretare. Puoi usare il "strumento di verifica e spiegazione" per ottenere riepiloghi semplificati dei messaggi di controllo nel registro di controllo. Puoi usare il "strumento di somma di controllo" per riepilogare quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto queste operazioni.

Utilizzare lo strumento di verifica e spiegazione

Puoi usare il audit-explain strumento per tradurre i messaggi di controllo nel registro di controllo in un formato di facile lettura.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Devi avere il Passwords.txt file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

Informazioni su questo compito

IL audit-explain strumento, disponibile sul nodo di amministrazione principale, fornisce riepiloghi semplificati dei messaggi di controllo in un registro di controllo.



IL audit-explain Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Elaborazione audit-explain le query possono consumare una grande quantità di potenza della CPU, il che potrebbe avere un impatto sulle operazioni StorageGRID .

Questo esempio mostra l'output tipico del audit-explain attrezzo. Questi quattro "PUT" sono stati generati messaggi di controllo quando il tenant S3 con ID account 92484777680322627870 ha utilizzato richieste PUT S3 per creare un bucket denominato "bucket1" e aggiungere tre oggetti a tale bucket.

```
PUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
PUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
PUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
PUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

IL audit-explain lo strumento può fare quanto segue:

- Elaborare registri di controllo semplici o compressi. Per esempio:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Elaborare più file contemporaneamente. Per esempio:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```

- Accetta input da una pipe, che consente di filtrare e preelaborare l'input utilizzando `grep` comando o altri mezzi. Per 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 eseguendo `audit-explain` sulle parti, anziché sull'intero file.

 IL `audit-explain` lo strumento non accetta file compressi come input inoltrato. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` strumento per decomprimere prima i file. Per esempio:

```
zcat audit.log.gz | audit-explain
```

Utilizzare il `help` (`-h`) opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-explain -h
```

Passi

1. Accedi al nodo di amministrazione principale:

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

Quando si accede 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
```

IL `audit-explain` Lo strumento stampa interpretazioni leggibili dall'uomo di tutti i messaggi nel file o nei file specificati.



Per ridurre la lunghezza delle righe e migliorare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se vuoi vedere i timestamp, usa il `timestamp(-t)` opzione.

Utilizzare lo strumento audit-sum

Puoi usare il `audit-sum` strumento per contare i messaggi di controllo di scrittura, lettura, intestazione ed eliminazione e per visualizzare il tempo minimo, massimo e medio (o dimensione) per ciascun tipo di operazione.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Devi avere il Passwords.txt file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

Informazioni su questo compito

IL audit-sum strumento, disponibile sul nodo di amministrazione primario, riepiloga quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto tali operazioni.



IL audit-sum Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Elaborazione audit-sum le query possono consumare una grande quantità di potenza della CPU, il che potrebbe avere un impatto sulle operazioni StorageGRID .

Questo esempio mostra l'output tipico del audit-sum attrezzo. Questo esempio mostra quanto tempo hanno richiesto le operazioni del protocollo.

message group	count	min(sec)	max(sec)
average(sec)	=====	=====	=====
=====	=====	=====	=====
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

IL audit-sum Lo strumento fornisce conteggi e orari per i seguenti messaggi di controllo S3, Swift e ILM in un registro di controllo.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione quando le funzionalità diventano obsolete. Se riscontri un codice di controllo non elencato qui, controlla le versioni precedenti di questo argomento per le versioni SG più vecchie. Ad esempio, ["StorageGRID 11.8 Utilizzo della documentazione dello strumento di somma di controllo"](#) .

Codice	Descrizione	Fare riferimento a
IDEL	Eliminazione avviata da ILM: registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: ILM ha avviato l'eliminazione"
SDEL	S3 DELETE: registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: S3 ELIMINA"

Codice	Descrizione	Fare riferimento a
SGET	S3 GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	" SGET: S3 GET "
KARITÉ	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	Swift DELETE: registra una transazione riuscita per eliminare un oggetto o un contenitore.	" WDEL: CANCELLA rapida "
WGET	Swift GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un contenitore.	" WGET: GET rapido "
WHEA	Swift HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un contenitore.	" WHEA: TESTA Veloce "
WPUT	Swift PUT: registra una transazione riuscita per creare un nuovo oggetto o contenitore.	" WPUT: PUT rapido "

IL audit-sum lo strumento può fare quanto segue:

- Elaborare registri di controllo semplici o compressi. Per esempio:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Elaborare più file contemporaneamente. Per esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Accetta input da una pipe, che consente di filtrare e preelaborare l'input utilizzando grep comando o altri mezzi. Per esempio:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

Questo strumento non accetta file compressi come input inoltrato. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando oppure utilizzare zcat strumento per decomprimere prima i file. Per 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 oppure 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 size (-s) opzione per guardare invece le dimensioni dell'oggetto.

Utilizzare il help (-h) opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-sum -h
```

Passi

1. Accedi al nodo di amministrazione principale:

- Immettere il seguente comando: ssh admin@*primary_Admin_Node_IP*
- Inserisci la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla root: su -
- Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da \$ A # .

2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, intestazione ed eliminazione, seguire questi passaggi:

- 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 del `audit-sum` attrezzo. Questo esempio mostra quanto tempo hanno richiesto le operazioni del protocollo.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media, con 1,13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano entrambe tempi molto lunghi nel caso peggiore, pari a circa 1.770 secondi.

- b. Per mostrare le 10 operazioni di recupero più lente, utilizzare il comando grep per selezionare solo i messaggi SGET e aggiungere l'opzione di output lunga(-l) per includere i percorsi degli oggetti:

```
grep SGET audit.log | audit-sum -l
```

I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di cercare nel registro di controllo 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/r901OaQ8JB-1566861764-4519.iso
  1624414429    10.96.101.125  object    5375001556
backup/r901OaQ8JB-1566861764-6618.iso
  1533143793    10.96.101.125  object    5183661466
backup/r901OaQ8JB-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 output di esempio, è possibile vedere che le tre richieste S3 GET più lente riguardavano oggetti di circa 5 GB di dimensione, ovvero molto più grandi degli altri oggetti. Le grandi dimensioni spiegano i lenti tempi di recupero nel caso peggiore.

3. Se vuoi determinare quali dimensioni degli oggetti vengono acquisiti e recuperati dalla tua griglia, usa l'opzione dimensione(-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 dell'oggetto per SPUT è inferiore a 2,5 MB, ma la dimensione media per SGET è molto più grande. Il numero di messaggi SPUT è molto più elevato del numero di messaggi SGET, il che indica che la maggior parte degli oggetti non viene mai recuperata.

4. Se vuoi determinare se i recuperi sono stati lenti ieri:

- a. Emettere il comando sul registro di controllo appropriato e utilizzare l'opzione di raggruppamento per ora(-gt), seguito 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 il traffico S3 GET ha registrato un picco tra le 06:00 e le 07:00. Anche i tempi massimi e medi sono considerevolmente più alti in questi momenti e non aumentano gradualmente con l'aumentare del conteggio. Ciò suggerisce che da qualche parte è stata superata la capacità, forse nella rete o nella capacità della griglia di elaborare le richieste.

- b. Per determinare la dimensione degli oggetti recuperati ogni ora ieri, aggiungi l'opzione dimensione(-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 alcuni recuperi molto grandi si sono verificati quando il traffico di recupero complessivo era al massimo.

- c. Per vedere più dettagli, usa il "[strumento di verifica e 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 composto da molte righe, aggiungere less comando per mostrare 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 sugli oggetti:
 - a. Inizia utilizzando il -go opzione, che raggruppa separatamente i messaggi per le operazioni su oggetti e bucket:

```
grep SPUT sample.log | audit-sum -go
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.bucket	1	0.125	0.125
0.125			
SPUT.object	12	0.025	1.019
0.236			

I risultati mostrano che le operazioni SPUT per i bucket presentano caratteristiche prestazionali diverse rispetto alle operazioni SPUT per gli oggetti.

- b. Per determinare quali bucket hanno le operazioni SPUT più lente, utilizzare `-gb` opzione, che raggruppa i messaggi per bucket:

```
grep SPUT audit.log | audit-sum -gb
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning	71943	0.046	1770.563
1.571			
SPUT.cho-versioning	54277	0.047	1736.633
1.415			
SPUT.cho-west-region	80615	0.040	55.557
1.329			
SPUT.ldt002	1564563	0.011	51.569
0.361			

- c. Per determinare quali bucket hanno la dimensione dell'oggetto SPUT più grande, utilizzare entrambi `-gb` e il `-s` opzioni:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group	count	min (B)	max (B)
average (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.1dt002 0.352	1564563	0.000	999.972

Formato del messaggio di controllo

Formato del messaggio di controllo

I messaggi di controllo scambiati all'interno del sistema StorageGRID includono informazioni standard comuni a tutti i messaggi e contenuti specifici che descrivono l'evento o l'attività segnalata.

Se le informazioni riassuntive fornite dal "[audit-spiegazione](#)" E "somma di controllo" strumenti non è sufficiente, fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di audit.

Di seguito è riportato un esempio di messaggio di controllo, così come potrebbe apparire nel file di registro di controllo:

```
2014-07-17T03:50:47.484627
[AUDT: [RSLT(FC32):VRGN] [AVER(UI32):10] [ATIM(UI64):1405569047484627] [ATYP(F
C32):SYSU] [ANID(UI32):11627225] [AMID(FC32):ARNI] [ATID(UI64):94457363265006
03516]]
```

Ogni messaggio di controllo 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 []
- Introdotto 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 attributo, un tipo di dati e un valore che vengono riportati nel seguente formato:

```
[ATTR(type) :value] [ATTR(type) :value]...
[ATTR(type) :value] \n
```

Il numero di elementi attributo nel messaggio dipende dal tipo di evento del messaggio. Gli elementi attributo non sono elencati in un ordine particolare.

L'elenco seguente descrive gli elementi dell'attributo:

- `ATTR` è un codice di quattro caratteri per l'attributo segnalato. Alcuni attributi sono comuni a tutti i messaggi di controllo, mentre altri sono specifici dell'evento.
- `type` è un identificatore di quattro caratteri del tipo di dati di programmazione del valore, ad esempio 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 controllo vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero lungo senza segno (32 bit); può memorizzare i numeri da 0 a 4.294.967.295.
UI64	Numero intero doppio lungo senza segno (64 bit); può memorizzare i numeri da 0 a 18.446.744.073.709.551.615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32 bit rappresentato da quattro caratteri ASCII, ad esempio "ABCD".
iPad	Utilizzato per gli indirizzi IP.
CSTR	Un array di lunghezza variabile di caratteri UTF-8. I caratteri possono essere sottoposti a escape con le seguenti convenzioni: <ul style="list-style-type: none"> • La barra rovesciata è `\\`. • Il ritorno a capo è `\\r`. • Le virgolette doppie sono `\"`. • L'avanzamento di riga (nuova riga) è `\\n`. • I caratteri possono essere sostituiti dai loro equivalenti esadecimali (nel formato `\\xHH`, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento

Ogni messaggio di controllo nel registro di controllo registra dati specifici di un evento di sistema.

Dopo l'apertura [AUDT : contenitore che identifica il messaggio stesso, il set successivo di attributi fornisce informazioni sull'evento o sull'azione descritta dal messaggio di controllo. Questi attributi sono evidenziati nel seguente esempio:

```
2018-12-05T08:24:45.921845 [AUDT:*]\[RSLT\FC32]:SUCS]*  
\[TIME\UI64:11454]\\[SAIP\IPAD\]:10.224.0.100"\]\[S3AI\CSTR\]:60025621595611246499"\]  
\[SACC\CSTR\]:account"\]\[S3AK\CSTR\]:SGKH4_Nc8SO1H6w3w0nCOFCGgk_E6dYzKlumRs  
KJA=="\]\[SUSR\CSTR\]:urn:sgws:identity::60025621595611246499:root"\]  
\[SBAI\CSTR\]:60025621595611246499"\]\[SBAC\CSTR\]:account"\]\[S3BK\CSTR\]:bucket"\]  
\[S3KY\CSTR\]:object"\]\[CBID\UI64:0xCC128B9B9E428347\]\[UUID\CSTR\]:B975D2CE-E4DA-  
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\UI64:30720]\[AVER\UI32:10]  
\[ATIM\UI64:1543998285921845]\[ATYP\FC32:SHEA]\[ANID\UI32:12281045]\[AMID\FC32:S3RQ]  
\[ATID\UI64:15552417629170647261]]
```

IL ATYP elemento (sottolineato nell'esempio) identifica quale evento ha generato il messaggio. Questo messaggio di esempio include il "["KARITÉ"](#)" codice messaggio ([ATYP(FC32):SHEA]), che indica che è stato generato da una richiesta S3 HEAD riuscita.

Elementi comuni nei messaggi di audit

Tutti i messaggi di audit contengono elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	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 controllo.
ANID	UI32	ID nodo: ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID . Questo ID non può essere modificato.
ASES	UI64	Identificatore della sessione di audit: nelle versioni precedenti, questo elemento indicava l'ora in cui il sistema di audit veniva inizializzato dopo l'avvio del servizio. Questo valore temporale è stato misurato in microsecondi a partire dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Nota: questo elemento è obsoleto e non compare più nei messaggi di controllo.

Codice	Tipo	Descrizione
ASQN	UI64	<p>Conteggio sequenza: nelle versioni precedenti, questo contatore veniva incrementato per ogni messaggio di controllo generato sul nodo della griglia (ANID) e reimpostato a zero al riavvio del servizio.</p> <p>Nota: questo elemento è obsoleto e non compare più nei messaggi di controllo.</p>
ATID	UI64	ID traccia: identificatore condiviso dall'insieme dei messaggi attivati da un singolo evento.
ATIM	UI64	<p>Timestamp: ora in cui è stato generato l'evento che ha attivato il messaggio di controllo, misurata in microsecondi a partire dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per convertire il timestamp in data e ora locali si basano sui millisecondi.</p> <p>Potrebbe essere necessario arrotondare o troncare il timestamp registrato. L'ora leggibile dall'uomo che appare all'inizio del messaggio di controllo nel audit.log il file è l'attributo ATIM nel formato ISO 8601. La data e l'ora sono rappresentate come YYYY-MM-DDTHH:MM:SS.UUUUUU, dove il T è un carattere stringa letterale che indica l'inizio del segmento temporale della data. UUUUUU sono microsecondi.</p>
ATYP	FC32	Tipo di evento: identificatore di quattro caratteri dell'evento registrato. Questo regola il contenuto del "payload" del messaggio: gli attributi che sono inclusi.
AVERE	UI32	Versione: la versione del messaggio di controllo. Con l'evoluzione del software StorageGRID, 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 elaborare 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, viene utilizzato NONE anziché SUCS, in modo che il messaggio non venga filtrato accidentalmente.

Esempi di messaggi di audit

Puoi trovare informazioni dettagliate in ogni messaggio di controllo. Tutti i messaggi di controllo utilizzano lo stesso formato.

Di seguito è riportato un esempio di messaggio di controllo come potrebbe apparire 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) :"s3small1"] [S3K
Y(CSTR) :"hello1"] [CBID(UI64) :0x50C4F7AC2BC8EDF7] [CSIZ(UI64) :0
] [AVER(UI32) :10] [ATIM(UI64) :1405631878959669] [ATYP(FC32) :SPUT
] [ANID(UI32) :12872812] [AMID(FC32) :S3RQ] [ATID(UI64) :1579224144
102530435]]
```

Il messaggio di controllo contiene informazioni sull'evento registrato, nonché informazioni sul messaggio di controllo stesso.

Per identificare quale evento viene registrato dal messaggio di controllo, 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) :"s3small1"] [S3K
Y(CSTR) :"hello1"] [CBID(UI64) :0x50C4F7AC2BC8EDF7] [CSIZ(UI64) :0
] [AVER(UI32) :10] [ATIM(UI64) :1405631878959669] [ATYP(FC32) :SP
UT] [ANID(UI32) :12872812] [AMID(FC32) :S3RQ] [ATID(UI64) :1579224
144102530435]]
```

Il valore dell'attributo ATYP è SPUT. "**SPUT**" rappresenta una transazione S3 PUT, che registra l'inserimento di un oggetto in un bucket.

Il seguente messaggio di controllo 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\) :"s3small1"] [S3
KY(CSTR) :"hello1"] [CBID(UI64) :0x50C4F7AC2BC8EDF7] [CSIZ(UI64) :0
] [AVER(UI32) :10] [ATIM(UI64) :1405631878959669] [ATYP(FC32) :SPU
T] [ANID(UI32) :12872812] [AMID(FC32) :S3RQ] [ATID(UI64) :157922414
4102530435]]
```

Per scoprire quando si è verificato l'evento PUT, annotare il timestamp UTC (Universal Coordinated Time) all'inizio del messaggio di controllo. Questo valore è una versione leggibile dall'uomo dell'attributo ATIM del messaggio di controllo 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, trascorso dall'inizio dell'epoca UNIX. Nell'esempio, il valore 1405631878959669 si traduce in giovedì 17-lug-2014 21:17:59 UTC.

Messaggi di audit e ciclo di vita degli oggetti

Quando vengono generati i messaggi di audit?

I messaggi di controllo 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 dell'API S3.

I messaggi di controllo sono collegati tramite identificatori specifici per ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (secchio), S3KY (chiave) o entrambi
Collegamento delle operazioni Swift	WCON (contenitore), WOBJ (oggetto) o entrambi
Collegamento delle operazioni interne	CBID (identificatore interno dell'oggetto)

Tempistica dei messaggi di audit

A causa di fattori quali le differenze di temporizzazione tra i nodi della griglia, le dimensioni degli oggetti e i ritardi di rete, l'ordine dei messaggi di controllo generati dai diversi servizi può variare da quello mostrato negli esempi di questa sezione.

Transazioni di acquisizione di oggetti

È possibile identificare le transazioni di acquisizione del client nel registro di controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di acquisizione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

Messaggi di controllo di acquisizione S3

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione di acquisizione S3 PUT è stata completata correttamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regole dell'oggetto soddisfatte	Per questo oggetto è stata soddisfatta la politica ILM.	CBID	"ORLM: Regole dell'oggetto soddisfatte"

Messaggi di controllo di acquisizione rapida

Codice	Nome	Descrizione	Traccia	Vedere
WPUT	Transazione PUT rapida	Una transazione di acquisizione Swift PUT è stata completata con successo.	CBID, WCON, WOBJ	"WPUT: PUT rapido"
ORLM	Regole dell'oggetto soddisfatte	Per questo oggetto è stata soddisfatta la politica ILM.	CBID	"ORLM: Regole dell'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 archiviazione (servizio LDR).

In questo esempio, la policy ILM attiva include la regola ILM Crea 2 copie.



Non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione di acquisizione S3 (SPUT).

In questo esempio si 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) :"SGKHyalRU_5cLflqajtaFmxJn9461AWRJfBF33gAOg=="] [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\ ) :PUT] [ANID (UI32) :12086324] [AMID (FC32)  
:S3RQ] [ATID (UI64) :14399932238768197038] ]
```

ORLM: Regole dell'oggetto soddisfatte

Il messaggio ORLM indica che la policy ILM è stata soddisfatta per questo oggetto. Il messaggio include il CBID dell'oggetto e il nome della regola ILM applicata.

Per gli oggetti replicati, il campo LOCS include l'ID del nodo LDR e l'ID del volume delle posizioni degli oggetti.

2019-07-

```
17T21:18:31.230669 [AUDT: [CBID\ (UI64\ ) :0x50C4F7AC2BC8EDF7] [RULE (CSTR) :"Make  
2 Copies"] [STAT (FC32) :DONE] [CSIZ (UI64) :0] [UUID (CSTR) :"0B344E18-98ED-4F22-  
A6C8-A93ED68F8D3F"] [LOCS (CSTR) :"CLDI 12828634 2148730112, CLDI 12745543  
2147552014"] [RSLT (FC32) :SUCS] [AVER (UI32) :10] [ATYP\ (FC32\ ) :ORLM] [ATIM (UI64)  
:1563398230669] [ATID (UI64) :15494889725796157557] [ANID (UI32) :13100453] [AMID  
(FC32) :BCMS] ]
```

Per gli oggetti con codice di cancellazione, il campo LOCS include l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione

2019-02-23T01:52:54.647537

```
[AUDT: [CBID (UI64) :0xFA8ABE5B5001F7E2] [RULE (CSTR) :"EC_2_plus_1"] [STAT (FC32)  
:DONE] [CSIZ (UI64) :10000] [UUID (CSTR) :"E291E456-D11A-4701-8F51-  
D2F7CC9AFECA"] [LOCS (CSTR) :"CLEC 1 A471E45D-A400-47C7-86AC-  
12E77F229831"] [RSLT (FC32) :SUCS] [AVER (UI32) :10] [ATIM (UI64) :1550929974537]\ [  
ATYP\ (FC32\ ) :ORLM\ ] [ANID (UI32) :12355278] [AMID (FC32) :ILMX] [ATID (UI64) :41685  
59046473725560] ]
```

Il campo PATH include informazioni sul bucket S3 e sulla chiave oppure informazioni sul contenitore 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_
1vf9q"] [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 controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

S3 elimina i messaggi di controllo

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta effettuata per eliminare l'oggetto da un bucket.	CBID, S3KY	"SDEL: S3 ELIMINA"

Eliminazione rapida dei messaggi di controllo

Codice	Nome	Descrizione	Traccia	Vedere
WDEL	Eliminazione rapida	Richiesta effettuata per eliminare l'oggetto da un contenitore o il contenitore stesso.	CBID, WOBJ	"WDEL: CANCELLA rapida"

Esempio: eliminazione dell'oggetto S3

Quando un client S3 elimina un oggetto da un nodo di archiviazione (servizio LDR), viene generato un messaggio di controllo che viene salvato nel registro di controllo.



Nell'esempio seguente non sono elencati tutti i messaggi di controllo generati durante una transazione di eliminazione. Sono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: Elimina S3

L'eliminazione dell'oggetto inizia quando il client invia una richiesta DeleteObject a un servizio LDR. Il messaggio contiene il bucket da cui eliminare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificarlo.

2017-07-

```
17T21:17:58.959669 [AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10.96.112.29"] [S3AI(CSTR):"70899244468554783528"] [SACC(CSTR):"test"] [S3AK(CSTR):"SGKHyalRU_5cLflqajtaFmxJn9461AWRJfBF33gAOg=="] [SUSR(CSTR):"urn:sgws:identity::70899244468554783528:root"] [SBAI(CSTR):"70899244468554783528"] [SBACK(CSTR):"test"] \ [S3BK\ (CSTR\):"example"\] \ [S3KY\ (CSTR\):"testobject-0-7"\] [CBID\ (UI64\):0x339F21C5A6964D89] [CSIZ(UI64):30720] [AVER(UI32):10] [ATIM(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 controllo specifici dell'API S3.

Non tutti i messaggi di controllo 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 del recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta effettuata per recuperare un oggetto da un bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Messaggi di controllo di recupero rapido

Codice	Nome	Descrizione	Traccia	Vedere
WGET	GET rapido	Richiesta effettuata per recuperare un oggetto da un contenitore.	CBID, WCON, WOBJ	"WGET: GET rapido"

Esempio: recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di archiviazione (servizio LDR), viene generato un messaggio di controllo che viene salvato nel registro di controllo.

Si noti che non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti inizia quando il client invia una richiesta GetObject a un servizio LDR. Il messaggio contiene il bucket da cui recuperare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificarlo.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUFS] [TIME(UI64):47807] [SAIP(IPAD) :"10.96.112.26"] [S3AI(
CSTR) :"43979298178977966408"] [SACC(CSTR) :"s3-account-
a"] [S3AK(CSTR) :"SGKht7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_Few=="] [SUSR(CSTR) :"urn:sgws:identity::43979298178977966408:root"] [SBAI(
CSTR) :"43979298178977966408"] [SBAC(CSTR) :"s3-account-
a"]\[S3BK\](CSTR\):"bucket-
anonymous"\]\[S3KY\](CSTR\):"Hello.txt"\] [CBID(UI64):0x83D70C6F1F662B02] [CS
IZ(UI64):12] [AVER(UI32):10] [ATIM(UI64):1505947988782605]\[ATYP\](FC32\):SGE
T\] [ANID(UI32):12272050] [AMID(FC32):S3RQ] [ATID(UI64):17742374343649889669]
]
```

Se la policy del bucket lo consente, un client può recuperare oggetti in modo anonimo oppure può recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di controllo contiene informazioni sull'account tenant del proprietario del bucket, in modo da poter monitorare queste richieste anonime e tra account.

Nel seguente messaggio di esempio, il client invia una richiesta GetObject per un oggetto archiviato in un bucket di cui non è proprietario. I valori per SBAI e SBAC registrano l'ID e il nome dell'account tenant del proprietario del bucket, che differiscono dall'ID e dal nome dell'account tenant del client registrati in S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUFS] [TIME(UI64):53244] [SAIP(IPAD) :"10.96.112.26"] \[S3AI
\](CSTR\):"17915054115450519830"\]\[SACC\](CSTR\):"s3-account-
b"] [S3AK(CSTR) :"SGKhpolW1P_kBkqSCbt1754Ls81BUog67I2L1SiUg=="] [SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\](CSTR\):"4397929817
8977966408"\]\[SBAC\](CSTR\):"s3-account-a"\] [S3BK(CSTR) :"bucket-
anonymous"] [S3KY(CSTR) :"Hello.txt"] [CBID(UI64):0x83D70C6F1F662B02] [CSIZ(UI
64):12] [AVER(UI32):10] [ATIM(UI64):1505947995876415] [ATYP(FC32):SGET] [ANID(
UI32):12272050] [AMID(FC32):S3RQ] [ATID(UI64):6888780247515624902]]
```

Esempio: S3 Selezione su un oggetto

Quando un client S3 emette una query S3 Select su un oggetto, vengono generati messaggi di controllo che vengono salvati nel registro di controllo.

Si noti che non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

Ogni query genera due messaggi di controllo: uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "select") e una successiva operazione GET standard che recupera i dati dall'archivio durante l'elaborazione.

```

2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]

```

```

2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"\\"x-forwarded-
for\":\\unix:\\}"] [S3AI(CSTR):"63147909414576125820"] [SACC(CSTR):"Tenant16
36027116"] [S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"] [SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"] [SBAI(CSTR):"63147909414576125820"] [SBAC(CST
R):"Tenant1636027116"] [S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"] [S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]

```

Messaggi di aggiornamento dei metadati

I messaggi di controllo vengono generati quando un client S3 aggiorna i metadati di un oggetto.

Messaggi di controllo dell'aggiornamento dei metadati S3

Codice	Nome	Descrizione	Traccia	Vedere
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati per 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 metadati S3

Il client S3 effettua una richiesta (SUPD) per aggiornare i metadati specificati(x-amz-meta-*) 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 controllo (**CONFIGURAZIONE > Monitoraggio > Server di controllo e syslog**). Vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)".

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUFS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):{"\\"accept-encoding\\":\\"identity\\",\\"authorization\\":\\"AWS
LIUF17FGJARQHPY2E761:jul/hnzs/uNY+aVvV0lTSYhEGts=\\"",

\"content-length\\":\"0\",\"date\\\":\"Tue, 11 Jul 2017 21:54:03
GMT\\\",\"host\\\":\"10.96.99.163:18082\",
\"user-agent\\\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\\\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\\\":\"REPLACE\",\"x-amz-meta-city\\\":\"Vancouver\\"\}]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Messaggi di controllo

Descrizioni dei messaggi di audit

Nelle sezioni seguenti sono elencate descrizioni dettagliate dei messaggi di controllo restituiti dal sistema. Ogni messaggio di controllo viene prima elencato in una tabella che raggruppa i messaggi correlati in base alla classe di attività che il messaggio rappresenta. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit, sia per selezionare il tipo desiderato di filtraggio dei messaggi di audit.

I messaggi di controllo sono inoltre elencati in ordine alfabetico in base ai rispettivi codici di 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 controllo, sulla modifica delle destinazioni dei registri e sull'utilizzo di un server syslog esterno per le informazioni di controllo, vedere "[Configurare i messaggi di controllo e le destinazioni dei registri](#)"

Categorie di messaggi di audit

Messaggi di controllo del sistema

I messaggi di audit appartenenti alla categoria di audit del sistema vengono utilizzati per eventi correlati al sistema di audit stesso, agli stati dei nodi della griglia, alle 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	Frammento di dati con codice di cancellazione mancante: indica che è stato rilevato un frammento di dati con codice di cancellazione mancante.	"ECMC: frammento di dati codificato in modo cancellabile mancante"
ECOC	Frammento di dati con codice di cancellazione danneggiato: indica che è stato rilevato un frammento di dati con codice di cancellazione danneggiato.	"ECOC: Frammento di dati corrotti con codice di cancellazione"
ETAF	Autenticazione di sicurezza non riuscita: un tentativo di connessione tramite Transport Layer Security (TLS) non è riuscito.	"ETAF: Autenticazione di sicurezza non riuscita"
GNRG	Registrazione GNDS: un servizio che aggiorna o regista informazioni su se stesso nel sistema StorageGRID .	"GNRG: Registrazione GNDS"
GNUR	Annullo della registrazione GNDS: un servizio ha annullato la registrazione dal sistema StorageGRID .	"GNUR: Annullo della registrazione GNDS"
GTED	Attività di griglia terminata: il servizio CMN ha terminato l'elaborazione dell'attività di griglia.	"GTED: attività di griglia terminata"
GTST	Attività di griglia avviata: il servizio CMN ha iniziato a elaborare l'attività di griglia.	"GTST: Attività di griglia avviata"
GTSU	Attività di griglia inviata: un'attività di griglia è stata inviata al servizio CMN.	"GTSU: compito di griglia inviato"

Codice	Titolo e descrizione del messaggio	Vedere
LLST	Posizione persa: questo messaggio di controllo viene generato quando una posizione viene persa.	" LLST: Posizione persa "
OLST	Oggetto perso: l'oggetto richiesto non può essere individuato nel sistema StorageGRID .	" OLST: il sistema ha rilevato un oggetto smarrito "
SADD	Disattivazione controllo di sicurezza: la registrazione dei messaggi di controllo è stata disattivata.	" SADD: Disabilitazione controllo sicurezza "
SADE	Abilitazione controllo di sicurezza: la registrazione dei messaggi di controllo è stata ripristinata.	" SADE: Abilitazione controllo sicurezza "
SVRF	Verifica fallita dell'archivio oggetti: un blocco di contenuto non ha superato i controlli di verifica.	" SVRF: Errore di verifica dell'archivio oggetti "
SVRU	Verifica archivio oggetti sconosciuta: rilevati dati oggetto inattesi nell'archivio oggetti.	" SVRU: Verifica archivio oggetti sconosciuto "
SYSD	Arresto del nodo: è stato richiesto un arresto.	" SYSD: arresto del nodo "
SISTEMA	Arresto del nodo: un servizio ha avviato un arresto regolare.	" SYST: Arresto del nodo "
SIST	Avvio nodo: un servizio avviato; la natura dell'arresto precedente è indicata nel messaggio.	" SYSU: Avvio del nodo "

Messaggi di controllo dell'archiviazione degli oggetti

I messaggi di controllo appartenenti alla categoria di controllo dell'archiviazione degli oggetti vengono utilizzati per gli eventi correlati all'archiviazione e alla gestione degli oggetti all'interno del sistema StorageGRID . Tra questi rientrano l'archiviazione e il recupero di oggetti, i trasferimenti da nodo griglia a nodo griglia e le verifiche.

 I codici di controllo vengono rimossi dal prodotto e dalla documentazione quando le funzionalità diventano obsolete. Se riscontri un codice di controllo non elencato qui, controlla le versioni precedenti di questo argomento per le versioni SG più vecchie. Ad esempio, "[Messaggi di controllo dell'archiviazione degli oggetti StorageGRID 11.8](#)" .

Codice	Descrizione	Vedere
FRATELLO	Richiesta di sola lettura del bucket: un bucket è entrato o uscito dalla modalità di sola lettura.	" BROR: Richiesta di sola lettura del bucket "

Codice	Descrizione	Vedere
CBSE	Fine invio oggetto: l'entità sorgente ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	" CBSE: Fine invio oggetto "
CBRE	Fine ricezione oggetto: l'entità di destinazione ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	" CBRE: Oggetto Ricevente Fine "
CGRR	Richiesta di replica tra griglie: StorageGRID ha tentato un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglia.	" CGRR: richiesta di replicazione tra griglie "
EBCD	Eliminazione bucket vuoto: lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione di bucket vuoto).	" EBCD: Eliminazione bucket vuoto "
EBKR	Richiesta di 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 archiviato e verificato e ora può essere richiesto.	" SCMT: richiesta di commit dell'archivio oggetti "
SREM	Rimozione archivio oggetti: un blocco di contenuto è stato eliminato da un nodo della griglia e non può più essere richiesto direttamente.	" SREM: Rimozione dell'archivio oggetti "

Il cliente ha letto i messaggi di controllo

I messaggi di controllo di lettura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
S3SL	Richiesta S3 Select: registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.	Cliente S3	" S3SL: Richiesta di selezione S3 "

Codice	Descrizione	Utilizzato da	Vedere
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 controllo includerà il campo S3SR.	Cliente S3	"SGET: S3 GET"
KARITÉ	S3 HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Cliente S3	"SHEA: TESTA S3"
WGET	Swift GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un contenitore.	Cliente Swift	"WGET: GET rapido"
WHEA	Swift HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un contenitore.	Cliente Swift	"WHEA: TESTA Veloce"

Il cliente scrive messaggi di audit

I messaggi di controllo di scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Sovrascrittura oggetto: registra una transazione per sovrascrivere un oggetto con un altro oggetto.	Client S3 e Swift	"OVWR: sovrascrittura oggetto"
SDEL	S3 DELETE: registra una transazione riuscita per eliminare un oggetto o un bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	Cliente S3	"SDEL: S3 ELIMINA"
SPOS	S3 POST: registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Cliente S3	"SPOS: S3 POST"
SPUT	S3 PUT: registra una transazione riuscita per creare un nuovo oggetto o bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	Cliente S3	"SPUT: S3 PUT"
SUPD	Metadati S3 aggiornati: registra una transazione riuscita per aggiornare i metadati per un oggetto o un bucket esistente.	Cliente S3	"SUPD: Metadati S3 aggiornati"

Codice	Descrizione	Utilizzato da	Vedere
WDEL	Swift DELETE: registra una transazione riuscita per eliminare un oggetto o un contenitore.	Cliente Swift	" WDEL: CANCELLA rapida "
WPUT	Swift PUT: registra una transazione riuscita per creare un nuovo oggetto o contenitore.	Cliente Swift	" WPUT: PUT rapido "

Messaggio di controllo di gestione

La categoria Gestione registra le richieste degli utenti nell'API di gestione.

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di controllo dell'API di gestione: un registro delle richieste degli utenti.	" MGAU: Messaggio di audit di gestione "

Messaggi di controllo ILM

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per eventi correlati alle operazioni di gestione del ciclo di vita delle informazioni (ILM).

Codice	Titolo e descrizione del messaggio	Vedere
IDEL	Eliminazione avviata da ILM: questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	" IDEL: ILM ha avviato l'eliminazione "
LKCU	Pulizia degli oggetti sovrascritti. Questo messaggio di controllo viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di archiviazione.	" LKCU: Pulizia degli oggetti sovrascritti "
ORLM	Regole oggetto soddisfatte: questo messaggio di controllo viene generato quando i dati dell'oggetto vengono archiviati come specificato dalle regole ILM.	" ORLM: Regole dell'oggetto soddisfatte "

Riferimento al messaggio di audit

BROR: Richiesta di sola lettura del bucket

Il servizio LDR genera questo messaggio di controllo quando un bucket entra o esce dalla modalità di sola lettura. Ad esempio, un bucket entra in modalità di sola lettura mentre tutti gli oggetti vengono eliminati.

Codice	Campo	Descrizione
BKHD	UUID del bucket	L'ID del bucket.

Codice	Campo	Descrizione
BROV	Valore della richiesta di sola lettura del bucket	Se il bucket viene reso di sola lettura o sta abbandonando lo stato di sola lettura (1 = di sola lettura, 0 = non di sola lettura).
FRATELLI	Motivo di sola lettura del bucket	Il motivo per cui il bucket viene reso di sola lettura o abbandona lo stato di sola lettura. Ad esempio, emptyBucket.
S3AI	ID account tenant S3	ID dell'account tenant che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.

CBRB: Oggetto Ricevi Inizio

Durante il normale funzionamento del sistema, i blocchi di contenuto vengono trasferiti continuamente tra diversi nodi man mano che i dati vengono consultati, replicati e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo a un altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo conteggio sequenziale richiesto. Se l'operazione ha esito positivo, il trasferimento inizia da questo conteggio sequenziale.
CTES	Conteggio previsto della sequenza finale	Indica l'ultimo conteggio sequenziale richiesto. In caso di esito positivo, il trasferimento è considerato completato quando è stato ricevuto questo conteggio sequenziale.

Codice	Campo	Descrizione
RSLT	Stato di inizio del trasferimento	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato con successo.

Questo messaggio di controllo indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo contenuto, come identificato dal suo identificatore del blocco di contenuto. L'operazione richiede i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale previsto". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e, se combinate con i messaggi di controllo dell'archiviazione, per verificare i conteggi delle repliche.

CBRE: Oggetto Ricevente Fine

Quando il trasferimento di un blocco di contenuto da un nodo a un altro è completato, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il conteggio della sequenza in cui è iniziato il trasferimento.
CTAS	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio sequenziale trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è andato a buon fine, non è stato scambiato alcun dato.

Codice	Campo	Descrizione
RSLT	Risultato del trasferimento	<p>Il risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente):</p> <p>SUCS: trasferimento completato con successo; tutti i conteggi delle sequenze richiesti sono stati inviati.</p> <p>CONL: connessione persa durante il trasferimento</p> <p>CTMO: timeout della connessione durante l'avvio 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 controllo indica che è stata completata un'operazione di trasferimento dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale effettivo". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se abbinato ai messaggi di controllo dell'archiviazione, può essere utilizzato anche per verificare i conteggi delle repliche.

CBSB: Inizio invio oggetto

Durante il normale funzionamento del sistema, i blocchi di contenuto vengono trasferiti continuamente tra diversi nodi man mano che i dati vengono consultati, replicati e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo a un altro, questo messaggio viene emesso dall'entità sorgente.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.

Codice	Campo	Descrizione
CTSS	Avvia conteggio sequenza	Indica il primo conteggio sequenziale richiesto. Se l'operazione ha esito positivo, il trasferimento inizia da questo conteggio sequenziale.
CTES	Conteggio previsto della sequenza finale	Indica l'ultimo conteggio sequenziale richiesto. In caso di esito positivo, il trasferimento è considerato completato quando è stato ricevuto questo conteggio sequenziale.
RSLT	Stato di inizio del trasferimento	Stato al momento dell'avvio del trasferimento: SUCS: trasferimento avviato con successo.

Questo messaggio di controllo indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo contenuto, come identificato dal suo identificatore del blocco di contenuto. L'operazione richiede i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale previsto". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e, se combinate con i messaggi di controllo dell'archiviazione, per verificare i conteggi delle repliche.

CBSE: Fine invio oggetto

Quando il trasferimento di un blocco di contenuto da un nodo a un altro è completato, questo messaggio viene emesso dall'entità sorgente.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a 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 sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il conteggio della sequenza in cui è iniziato il trasferimento.

Codice	Campo	Descrizione
CTAS	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio sequenziale trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è andato a buon fine, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	<p>Il risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente):</p> <p>SUCS: Trasferimento completato con successo; tutti i conteggi delle sequenze richiesti sono stati inviati.</p> <p>CONL: connessione persa durante il trasferimento</p> <p>CTMO: timeout della connessione durante l'avvio 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 controllo indica che è stata completata un'operazione di trasferimento dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale effettivo". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se abbinato ai messaggi di controllo dell'archiviazione, può essere utilizzato anche per verificare i conteggi delle repliche.

CGRR: richiesta di replicazione tra griglie

Questo messaggio viene generato quando StorageGRID tenta un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglie.

Codice	Campo	Descrizione
CSIZ	Dimensione dell'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 tra griglie che coprono un aggiornamento StorageGRID dalla versione 11.7 alla 11.8 potrebbero avere una dimensione totale degli oggetti non accurata.</p>
S3AI	ID account tenant S3	ID dell'account tenant proprietario del bucket da cui viene replicato l'oggetto.
GFID	ID di connessione della federazione di rete	ID della connessione di federazione della griglia utilizzata per la replica tra griglie.

Codice	Campo	Descrizione
OPER	operazione CGR	Tipo di operazione di replicazione tra griglie tentata: <ul style="list-style-type: none"> • 0 = Replica oggetto • 1 = Replica oggetto multipart • 2 = Replica elimina marcatore
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket.
VSID	ID versione	ID della versione specifica di un oggetto che è stato replicato.
RSLT	Codice risultato	Restituisce un errore riuscito (SUCC) o generale (GERR).

EBDL: Eliminazione bucket vuoto

Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione di svuotamento del bucket).

Codice	Campo	Descrizione
CSIZ	Dimensione dell'oggetto	La dimensione dell'oggetto in byte.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	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, viene utilizzato NONE anziché SUCC, in modo che il messaggio non venga filtrato accidentalmente.

EBKR: Richiesta bucket vuoto

Questo messaggio indica che un utente ha inviato una richiesta per attivare o disattivare un bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).

Codice	Campo	Descrizione
COSTRUIRE	UUID del bucket	L'ID del bucket.
EBJS	Configurazione JSON del bucket vuoto	Contiene il JSON che rappresenta la configurazione corrente del bucket vuoto.
S3AI	ID account tenant S3	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.

ECMC: frammento di dati codificato in modo cancellabile mancante

Questo messaggio di controllo indica che il sistema ha rilevato un frammento di dati mancante con codice di cancellazione.

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il blocco mancante.
MCID	ID del blocco	L'identificatore del frammento mancante con codice di cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo specifico messaggio. Viene utilizzato 'NONE' anziché 'SUICS' in modo che il messaggio non venga filtrato.

ECOC: Frammento di dati corrotti con codice di cancellazione

Questo messaggio di controllo indica che il sistema ha rilevato un frammento di dati con codice di cancellazione corrotto.

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco danneggiato.
VLID	ID volume	Il volume RangeDB che contiene il frammento con codice di cancellazione danneggiato.
CCID	ID del blocco	L'identificatore del frammento corrotto con codice di cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo specifico messaggio. Viene utilizzato 'NONE' anziché 'SUICS' in modo che il messaggio non venga filtrato.

ETAF: Autenticazione di sicurezza non riuscita

Questo messaggio viene generato quando un tentativo di connessione tramite Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP su cui l'autenticazione non è riuscita.
RUID	Identità utente	Un identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.
RSLT	Codice motivo	Motivo del fallimento: SCNI: Impossibile stabilire una connessione sicura. CERM: Certificato mancante. CERT: Il certificato non è valido. CERE: Il certificato è scaduto. CERR: Il certificato è stato revocato. CSGN: la firma del certificato non è valida. CSGU: Il firmatario del certificato era sconosciuto. UCRM: le credenziali utente erano mancanti. UCRI: Le credenziali utente non erano valide. UCRU: Le credenziali utente non erano consentite. TOUT: Autenticazione scaduta.

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 fallisce a causa di certificati o credenziali non validi, inattesi o non consentiti, viene registrato un messaggio di controllo. Ciò consente di effettuare query su tentativi di accesso non autorizzati e altri problemi di connessione correlati alla sicurezza.

Il messaggio potrebbe essere causato da un'entità remota con una configurazione errata o da tentativi di presentare al sistema credenziali non valide o non consentite. Questo messaggio di controllo deve essere monitorato per rilevare tentativi di accesso non autorizzato al sistema.

GNRG: Registrazione GNDS

Il servizio CMN genera questo messaggio di controllo quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID .

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: <ul style="list-style-type: none"> • SUCS: Riuscito • SUNV: Servizio non disponibile • GERR: Altro fallimento
GNID	Nodo ID	ID nodo del servizio che ha avviato la richiesta di aggiornamento.
GNTP	Tipo di dispositivo	Il tipo di dispositivo del nodo della griglia (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello del dispositivo del nodo della griglia nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo della griglia (nel contesto dei costi dei collegamenti 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 Grid Nodes Bundle.

GNUR: Annullamento della registrazione GNDS

