Monitorare il sistema StorageGRID

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-118/monitor/index.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommario

Monitorare il sistema StorageGRID . . . 1
- Monitorare un sistema StorageGRID: Panoramica . . . 1
- Visualizzare e gestire la dashboard . . . 1
  - Visualizza la dashboard . . . 2
  - Gestire i dashboard . . . 3
  - Configurare i dashboard . . . 4
- Visualizzare la pagina nodi . . . 4
  - Visualizza la pagina nodi: Panoramica . . . 4
  - Visualizzare la scheda Panoramica . . . 7
  - Visualizzare la scheda hardware . . . 9
  - Visualizzare la scheda rete . . . 26
  - Visualizzare la scheda Storage (archiviazione) . . . 27
  - Visualizzare la scheda oggetti . . . 29
  - Visualizzare la scheda ILM . . . 31
  - Utilizzare la scheda attività . . . 32
  - Visualizzare la scheda bilanciamento del carico . . . 32
  - Visualizzare la scheda Platform Services (servizi piattaforma) . . . 34
  - Visualizza la scheda Gestisci unità (solo SGF6112) . . . 35
  - Visualizza la scheda SANtricity System Manager (solo e-Series) . . . 36
- Informazioni da monitorare regolarmente . . . 38
  - Cosa e quando monitorare . . . 38
  - Monitorare lo stato del sistema . . . 39
  - Monitorare la capacità dello storage . . . 43
  - Monitorare la gestione del ciclo di vita delle informazioni . . . 51
  - Monitorare le risorse di rete e di sistema . . . 52
  - Monitorare l’attività del tenant . . . 56
  - Monitoraggio di operazioni client S3 e Swift . . . 61
  - Monitorare le operazioni di bilanciamento del carico . . . 62
  - Monitorare le connessioni a federazione di griglie . . . 63
  - Monitorare la capacità di archiviazione . . . 68
- Avvisi e allarmi . . . 68
  - Gestire avvisi e allarmi: Panoramica . . . 68
  - Confrontare avvisi e allarmi . . . 69
  - Gestire gli avvisi . . . 73
  - Riferimenti agli avvisi . . . 93
  - Metriche Prometheus comunemente utilizzate . . . 105
  - