Monitora il sistema StorageGRID

StorageGRID software

NetApp
July 23, 2026

Sommario

Monitora il sistema StorageGRID

Monitora un sistema StorageGRID

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

Prima di iniziare

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

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

Informazioni su questa attività

Queste istruzioni descrivono come:

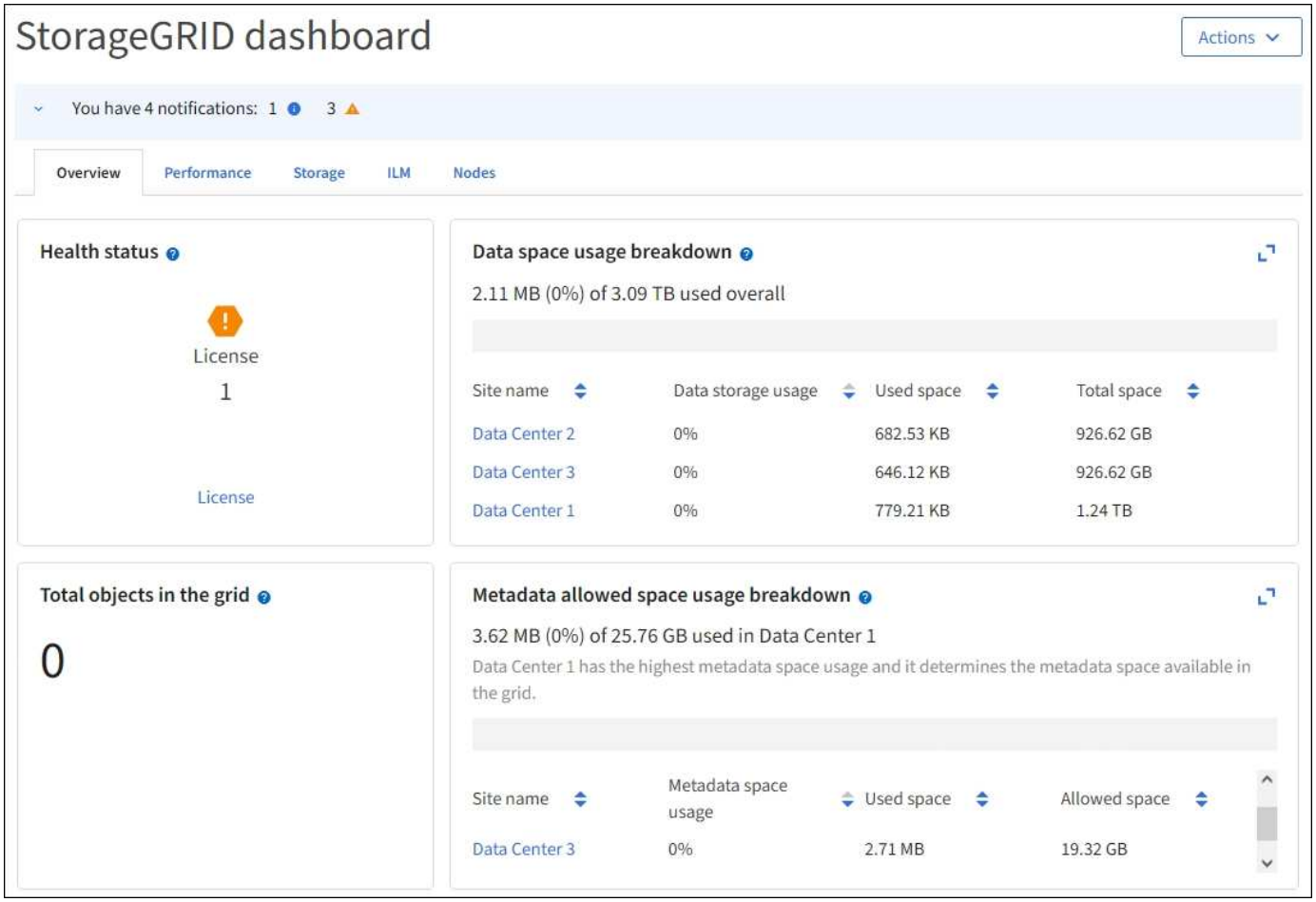
- "Visualizza e gestisci la dashboard"
- "Visualizza la pagina dei nodi"
- "Monitora regolarmente questi aspetti del sistema:"
  - "Stato di salute del sistema"
  - "Capacità di storage"
  - "Gestione del ciclo di vita delle informazioni"
  - "Risorse di rete e di sistema"
  - "Attività tenant"
  - "Operazioni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

Visualizza e gestisci la dashboard in StorageGRID

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

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

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



Visualizza la dashboard

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

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

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

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

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

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

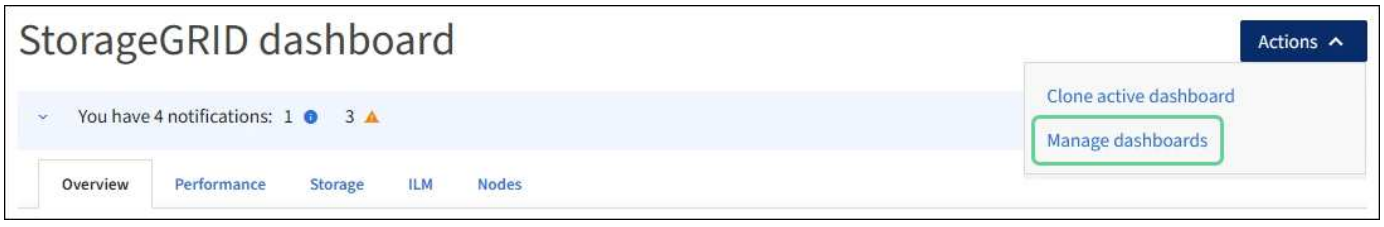
Gestisci dashboard

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

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

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

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



Configura le dashboard

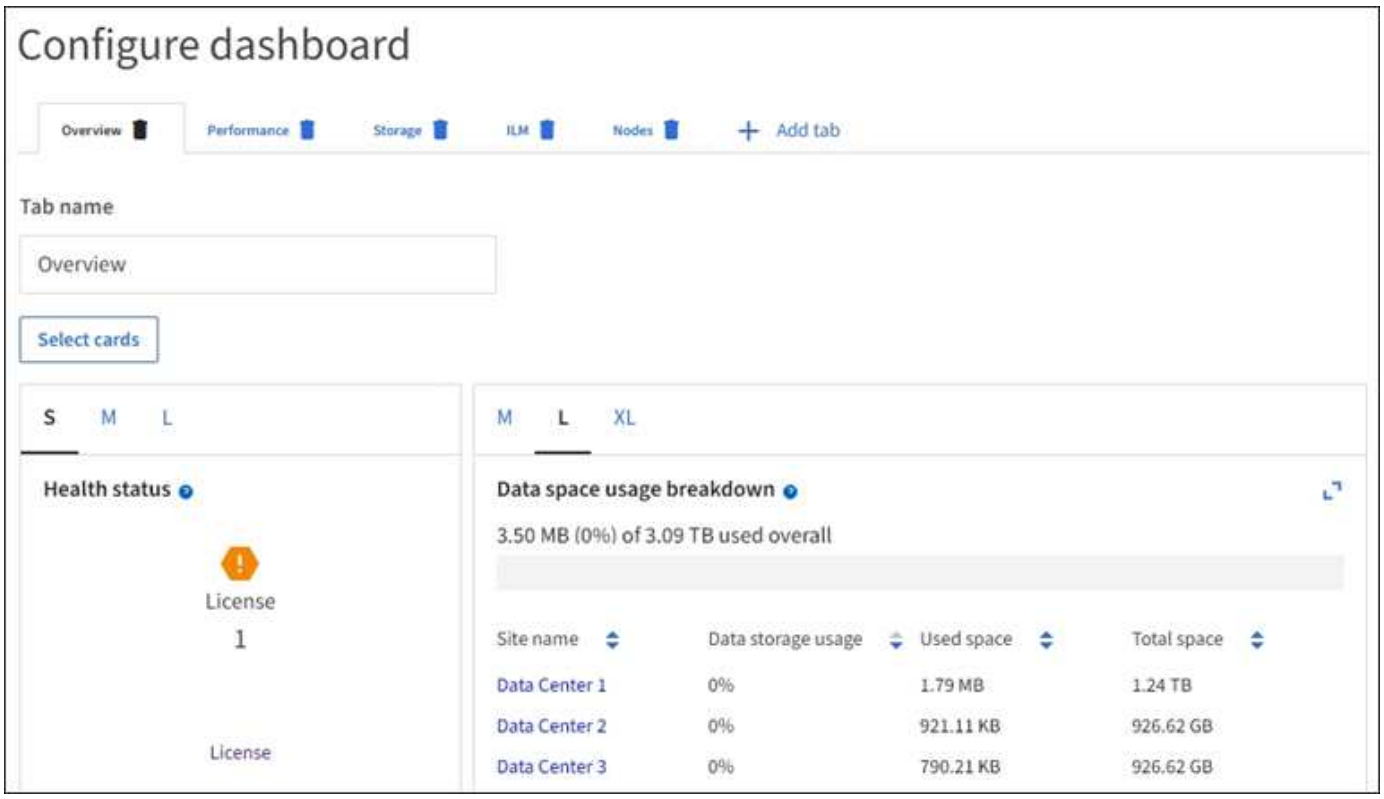
Per creare una nuova dashboard clonando la dashboard attiva, seleziona **Azioni** > **Clona dashboard attiva**.

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

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

Quando configuri una dashboard, puoi:

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



Visualizza la pagina dei nodi

Visualizza la pagina dei nodi StorageGRID

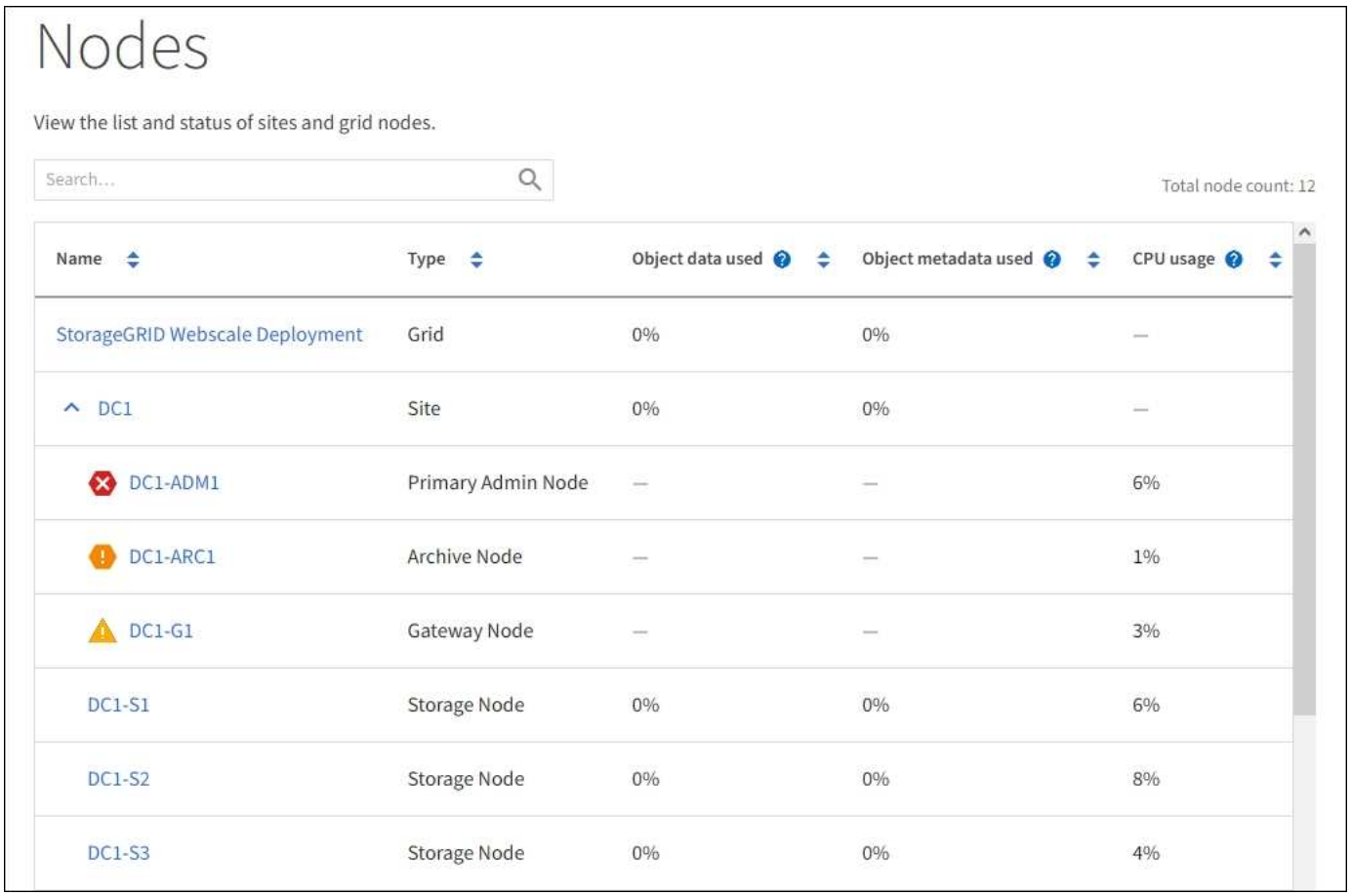
Quando hai bisogno di informazioni più dettagliate sul tuo sistema StorageGRID rispetto a quelle fornite dalla dashboard, puoi utilizzare la pagina Nodi per visualizzare le metriche per l'intera griglia, per ogni sito nella griglia e per ogni nodo in un sito.

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

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

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

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



Icone di stato della connessione

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

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

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

Icone di avviso

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

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

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

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

Visualizza i dettagli di un sistema, sito o nodo

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

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

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

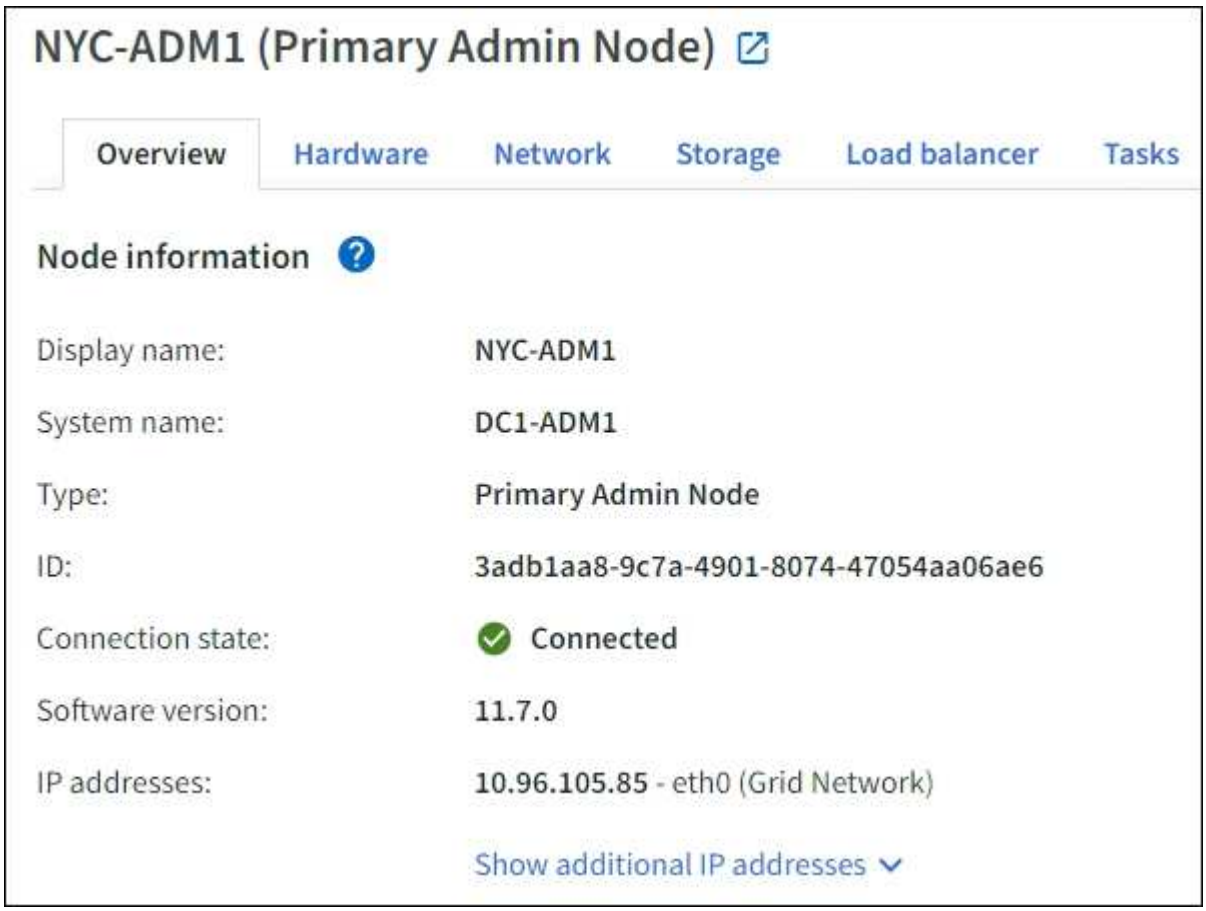
Visualizza la scheda Panoramica di StorageGRID

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

La scheda Panoramica viene mostrata per tutti i nodi.

Informazioni sul nodo

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



Le informazioni generali relative a un nodo includono quanto segue:

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

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

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

Avvisi

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

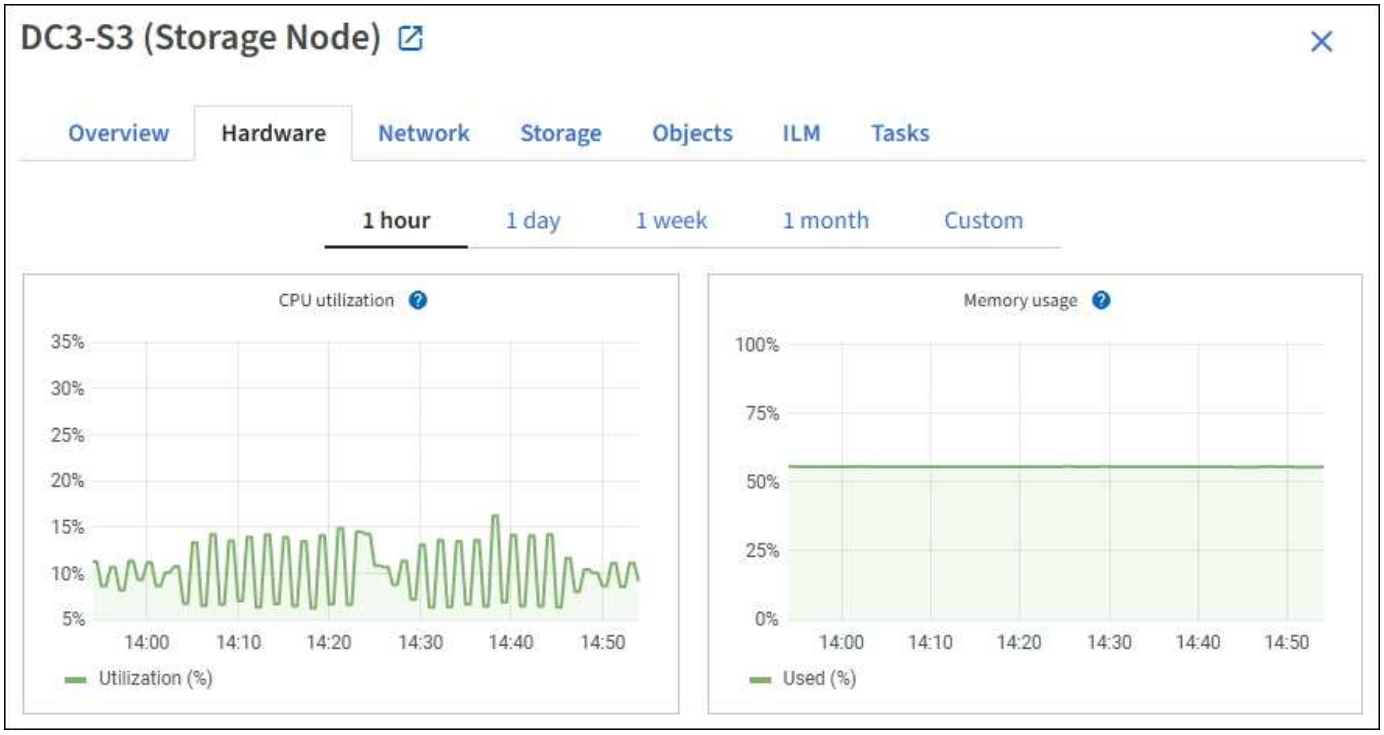
Sono inclusi anche gli avvisi per "stati di connessione del nodo".

Visualizza la scheda Hardware di StorageGRID

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

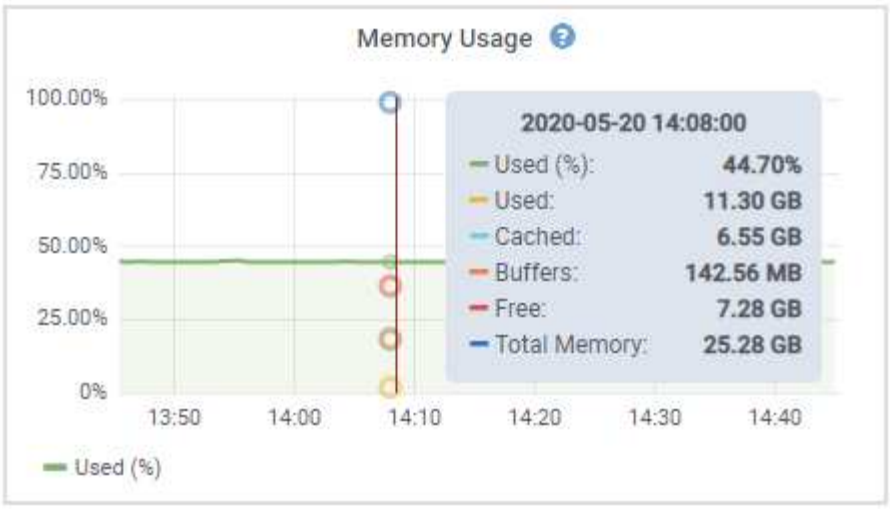
> Il Grid Manager viene aggiornato a ogni release e potrebbe non corrispondere alle schermate di esempio presenti in questa pagina.

La scheda Hardware viene visualizzata per tutti i nodi.



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

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



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

Visualizza informazioni sui nodi di storage dell'appliance

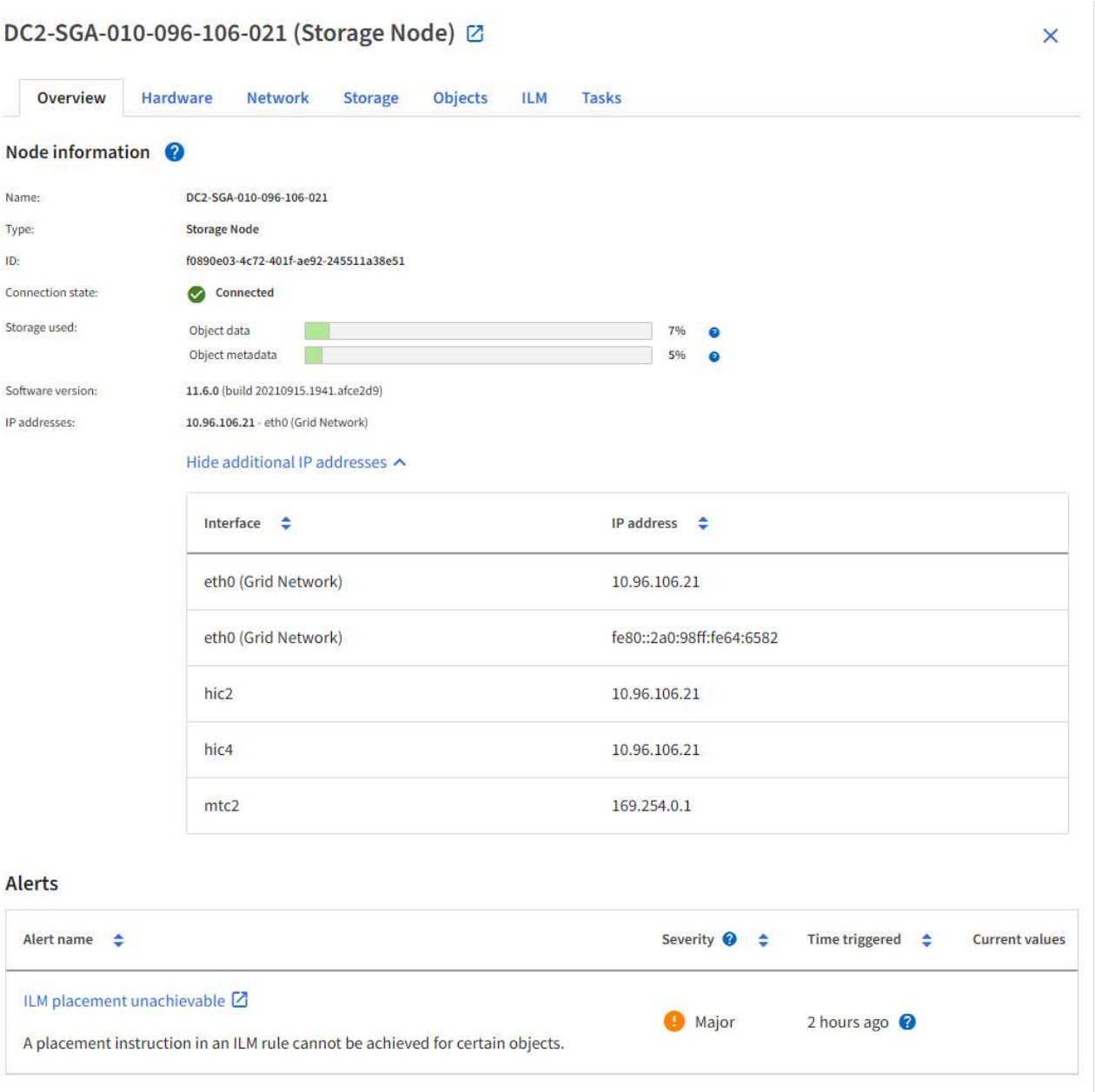
La pagina Nodi elenca le informazioni sullo stato del servizio e su tutte le risorse di calcolo, i dispositivi disco e le risorse di rete per ciascun Storage Node dell'appliance. Puoi anche vedere memoria, hardware di storage, versione del firmware del controller, risorse di rete, interfacce di rete,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

Passaggi

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

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

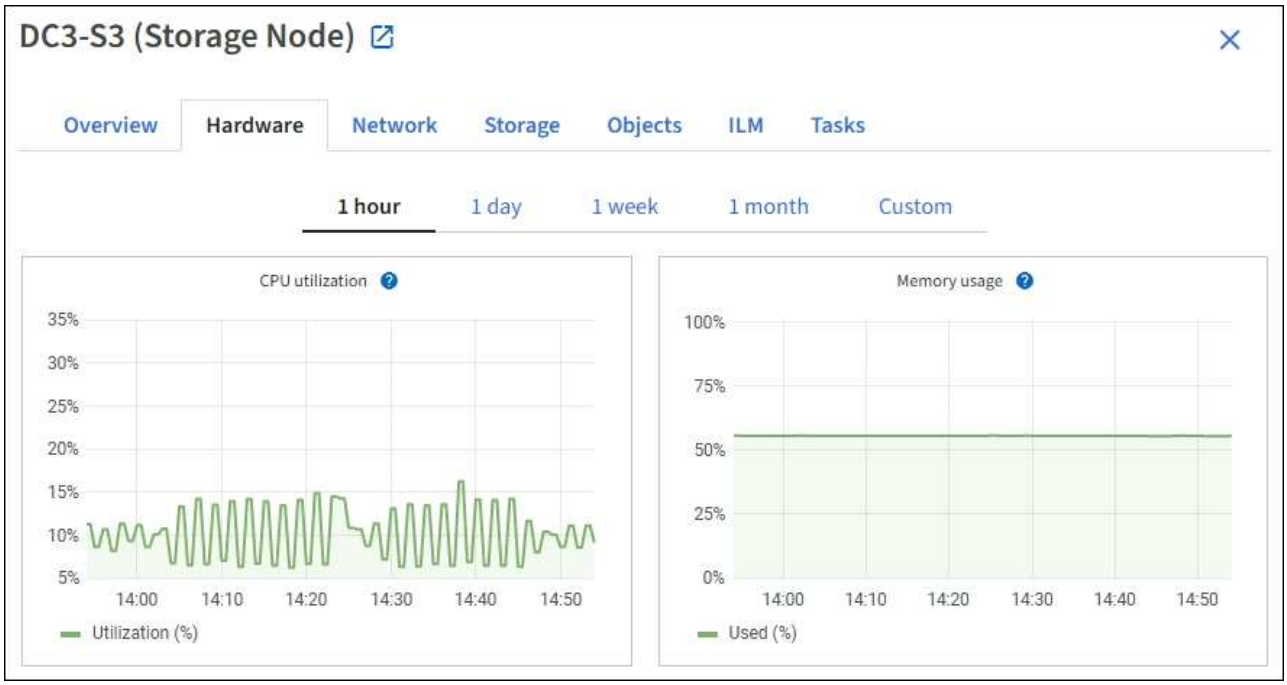
   - **eth**: La Grid Network, l'Admin Network o la Client Network.
   - **hic**: Una delle porte fisiche da 10, 25 o 100 GbE presenti sull'appliance. Queste porte possono essere aggregate e connesse alla StorageGRID Grid Network (eth0) e alla Client Network (eth2).
   - **mtc**: Una delle porte fisiche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



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

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

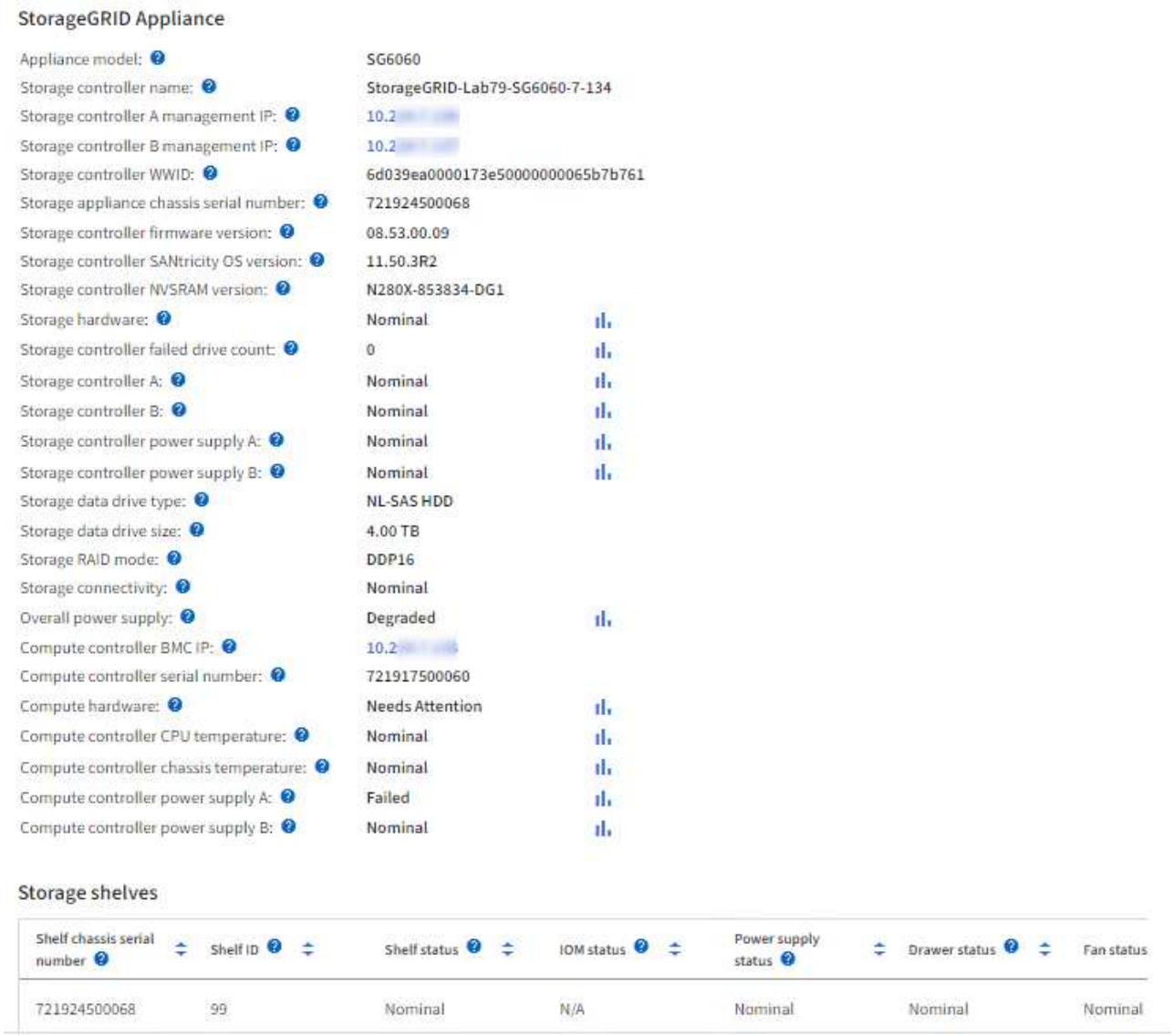
   a. Visualizza i grafici di utilizzo della CPU e della memoria per determinare le percentuali di utilizzo di CPU e memoria nel tempo. Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. Puoi visualizzare le informazioni disponibili per intervalli di 1 ora, 1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



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

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

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



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

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

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

+

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

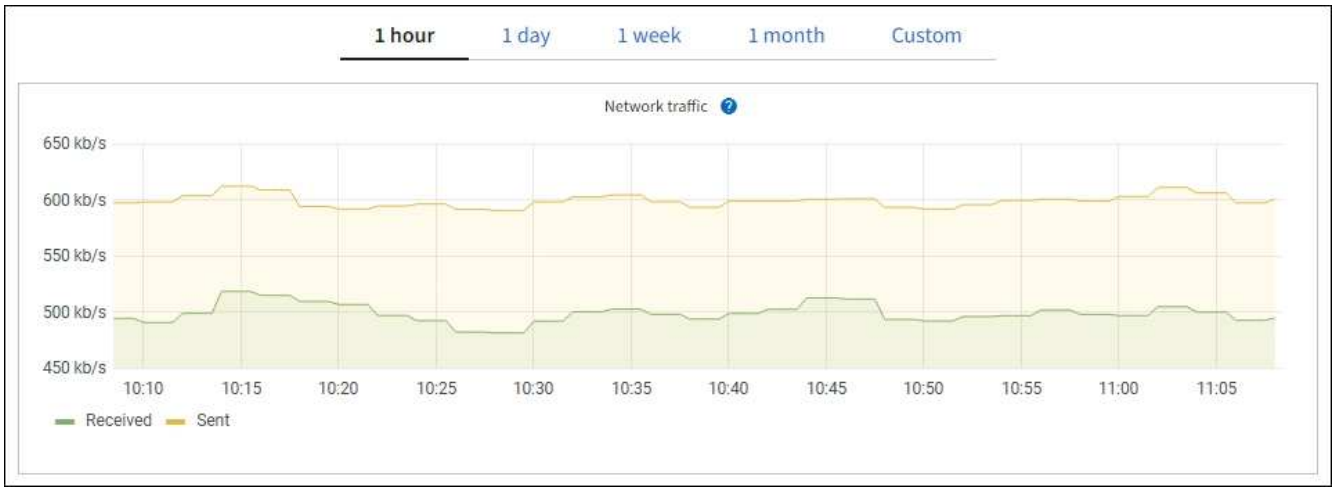
Colonna nella tabella degli shelf di storage	Descrizione
ID shelf	L'identificativo numerico dello shelf di storage. • 99: Shelf dello storage controller • 0: Primo shelf di espansione • 1: Secondo shelf di espansione **Nota:** Gli shelf di espansione si applicano solo a SG6060 e SG6160.
Stato dello shelf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

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

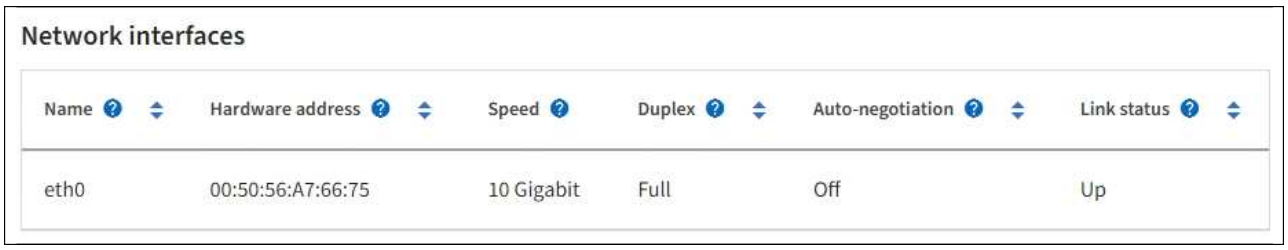
   Se lo stato non è "Nominale", controlla gli avvisi correnti. Puoi anche usare SANtricity System Manager per saperne di più su alcuni di questi valori hardware. Consulta le istruzioni per installare e mantenere il tuo appliance.

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

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



a. Esamina la sezione Interfacce di rete.



Network interfaces

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

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

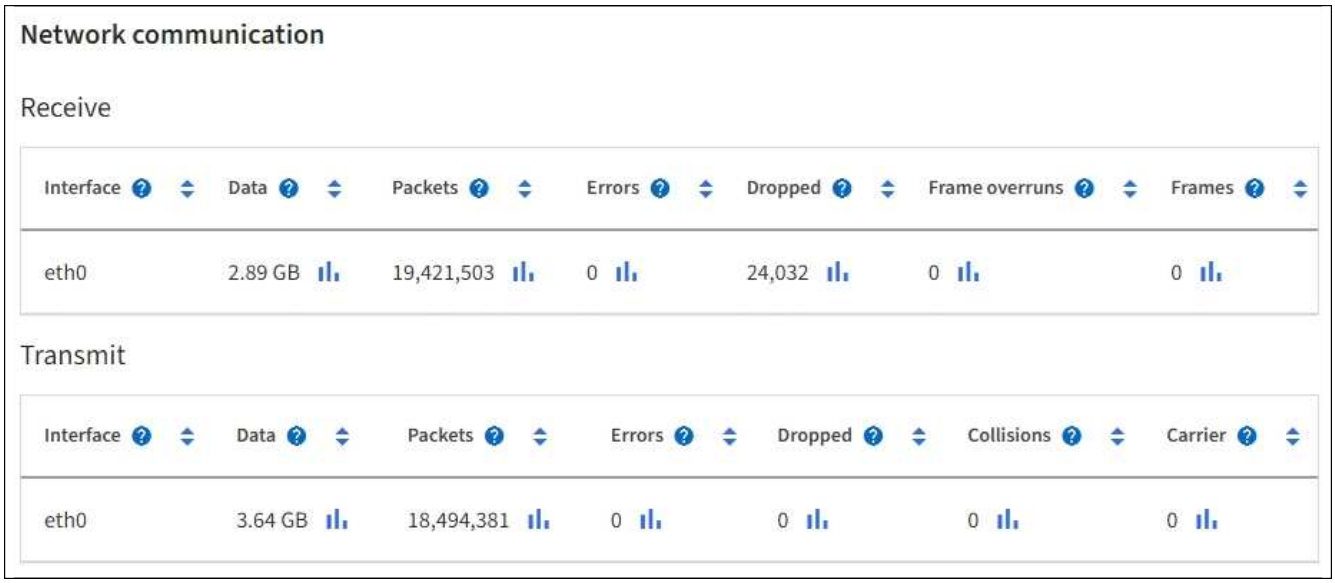
I valori riportati nella tabella presuppongono l'utilizzo di tutti e quattro i collegamenti.

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

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

b. Consulta la sezione Comunicazione di rete.

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



Network communication

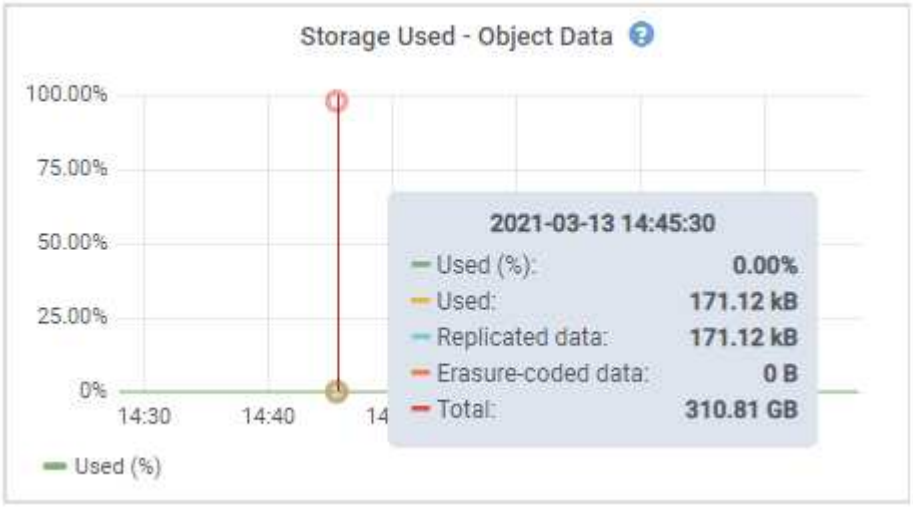
Receive

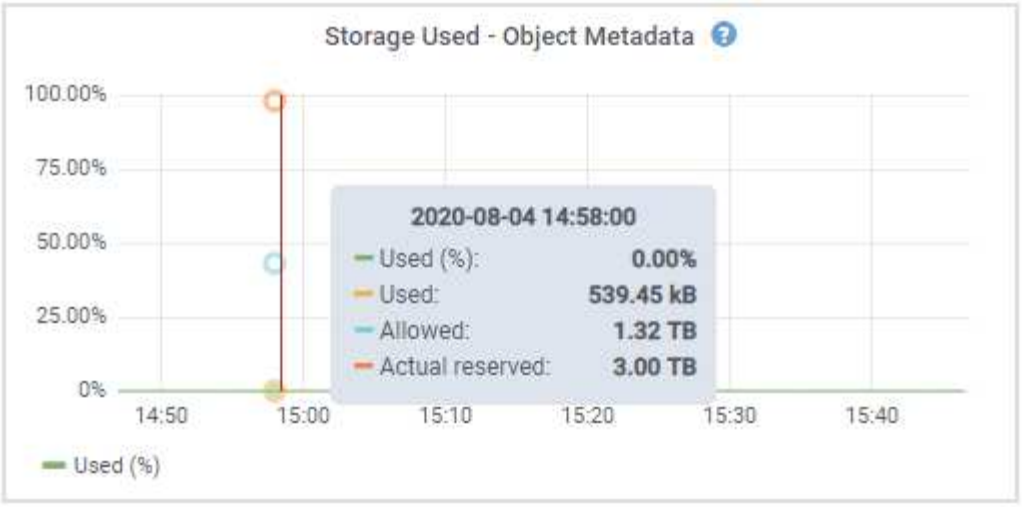
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

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

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

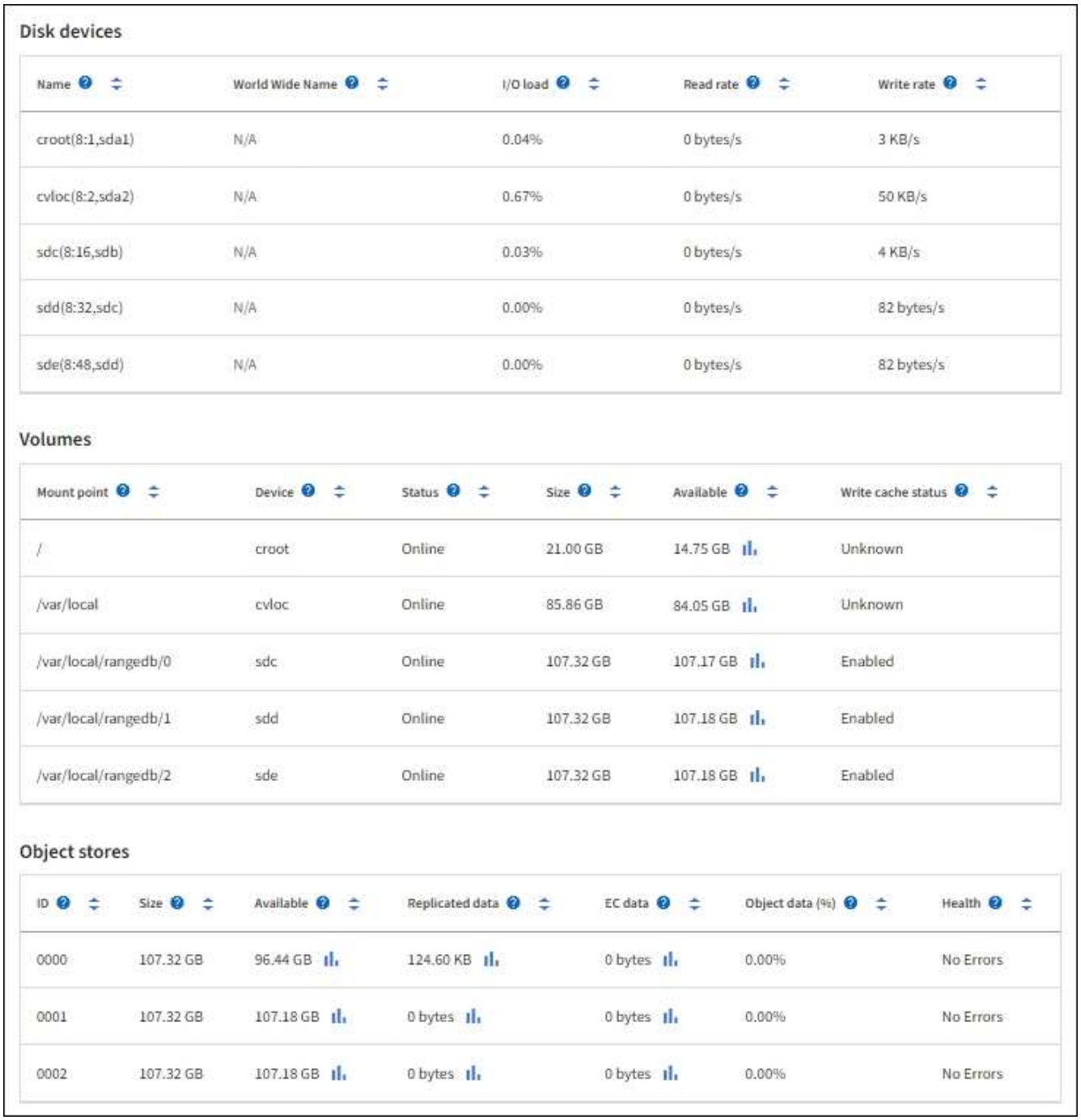




a. Scorri verso il basso per visualizzare la quantità di spazio di storage disponibile per ciascun volume e archivio di oggetti.

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

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



Disk devices

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

Volumes

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

Object stores

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

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

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

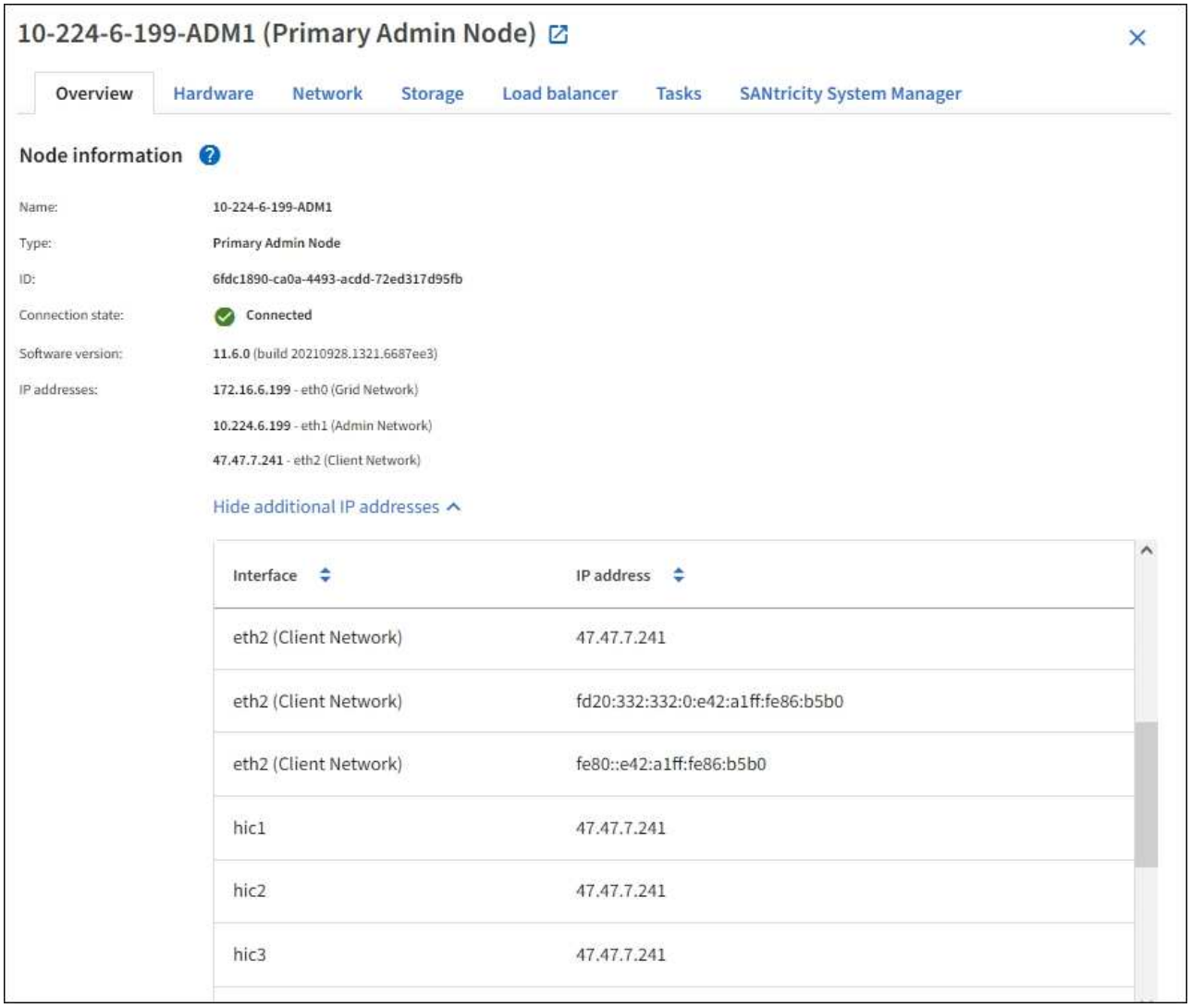
Passaggi

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

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

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

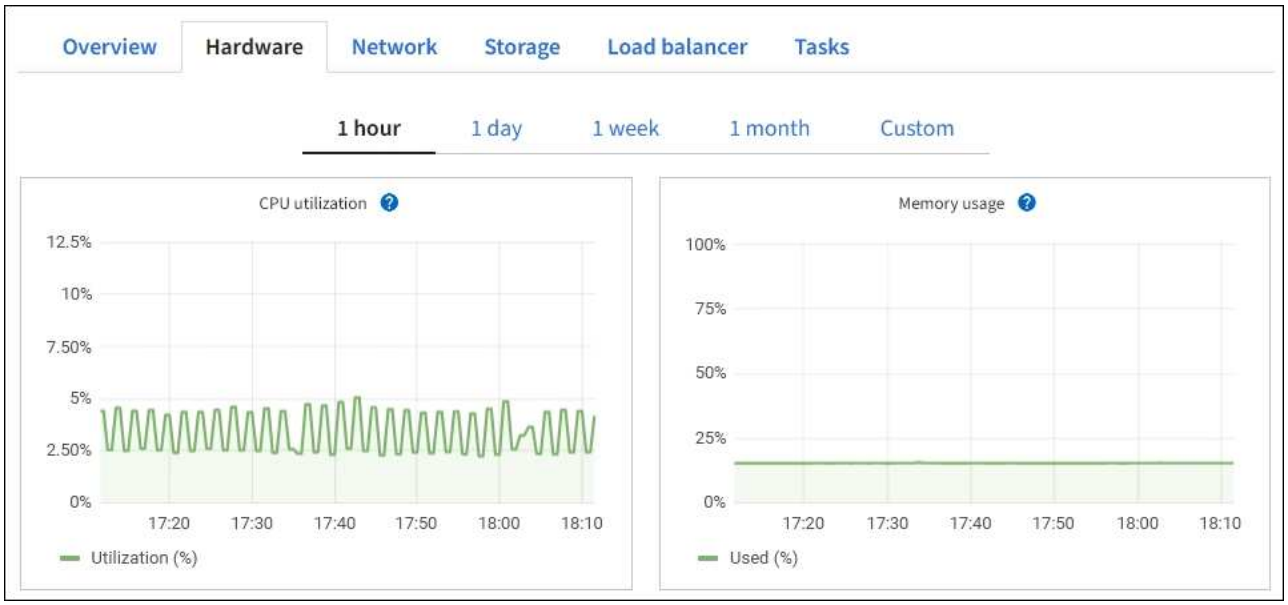
- **adllb** e **adlli**: visualizzati se viene utilizzato il bonding attivo/backup per l'interfaccia Admin Network
- **eth**: La Grid Network, l'Admin Network o la Client Network.
- **hic**: Una delle porte fisiche da 10, 25 o 100 GbE presenti sull'appliance. Queste porte possono essere aggregate e connesse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



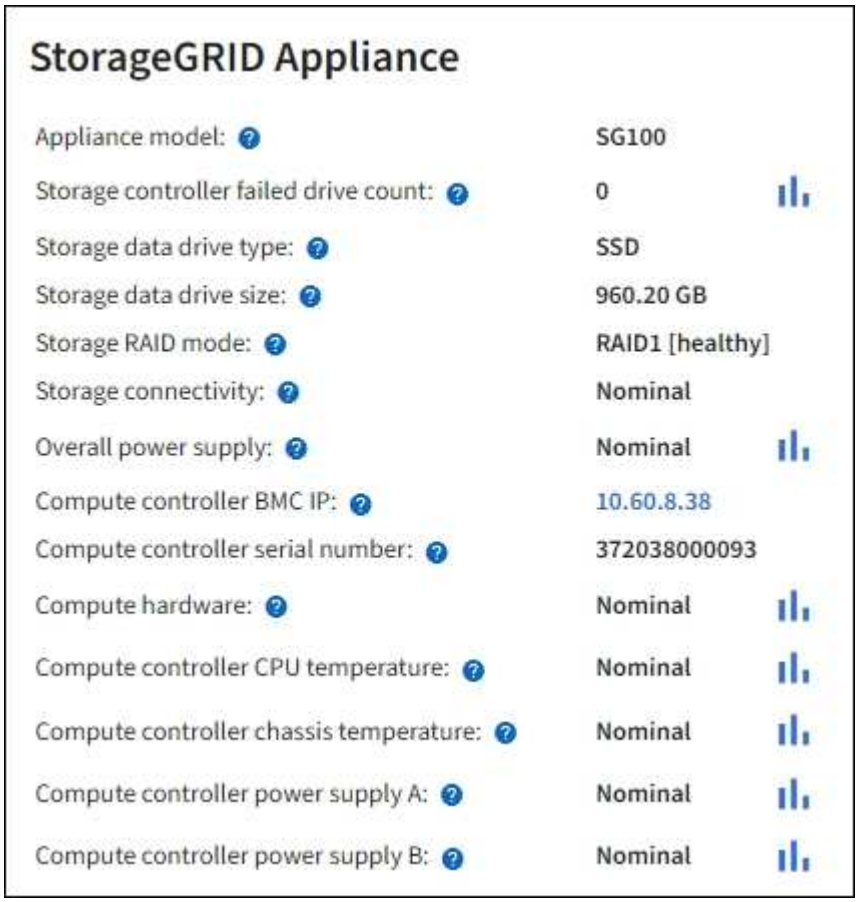
La sezione Avvisi della scheda Panoramica visualizza eventuali avvisi attivi per il nodo.

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

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



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



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

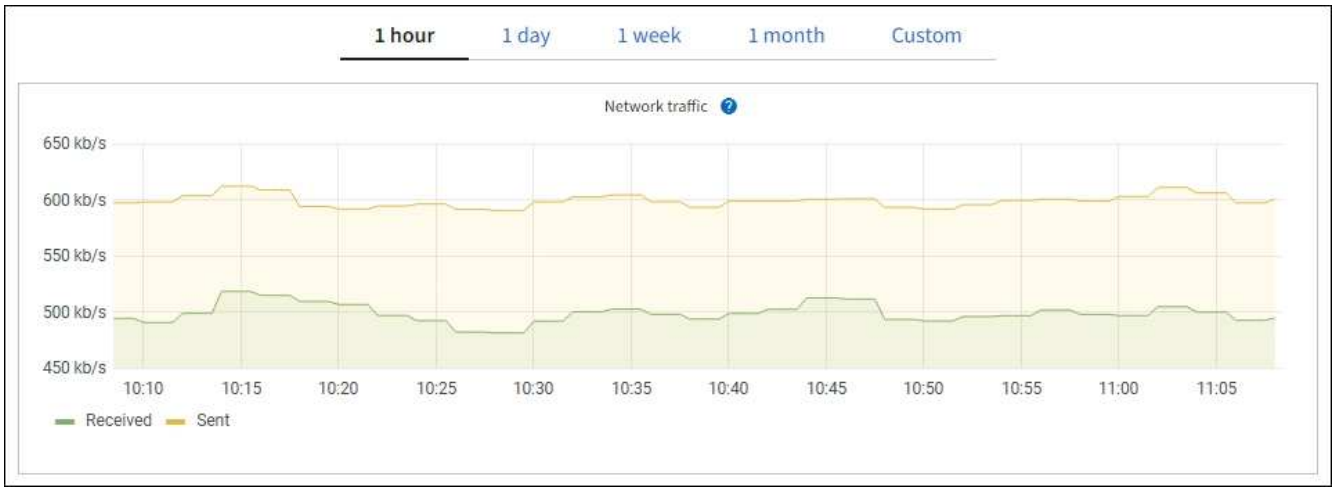
Campo nella tabella Appliance	Descrizione
Conteggio delle unità guaste dello storage controller	Il numero di unità che non sono ottimali.
Tipo di unità dati di storage	Il tipo di drive presenti nell'appliance, come HDD (hard drive) o SSD (solid state drive).
Dimensione dell'unità dati di storage	La dimensione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

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

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

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

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



a. Esamina la sezione Interfacce di rete.

Network interfaces

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

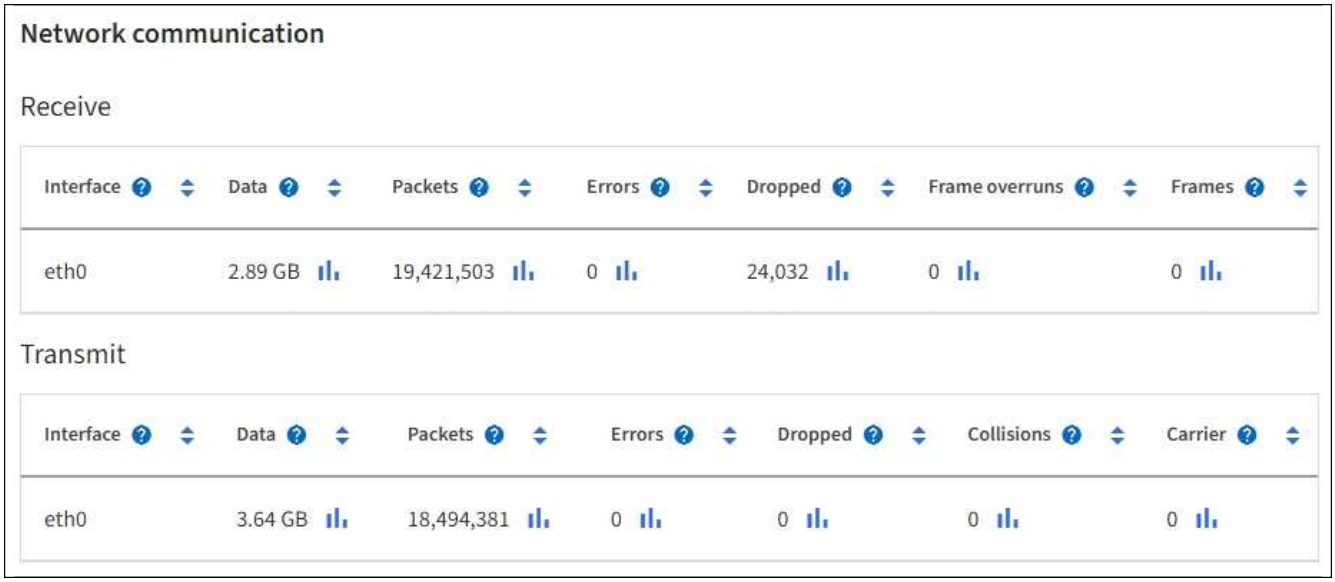
Usa la seguente tabella con i valori nella colonna **Velocità** della tabella Interfacce di rete per capire se le quattro porte di rete 40/100-GbE sull'appliance sono state configurate per usare la modalità attivo/backup o la modalità LACP.

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

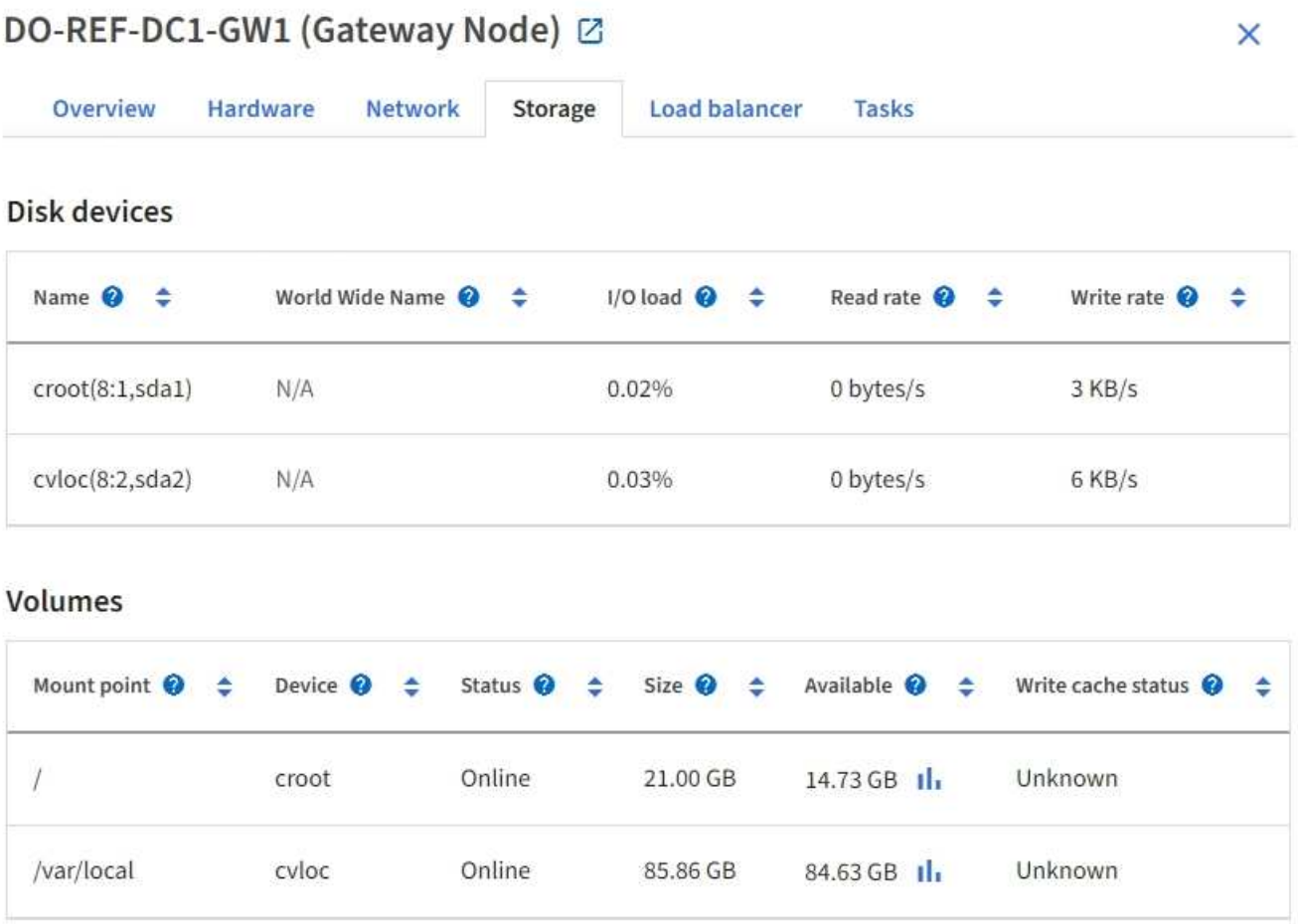
Modalità di collegamento	Modalità bond	Velocità di collegamento HIC individuale (hic1, hic2, hic3, hic4)	Velocità prevista della rete Grid/Client (eth0, eth2)
Aggregato	LACP	100	400
Fisso	LACP	100	200
Fisso	Attivo/Backup	100	100
Aggregato	LACP	40	160
Fisso	LACP	40	80
Fisso	Attivo/Backup	40	40

b. Consulta la sezione Comunicazione di rete.

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



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



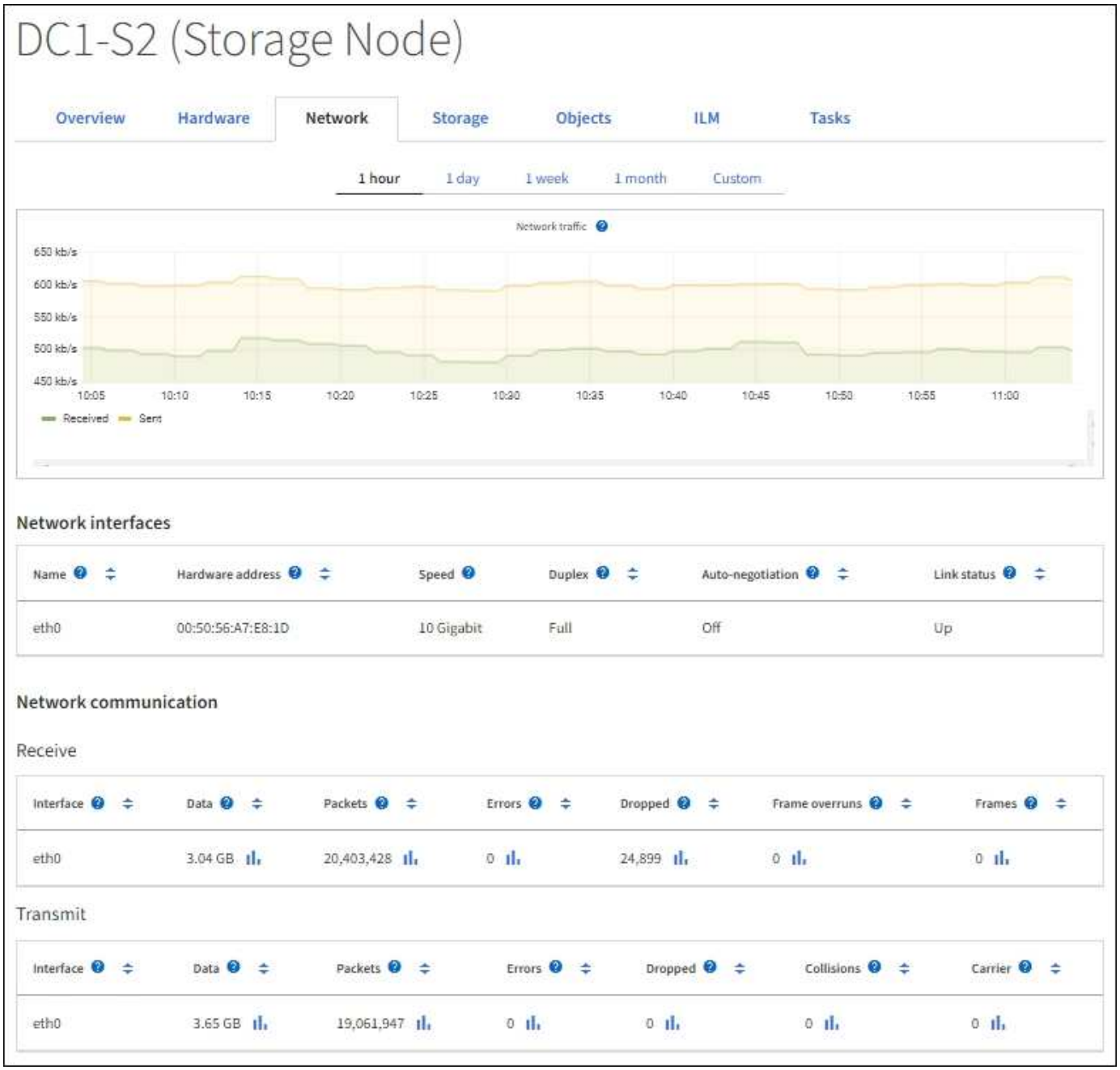
Visualizza la scheda Rete di StorageGRID

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

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

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

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



Informazioni correlate

"Monitora le connessioni di rete e le prestazioni"

Visualizza la scheda Storage della StorageGRID

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

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

Grafici dello storage utilizzato

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

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

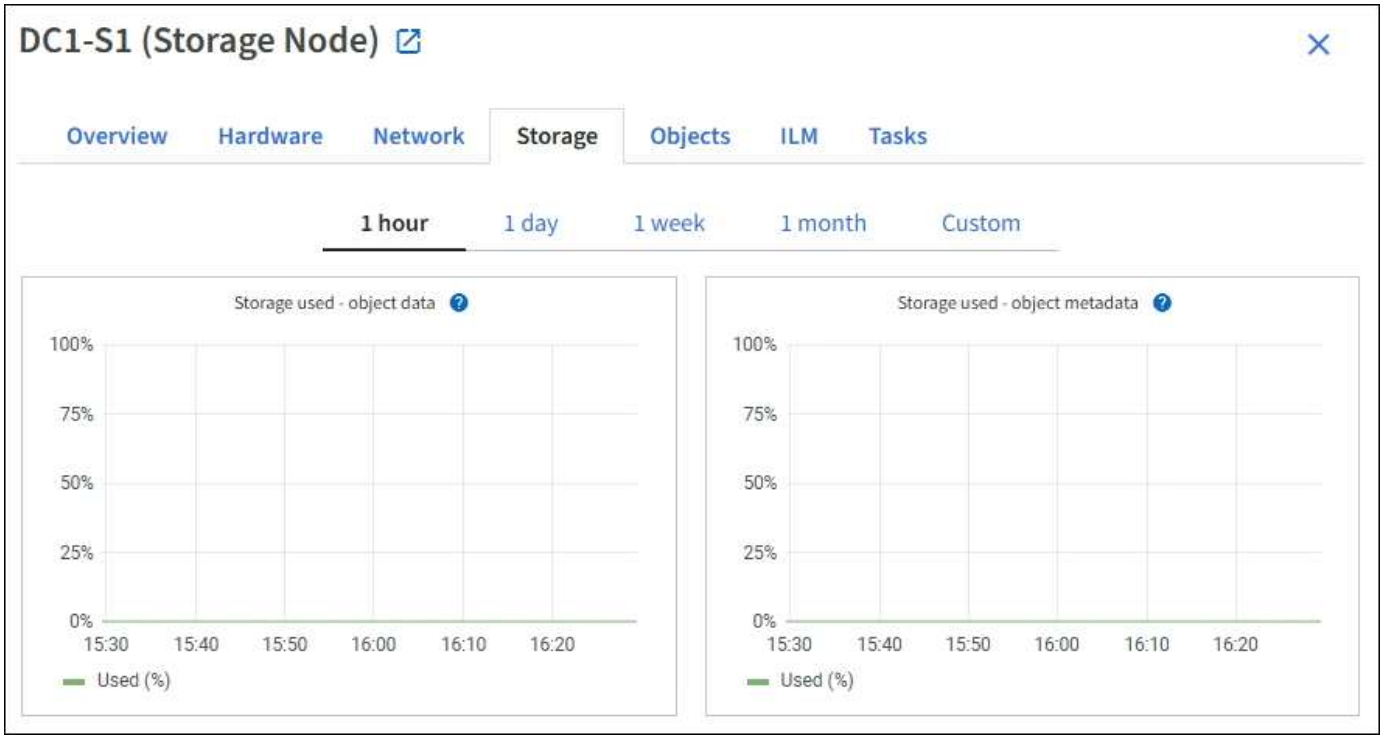
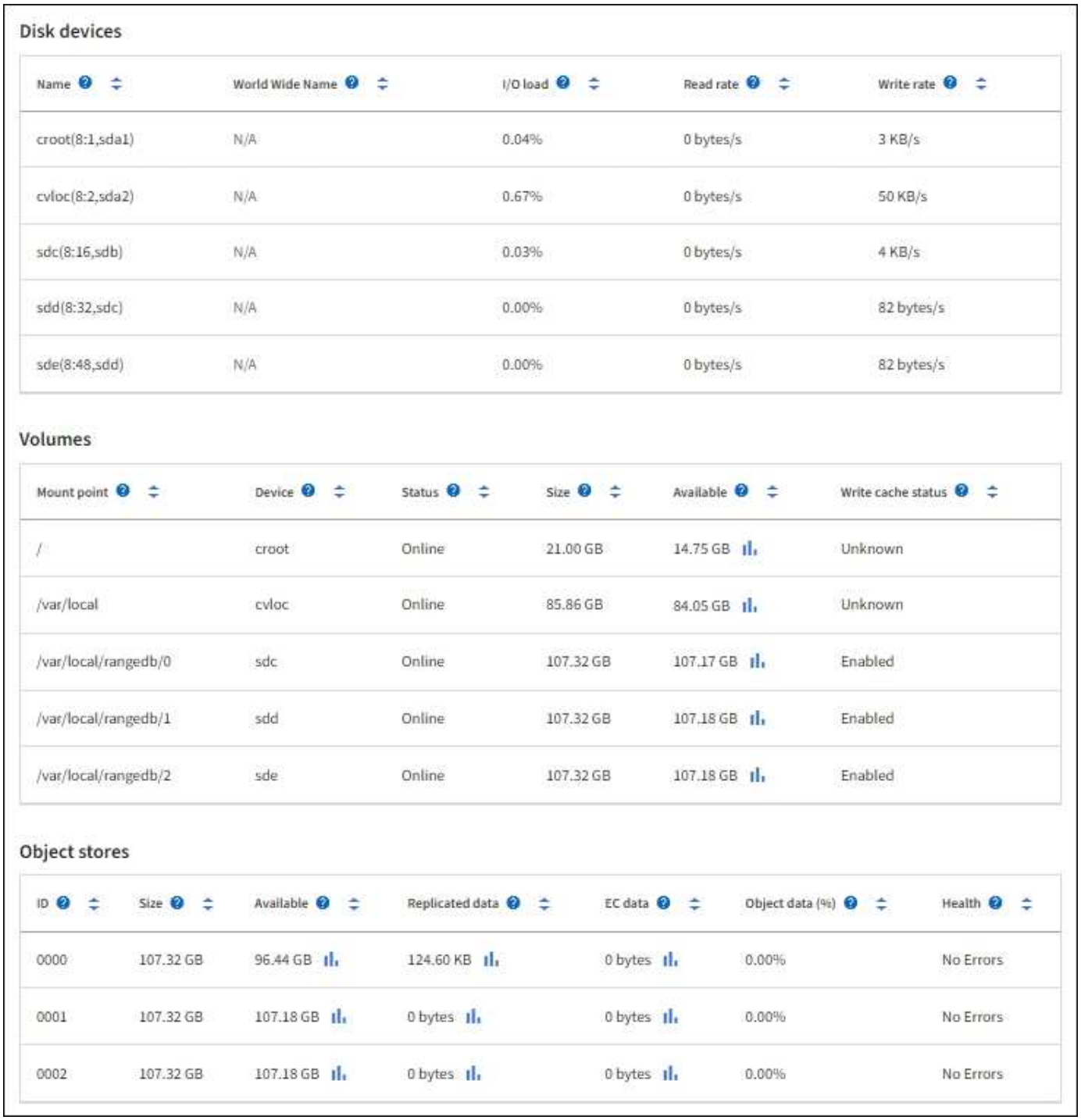


Tabelle dispositivi disco, volumi e archivi di oggetti

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



Disk devices

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

Volumes

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

Object stores

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

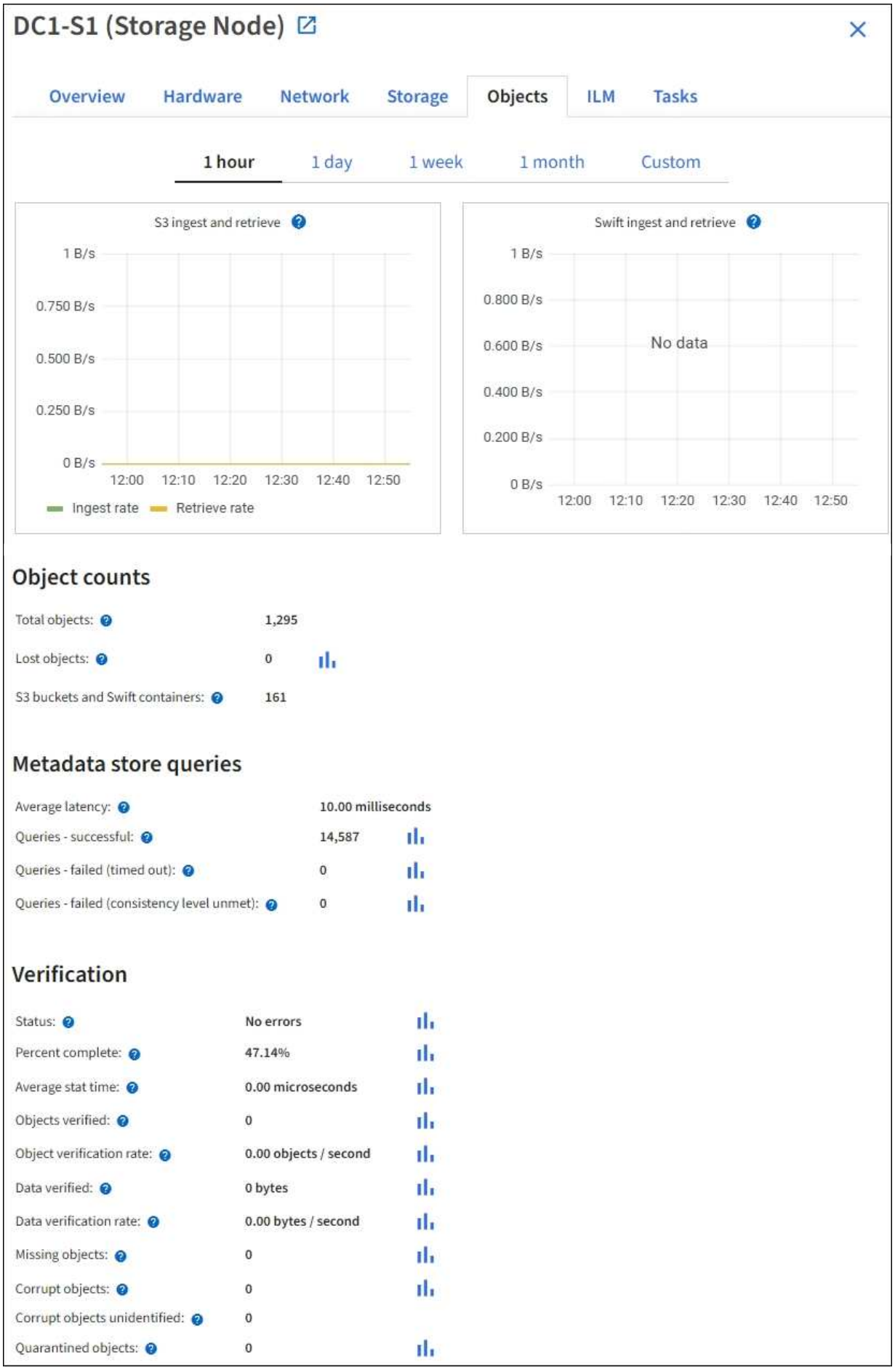
Informazioni correlate

"Monitora la capacità di archiviazione"

Visualizza la scheda Oggetti di StorageGRID

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

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

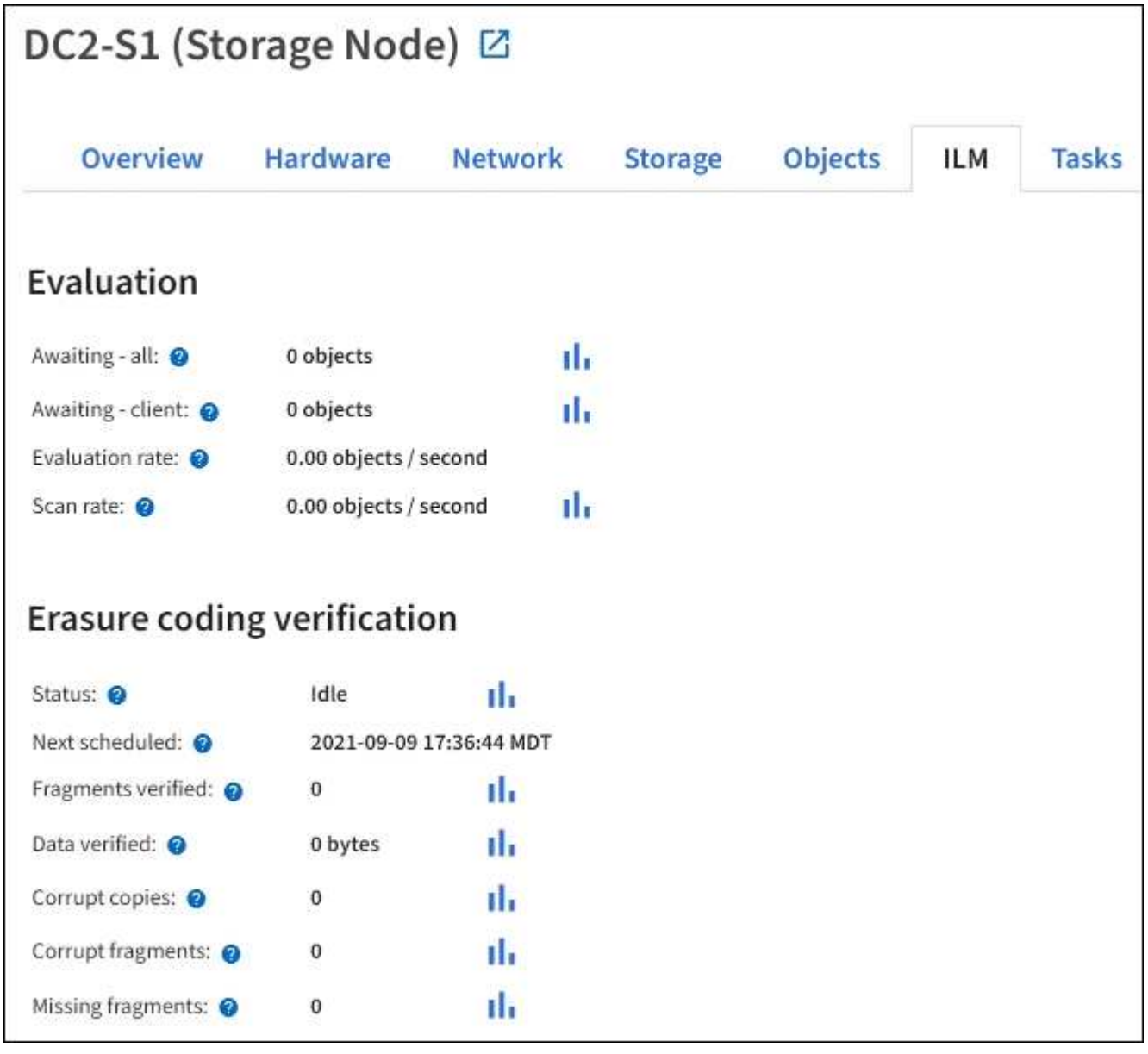

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

Visualizza la scheda StorageGRID ILM

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

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

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



Informazioni correlate

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

Visualizza la scheda del bilanciatore del carico StorageGRID

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

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

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

Traffico di richiesta

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

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

Tasso di richieste in entrata

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

Durata media della richiesta (senza errori)

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

Tasso di risposta agli errori

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

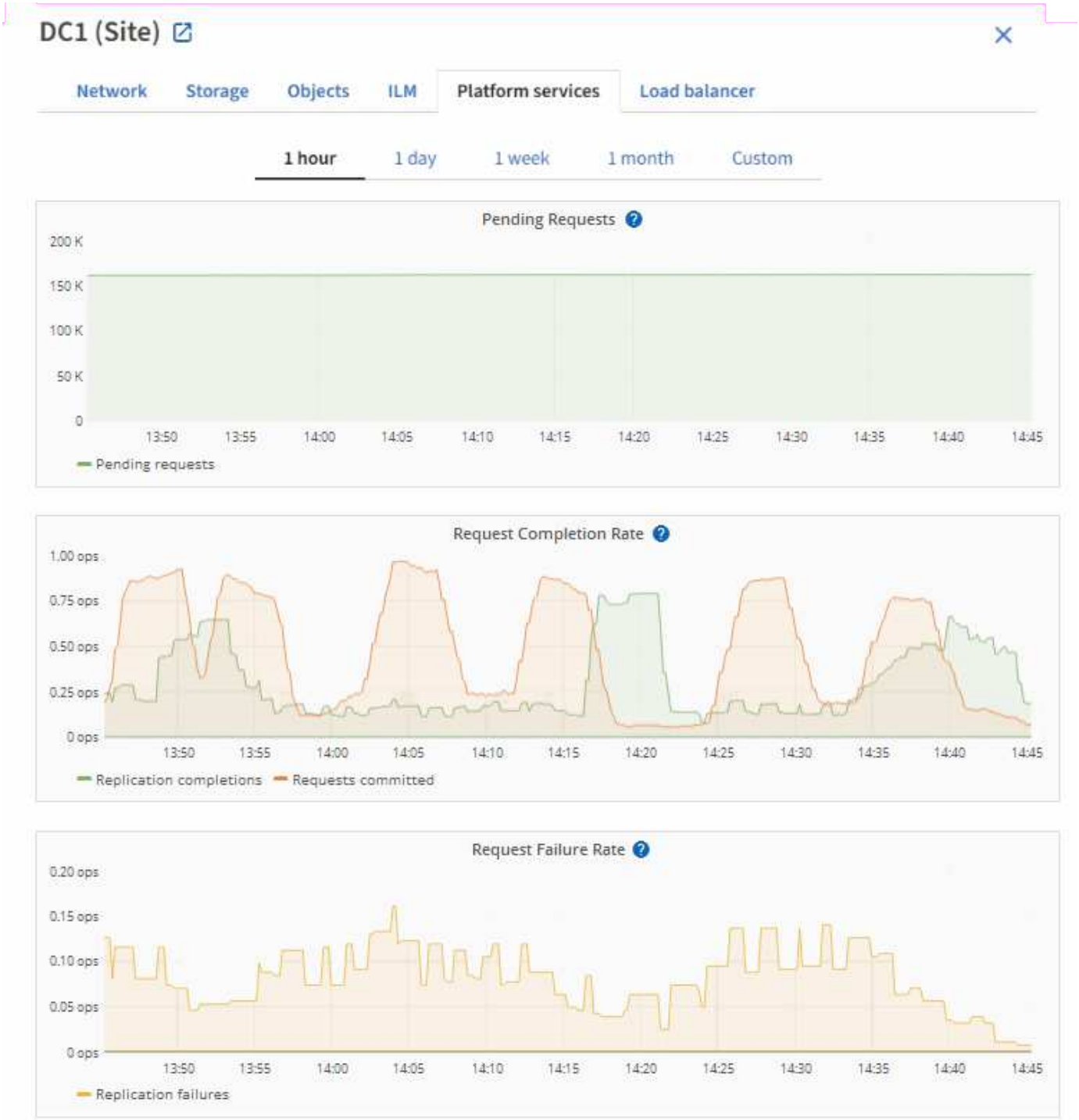
Informazioni correlate

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

Visualizza la scheda Servizi della piattaforma StorageGRID

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

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



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

Visualizza la scheda Gestisci unità di StorageGRID

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

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

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

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

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

Visualizza la scheda SANtricity System Manager di StorageGRID

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

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

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

Utilizzando SANtricity System Manager, puoi fare quanto segue:

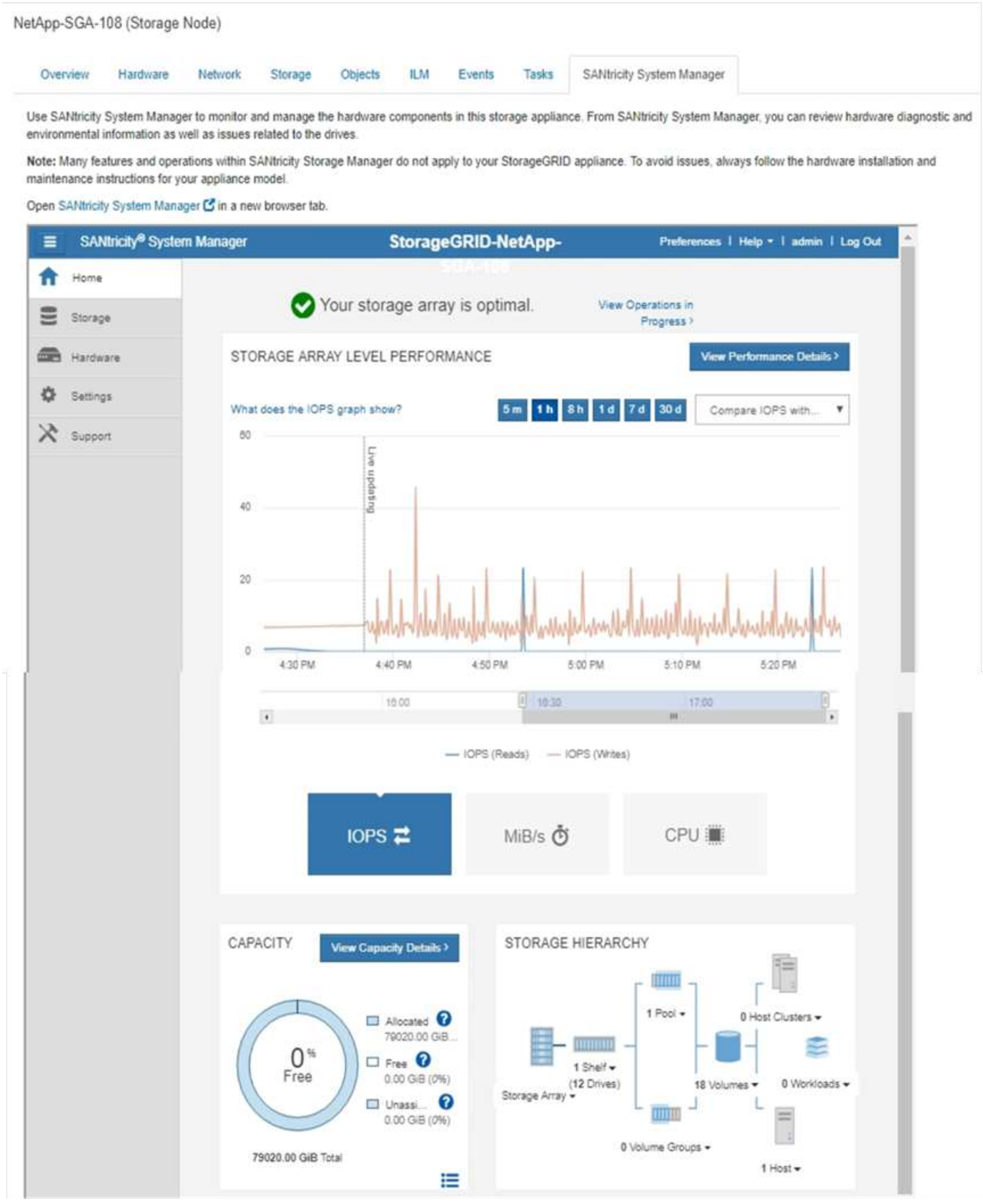
- Visualizza dati sulle prestazioni come le prestazioni a livello di array di storage, la latenza I/O, l'utilizzo della CPU dello storage controller e il throughput.
- Controlla lo stato dei componenti hardware.
- Esegui funzioni di supporto, tra cui la visualizzazione dei dati diagnostici e la configurazione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

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

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

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

La scheda visualizza la pagina iniziale di SANtricity System Manager.



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

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

cursore su ciascun grafico.

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

Informazioni da monitorare regolarmente

Cosa e quando monitorare in StorageGRID

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

Prima di iniziare

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

Informazioni sulle attività di monitoraggio

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

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

Monitorare lo stato di salute del sistema in StorageGRID

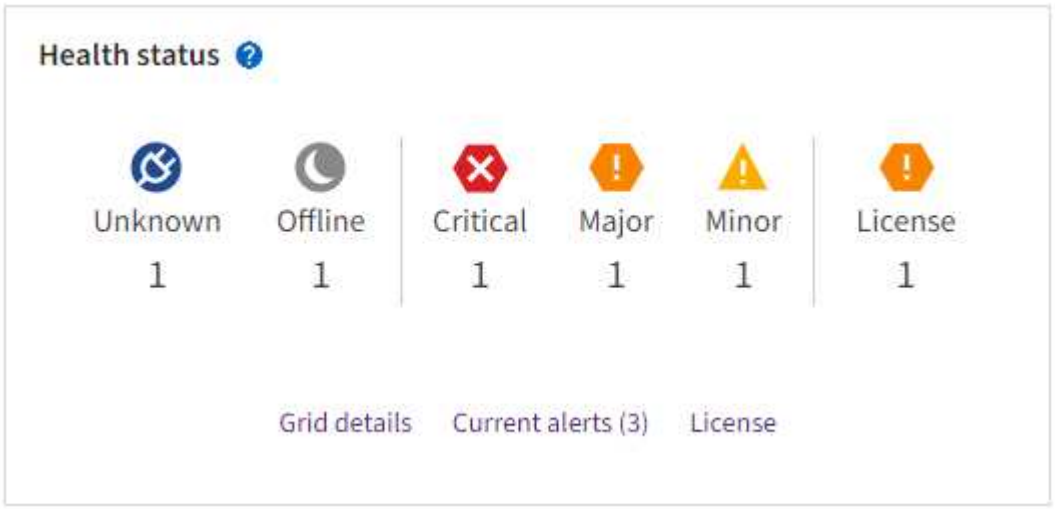
Monitora quotidianamente lo stato di salute generale del tuo sistema StorageGRID.

Informazioni su questa attività

Il sistema StorageGRID può continuare a funzionare quando alcune parti della grid non sono disponibili. I

potenziali problemi indicati dagli avvisi non sono necessariamente problemi nelle operazioni del sistema. Indaga sui problemi riassunti nella scheda Stato di salute della Dashboard di Grid Manager.

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



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

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

Monitora lo stato di connessione dei nodi

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

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

Visualizza gli avvisi correnti e risolti

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

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

Facoltativamente, hai guardato il video:

Panoramica degli avvisi

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

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

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

Passaggi

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

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

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

     La pagina degli avvisi correnti si aggiorna ogni due minuti.

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

   Vedi "Silenzia le notifiche di avviso".

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

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

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

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

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

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

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

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

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

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

Monitora la capacità di archiviazione in StorageGRID

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

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

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

Monitora la capacità di storage dell'intera grid

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

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

metadati degli oggetti.

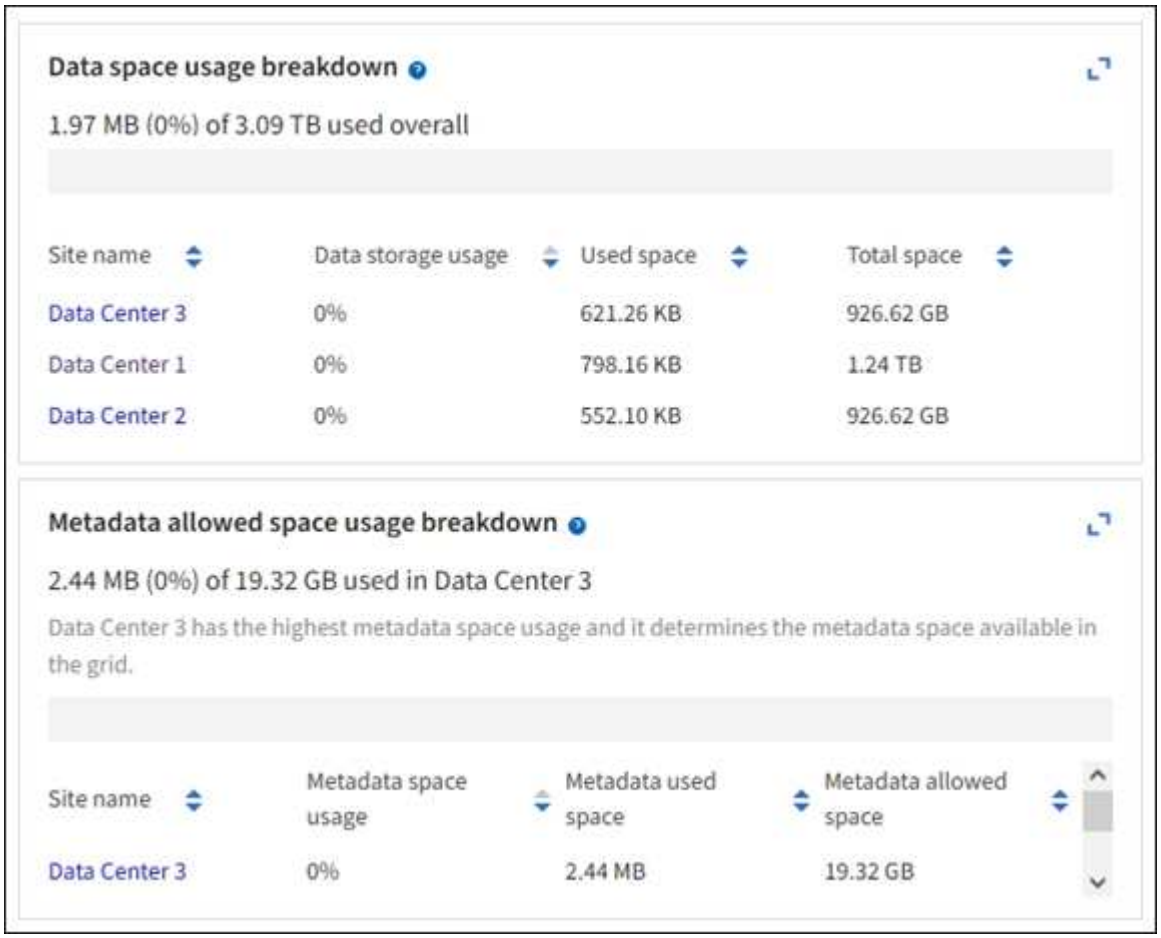
Passaggi

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

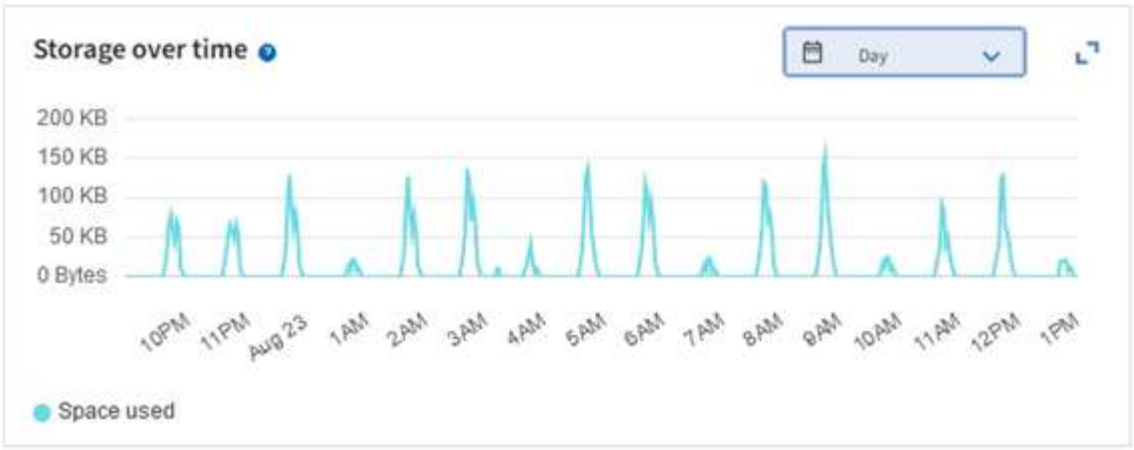
   a. Seleziona **Dashboard > Overview**.

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

   > Il riepilogo non include i supporti di archiviazione.



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



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

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

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

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

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

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

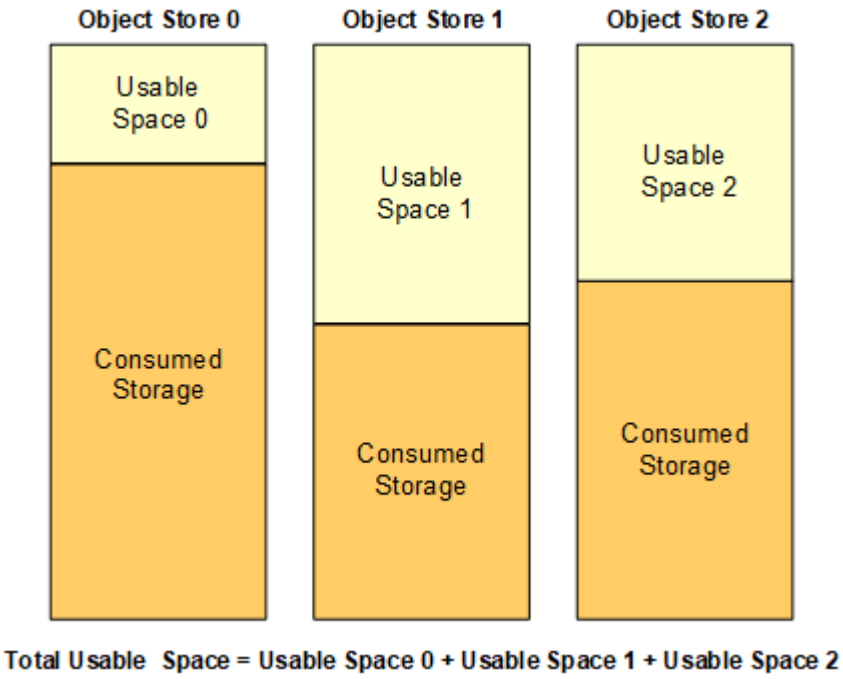
Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, consulta la "istruzioni per l'espansione di StorageGRID".

Monitora la capacità di storage per ciascun Storage Node

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

Informazioni su questa attività

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



Passaggi

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

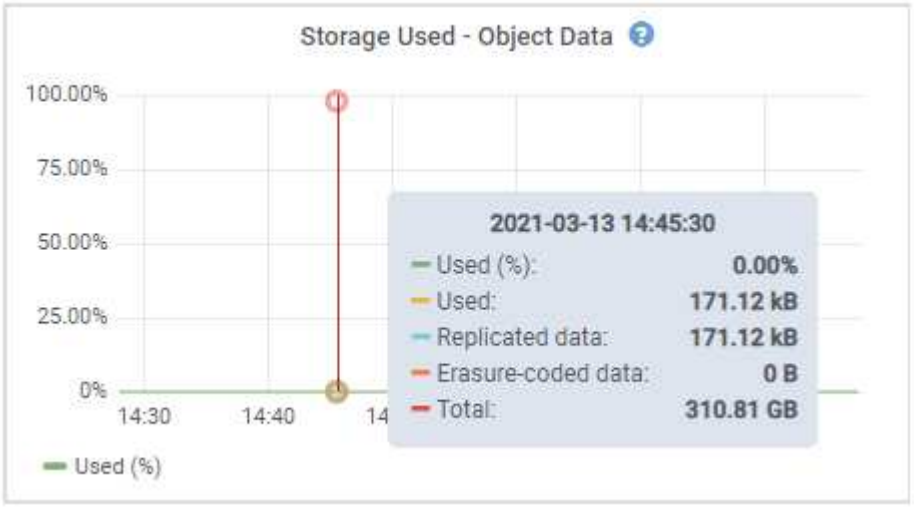
   Vengono visualizzati i grafici e le tabelle relativi al nodo.

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

   Vengono visualizzati i seguenti valori:

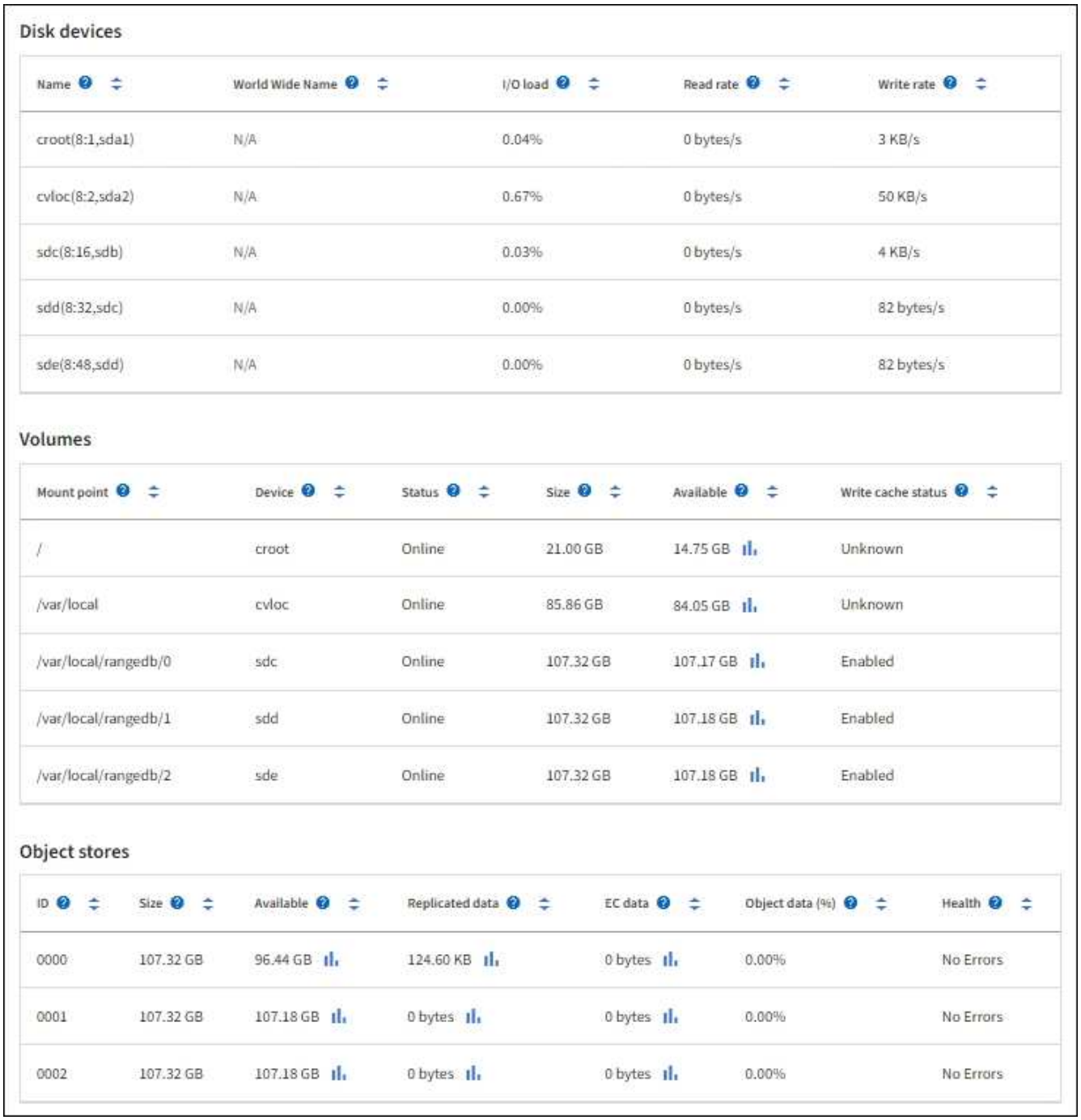
   - **Utilizzato (%)**: La percentuale dello spazio totale utilizzabile che hai usato per i dati degli oggetti.
   - **Utilizzato**: La quantità di spazio totale utilizzabile che hai usato per i dati degli oggetti.
   - **Dati replicati**: una stima della quantità di dati oggetto replicati su questo nodo,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

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



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

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



Disk devices

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

Volumes

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

Object stores

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

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

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

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

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

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

Monitora la capacità dei metadati degli oggetti per ciascun Storage Node

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

Informazioni su questa attività

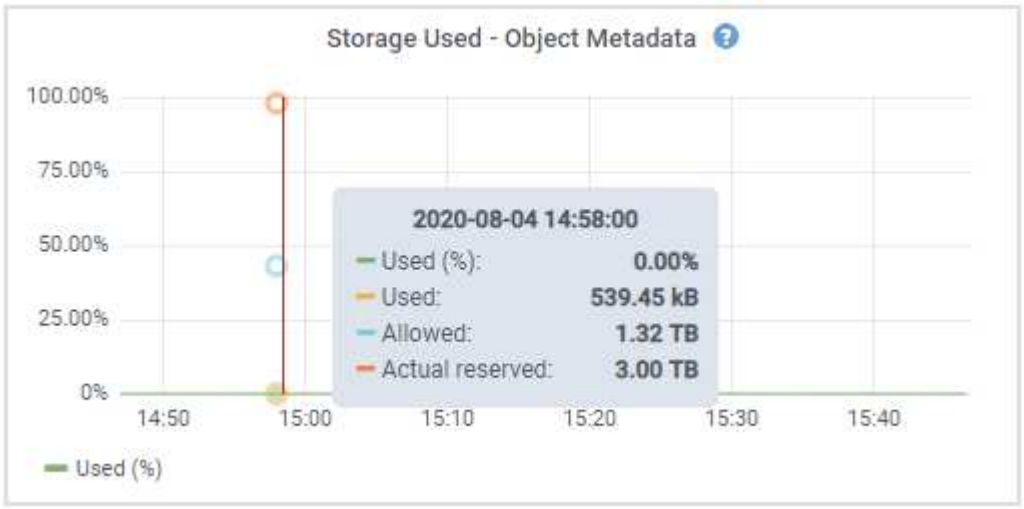
StorageGRID mantiene tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie sono distribuite uniformemente su tutti i nodi di storage di ciascun sito, utilizzando lo spazio riservato ai metadati sul volume di storage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

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

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

Passaggi

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



Usato (%)

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

metriche Prometheus: `storagegrid_storage_utilization_metadata_bytes` e `storagegrid_storage_utilization_metadata_allowed_bytes`

Usato

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

Metrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Consentito

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

Metrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Riservato effettivo

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

La metrica Prometheus sarà aggiunta in una versione futura.

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

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

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

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

Monitora le previsioni di utilizzo dello spazio

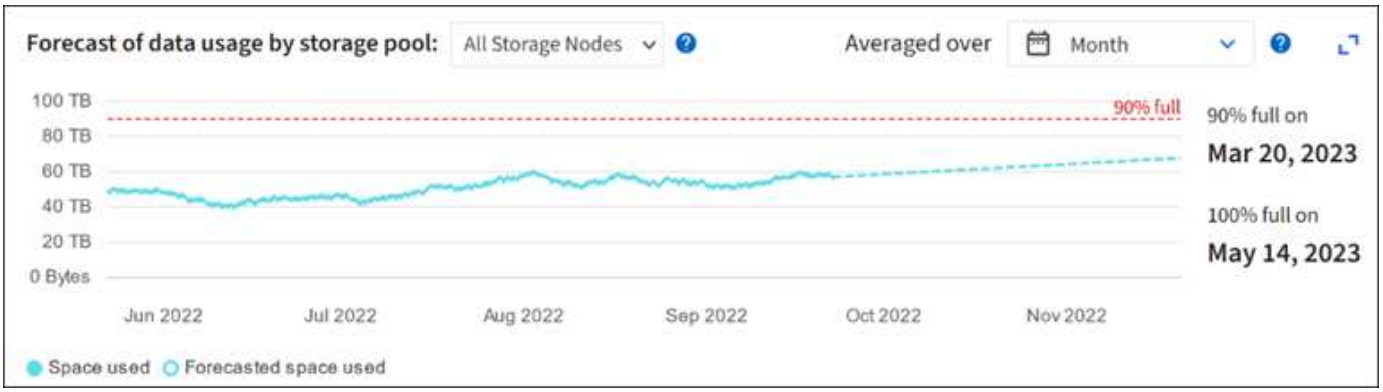
Monitora le previsioni di utilizzo dello spazio per i dati utente e metadati per stimare quando dovrai "espandi una griglia".

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

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

Passaggi

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



Monitorare la gestione del ciclo di vita delle informazioni in StorageGRID

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

Informazioni su questa attività

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

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

Usa la scheda dashboard di Grid Manager

Passaggi

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

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

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

Usa la pagina Nodi

Passaggi

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

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

1. Selezionare **Nodi**.

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

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

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

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

Monitora le risorse di rete e di sistema in StorageGRID

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

Monitora le connessioni di rete e le prestazioni

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

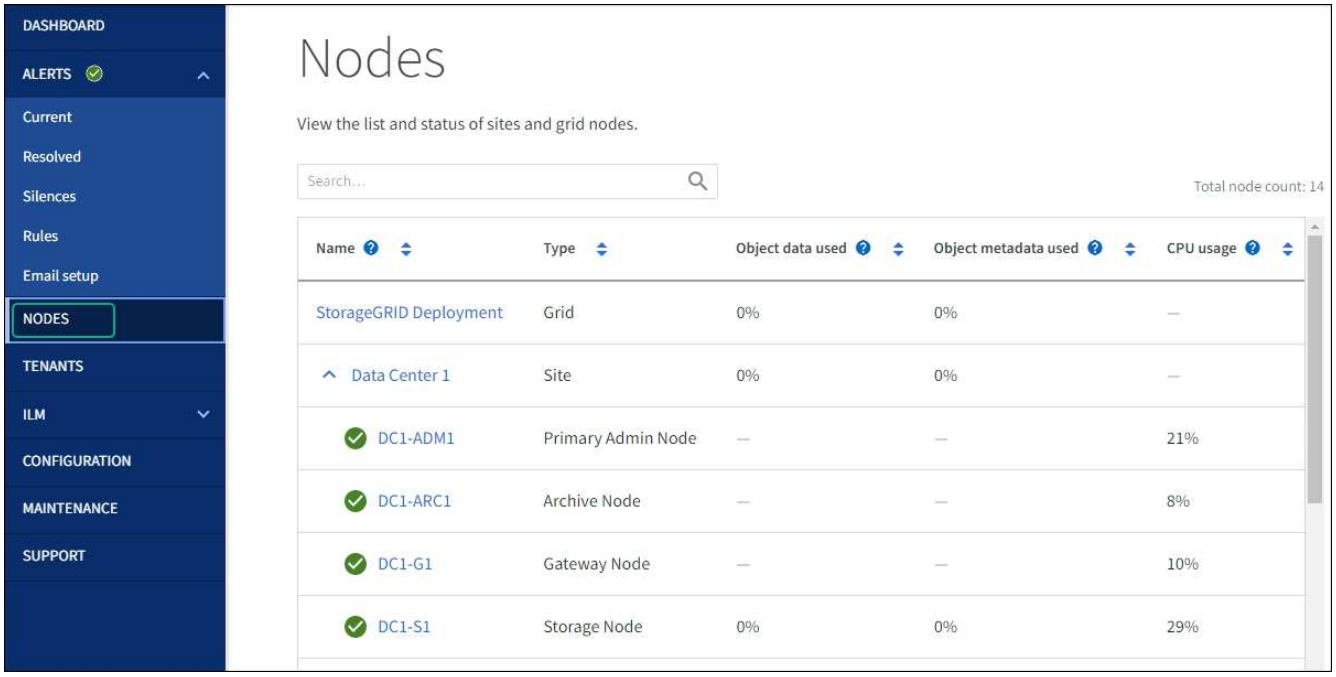
Utilizza Grid Manager per monitorare la connettività e le prestazioni della rete, così puoi risolvere subito eventuali problemi.

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

Passaggi

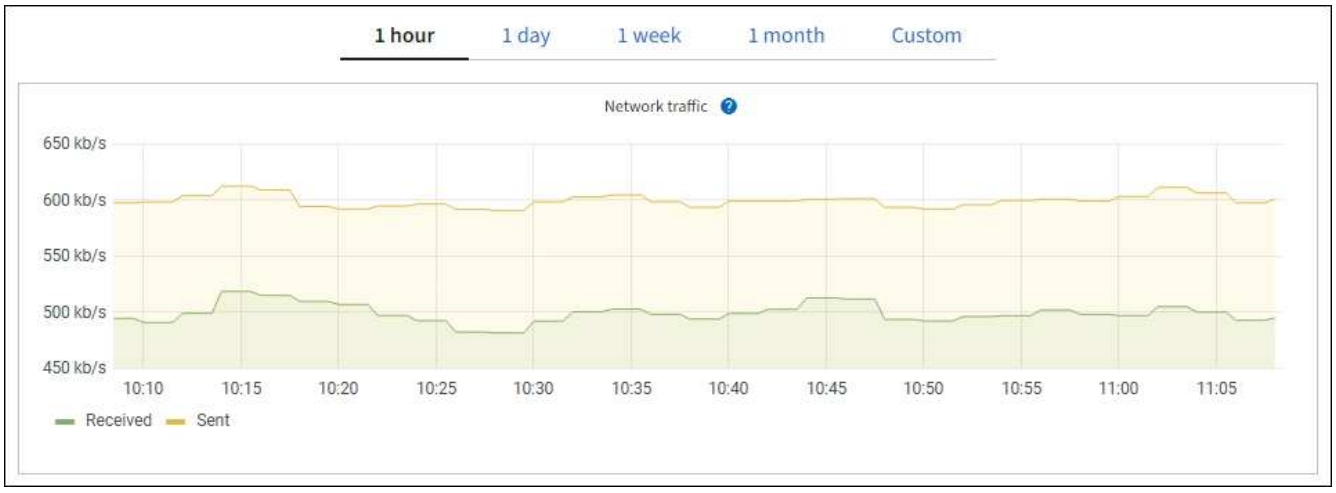
1. Selezionare **Nodi**.

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

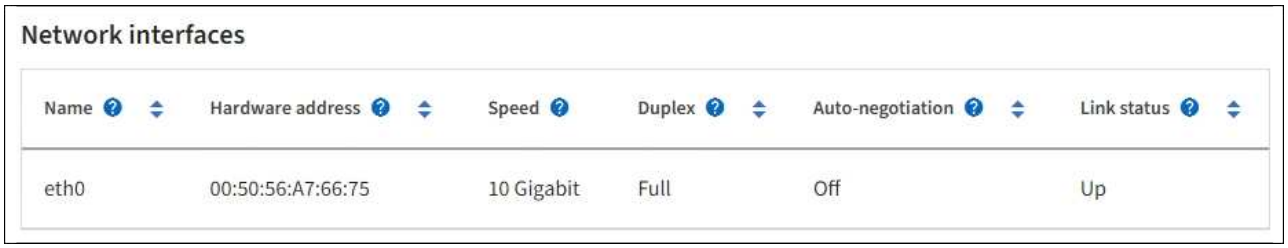


2. Seleziona il nome della griglia, un sito specifico del data center o un nodo della griglia, quindi seleziona la scheda **Network**.

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

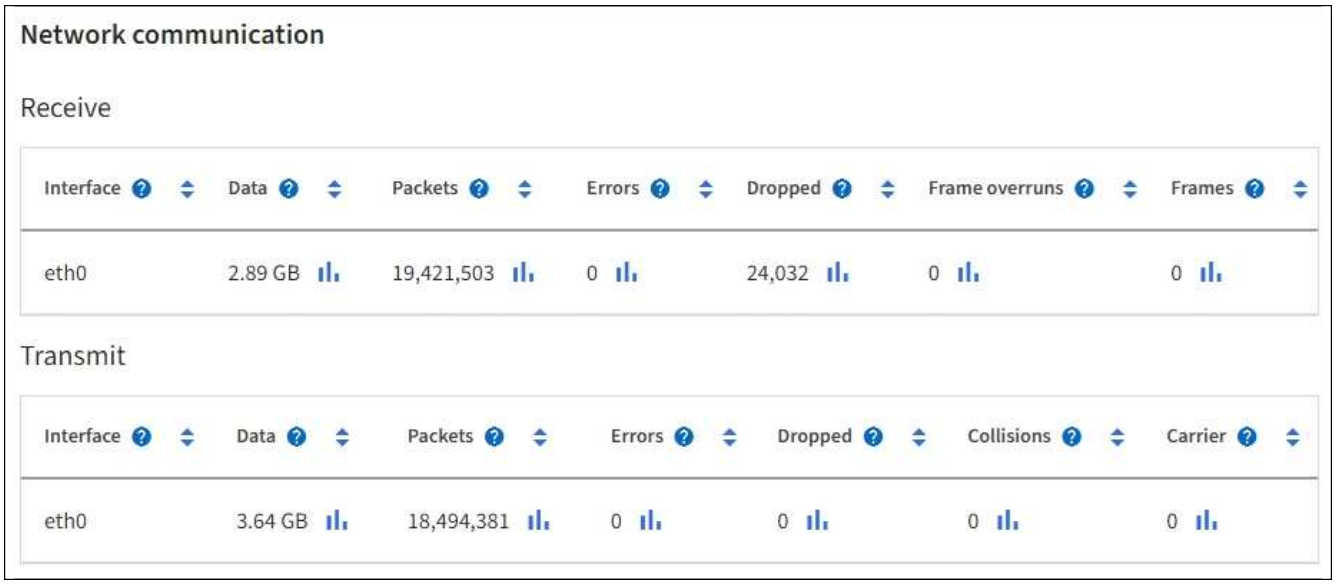


   a. Se hai selezionato un nodo della griglia, scorri verso il basso per visualizzare la sezione **Interfacce di rete** della pagina.



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

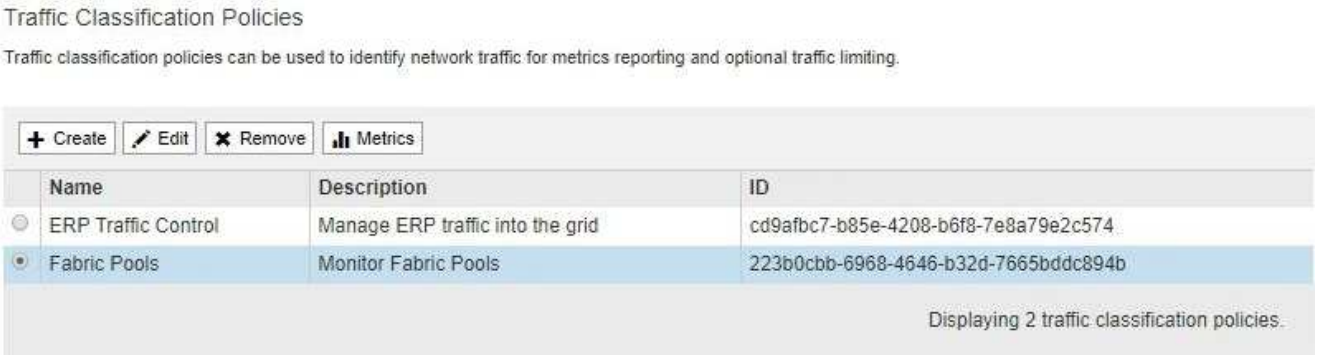
   Le tabelle Ricezione e Trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, oltre ad altre metriche di ricezione e trasmissione.



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

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

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



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

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

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

Informazioni correlate

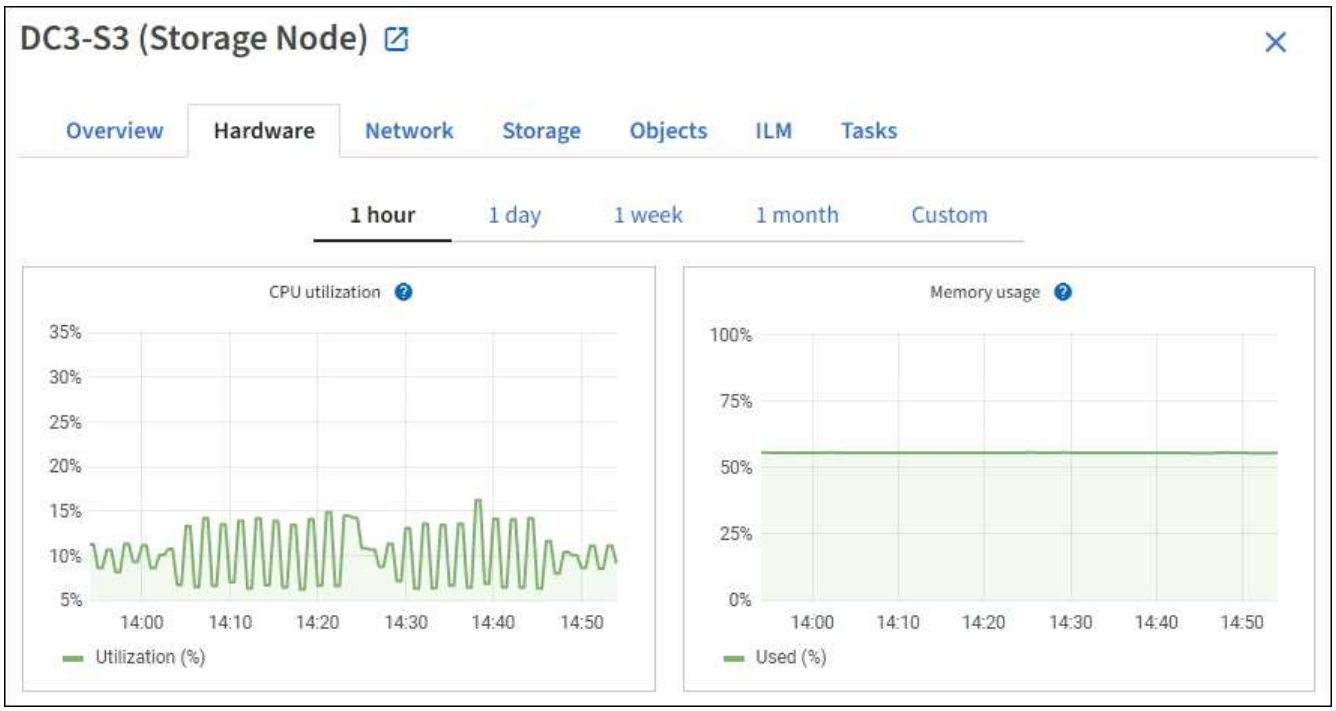
- "Visualizza la scheda Rete"
- "Monitora lo stato di connessione dei nodi"

Monitora le risorse a livello di nodo

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

Passaggi

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



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

Informazioni correlate

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

Monitorare l’attività dei tenant in StorageGRID

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

Prima di iniziare

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

Visualizza tutti i tenant

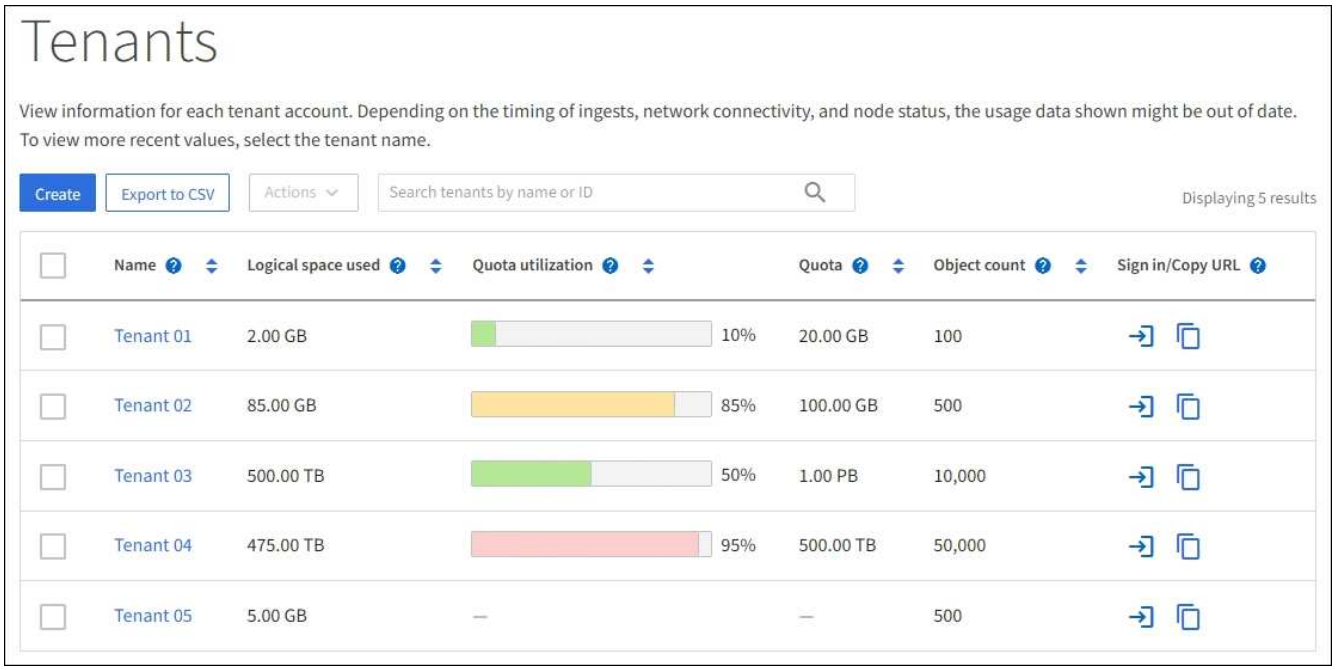
La pagina Tenant mostra le informazioni di base per tutti gli account tenant attivi.

Passaggi

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

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

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



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

nella colonna **Accedi/Copia URL**.

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

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

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

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

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

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

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

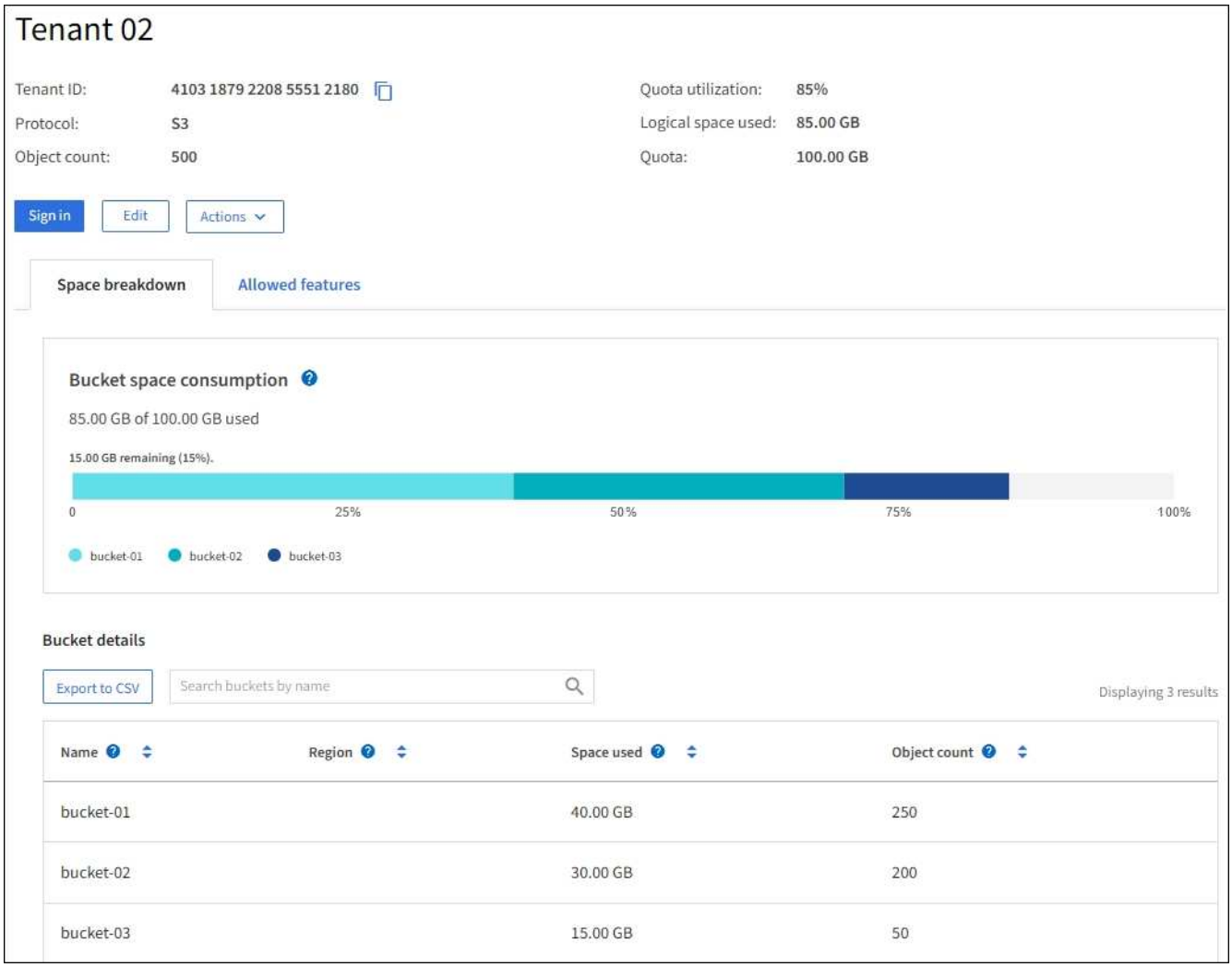
Visualizza un tenant specifico

Puoi visualizzare i dettagli di uno specifico tenant.

Passaggi

1. Seleziona il nome del tenant dalla pagina Tenant.

   Viene visualizzata la pagina dei dettagli del tenant.



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

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

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

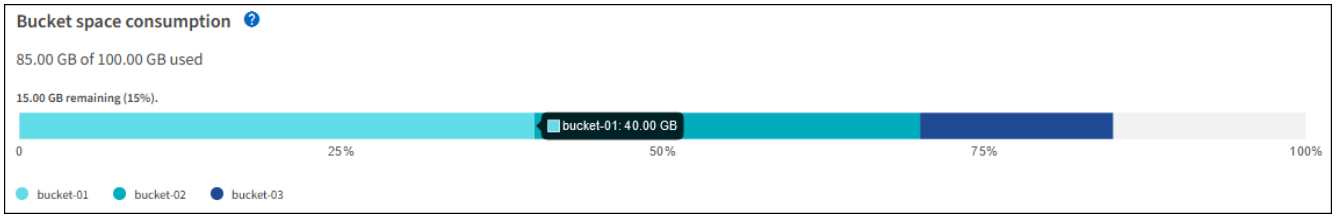
3. Dalla scheda **Ripartizione dello spazio**, controlla il grafico **Consumo di spazio**.

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

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

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

di archiviazione rimanente.



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

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

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

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

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

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

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

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

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

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

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

Visualizza traffico di rete

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

Passaggi

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

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

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

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

Usa il registro di controllo

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

Ad esempio, puoi monitorare i seguenti tipi di informazioni:

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

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

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

Usa le metriche Prometheus

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

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

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

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

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

Monitorare le operazioni del client S3 in StorageGRID

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

Prima di iniziare

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

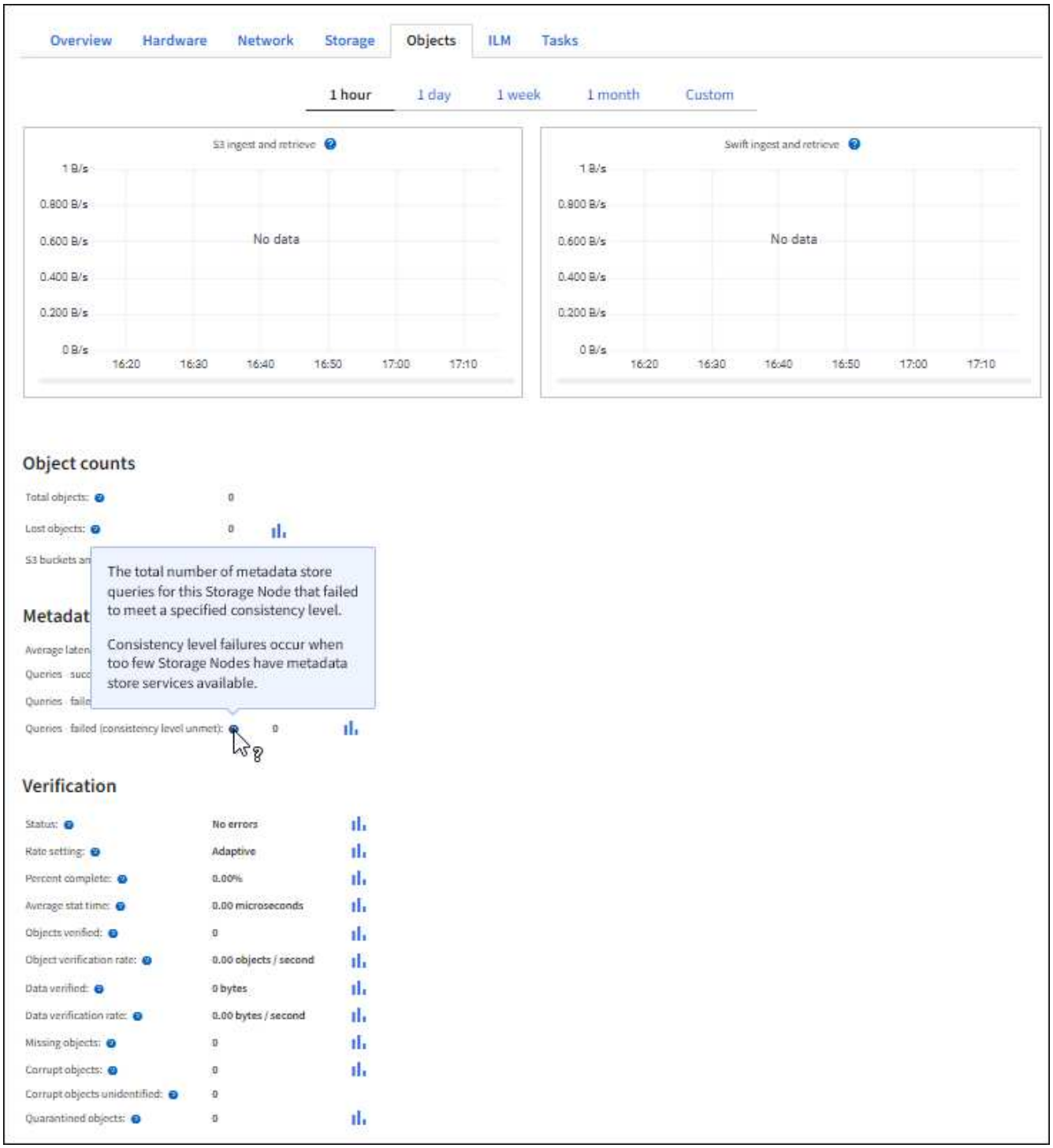
Passaggi

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

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

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

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



Monitorare le operazioni di bilanciamento del carico in StorageGRID

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

Informazioni su questa attività

Puoi usare il servizio Load Balancer sui nodi di amministrazione, sui nodi gateway oppure un bilanciatore di

carico esterno di terze parti per distribuire le richieste dei client su più nodi di Storage.

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

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

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

Passaggi

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

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

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

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

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

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

Monitorare le connessioni della federazione della griglia StorageGRID

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

Prima di iniziare

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

Visualizza tutte le connessioni

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

Passaggi

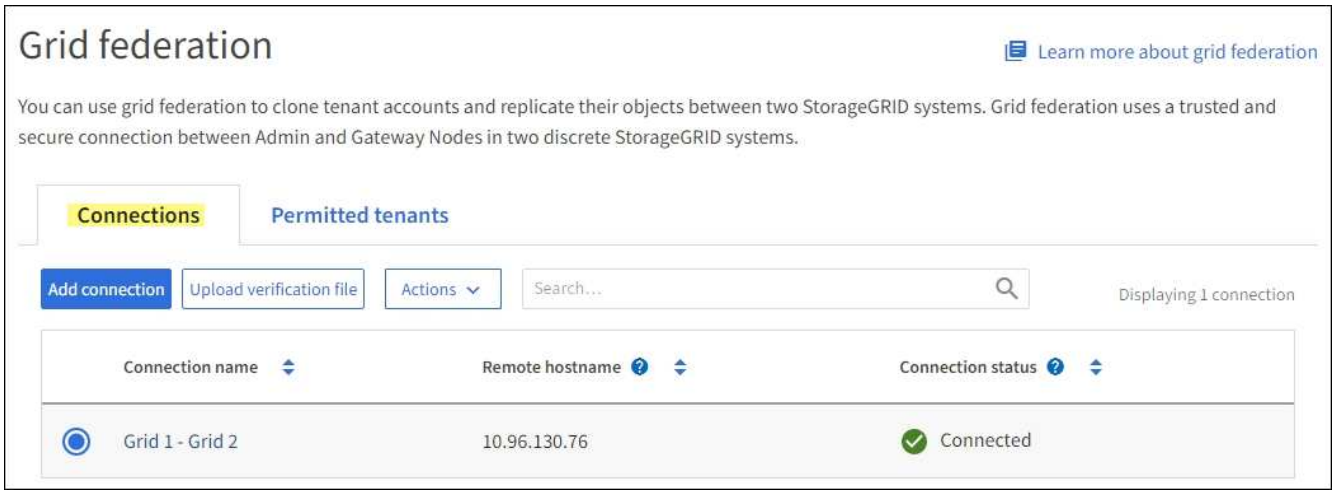
1. Seleziona **Configurazione** > **Sistema** > **Grid federation**.

   Viene visualizzata la pagina Grid federation.

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

   Da questa scheda puoi:

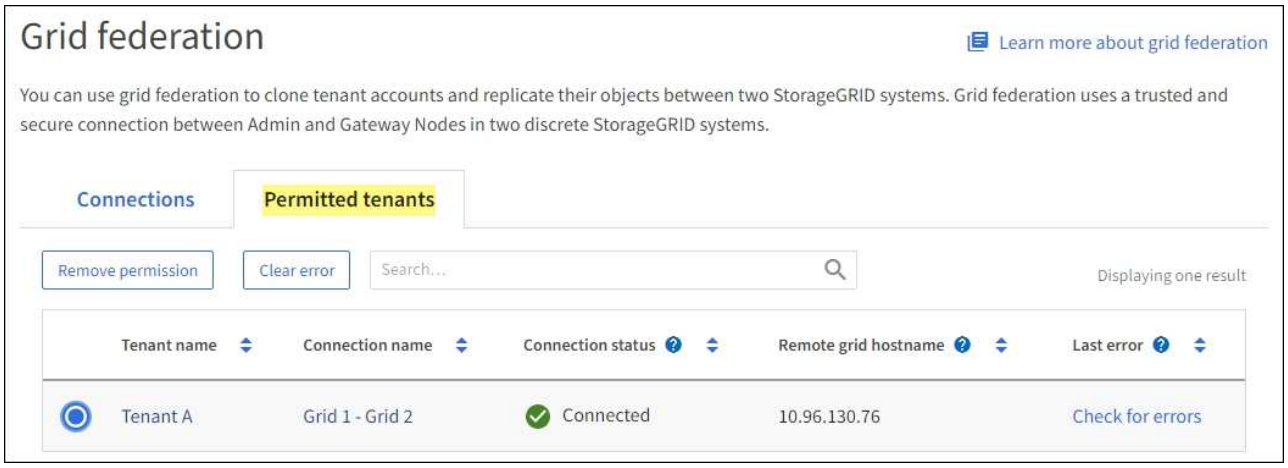
   - "Crea una nuova connessione".
   - Seleziona una connessione esistente a "modifica o prova".



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

   Da questa scheda puoi:

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



Visualizza una connessione specifica

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

Passaggi

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

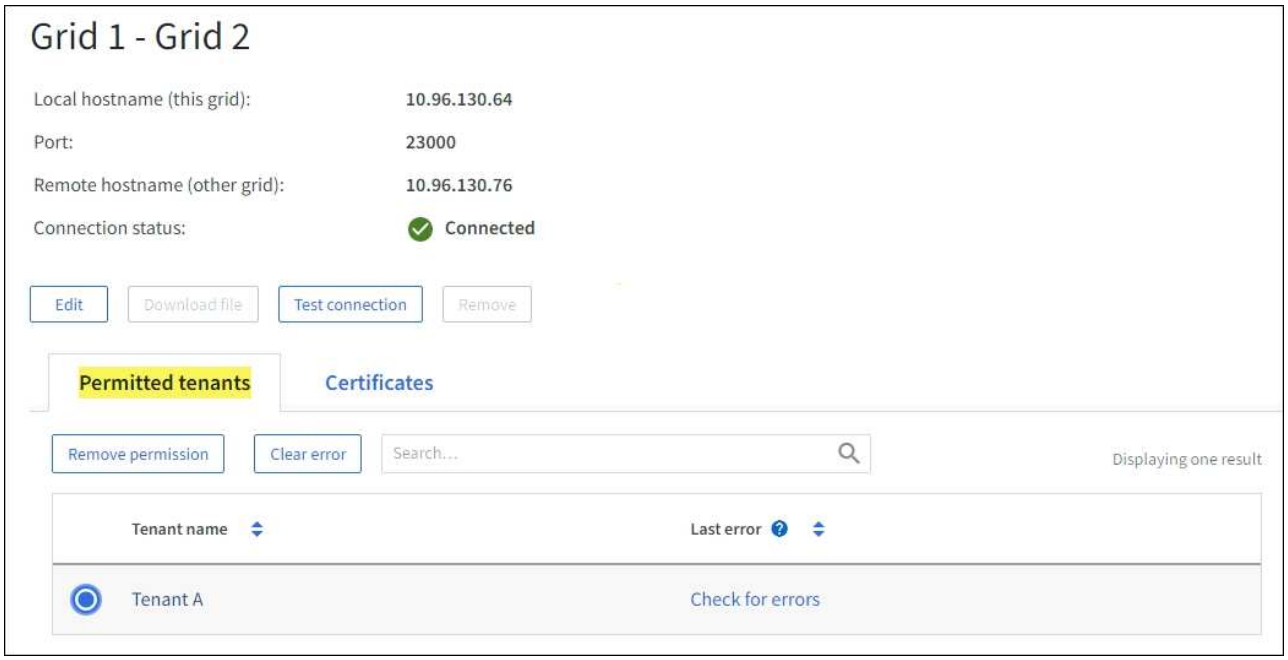
   Dalla pagina dei dettagli della connessione puoi:

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

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

   Da questa scheda puoi:

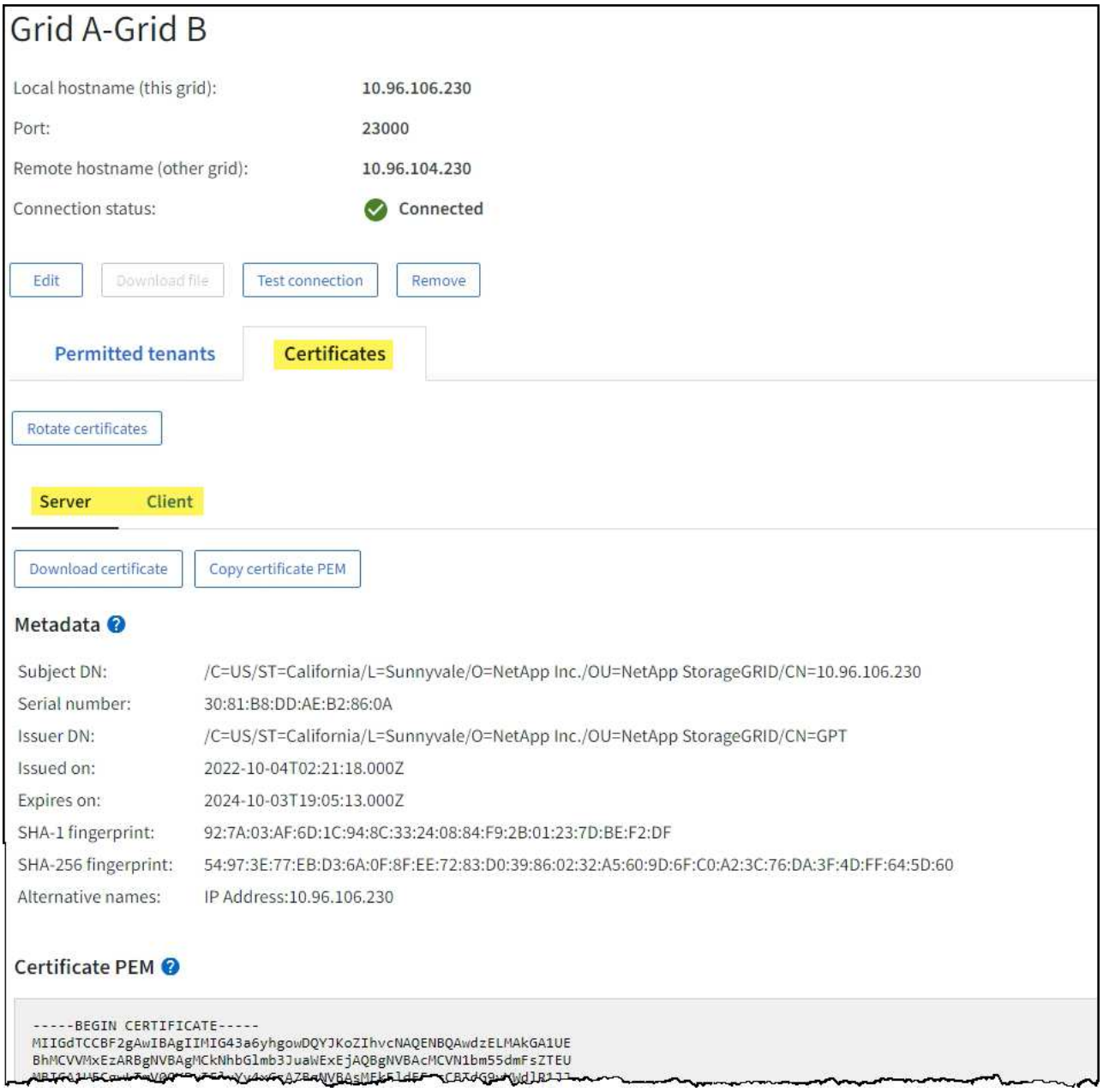
   - "Visualizza la pagina dei dettagli per ogni tenant".
   - "Rimuovi il permesso di un tenant" per utilizzare la connessione.
   - Verifica la presenza di errori di replica tra griglie e cancella l'ultimo errore. Vedi "Risolvi i problemi relativi agli errori di federazione della griglia".