Il servizio CMN genera questo messaggio di controllo quando un servizio dispone di 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"> • SUCS: Riuscito • SUNV: Servizio non disponibile • GERR: Altro fallimento
GNID	Nodo ID	ID nodo del servizio che ha avviato la richiesta di aggiornamento.

GTED: attività di griglia terminata

Questo messaggio di controllo indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e ha spostato l'attività nella tabella Cronologica. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato il messaggio di controllo corrispondente Grid Task Started. Gli altri risultati indicano che l'elaborazione di questa attività di griglia non è mai iniziata.

Codice	Campo	Descrizione
TSID	ID attività	<p>Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita.</p> <p>Nota: l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.</p>
RSLT	Risultato	<p>Il risultato finale dello stato dell'attività della griglia:</p> <ul style="list-style-type: none"> • SUCS: L'attività della griglia è stata completata con successo. • ABRT: L'attività della griglia è stata terminata senza un errore di rollback. • ROLF: L'attività di griglia è stata terminata e non è stato possibile completare il processo di rollback. • CANC: l'attività della griglia è stata annullata dall'utente prima di essere avviata. • EXPR: L'attività della griglia è scaduta prima di essere avviata. • IVLD: L'attività della griglia non era valida. • AUTH: L'attività di griglia non era autorizzata. • DUPL: l'attività della griglia è stata rifiutata come duplicata.

GTST: Attività di griglia avviata

Questo messaggio di controllo indica che il servizio CMN ha iniziato a elaborare l'attività di griglia specificata. Il messaggio di controllo segue immediatamente il messaggio Grid Task Submitted per le attività della griglia avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inviate alla tabella In sospeso, questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	<p>Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita.</p> <p>Nota: l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.</p>

Codice	Campo	Descrizione
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: <ul style="list-style-type: none">• SUCS: L'attività della griglia è stata avviata correttamente.

GTSU: compito di griglia inviato

Questo messaggio di controllo indica che un'attività di griglia è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	Identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita. Nota: l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.
TTYP	Tipo di attività	Il tipo di attività della griglia.
TVER	Versione dell'attività	Un numero che indica la versione dell'attività della griglia.
TDSC	Descrizione dell'attività	Una descrizione leggibile dall'uomo dell'attività della griglia.
IVA	Valido dopo il timestamp	Il momento più remoto (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui l'attività della griglia è valida.
VBTS	Valido prima del timestamp	L'ultima ora (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui l'attività della griglia è valida.
TSRC	Fonte	La fonte del compito: <ul style="list-style-type: none">• TXTB: l'attività della griglia è stata inviata tramite il sistema StorageGRID come blocco di testo firmato.• GRIGLIA: l'attività della griglia è stata inviata tramite il servizio interno di invio delle attività della griglia.
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 della griglia è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per la sorgente TXTB.

Codice	Campo	Descrizione
RSLT	Risultato	Il risultato dell'invio: <ul style="list-style-type: none"> SUCS: L'attività della griglia è stata inviata correttamente. FAIL: l'attività è stata spostata direttamente nella tabella storica.

IDEI: ILM ha avviato l'eliminazione

Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto.

Il messaggio IDEI viene generato in una di queste situazioni:

- Per gli oggetti nei bucket S3 conformi:** questo messaggio viene generato quando ILM avvia il processo di eliminazione automatica di un oggetto perché il suo periodo di conservazione è scaduto (presupponendo che l'impostazione di eliminazione automatica sia abilitata e la conservazione legale sia disattivata).
- Per gli oggetti nei bucket S3 non conformi.** Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto perché nessuna istruzione di posizionamento nei criteri ILM attivi è attualmente applicabile all'oggetto.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Conformità: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), indica se un oggetto conforme deve essere eliminato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale.
CMPL	Conformità: Conservazione legale	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), indica se il bucket è attualmente sottoposto a un blocco legale.
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. Durata del periodo di conservazione dell'oggetto in minuti.
CTME	Conformità: tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Tempo di ingestione dell'oggetto. È possibile aggiungere a questo valore il periodo di conservazione in minuti per determinare quando l'oggetto può essere eliminato dal bucket.
DMRK	Elimina ID versione marcitore	ID versione del marcitore di eliminazione creato durante l'eliminazione di un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCATION	Posizioni	<p>Posizione di archiviazione dei dati degli oggetti all'interno del sistema StorageGRID . Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato eliminato).</p> <p>CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione 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 del nodo ARC della posizione dell'oggetto se i dati dell'oggetto sono archiviati.</p>
SENTIERO	Secchio/chiaue S3	Nome del bucket S3 e nome della chiave S3.
RSLT	Risultato	<p>Il risultato dell'operazione ILM.</p> <p>SUCS: L'operazione ILM ha avuto successo.</p>
REGOLA	Etichetta delle regole	<ul style="list-style-type: none"> Se un oggetto in un bucket S3 conforme viene eliminato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. Se l'oggetto viene eliminato perché non ci sono più istruzioni di posizionamento applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM applicata all'oggetto.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto che è stato eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

LKCU: Pulizia degli oggetti sovrascritti

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza necessitava di essere ripulito per liberare spazio di archiviazione. Un oggetto viene sovrascritto quando un client S3 scrive un oggetto in un percorso che contiene già un oggetto. Il processo di rimozione avviene automaticamente e in

background.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LTYP	Tipo di pulizia	<i>Solo per uso interno.</i>
LUID	UUID dell'oggetto rimosso	L'identificatore dell'oggetto che è stato rimosso.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	L'identificatore dell'oggetto che esiste ancora. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

LKDM: Pulizia degli oggetti trapelati

Questo messaggio viene generato quando un blocco trapelato viene pulito o eliminato. Un blocco può essere parte di un oggetto replicato o di un oggetto codificato tramite cancellazione.

Codice	Campo	Descrizione
OROLOGIO	Posizione del blocco	Il percorso del file del frammento trapelato che è stato eliminato.
CTYP	Tipo di blocco	Tipo di pezzo: ec: Erasure-coded object chunk repl: Replicated object chunk

Codice	Campo	Descrizione
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	Tempo di creazione del blocco	Ora in cui è stato creato il frammento trapelato.
UUID	Identificatore univoco universale	L'identificatore dell'oggetto a cui appartiene il blocco.
CBID	Identificatore del blocco di contenuto	CBID dell'oggetto a cui appartiene il frammento trapelato.
CSIZ	Dimensione del contenuto	La dimensione del blocco in byte.

LLST: Posizione persa

Questo messaggio viene generato ogni volta che non è possibile trovare la posizione per una copia di un oggetto (replicata o con codice di cancellazione).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.
ECPR	Profilo di codifica di cancellazione	Per dati di oggetti codificati tramite cancellazione. ID del profilo di codifica di cancellazione utilizzato.

Codice	Campo	Descrizione
LTYP	Tipo di posizione	CLDI (online): per dati di oggetti replicati CLEC (online): per dati di oggetti codificati con cancellazione CLNL (Nearline): per dati di oggetti replicati archiviati
NOID	ID nodo sorgente	L'ID del nodo su cui sono andate perse le posizioni.
PCLD	Percorso verso l'oggetto replicato	Il percorso completo alla posizione del disco in cui si trovano i dati dell'oggetto perso. Restituito solo quando LTYP ha un valore di CLDI (ovvero, per oggetti replicati). Prende la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Risultato	Sempre NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.
TSRC	Sorgente di attivazione	UTENTE: attivato dall'utente SYST: Sistema attivato
UUID	ID univoco universale	Identificatore dell'oggetto interessato nel sistema StorageGRID .

MGAU: Messaggio di audit di gestione

La categoria Gestione registra le richieste degli utenti nell'API di gestione. Ogni richiesta HTTP che non sia una richiesta GET o HEAD a un URI API valido registra una risposta contenente il nome utente, l'IP e il tipo di richiesta all'API. Gli URI API non validi (ad esempio /api/v3-authorize) e le richieste non valide agli URI API validi non vengono registrati.

Codice	Campo	Descrizione
MDIP	Indirizzo IP di destinazione	L'indirizzo IP del server (destinazione).
MDNA	Nome di dominio	Il nome di dominio dell'host.
MPAT	Richiedi PATH	Il percorso della richiesta.

Codice	Campo	Descrizione
MPQP	Richiedi parametri di query	I parametri di query per la richiesta.
MRBD	Corpo della richiesta	<p>Il contenuto del corpo della 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 ricavate 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 dismessi in POST /grid/servers/decommission <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	Metodo di richiesta HTTP: <ul style="list-style-type: none"> • INVIARE • METTERE • ELIMINARE • TOPPA
MRSC	Codice di risposta	Il codice di risposta.
Prezzo consigliato al pubblico	Corpo della risposta	<p>Per impostazione predefinita, il contenuto della risposta (il corpo della risposta) viene registrato.</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 del client (sorgente).
MUUN	URN utente	L'URN (nome uniforme della risorsa) dell'utente che ha inviato la richiesta.
RSLT	Risultato	Restituisce l'esito positivo (SUCS) oppure l'errore segnalato dal backend.

OLST: il sistema ha rilevato un oggetto smarrito

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 smarrito.
NOID	Nodo ID	Se disponibile, l'ultima posizione nota, diretta o prossima alla linea, dell'oggetto smarrito. È possibile avere solo l'ID nodo senza un ID volume se le informazioni sul volume non sono disponibili.
SENTIERO	Secchio/chiave S3	Se disponibili, il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.
UUID	ID univoco universale	Identificatore dell'oggetto smarrito all'interno del sistema StorageGRID .
VOLI	ID volume	Se disponibile, l'ID volume del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

ORLM: Regole dell'oggetto soddisfatte

Questo messaggio viene generato quando l'oggetto viene archiviato e copiato correttamente come specificato dalle regole ILM.



Il messaggio ORLM non viene generato quando un oggetto viene archiviato correttamente dalla regola predefinita Crea 2 copie se un'altra regola nel criterio utilizza il filtro avanzato Dimensione oggetto.

Codice	Campo	Descrizione
COSTRUIRE	Testata della benna	Campo ID bucket. Utilizzato per operazioni interne. Appare solo se STAT è PRGD.
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.

Codice	Campo	Descrizione
LOCATION	Posizioni	<p>Posizione di archiviazione dei dati degli oggetti all'interno del sistema StorageGRID . Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato eliminato).</p> <p>CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione 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 del nodo ARC della posizione dell'oggetto se i dati dell'oggetto sono archiviati.</p>
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
RSLT	Risultato	<p>Il risultato dell'operazione ILM.</p> <p>SUCS: L'operazione ILM ha avuto successo.</p>
REGOLA	Etichetta delle regole	Etichetta leggibile dall'uomo assegnata alla regola ILM applicata a questo oggetto.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	Contenitore CBID	CBID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo per oggetti segmentati e multipartite.
STATISTICHE	Stato	<p>Lo stato di funzionamento dell'ILM.</p> <p>FATTO: le operazioni ILM sull'oggetto sono state completate.</p> <p>DFER: L'oggetto è stato contrassegnato per una futura rivalutazione ILM.</p> <p>PRGD: L'oggetto è stato eliminato dal sistema StorageGRID .</p> <p>NLOC: i dati dell'oggetto non sono più disponibili nel sistema StorageGRID . Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.</p>
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .

Codice	Campo	Descrizione
VSID	ID versione	ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Il messaggio di controllo ORLM può essere emesso più di una volta per un singolo oggetto. Ad esempio, viene emesso ogni volta che si verifica uno dei seguenti eventi:

- Le regole ILM per l'oggetto sono soddisfatte per sempre.
- Per questa epoca sono soddisfatte le regole ILM per l'oggetto.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati dell'oggetto replicato è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto danneggiato.

Informazioni correlate

- "[Transazioni di acquisizione di oggetti](#)"
- "[Transazioni di eliminazione degli oggetti](#)"

OVWR: sovrascrittura oggetto

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	Identificatore del blocco di contenuto (nuovo)	Il CBID del nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto sovrascritto.
Disturbo ossessivo-compulsivo (OCBD)	Identificatore del blocco di contenuto (precedente)	Il CBID dell'oggetto precedente.
UUID	ID univoco universale (nuovo)	Identificatore del nuovo oggetto all'interno del sistema StorageGRID .
OID	ID univoco universale (precedente)	Identificatore dell'oggetto precedente all'interno del sistema StorageGRID .

Codice	Campo	Descrizione
SENTIERO	Percorso oggetto S3	Il percorso dell'oggetto S3 utilizzato sia per l'oggetto precedente che per quello nuovo
RSLT	Codice risultato	Risultato della transazione di sovrascrittura dell'oggetto. Il risultato è sempre: SUCS: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.

S3SL: Richiesta di selezione S3

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.

Codice	Campo	Descrizione
BYSC	Byte scansionati	Numero di byte scansionati (ricevuti) dai nodi di archiviazione. È probabile che BYSC e BYPR siano diversi se l'oggetto è compresso. Se l'oggetto è compresso, BYSC avrà il conteggio dei byte compressi e BYPR i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "Byte scansionati" sono stati effettivamente elaborati o utilizzati da un processo S3 Select.
BYRT	Byte restituiti	Numero di byte restituiti al client da un processo S3 Select.
RIPRISTINO	Record elaborati	Numero di record o righe che un processo S3 Select ha ricevuto dai nodi di archiviazione.
RERT	Record restituiti	Numero di record o righe che un processo S3 Select ha restituito al client.
JOFI	Lavoro terminato	Indica se l'elaborazione del lavoro S3 Select è terminata o meno. Se questo è falso, il lavoro non è stato completato e i campi di errore probabilmente conterranno dati. Il cliente potrebbe aver ricevuto risultati parziali o nessun risultato.
REID	ID richiesta	Identificatore per la richiesta S3 Select.
EXTM	Tempo di esecuzione	Tempo, in secondi, impiegato per completare il processo S3 Select.

Codice	Campo	Descrizione
ERMG	Messaggio di errore	Messaggio di errore generato dal processo S3 Select.
ERTY	Tipo di errore	Tipo di errore generato dal processo S3 Select.
PRIMO	Stacktrace degli errori	Stacktrace di errore generato dal processo S3 Select.
S3BK	Secchio S3	Nome del bucket S3.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 dell'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket.

SADD: Disabilitazione controllo sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di controllo; i messaggi di controllo non vengono più raccolti o recapitati.

Codice	Campo	Descrizione
AETM	Abilita metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Nome utente che ha eseguito il comando per disabilitare la registrazione degli audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.

Il messaggio implica che la registrazione era precedentemente abilitata, ma ora è stata disabilitata. In genere, questa opzione viene utilizzata solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. Dopo l'attività di massa, l'audit viene ripristinato (SADE) e la possibilità di disabilitarlo viene bloccata in modo permanente.

SADE: Abilitazione controllo sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione dei messaggi di controllo; i messaggi di controllo vengono nuovamente raccolti e

recapitati.

Codice	Campo	Descrizione
AETM	Abilita metodo	Il metodo utilizzato per abilitare l'audit.
AEUN	Nome utente	Nome utente che ha eseguito il comando per abilitare la registrazione di controllo.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.

Il messaggio implica che la registrazione era stata precedentemente disabilitata (SADD), ma ora è stata ripristinata. In genere, questa opzione viene utilizzata solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. Dopo l'attività di massa, l'audit viene ripristinato e la possibilità di disabilitarlo viene bloccata in modo permanente.

SCMT: Commit dell'archivio oggetti

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato finché non viene eseguito il commit (ovvero finché non viene memorizzato in modo persistente). Il contenuto memorizzato in modo persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene visualizzato quando un blocco di contenuto viene salvato nell'archivio.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto impegnato nell'archiviazione permanente.
RSLT	Codice risultato	Stato al momento in cui l'oggetto è stato memorizzato sul disco: SUCC: Oggetto memorizzato correttamente.

Questo messaggio significa che un determinato blocco di contenuto è stato completamente archiviato e verificato e ora può essere richiesto. Può essere utilizzato per tracciare il flusso di dati all'interno del sistema.

SDEL: S3 ELIMINA

Quando un client S3 emette una transazione DELETE, viene effettuata una richiesta per rimuovere l'oggetto o il bucket specificato oppure per rimuovere una sotto-risorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto eliminato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marcitore	ID versione del marcitore di eliminazione creato durante l'eliminazione di un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
GFID	ID di connessione della federazione di griglia	ID di connessione della federazione di griglia associata a una richiesta di eliminazione della replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
GFSA	ID account sorgente della federazione di griglia	ID account del tenant sulla griglia di origine per una richiesta di eliminazione della replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> <p>`x-amz-bypass-governance-retention` viene incluso automaticamente se presente nella richiesta.</p> </div>
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione DELETE. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.

Codice	Campo	Descrizione
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: urn:sgws:identity::03393893651506583485:root Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUDM	Identificatore univoco universale per un marcitore di eliminazione	L'identificatore di un marcitore di eliminazione. I messaggi del registro di controllo specificano UUDM o UUID, dove UUDM indica un marcitore di eliminazione creato in seguito a una richiesta di eliminazione di un oggetto e UUID indica un oggetto.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto che è stato eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SGET: S3 GET

Quando un client S3 emette una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket, oppure 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	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato 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 registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Il campo `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div>
LITÀ	ListObjectsV2	È stata richiesta una risposta in formato v2. Per i dettagli, vedere " AWS ListObjectsV2 ". Solo per operazioni bucket GET.
NCHD	Numero di bambini	Include chiavi e prefissi comuni. Solo per operazioni bucket GET.
RANG	Lettura dell'intervallo	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) indica la dimensione dell'intero oggetto.
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCC: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: urn:sgws:identity::03393893651506583485:root Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
Repubblica Ceca del Nord	Troncato o non troncato	Impostare su false se sono stati restituiti tutti i risultati. Impostare su true se sono disponibili più risultati da restituire. Solo per operazioni bucket GET.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SHEA: TESTA S3