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

   Da questa scheda puoi:

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



Esamina le metriche di replica cross-grid

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

Passaggi

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

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

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

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

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

Gestisci gli avvisi

Gestisci gli avvisi in StorageGRID

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

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

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

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

Per saperne di più:

- Guarda i video:

  Panoramica degli avvisi

  Avvisi personalizzati

- Fai riferimento a "Riferimento agli avvisi".

Visualizza le regole di avviso di StorageGRID

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

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

Prima di iniziare

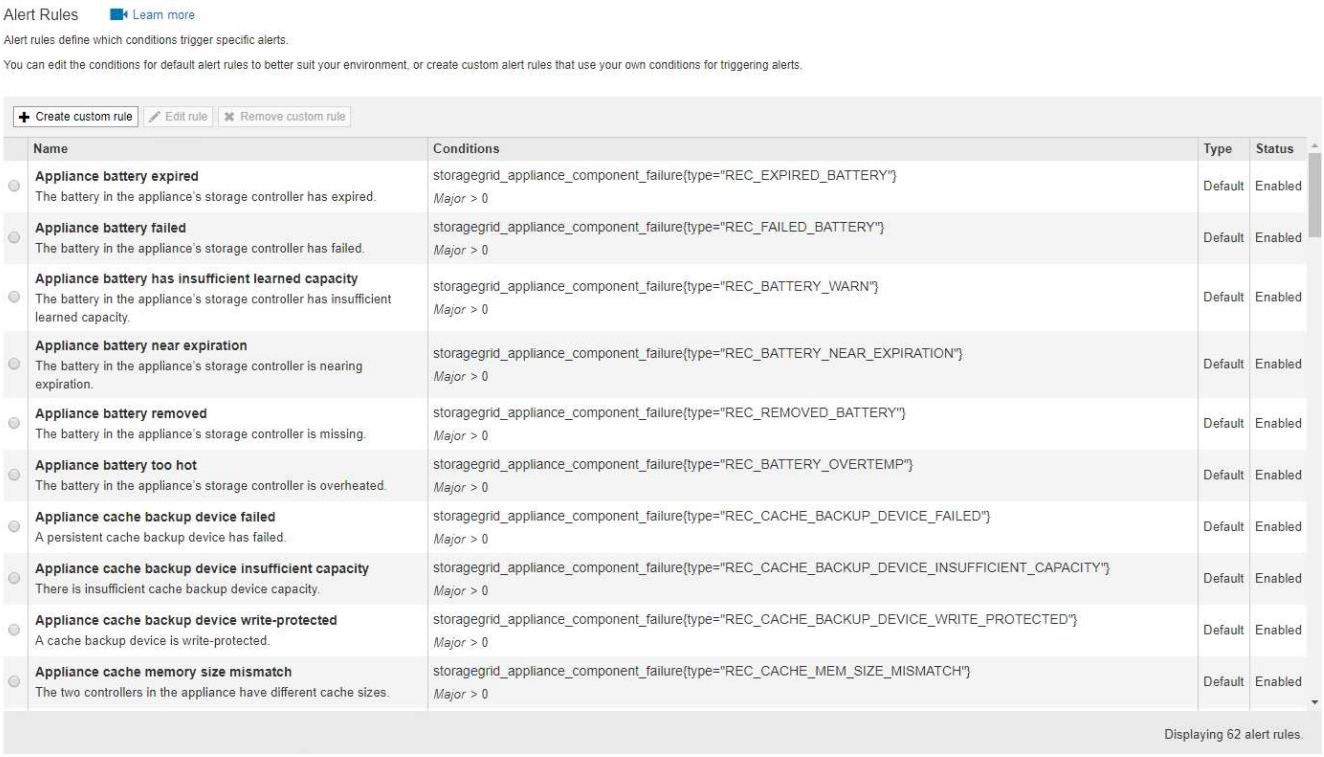
- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestisci gli avvisi o i permessi di accesso root".
- Facoltativamente, hai guardato il video:

  Panoramica degli avvisi

Passaggi

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

   Viene visualizzata la pagina Regole di avviso.



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

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

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

Crea regole di avviso personalizzate in StorageGRID

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

Prima di iniziare

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

- Facoltativamente, hai guardato il video:

  Avvisi personalizzati

Informazioni su questa attività

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

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

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

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

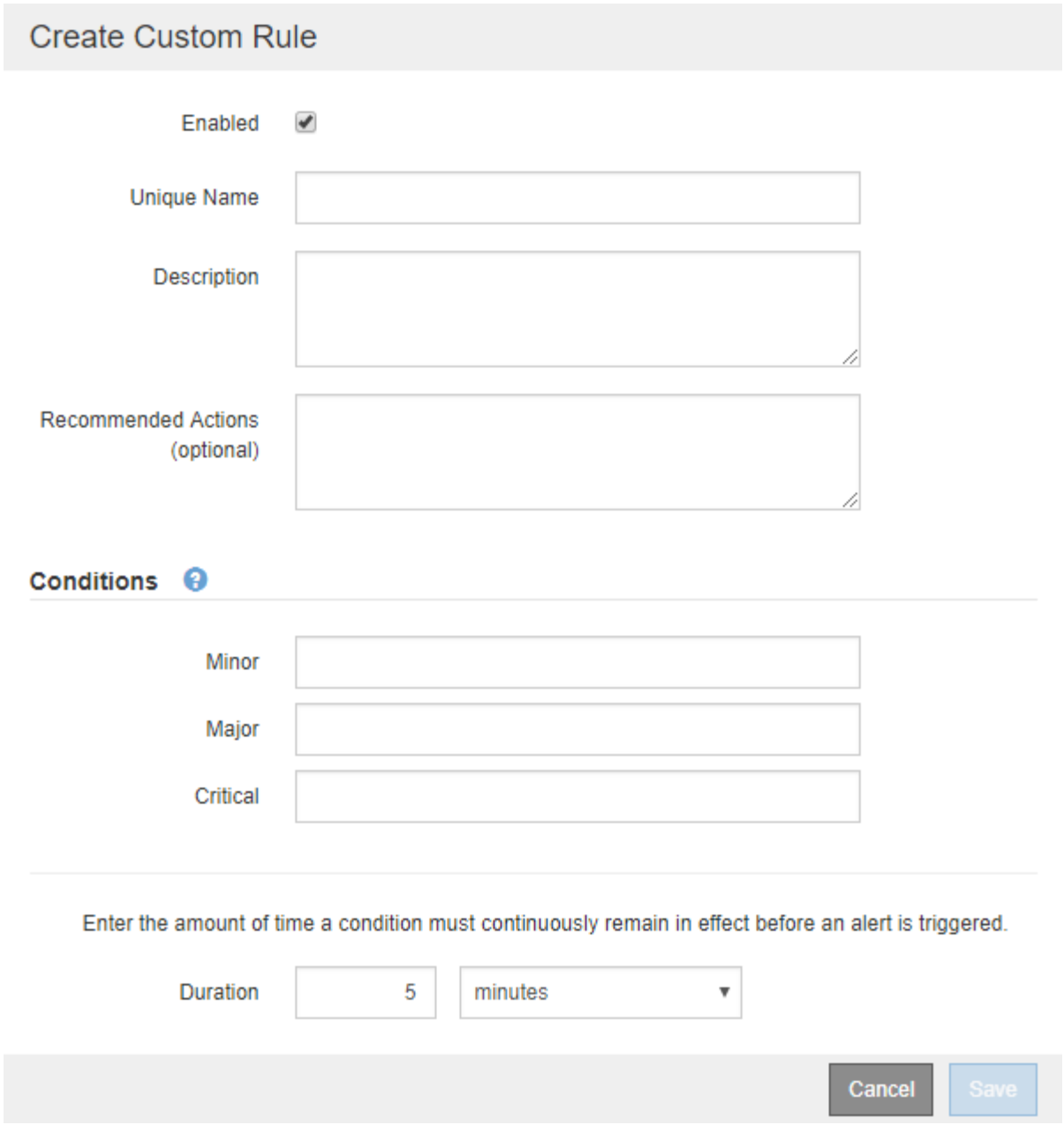
Passaggi

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

   Viene visualizzata la pagina Regole di avviso.

2. Seleziona **Crea regola personalizzata**.

   Viene visualizzata la finestra di dialogo Crea regola personalizzata.



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

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

4. Inserisci le seguenti informazioni:

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

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

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

   Un'espressione di base è solitamente della forma:

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

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

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

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

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

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

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

   Il valore predefinito è 5 minuti.

7. Seleziona **Salva**.

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

Modifica le regole di avviso in StorageGRID

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

Prima di iniziare

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

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

Informazioni su questa attività

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

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

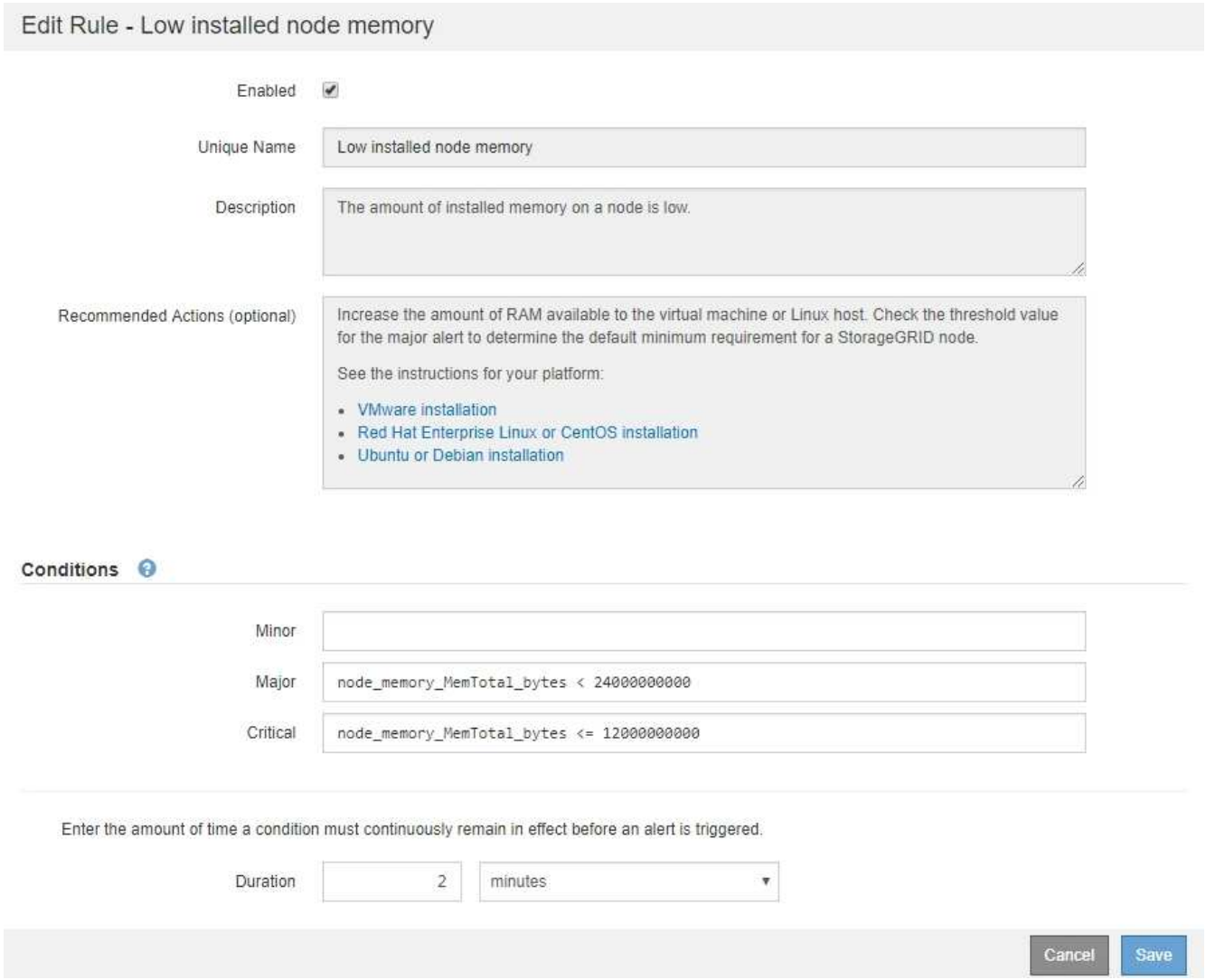
Passaggi

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

   Viene visualizzata la pagina Regole di avviso.

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

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



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

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

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

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

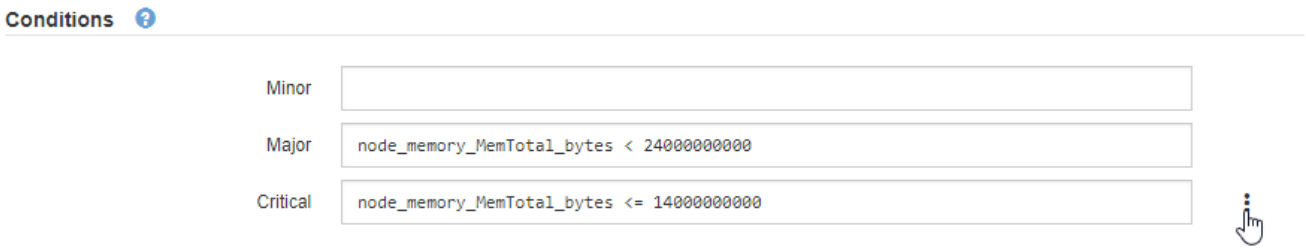
5. Per le regole di avviso personalizzate, aggiorna le seguenti informazioni secondo necessità.

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

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

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

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



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

Un'espressione di base è solitamente della forma:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

Il valore predefinito è 5 minuti.

8. Seleziona **Salva**.

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

Disabilita le regole di avviso in StorageGRID

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

Prima di iniziare

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

Informazioni su questa attività

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

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

Passaggi

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

   Viene visualizzata la pagina Regole di avviso.

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

   Viene visualizzata la finestra di dialogo Modifica regola.

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

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

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

5. Seleziona **Salva**.

   Disabilitato compare nella colonna **Stato**.

Rimuovi le regole di avviso personalizzate in StorageGRID

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

Prima di iniziare

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

Passaggi

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

   Viene visualizzata la pagina Regole di avviso.

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

   Non puoi rimuovere una regola di avviso predefinita.

3. Seleziona **Rimuovi regola personalizzata**.

   Viene visualizzata una finestra di dialogo di conferma.

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

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

Gestisci le notifiche di avviso

Imposta le notifiche SNMP per gli avvisi StorageGRID

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

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

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

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

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

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

l'avviso. Vedi "Silenzia le notifiche di avviso".

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

Configura le notifiche e-mail per gli avvisi di StorageGRID

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

Prima di iniziare

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

Informazioni su questa attività

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

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

Passaggi

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

   Viene visualizzata la pagina di configurazione della posta elettronica.

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

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

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

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

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

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

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

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

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

      Seleziona l'icona più ➕ per aggiungere i destinatari.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Seleziona **Salva**.

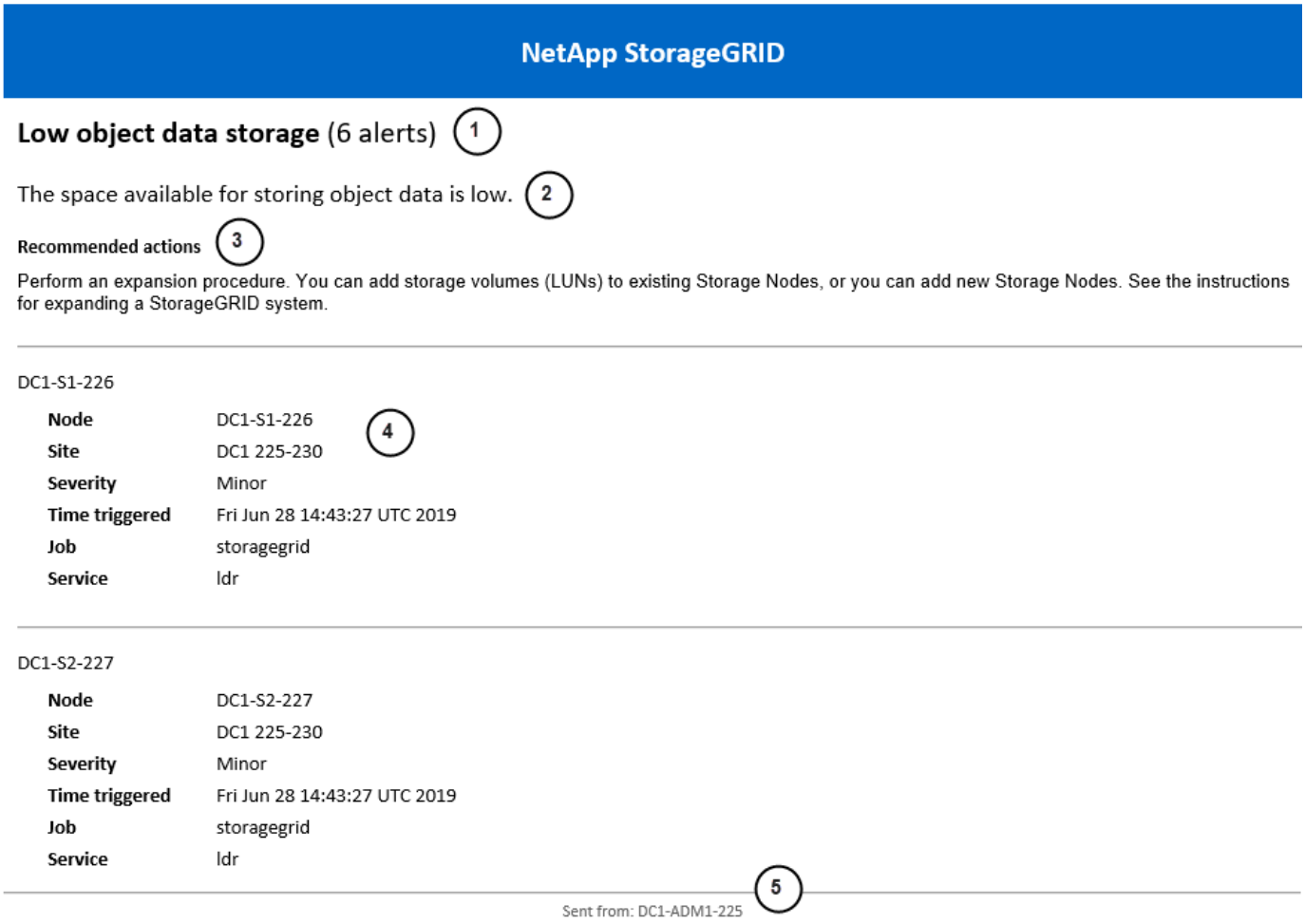
   L'invio di un'email di prova non salva le impostazioni. Devi selezionare **Salva**.

   Le impostazioni e-mail sono state salvate.

Informazioni incluse nelle notifiche e-mail di avviso

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

Le notifiche via e-mail includono le seguenti informazioni:



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

Come vengono raggruppati gli avvisi

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

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

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

Risolvi i problemi delle notifiche email di avviso

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

Prima di iniziare

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

Passaggi

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

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

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

Silenzia le notifiche di alert in StorageGRID

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

Prima di iniziare

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

Informazioni su questa attività

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

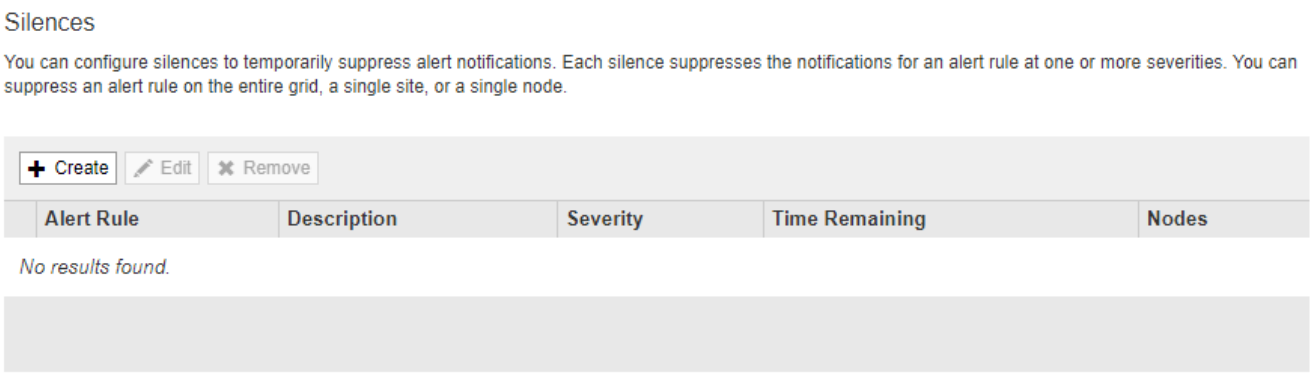
Se hai abilitato l'agente SNMP, le funzioni di silenziamento sopprimono anche le trap e le inform SNMP.

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

Passaggi

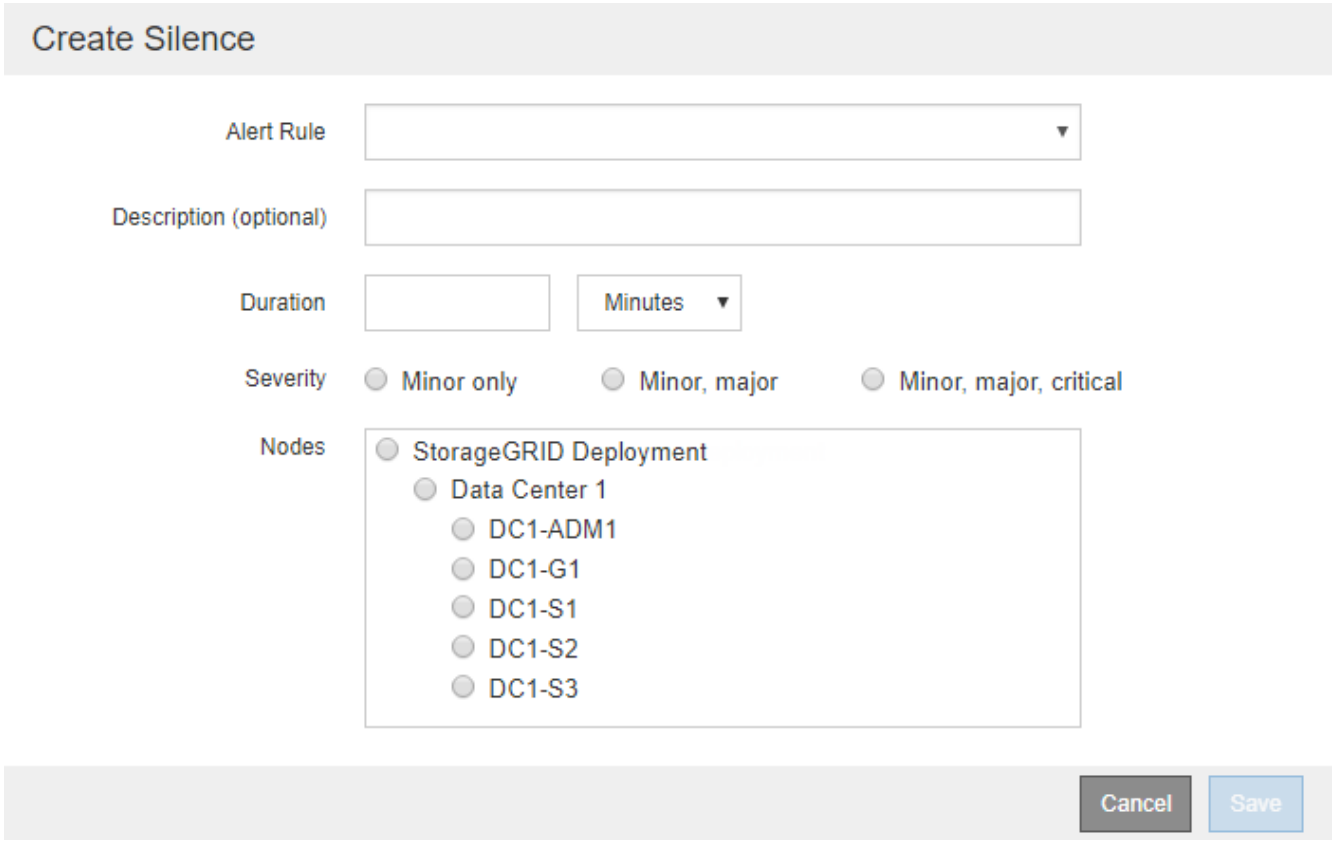
1. Seleziona **Avvisi** > **Silenzi**.

   Viene visualizzata la pagina Silences.



2. Seleziona **Create**.

   Viene visualizzata la finestra di dialogo Crea Silence.



3. Seleziona o inserisci le seguenti informazioni:

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

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

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

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

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

Informazioni correlate

"Configura l'agente SNMP"

Avvisi in StorageGRID

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

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

Alcuni degli avvisi predefiniti utilizzano "metriche Prometheus".

Avvisi sull'appliance

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

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

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

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

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

Avvisi di audit e syslog

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

Avvisi bucket

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

Avvisi Cassandra

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

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

Avvisi relativi ai Cloud Storage Pool

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

Avvisi di replica cross-grid

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

Avvisi DHCP

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

Avvisi di debug e tracciamento

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

Email e avvisi AutoSupport

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

Avvisi di erasure coding (EC)

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

Avvisi di scadenza dei certificati

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

Avvisi della Grid Network

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

Avvisi di federazione della grid

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

Avvisi di utilizzo elevato o latenza elevata

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

Avvisi di federazione delle identità

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

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

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

Avvisi del server di gestione delle chiavi (KMS)

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

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

Avvisi del load balancer

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

Avvisi di scostamento dell’orologio locale

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

Avvisi di memoria insufficiente o spazio insufficiente

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

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

Avvisi relativi al nodo o alla rete di nodi

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

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

Nome dell'allerta	Descrizione
Collegamento del dispositivo di storage interrotto sulla porta di rete 2	La porta di rete 2 sull'appliance è offline o disconnessa.
Collegamento storage appliance interrotto sulla porta di rete 3	La porta di rete 3 sull'appliance è offline o disconnessa.
Collegamento del dispositivo di storage interrotto sulla porta di rete 4	La porta di rete 4 sull'appliance è down o disconnessa.
Il nodo di storage non è nello stato di storage desiderato	Il servizio LDR su un nodo di archiviazione non può passare allo stato desiderato a causa di un errore interno o di un problema relativo al volume
utilizzo della connessione TCP	Il numero di connessioni TCP su questo nodo si sta avvicinando al numero massimo che può essere tracciato.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono oppure il nodo non è raggiungibile.
Riavvio imprevisto del nodo	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore.

Avvisi sugli oggetti

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

Avvisi di danneggiamento degli oggetti

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

Avvisi dei servizi della piattaforma

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

Avvisi relativi al volume di storage

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

Avvisi dei servizi StorageGRID

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

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

Avvisi tenant

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

Metriche Prometheus comunemente utilizzate in StorageGRID

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

Puoi anche ottenere un elenco completo di tutte le metriche.

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

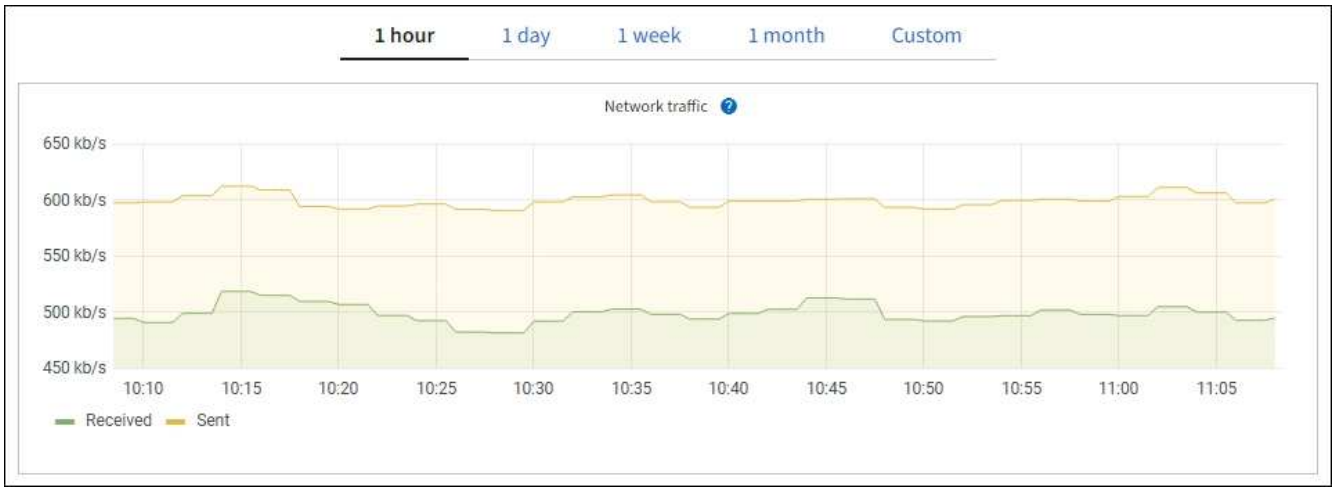
Che cosa sono le metriche di Prometheus?

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

Dove vengono utilizzate le metriche di Prometheus?

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

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



- **Avvisi**: Gli avvisi vengono attivati a specifici livelli di gravità quando le condizioni delle regole di avviso che utilizzano metriche Prometheus risultano vere.
- **Grid Management API**: Puoi usare le metriche Prometheus nelle regole di avviso personalizzate o con strumenti di automazione esterni per monitorare il tuo sistema StorageGRID. Un elenco completo delle metriche Prometheus è disponibile tramite la Grid Management API. (Dalla parte superiore di Grid Manager, seleziona l'icona di aiuto e scegli **API documentation** > **metrics**.) Anche se sono disponibili oltre mille metriche, solo un numero relativamente piccolo è necessario per monitorare le operazioni StorageGRID più critiche.

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

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

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

Elenco delle metriche più comuni

Il seguente elenco contiene le metriche Prometheus più comunemente utilizzate.