Quando un client S3 emette una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un oggetto o di un bucket e recuperare i metadati relativi a un oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del 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 registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Il campo `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div>
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCC: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: urn:sgws:identity::03393893651506583485:root Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SPOS: S3 POST

Quando un client S3 invia una richiesta POST Object, questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid black; padding: 10px;"> <p>`X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div> <p>(Non previsto per SPOS).</p>
RSLT	Codice risultato	Risultato della richiesta RestoreObject. Il risultato è sempre: SUOS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando. Impostare su "seleziona" per un'operazione di selezione S3.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: urn:sgws:identity::03393893651506583485:root Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SPUT: S3 PUT

Quando un client S3 emette una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket oppure per rimuovere una sotto-risorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di conformità	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	ID di connessione della federazione di griglia	ID di connessione della federazione di griglia associata a una richiesta PUT di replicazione tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
GFSA	ID account sorgente della federazione di griglia	ID account del tenant sulla griglia di origine per una richiesta PUT di replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div> <p>`x-amz-bypass-governance-retention` viene incluso automaticamente se presente nella richiesta.</p>

Codice	Campo	Descrizione
LKEN	Blocco oggetto abilitato	Valore dell'intestazione della richiesta <code>x-amz-bucket-object-lock-enabled</code> , se presente nella richiesta.
LKLH	Blocco oggetto in attesa legale	Valore dell'intestazione della richiesta <code>x-amz-object-lock-legal-hold</code> , se presente nella richiesta PutObject.
LKMD	Modalità di mantenimento 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 a 100 anni dalla data in cui l'oggetto è stato ingerito.
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.

Codice	Campo	Descrizione
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: urn:sgws:identity::03393893651506583485:root Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
ULID	Carica ID	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.
VSST	Stato di controllo delle versioni	Il nuovo stato di controllo delle versioni di un bucket. Vengono utilizzati due stati: "abilitato" o "sospeso". Le operazioni sugli oggetti non includono questo campo.

SREM: Rimozione dell'archivio oggetti

Questo messaggio viene visualizzato quando il contenuto viene rimosso dall'archiviazione persistente e non è più accessibile tramite le API standard.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto eliminato dalla memoria permanente.
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è: SUCS: Contenuto rimosso dall'archiviazione persistente

Questo messaggio di controllo indica che un determinato blocco di contenuto è stato eliminato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tracciare il flusso di contenuti eliminati 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	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, durante l'aggiornamento delle impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del 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 registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid black; padding: 10px;"> <p>Il campo `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div>
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCC: riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: urn:sgws:identity::03393893651506583485:root Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SVRF: Errore di verifica dell'archivio oggetti

Questo messaggio viene visualizzato ogni volta che un blocco di contenuto non supera il processo di verifica. Ogni volta che i dati degli oggetti replicati vengono letti o scritti sul disco, vengono eseguiti diversi controlli di verifica e integrità per garantire che i dati inviati all'utente richiedente siano identici ai dati originariamente inseriti nel sistema. Se uno di questi controlli fallisce, il sistema mette automaticamente in quarantena i dati dell'oggetto replicato corrotti 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.

Codice	Campo	Descrizione
RSLT	Codice risultato	<p>Tipo di errore di verifica:</p> <p>CRCF: Controllo di ridondanza ciclico (CRC) non riuscito.</p> <p>HMAC: controllo del codice di autenticazione dei messaggi basato su hash (HMAC) non riuscito.</p> <p>EHSH: Hash del contenuto crittografato inaspettato.</p> <p>PHSH: Hash del contenuto originale inaspettato.</p> <p>SEQC: sequenza di dati errata sul disco.</p> <p>PERR: Struttura non valida del file su disco.</p> <p>DERR: Errore del disco.</p> <p>FNAM: Nome file errato.</p>



Questo messaggio deve essere monitorato attentamente. Gli errori nella verifica del contenuto possono indicare imminenti guasti hardware.

Per determinare quale operazione ha attivato il messaggio, vedere il valore del campo AMID (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, ovvero una verifica in background, mentre STOR indica che il messaggio è stato attivato dal recupero del contenuto.

SVRU: Verifica archivio oggetti sconosciuto

Il componente di archiviazione del servizio LDR esegue continuamente la scansione di tutte le copie dei dati degli oggetti replicati nell'archivio oggetti. Questo messaggio viene visualizzato quando una copia sconosciuta o imprevista di dati di oggetti replicati viene rilevata nell'archivio oggetti e spostata nella directory di quarantena.

Codice	Campo	Descrizione
FPTH	Percorso del file	Percorso del file della copia dell'oggetto inaspettato.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato 'NONE' anziché 'SUCS' in modo che il messaggio non venga filtrato.



Il messaggio di controllo SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie inaspettate di dati oggetto nell'archivio oggetti. Questa situazione dovrebbe essere indagata immediatamente per stabilire come sono state create queste copie, perché potrebbe indicare imminenti guasti hardware.

SYSD: arresto del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto l'arresto. In genere questo messaggio viene inviato solo dopo un successivo riavvio, perché 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	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente.

Il messaggio non indica se il server host è stato arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno spegnimento "sporco", perché il messaggio viene generato solo da spegnimenti "puliti".

SYST: Arresto del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto l'arresto e che il servizio ha avviato la sequenza di arresto. SYST può essere utilizzato per determinare se l'arresto è stato richiesto prima del riavvio del servizio (a differenza di SYSD, che in genere viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente.

Il messaggio non indica se il server host è stato arrestato, ma solo il servizio di reporting. Il codice RSLT di un messaggio SYST non può indicare uno spegnimento "sporco", perché il messaggio viene generato solo da spegnimenti "puliti".

SYSU: Avvio del nodo

Quando un servizio viene riavviato, questo messaggio viene generato per indicare se l'arresto precedente è stato pulito (comandato) o disordinato (inaspettato).

Codice	Campo	Descrizione
RSLT	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente. DSDN: Il sistema non è stato arrestato 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 discontinuità nella traccia di controllo.
- Determinare se un servizio non funziona correttamente durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio non riuscito.

WDEL: CANCELLA rapida

Quando un client Swift emette una transazione DELETE, viene effettuata una richiesta per rimuovere l'oggetto o il contenitore specificato. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto eliminato in byte. Le operazioni sui contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). </div>
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DELETE. Il risultato è sempre: SUCC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato 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.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.

Codice	Campo	Descrizione
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni sui contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WGET: GET rapido

Quando un client Swift emette una transazione GET, viene effettuata una richiesta per recuperare un oggetto, elencare gli oggetti in un contenitore o elencare i contenitori in un account. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni su account e contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). </div>

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni su account e contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WHEA: TESTA Veloce

Quando un client Swift emette una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un account, di un contenitore o di un oggetto e recuperare eventuali metadati rilevanti. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni su account e contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e contenitori non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). </div>
RSLT	Codice risultato	Risultato della transazione HEAD. Il risultato è sempre: SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni su account e contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WPUT: PUT rapido

Quando un client Swift emette una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o contenitore. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). </div>
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUCC: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni sui contenitori non includono questo campo.

Codice	Campo	Descrizione
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

Informazioni sul copyright

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

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

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