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

alertmanager_notifications_failed_total

Il numero totale di notifiche di avviso non riuscite.

node_filesystem_avail_bytes

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

node_memory_MemAvailable_bytes

Campo delle informazioni sulla memoria MemAvailable_bytes.

node_network_carrier

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

node_network_receive_errs_total

Statistiche del dispositivo di rete `receive_errs`.

node_network_transmit_errs_total

Statistiche del dispositivo di rete `transmit_errs`.

storagegrid_amministrativamente_disattivato

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

stato hardware del controller di calcolo dell'appliance StorageGRID

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

dischi guasti dell'appliance StorageGRID

Per lo storage controller in un appliance, il numero di drive che non sono ottimali.

storagegrid_appliance_storage_controller_hardware_status

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

bucket e container di StorageGRID

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

storagegrid_content_objects

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

storagegrid_content_objects_lost

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

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

storagegrid_http_sessions_incoming_attempted

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

storagegrid_http_sessions_incoming_currently_established

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

storagegrid_http_sessions_incoming_failed

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

storagegrid_http_sessions_incoming_successful

Il numero totale di sessioni HTTP completate con successo.

storagegrid_ilm_awaiting_background_objects

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

storagegrid_ilm_awaiting_client_evaluation_objects_per_second

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

storagegrid_ilm_awaiting_client_objects

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

storagegrid_ilm_awaiting_total_objects

Il numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_objects_per_second

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

minuti stimati del periodo di scansione ILM di StorageGRID

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

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

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

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

latenza media delle query sui metadati di StorageGRID in millisecondi

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

byte ricevuti dalla rete StorageGRID

Quantità totale di dati ricevuti dall'installazione.

byte trasmessi dalla rete StorageGRID

Quantità totale di dati inviati dall'installazione.

percentuale di utilizzo della CPU del nodo StorageGRID

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

storagegrid_ntp_chosen_time_source_offset_milliseconds

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

storagegrid_ntp_locked

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

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

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

storagegrid_s3_operations_failed

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

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_unauthorized

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

storagegrid_servercertificate_management_interface_cert_expiry_days

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

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

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

storagegrid_service_cpu_seconds

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

storagegrid_service_memory_usage_bytes

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

byte ricevuti dalla rete di servizi di StorageGRID

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

byte trasmessi dalla rete del servizio StorageGRID

Quantità totale di dati inviati da questo servizio.

riavvii del servizio StorageGRID

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

storagegrid_service_runtime_seconds

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

storagegrid_service_uptime_seconds

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

storagegrid_storage_state_current

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

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

storagegrid_storage_status

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

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

- 40 = Errore

storagegrid_storage_utilization_data_bytes

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

storagegrid_storage_utilization_metadata_allowed_bytes

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

utilizzo dei metadati di StorageGRID

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

storagegrid_storage_utilization_total_space_bytes

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

storagegrid_storage_utilization_usable_space_bytes

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

storagegrid_tenant_usage_data_bytes

La dimensione logica di tutti gli oggetti per il tenant.

conteggio degli oggetti utilizzati dal tenant in StorageGRID

Il numero di oggetti per il tenant.

storagegrid_tenant_usage_quota_bytes

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

Ottieni un elenco di tutte le metriche

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

Passaggi

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

Riferimento ai file di registro

File di log di StorageGRID

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

I log sono classificati come segue:

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

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

Accedi ai registri

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

Passaggi

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

Esporta i log sul server syslog

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

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

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

Categorie dei file di log

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

Posizione archivio	Descrizione
audit	Messaggi di audit generati durante il normale funzionamento del sistema.
log del sistema operativo di base	Informazioni di base sul sistema operativo, incluse le versioni dell'immagine StorageGRID.
bundle	Informazioni di configurazione globali (bundle).

Posizione archivio	Descrizione
cache-svc	Log del servizio cache (solo sui nodi gateway).
cassandra	Informazioni sul database Cassandra e file di log di riparazione di Reaper.
ec	Informazioni VCS sul nodo corrente e informazioni sul gruppo EC tramite ID profilo.
griglia	Registri generali della griglia, inclusi i log di debug (`bycast.log`) e `servermanager` log.
grid.json	File di configurazione della grid condiviso tra tutti i nodi. Inoltre, `node.json` è specifico per il nodo corrente.
hagroups	Metriche e log dei gruppi ad alta disponibilità.
installare	`Gdu-server` e i log di installazione.
Lambda-arbitrator	Registri relativi alla richiesta proxy S3 Select.
leakd	Log dal servizio leakd.
lumberjack.log	Messaggi di debug relativi alla raccolta dei log.
Metriche	Log di servizio per Grafana, Jaeger, node exporter e Prometheus.
miscd	Registri di accesso ed errore di Miscd.
mysql	La configurazione del database mariaDB e i relativi log.
net	Log generati dagli script relativi alla rete e dal servizio Dynip.
nginx	File di configurazione e log del bilanciatore di carico e della federazione della grid. Include anche i log del traffico di Grid Manager e Tenant Manager.

Posizione archivio	Descrizione
nginx-gw	• `access.log`: Messaggi di log delle richieste di Grid Manager e Tenant manager. ◦ Questi messaggi sono preceduti da `mgmt:` quando vengono esportati tramite syslog. ◦ Il formato di questi messaggi di registro è `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: Richieste di replica cross-grid in entrata. ◦ Questi messaggi sono preceduti da `cgr:` quando vengono esportati tramite syslog. ◦ Il formato di questi messaggi di registro è `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`Richieste S3 agli endpoint del bilanciatore di carico. ◦ Questi messaggi sono preceduti da `endpoint:` quando vengono esportati tramite syslog. ◦ Il formato di questi messaggi di registro è `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Relativo al nuovo avviso di controllo DNS.
ntp	File di configurazione NTP e log.
Oggetti orfani	Registri relativi agli oggetti orfani.
sistema operativo	File di stato dei nodi e della griglia, inclusi i servizi `pid`.
altro	File di registro sotto `/var/local/log` che non vengono raccolti in altre cartelle.
perf	Informazioni sulle prestazioni di CPU, rete e I/O del disco.
prometheus-data	Metriche Prometheus correnti, se la raccolta dei log include dati Prometheus.
provisioning	Registri relativi al processo di provisioning del grid.
raft	Log dal cluster Raft utilizzati nei servizi della piattaforma.
ssh	Registri relativi alla configurazione e al servizio SSH.

Posizione archivio	Descrizione
snmp	Configurazione dell'agente SNMP utilizzata per l'invio di notifiche SNMP.
dati dei socket	Dati dei socket per il debug di rete.
system-commands.txt	Output dei comandi del container StorageGRID. Contiene informazioni di sistema, come networking e utilizzo del disco.
sincronizza-pacchetto-di-ripristino	Relativo al mantenimento della coerenza del pacchetto di ripristino più recente su tutti i nodi di amministrazione e Storage Nodes che ospitano il servizio ADC.

Registri software StorageGRID

Puoi usare i log di StorageGRID per risolvere i problemi.

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

Registri generali di StorageGRID

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

Registri relativi alla cifratura

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

Log della federazione di grid

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

Registri NMS

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

Log di Server Manager

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

Registri dei servizi StorageGRID

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

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

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

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

Informazioni correlate

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

Registri di distribuzione e manutenzione in StorageGRID

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

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

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

Scopri il file bycast.log di StorageGRID

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

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

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

Rotazione dei file per bycast.log

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

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

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

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

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

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

Informazioni correlate

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

Messaggi in bycast.log

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

Esempio di messaggio ADE:

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

I messaggi ADE contengono le seguenti informazioni:

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

Gravità dei messaggi nel file bycast.log

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

Ad esempio:

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

Codici di errore in `bycast.log`

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

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

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

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

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

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

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

Numero di errore	Codice di errore	Significato
046	EL3HLT	Livello 3 sospeso
047	EL3RST	Ripristino del livello 3
048	ELNRNG	Numero di collegamento fuori intervallo
049	EUNATCH	Driver di protocollo non collegato
050	ENOCSI	Nessuna struttura CSI disponibile
051	EL2HLT	Livello 2 sospeso
052	EBADE	Scambio non valido
053	EBADR	Descrizione richiesta non valida
054	EXFULL	Exchange completo
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato del file del font errato
060	ENOSTR	Dispositivo non è uno stream
061	ENODATA	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse di stream esaurite
064	ENONET	La macchina non è sulla rete
065	ENOPKG	Pacchetto non installato
066	EREMOTE	L'oggetto è remoto

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

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

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

Numero di errore	Codice di errore	Significato
128	CHIAVE REVOCATA	La chiave è stata revocata
129	EKEYREJECTED	La chiave è stata rifiutata dal servizio
130	EOWNERDEAD	Per mutex robusti: proprietario morto
131	ENOTRECOVERABLE	Per i mutex robusti: stato non recuperabile

Configura la gestione dei log e il server syslog esterno

Server syslog esterni in StorageGRID

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

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

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

Quando utilizzare un syslog server esterno

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

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

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

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

Come configurare un server syslog esterno

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

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

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

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

Come stimare le dimensioni del syslog server esterno

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

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

Usa le operazioni S3 al secondo nelle formule di stima

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

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

Formule di stima per i registri di controllo

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

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

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

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

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

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

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

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

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

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

al secondo.

Formule di stima per i livelli di audit non predefiniti

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

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

Formule di stima per eventi di sicurezza

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

Formule di stima per i log delle applicazioni

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

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

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

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

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

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

Esempi di stime dimensionali

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

- Replica
- Erasure coding

Se usi la replica per la protezione dei dati

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

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

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

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

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

Se usi la codifica di cancellazione per la protezione dei dati

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

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

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

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

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

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

Configura la gestione dei log in StorageGRID

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

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

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

Prima di iniziare

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

Modifica i livelli dei messaggi di audit

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

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

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

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

Passaggi

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

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

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

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

3. Seleziona **Salva**.

Definisci le intestazioni della richiesta HTTP

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

Passaggi

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

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

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

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

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

3. Seleziona **Save**

Configura la posizione del registro

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

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

Utilizza un server syslog esterno

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

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

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

Inserisci le informazioni di syslog

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

Passaggi

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

   Viene visualizzata la procedura guidata Configura server syslog esterno.

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

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

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

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

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

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

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

Gestisci il contenuto di syslog

Puoi selezionare quali informazioni inviare al server syslog esterno.

Passaggi

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

        - `hagroups.log`
    - **Invio dei log di accesso**: Invia i log di accesso HTTP per le richieste esterne a Grid Manager, Tenant Manager, endpoint del bilanciatore di carico configurati e richieste di federazione della griglia da sistemi remoti.
2. Utilizza i menu a tendina per selezionare il livello di gravità e la facility (tipo di messaggio) per ciascuna categoria di informazioni di audit che desideri inviare.

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

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

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

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

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

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

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

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

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

3. Seleziona **Continue**.

Invia messaggi di prova

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

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

Passaggi

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

   Un banner verde indica che la configurazione è stata salvata.

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

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

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

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

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

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

6. Seleziona **Interrompi e termina**.

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

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

${post_edited_translations.segment}

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

> StorageGRID utilizza per impostazione predefinita le destinazioni di audit dei nodi locali e memorizza le informazioni di audit in `/var/local/log/localaudit.log`.
>
> Quando usi `/var/local/log/localaudit.log`, le voci del registro di audit di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo Storage. Puoi trovare quale nodo ha le voci più recenti usando il comando `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`.
>
> Alcune destinazioni sono disponibili solo se hai configurato un server syslog esterno.

Passaggi

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

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

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

3. Seleziona **Salva**.

   Viene visualizzato un messaggio di avviso.

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

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

Usa un bucket

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

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

   Crea tenant e bucket

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

   Seleziona tenant e bucket

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

4. Seleziona **Salva**.

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

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

   Ad esempio:

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

Usa il monitoraggio SNMP

Utilizza il monitoraggio SNMP in StorageGRID

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

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

Capacità

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

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

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

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

Trappole

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

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

Informa

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

Gli inform sono supportati in SNMPv2c e SNMPv3.

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

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

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

Supporto versioni SNMP

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

	SNMPv1	SNMPv2c	SNMPv3
Query (GET e GETNEXT)	Query MIB di sola lettura	Query MIB di sola lettura	Query MIB di sola lettura

	SNMPv1	SNMPv2c	SNMPv3
Autenticazione della query	Stringa community	Stringa community	Utente del modello di sicurezza basato sull'utente (USM)
Notifiche (TRAP e INFORM)	Solo trap	Trappole e informa	Trappole e informa
Autenticazione della notifica	Comunità di trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Comunità di trap predefinita o una stringa di comunità personalizzata per ogni destinazione trap	Utente USM per ogni destinazione trap

Limitazioni

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

Configura l'agente SNMP in StorageGRID

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

Prima di iniziare

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

Informazioni su questa attività

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

Tutti i nodi della griglia utilizzano la stessa configurazione SNMP.

Specifica la configurazione di base

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

Passaggi

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

   Viene visualizzata la pagina dell'agente SNMP.

2. Per abilitare l'agente SNMP su tutti i nodi della griglia, seleziona la casella di controllo **Abilita SNMP**.

3. Inserisci le seguenti informazioni nella sezione Configurazione di base.

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

Inserisci le stringhe della community

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

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

Passaggi

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

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

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

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

   Sono consentite fino a cinque stringhe.

Crea destinazioni trap

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

Passaggi

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

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

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

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

SNMPv1

Se hai selezionato SNMPv1 come versione, compila questi campi.

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

SNMPv2c

Se hai selezionato SNMPv2c come versione, compila questi campi.

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

SNMPv3

Se hai selezionato SNMPv3 come versione, compila questi campi.

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

5. Seleziona **Create**.

   La destinazione trap viene creata e aggiunta alla tabella.

Crea indirizzi agente

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

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

Passaggi

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

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

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

3. Seleziona **Create**.

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

Crea utenti USM

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

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

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

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

Passaggi

1. Seleziona **Create**.

2. Inserisci le seguenti informazioni.

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

3. Seleziona **Create**.

   L'utente USM viene creato e aggiunto alla tabella.

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

   La nuova configurazione dell'agente SNMP diventa attiva.

Aggiorna l'agente SNMP di StorageGRID

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

Prima di iniziare

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

Informazioni su questa attività

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

Passaggi

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

   Viene visualizzata la pagina dell'agente SNMP.

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

   Se riattivi l'agente SNMP, le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Facoltativamente, aggiorna le informazioni nella sezione Configurazione di base:
   a. Se necessario, aggiorna il **contatto di sistema** e la **posizione del sistema**.
   b. Facoltativamente, seleziona o deseleziona la casella di controllo **Abilita notifiche agente SNMP** per controllare se l'agente SNMP di StorageGRID invia notifiche trap e inform.

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

   c. Facoltativamente, seleziona o deseleziona la casella di controllo **Abilita trap di autenticazione** per controllare se l'agente SNMP di StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo non autenticati correttamente.
4. Se usi SNMPv1 o SNMPv2c, puoi aggiornare o aggiungere una **community di sola lettura** nella sezione Stringhe della community.
5. Per aggiornare le destinazioni trap, seleziona la scheda Destinazioni trap nella sezione Altre configurazioni.

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

   Per i dettagli su cosa inserire, vedi "Crea destinazioni trap".

   - Facoltativamente, aggiorna o rimuovi la trap community predefinita.

Se rimuovi la community predefinita per le trap, devi prima assicurarti che tutte le destinazioni delle trap esistenti utilizzino una stringa di community personalizzata.

- Per aggiungere una destinazione trap, seleziona **Crea**.
- Per modificare una destinazione trap, seleziona il pulsante di opzione e seleziona **Modifica**.
- Per rimuovere una destinazione trap, seleziona il pulsante di opzione e seleziona **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

6. Per aggiornare gli indirizzi degli agenti, seleziona la scheda Indirizzi degli agenti nella sezione Altre configurazioni.

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

   Per i dettagli su cosa inserire, vedi "Crea indirizzi agente".

   - Per aggiungere un indirizzo agente, seleziona **Crea**.
   - Per modificare l'indirizzo di un agente, seleziona il pulsante di opzione e seleziona **Modifica**.
   - Per rimuovere un indirizzo agente, seleziona il pulsante di opzione e seleziona **Rimuovi**.
   - Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

7. Per aggiornare gli utenti USM, seleziona la scheda Utenti USM nella sezione Altre configurazioni.

   Usa questa scheda per definire gli utenti USM autorizzati a interrogare la MIB o a ricevere trap e inform.

   Per i dettagli su cosa inserire, vedi "Crea utenti USM".

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

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

     > Se aggiungi o rimuovi l'ID motore autorevole di un utente e quell'utente è attualmente selezionato per una destinazione, devi modificare o rimuovere la destinazione. Altrimenti, si verifica un errore di convalida quando salvi la configurazione dell'agente SNMP.

   - Per rimuovere un utente USM, seleziona il pulsante di opzione e seleziona **Rimuovi**.

     > Se l'utente che hai rimosso è attualmente selezionato per una destinazione trap, devi modificare o rimuovere la destinazione. Altrimenti, si verifica un errore di convalida quando salvi la configurazione dell'agente SNMP.

   - Per confermare le modifiche, seleziona **Salva** in fondo alla pagina.

8. Quando hai aggiornato la configurazione dell'agente SNMP, seleziona **Salva**.

Accedere ai file MIB di StorageGRID

I file MIB contengono definizioni e informazioni sulle proprietà delle risorse e dei servizi gestiti per i nodi della tua griglia. Puoi accedere ai file MIB che definiscono gli oggetti e le

notifiche per StorageGRID. Questi file possono essere utili per monitorare la tua griglia.

Vedi "Usa il monitoraggio SNMP" per ulteriori informazioni su SNMP e sui file MIB.

Accedi ai file MIB

Segui questi passaggi per accedere ai file MIB.

Passaggi

1. Seleziona **Configurazione** > **Monitoraggio** > **Agente SNMP**.
2. Nella pagina dell'agente SNMP, seleziona il file che vuoi scaricare:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definisce la tabella degli avvisi e le notifiche (trap) accessibili su tutti i nodi di amministrazione.
   - **ES-NETAPP-06-MIB.mib**: Definisce oggetti e notifiche per appliance basati su E-Series.
   - **MIB_1_10.zip**: Definisce oggetti e notifiche per dispositivi con interfaccia BMC.

   Puoi anche accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID di StorageGRID dal file MIB:
   a. Ottieni l'OID della radice della MIB di StorageGRID:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Risultato: `.1.3.6.1.4.1.789.28669` (`28669` è sempre l'OID per StorageGRID)

   b. Cerca l'OID di StorageGRID nell'intero albero (utilizzando `paste` per unire le righe):

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

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

Contenuto del file MIB

Tutti gli oggetti sono sotto l'OID di StorageGRID.

Nome oggetto	ID oggetto (OID)	Descrizione
		Il modulo MIB per le entità NetApp StorageGRID.

oggetti MIB

Nome oggetto	ID oggetto (OID)	Tipo	Accesso	Modulo MIB	Descrizione
activeAlertCount		Integer32	Sola lettura	NETAPP-STORAGEGRID-MIB	Il numero di avvisi attivi nella activeAlertTable.
activeAlertTable		Sequenza di ActiveAlertEntry	Non accessibile	NETAPP-STORAGEGRID-MIB	Una tabella degli avvisi attivi in StorageGRID.
activeAlertEntry		Sequenza	Non accessibile	NETAPP-STORAGEGRID-MIB	Un singolo avviso StorageGRID, indicizzato tramite ID avviso.
activeAlertId		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	L'ID dell'avviso. Univoco solo nell'insieme corrente di avvisi attivi.
activeAlertName		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	Il nome dell'allerta.
activeAlertInstance		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
activeAlertSeverity		stringa di ottetto	Sola lettura	NETAPP-STORAGEGRID-MIB	La gravità dell'allerta.
activeAlertStartTime		Data e ora	Sola lettura	NETAPP-STORAGEGRID-MIB	L'ora in cui è scattato l'allarme.

Raccogli ulteriori dati StorageGRID

Monitorare le prestazioni PUT e GET in StorageGRID

Puoi monitorare le prestazioni di alcune operazioni, come archivio di oggetti e recupero, per aiutarti a identificare cambiamenti che potrebbero richiedere ulteriori indagini.

Informazioni su questa attività

Per monitorare le prestazioni delle operazioni PUT e GET, puoi eseguire i comandi S3 direttamente da una workstation oppure utilizzando l'applicazione open source S3tester. Usando questi metodi puoi valutare le prestazioni indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o con una rete esterna.

Quando esegui test delle operazioni PUT e GET, segui queste linee guida:

- Utilizza dimensioni degli oggetti paragonabili a quelle degli oggetti che solitamente inserisci nella tua grid.
- Esegui operazioni sia su siti locali che remoti.

I messaggi "registro di controllo" indicano il tempo totale necessario per eseguire determinate operazioni. Ad esempio, per determinare il tempo totale di elaborazione per una richiesta S3 GET, puoi esaminare il valore dell'attributo TIME nel messaggio di audit SGET. Puoi anche trovare l'attributo TIME nei messaggi di audit per le seguenti operazioni S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Quando analizzi i risultati, guarda il tempo medio necessario per soddisfare una richiesta, così come il throughput complessivo che puoi ottenere. Ripeti regolarmente gli stessi test e registra i risultati, così puoi individuare tendenze che potrebbero richiedere un'indagine.

- È possibile "Scarica S3tester da GitHub".

Monitorare le operazioni di verifica degli oggetti in StorageGRID

Il sistema StorageGRID può verificare l'integrità dei dati degli oggetti sui nodi di archiviazione, controllando sia gli oggetti danneggiati che quelli mancanti.

Prima di iniziare

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

Informazioni su questa attività

Due "processi di verifica" lavorano insieme per garantire l'integrità dei dati:

- **La verifica in background** viene eseguita automaticamente, controllando continuamente la correttezza dei dati degli oggetti.

  La verifica in background controlla automaticamente e continuamente tutti i nodi di Storage per determinare se sono presenti copie danneggiate dei dati degli oggetti replicati e codificati per la cancellazione. Se vengono rilevati problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati degli oggetti danneggiati con copie archiviate altrove nel sistema. La verifica in background non viene eseguita sugli oggetti in un Cloud Storage Pool.

  > ⓘ L'avviso **Rilevato oggetto danneggiato non identificato** viene attivato se il sistema rileva un oggetto danneggiato che non può essere corretto automaticamente.

- La funzione **Controllo esistenza oggetto** può essere attivata da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) dei dati oggetto.

  Il controllo di esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti codificati per la cancellazione esistono su un Storage Node. Il controllo di esistenza degli oggetti offre un modo per verificare l'integrità dei dispositivi di storage, soprattutto se un recente problema hardware potrebbe aver influenzato l'integrità dei dati.

Dovresti esaminare regolarmente i risultati delle verifiche in background e dei controlli di esistenza degli oggetti. Indaga subito su eventuali casi di dati degli oggetti corrotti o mancanti per determinarne la causa principale.

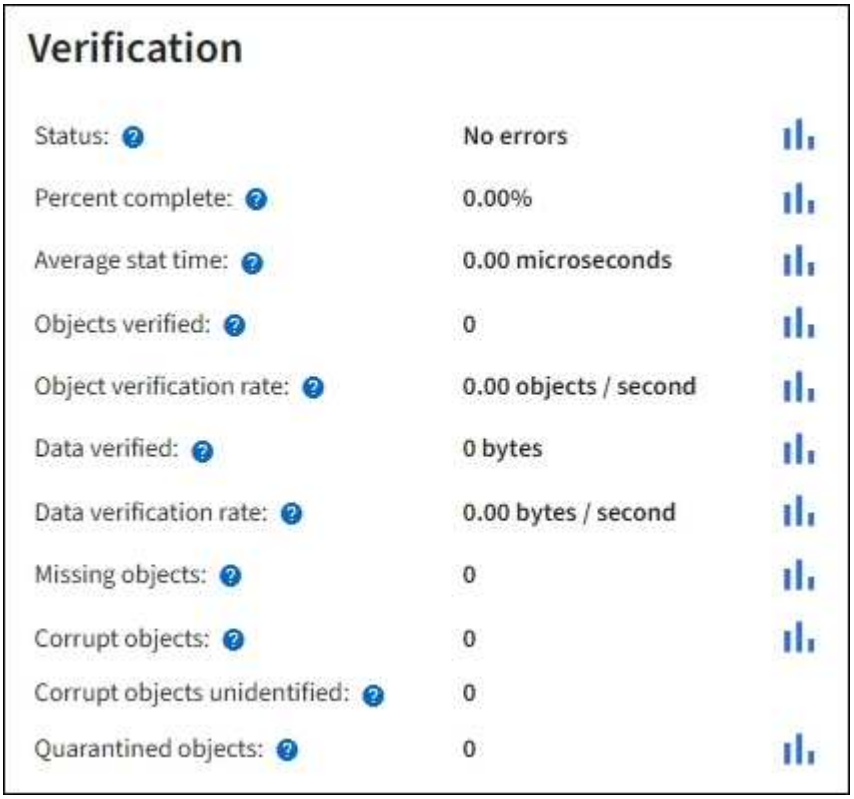
Passaggi

1. Esamina i risultati delle verifiche dei precedenti:

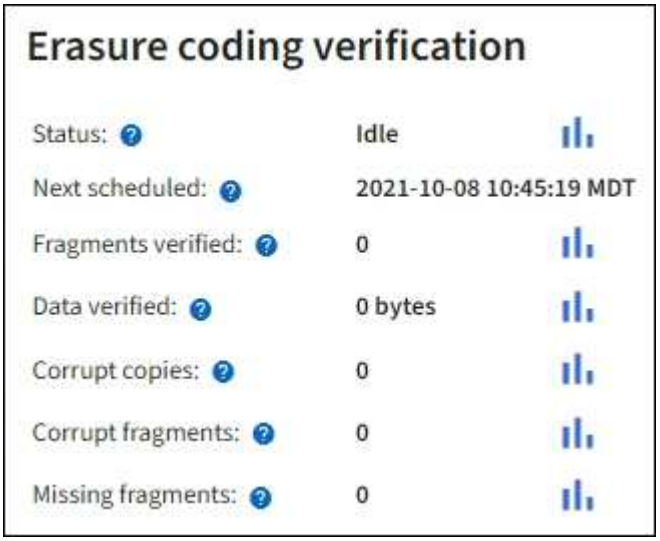
   a. Seleziona **Nodes** > ***Storage Node*** > **Objects**.

   b. Controlla i risultati della verifica:

      - Per verificare la validità dei dati degli oggetti replicati, guarda gli attributi nella sezione Verifica.



      - Per controllare la verifica dei frammenti con codifica di cancellazione, seleziona ***Storage Node*** > **ILM** e consulta gli attributi nella sezione Verifica della codifica di cancellazione.

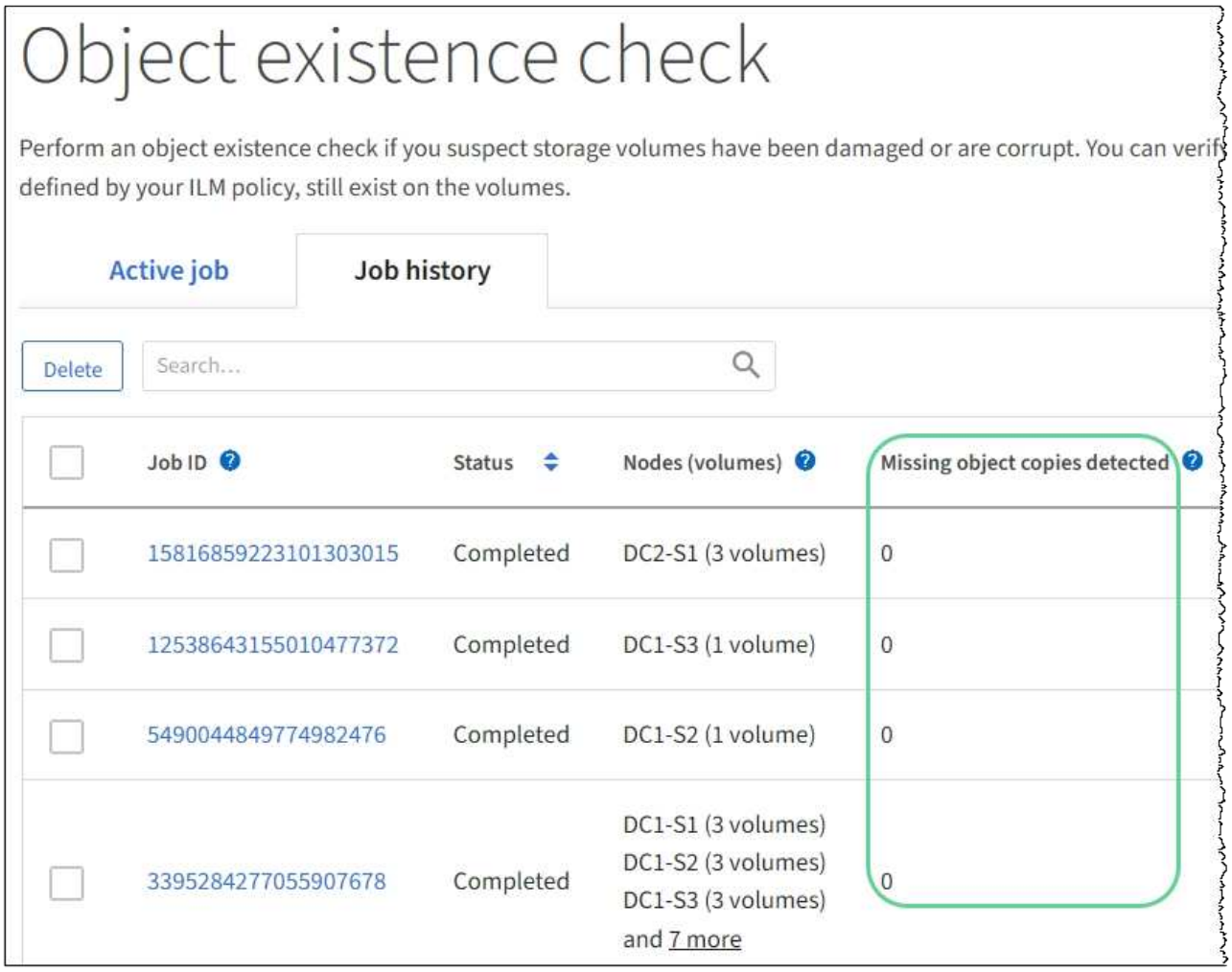


   Seleziona il punto interrogativo (?) accanto al nome di un attributo per visualizzare il testo di aiuto.

2. Esamina i risultati delle operazioni di verifica dell'esistenza degli oggetti:

a. Seleziona **Manutenzione** > **Verifica esistenza oggetto** > **Cronologia interventi**.

b. Esamina la colonna "Copie di oggetti mancanti rilevate". Se uno qualsiasi dei processi ha generato 100 o più copie di oggetti mancanti e l'avviso **Oggetti potenzialmente persi** è stato attivato, contatta il supporto tecnico.



Esaminare i messaggi di audit di StorageGRID

I messaggi di audit possono aiutarti a comprendere meglio il funzionamento dettagliato del tuo sistema StorageGRID. Puoi utilizzare i log di audit per risolvere i problemi e valutare le prestazioni.

Durante il normale funzionamento del sistema, tutti i servizi di StorageGRID generano messaggi di audit, come segue:

- I messaggi di audit del sistema sono correlati al sistema di auditing stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema e alle operazioni di backup dei servizi.
- I messaggi di controllo dello storage a oggetti sono correlati allo storage e alla gestione degli oggetti all'interno di StorageGRID, inclusi lo storage a oggetti e i recuperi, i trasferimenti da nodo della griglia a nodo della griglia e le verifiche.
- I messaggi di audit di lettura e scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare, modificare o recuperare un oggetto.

- I messaggi di audit della gestione registrano le richieste degli utenti all'API di Management.

Ogni nodo amministratore memorizza i messaggi di audit in file di testo. La cartella condivisa di audit contiene il file attivo (audit.log) e i log di audit compressi dei giorni precedenti. Ogni nodo della griglia memorizza inoltre una copia delle informazioni di audit generate sul nodo stesso.

Puoi accedere ai file di log di audit direttamente dalla riga di comando dell'Admin Node.

StorageGRID può inviare le informazioni di audit per impostazione predefinita, oppure puoi cambiarne la destinazione:

- StorageGRID utilizza come destinazione predefinita per l'audit le destinazioni dei nodi locali.
- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di storage.
- Facoltativamente, puoi modificare la destinazione dei log di audit e inviare le informazioni di audit a un server syslog esterno. I log locali dei record di audit continuano a essere generati e archiviati quando è configurato un server syslog esterno.
- "Scopri come configurare la gestione dei log".

Per dettagli sul file di log di audit, sul formato dei messaggi di audit, sui tipi di messaggi di audit e sugli strumenti disponibili per analizzare i messaggi di audit, vedi "${post_edited_translations.segment}".

Raccogli i file di registro StorageGRID e i dati di sistema

Puoi recuperare i file di log di StorageGRID e i dati di sistema, inclusi i dati di configurazione, e inviarli al supporto tecnico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su qualsiasi nodo Admin utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- ${post_edited_translations.segment}

Informazioni su questa attività

Utilizza Grid Manager per raccogliere "file di log", dati di sistema e dati di configurazione da qualsiasi nodo della griglia per il periodo di tempo che selezioni. I dati vengono raccolti e archiviati in un `.tar.gz` file che puoi quindi scaricare sul tuo computer locale o inviare al supporto tecnico.

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

Passaggi

1. Seleziona **Support** > **Tools** > **Log collection**. Viene visualizzata una tabella di nodi.
2. Seleziona i nodi della griglia per i quali vuoi raccogliere i file di log.

   Puoi ordinare per nome del nodo, sito e tipo di nodo. Le colonne Sito e Tipo di nodo contengono filtri per selezionare singoli siti e tipi di nodo.

3. Seleziona **Continue**.
4. Seleziona l'intervallo di date e orari dei dati da includere nei file di log.

Se selezioni un periodo di tempo molto lungo o raccogli i log da tutti i nodi di una griglia di grandi dimensioni, l'archivio dei log potrebbe diventare troppo grande per essere memorizzato su un nodo o troppo grande per essere raccolto da un Admin Node per il download. Se si verifica uno di questi scenari, riavvia la raccolta dei log con un set di dati più piccolo.

5. Seleziona i tipi di log che desideri raccogliere.
   - **Log delle applicazioni**: Log specifici delle applicazioni che il supporto tecnico utilizza più frequentemente per la risoluzione dei problemi. I log raccolti rappresentano un sottoinsieme dei log delle applicazioni disponibili.
   - **Registri di controllo**: Registri contenenti i messaggi di controllo generati durante il normale funzionamento del sistema.
   - **Traccia di rete**: Log utilizzati per il debug della rete.
   - **Database Prometheus**: metriche delle serie temporali dai servizi su tutti i nodi.
6. Facoltativamente, utilizza la casella di testo **Note** per inserire note sui file di log che stai raccogliendo.

   Puoi usare queste note per fornire informazioni di supporto tecnico sul problema che ti ha spinto a raccogliere i file di log. Le tue note vengono aggiunte a un file chiamato `info.txt`, insieme ad altre informazioni sulla raccolta dei file di log. Il file `info.txt` viene salvato nel pacchetto di archivio dei file di log.

7. Nella casella di testo **Passphrase di provisioning**, inserisci la passphrase di provisioning per il tuo sistema StorageGRID.
8. Seleziona **Raccogli log**.

   Puoi usare la pagina di raccolta dei log per monitorare l'avanzamento della raccolta dei file di log per ogni nodo della griglia.

   Se ricevi un messaggio di errore relativo alle dimensioni del file di log, prova a raccogliere i log per un periodo di tempo più breve o per un numero inferiore di nodi.

9. Se la raccolta dei log non riesce:
   - Se viene visualizzato il messaggio "Raccolta dei log non riuscita", puoi riprovare la raccolta dei log oppure terminare la sessione senza riprovare.
   - Se viene visualizzato il messaggio "Raccolta dei log parzialmente non riuscita", puoi riprovare la raccolta dei log, terminare la sessione, scaricare il file di log o inviare il file di log a AutoSupport.
10. Quando la raccolta dei file di log è completa:
    - Seleziona **Scarica** per scaricare il `.tar.gz` file.
    - Seleziona **Invia a AutoSupport** per inviare il file `.tar.gz` al supporto tecnico.

      Il `.tar.gz`file contiene tutti i file di log di tutti i nodi della griglia in cui la raccolta dei log è andata a buon fine. Il `.tar.gz`file combinato contiene un archivio di file di log per ciascun nodo della griglia.

    L'oggetto del pacchetto AutoSupport è `USER_TRIGGERED_SUPPORT_BUNDLE`.

11. Seleziona **Fine**.

    Il `.tar.gz`file viene eliminato quando selezioni **Fine**. Assicurati di scaricare o inviare prima il file.

Attivare manualmente un pacchetto StorageGRID AutoSupport

Per aiutare il supporto tecnico a risolvere i problemi del tuo sistema StorageGRID, puoi inviare manualmente un pacchetto AutoSupport.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai l'accesso Root o l'autorizzazione per altre configurazioni della grid.

Passaggi

1. Seleziona **Support** > **Tools** > **AutoSupport**.
2. Nella scheda **Azioni**, seleziona **Invia AutoSupport attivato dall'utente**.

   StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp. Se il tentativo ha esito positivo, i valori **Risultato più recente** e **Ultimo momento in cui l'operazione è andata a buon fine** nella scheda **Risultati** vengono aggiornati. Se c'è un problema, il valore **Risultato più recente** viene aggiornato a "Non riuscito" e StorageGRID non prova a inviare di nuovo il pacchetto AutoSupport.

3. Dopo 1 minuto, aggiorna la pagina AutoSupport nel tuo browser per accedere ai risultati più recenti.

Inoltre, puoi "raccogli file di registro e dati di sistema più completi" e inviarli al NetApp Support Site.

Esaminare le metriche di StorageGRID

Quando risolvi un problema, puoi collaborare con il supporto tecnico per esaminare metriche e grafici dettagliati del tuo sistema StorageGRID.

Prima di iniziare

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

Informazioni su questa attività

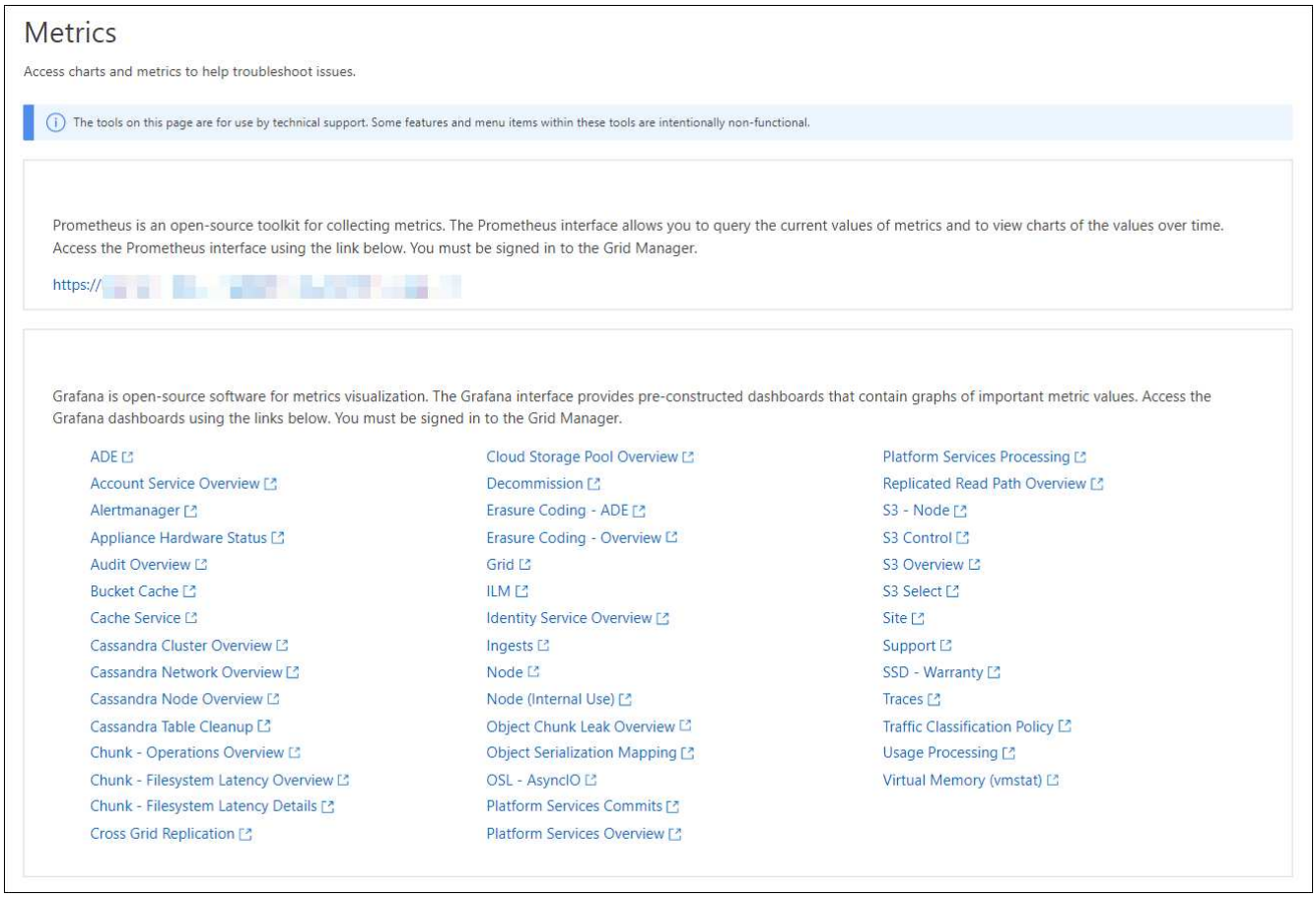
La pagina Metriche consente di accedere alle interfacce utente di Prometheus e Grafana. Prometheus è un software open source per la raccolta delle metriche. Grafana è un software open source per la visualizzazione delle metriche.

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

Passaggi

1. Come indicato dal supporto tecnico, seleziona **Support** > **Tools** > **Metrics**.

   Ecco un esempio della pagina delle metriche:



2. Per interrogare i valori correnti delle metriche di StorageGRID e per visualizzare i grafici dei valori nel tempo, fai clic sul link nella sezione Prometheus.

   Viene visualizzata l'interfaccia di Prometheus. Puoi utilizzare questa interfaccia per eseguire query sulle metriche di StorageGRID e per visualizzare graficamente le metriche di StorageGRID nel tempo.

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

3. Per accedere a dashboard predefinite contenenti grafici delle metriche di StorageGRID nel tempo, fai clic sui collegamenti nella sezione Grafana.

   Viene visualizzata l'interfaccia di Grafana per il link che hai selezionato.

Modifica la priorità di I/O in StorageGRID

La prioritizzazione di input/output (I/O) ti permette di modificare le priorità relative delle operazioni di I/O sul grid.

Per impostazione predefinita, al traffico I/O PUT e GET dei client viene assegnata la massima priorità rispetto alle attività in background come la cancellazione dei dati erasure-coded (EC) e la riparazione EC. Aumentando la priorità delle attività di cancellazione dei dati erasure-coded (EC) e di riparazione EC, queste attività possono essere completate più rapidamente. L'efficacia delle modifiche alla priorità I/O è influenzata dalla frequenza delle richieste dei client, dalle fluttuazioni del traffico di rete e da altre attività di rete in corso.

Prima di iniziare

- Esamina la pagina di prioritizzazione I/O per determinare quali opzioni potrebbero influire sul tuo grid.
- Valuta se il traffico di client in corso può gestire in sicurezza tempi di attesa più lunghi o timeout dei client.
- Preparati a monitorare l'effetto della modifica delle priorità e ad apportare le modifiche necessarie. Queste modifiche vengono implementate rapidamente, ma potrebbero essere necessarie alcune ore prima che il loro effetto diventi visibile.

Passaggi

1. Seleziona **Support** > **I/O prioritization**.
2. (Facoltativo) Cambia la priorità di eliminazione e riparazione EC, per le operazioni in background che eliminano i dati EC, rispetto ai valori predefiniti.

> Usa la priorità predefinita bassa di eliminazione e riparazione EC per le griglie che hanno nodi basati su RAID.

3. Seleziona **Salva**.
4. Monitora "metriche" per valutare l'effetto delle modifiche di priorità.

Esegui la diagnostica in StorageGRID

Quando risolvi un problema, puoi collaborare con il supporto tecnico per eseguire la diagnostica sul tuo sistema StorageGRID e analizzarne i risultati.

- "Esamina le metriche di supporto"
- "Metriche Prometheus comunemente utilizzate"

Prima di iniziare

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

Informazioni su questa attività

La pagina Diagnostica esegue una serie di controlli diagnostici sullo stato attuale della griglia. Ogni controllo diagnostico può avere uno dei tre stati seguenti:

- **Normale**: Tutti i valori rientrano nell'intervallo normale.
- **Attenzione**: uno o più valori sono al di fuori dell'intervallo normale.
- **Attenzione**: uno o più valori sono significativamente al di fuori dell'intervallo normale.

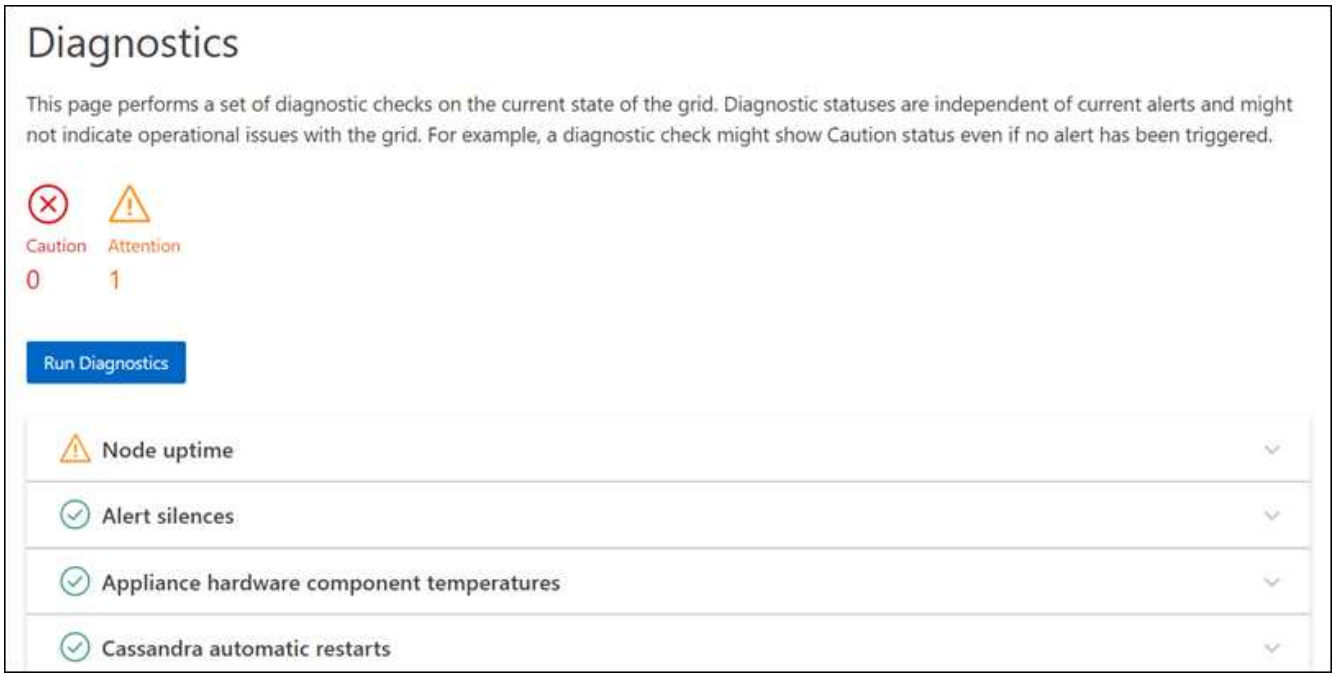
Gli stati diagnostici sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con il grid. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato Caution anche se non è stato attivato alcun avviso.

Passaggi

1. Seleziona **Support** > **Tools** > **Diagnostics**.

   Viene visualizzata la pagina Diagnostica, che elenca i risultati di ogni controllo diagnostico. I risultati sono ordinati per gravità (Caution, Attention e poi Normale). All'interno di ciascun livello di gravità, i risultati sono ordinati alfabeticamente.

   In questo esempio, una diagnosi ha lo stato Attenzione e tre diagnosi hanno lo stato Normale.



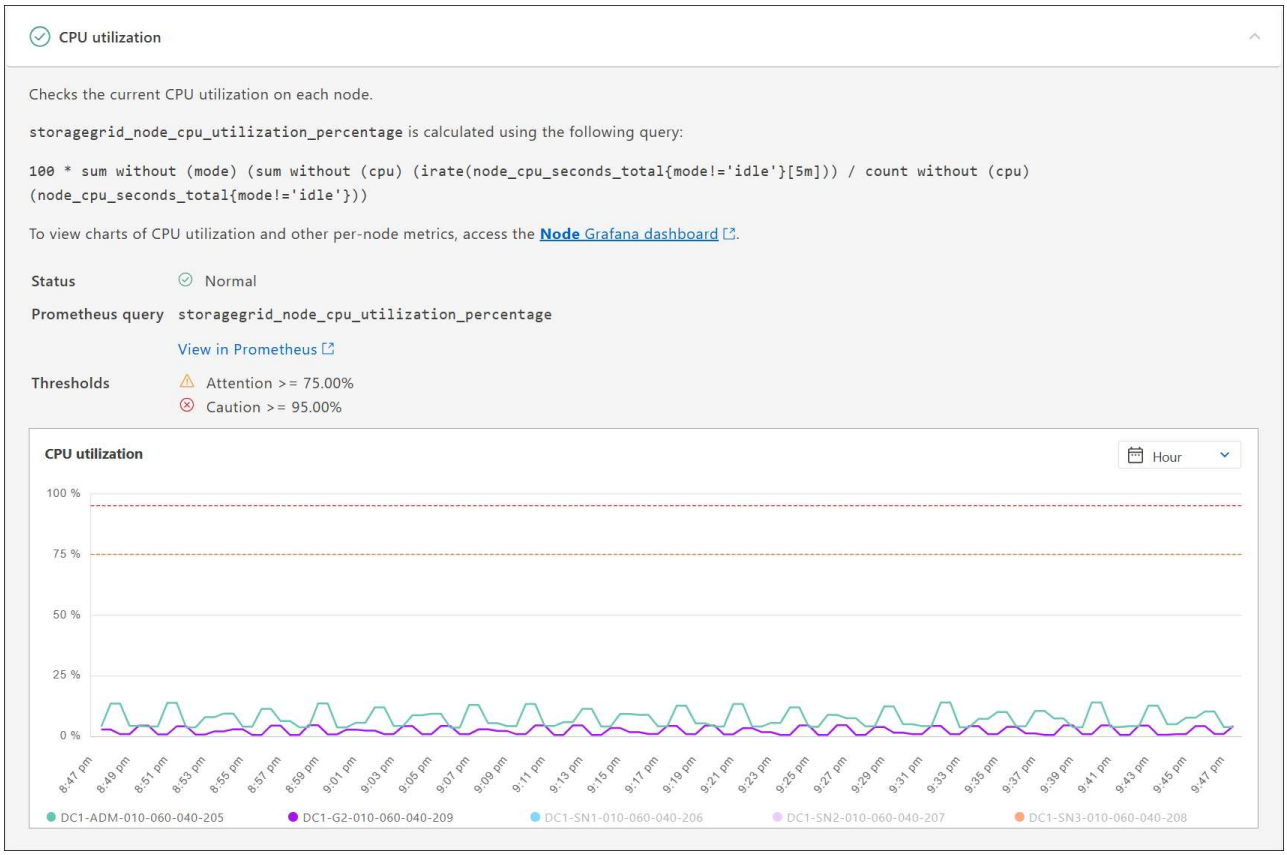
2. Per saperne di più su una diagnosi specifica, fai clic in un punto qualsiasi della riga.

   Vengono visualizzati i dettagli relativi alla diagnosi e i relativi risultati attuali. Di seguito sono elencati i dettagli:

   - **Stato**: Lo stato attuale di questa diagnosi: Normale, Attenzione o Cautela.
   - **Query Prometheus**: Se usata per la diagnostica, l'espressione Prometheus che è stata utilizzata per generare i valori di stato. (Non tutte le diagnostiche usano un'espressione Prometheus.)
   - **Soglie**: Se disponibili per la diagnostica, le soglie definite dal sistema per ogni stato diagnostico anomalo. (I valori di soglia non vengono utilizzati per tutte le diagnostiche.)

     Non puoi modificare queste soglie.

   - **Valori di stato**: Un grafico e una tabella (tabella non mostrata nello screenshot) che mostrano lo stato e il valore della diagnostica in tutto il sistema StorageGRID. In questo esempio, viene mostrato l'utilizzo corrente della CPU per ogni nodo in un sistema StorageGRID. Tutti i valori dei nodi sono al di sotto delle soglie di Attenzione e Cautela, quindi lo stato generale della diagnostica è Normale.



3. **Facoltativo**: Per vedere i grafici di Grafana relativi a questa diagnostica, seleziona **Grafana dashboard**.

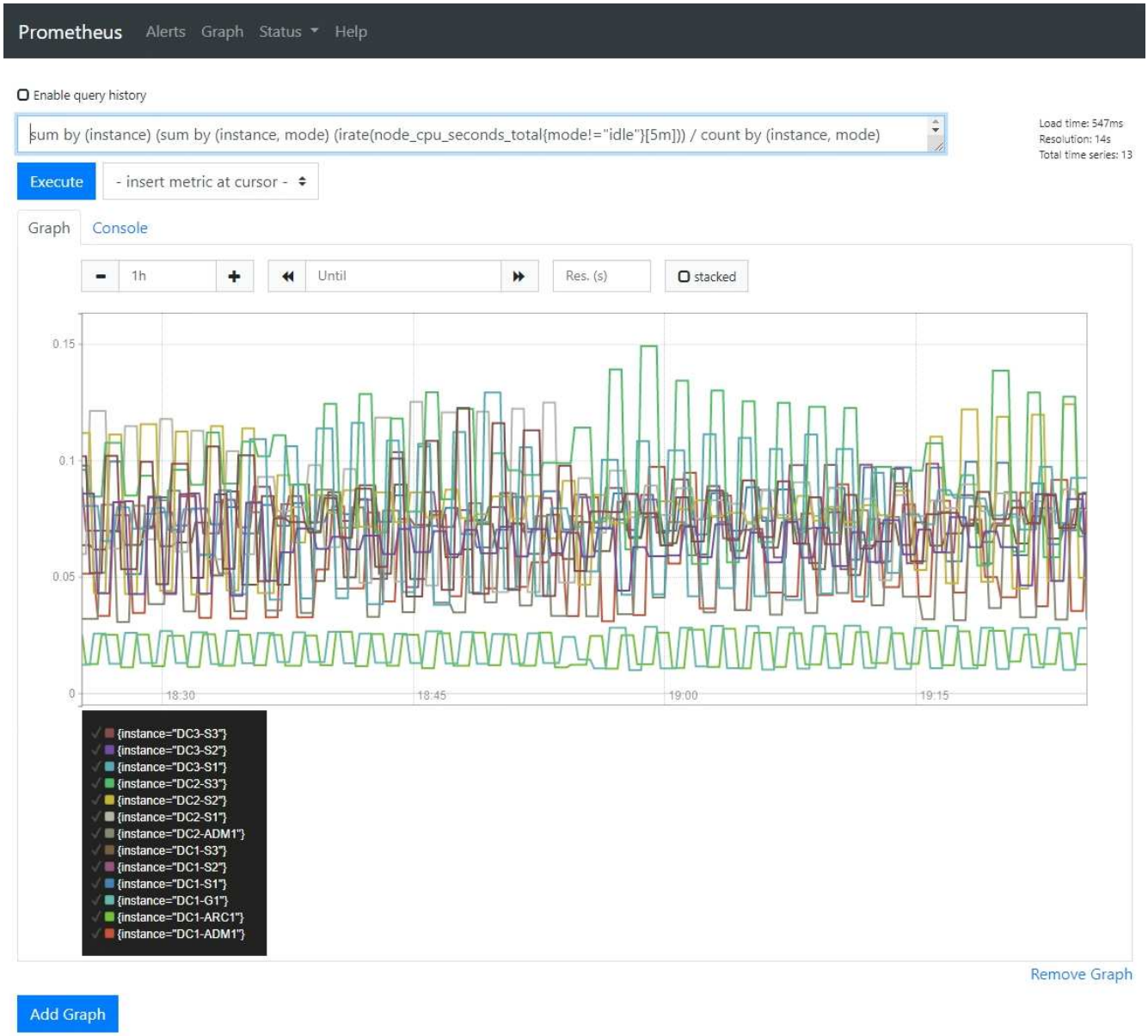
   Questo collegamento non viene visualizzato per tutte le diagnostiche.

   Viene visualizzata la dashboard di Grafana corrispondente. In questo esempio, viene visualizzata la dashboard del nodo che mostra l'utilizzo della CPU nel tempo per questo nodo, oltre ad altri grafici di Grafana relativi al nodo.

   > Puoi anche accedere alle dashboard Grafana predefinite dalla sezione Grafana della pagina **Supporto** > **Strumenti** > **Metriche**.

4. **Opzionale**: Per vedere un grafico dell'espressione Prometheus nel tempo, fai clic su **Visualizza in Prometheus**.

   Viene visualizzato un grafico Prometheus dell'espressione utilizzata nella diagnostica.



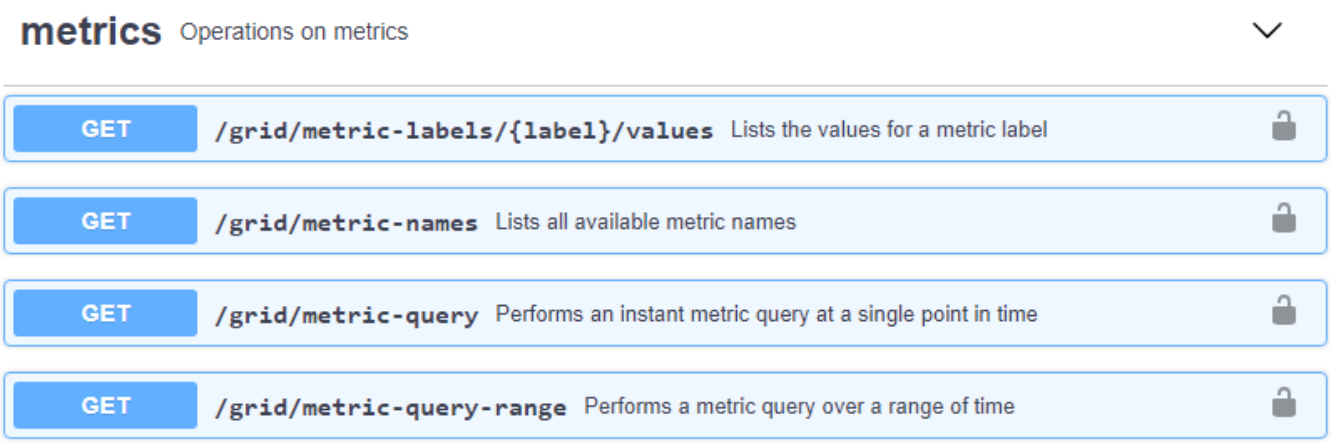
Crea applicazioni di monitoraggio personalizzate per StorageGRID

Puoi creare applicazioni di monitoraggio e dashboard personalizzate utilizzando le metriche StorageGRID disponibili tramite l'API di gestione della griglia.

Se vuoi monitorare metriche che non sono visualizzate in una pagina esistente del Grid Manager, o se vuoi creare dashboard personalizzate per StorageGRID, puoi usare l'API di Grid Management per interrogare le metriche di StorageGRID.

Puoi anche accedere alle metriche Prometheus direttamente con uno strumento di monitoraggio esterno, come Grafana. L'uso di uno strumento esterno richiede che tu carichi o generi un certificato client amministrativo per permettere a StorageGRID di autenticare lo strumento per la sicurezza. Vedi la "Istruzioni per l'amministrazione di StorageGRID".

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, vai su Grid Manager. Dalla parte superiore della pagina, seleziona l'icona di aiuto e seleziona **API documentation** > **metrics**.



I dettagli relativi all'implementazione di un'applicazione di monitoraggio personalizzata esulano dall'ambito di questa documentazione.

Informazioni sul copyright

Informazioni sul marchio commerciale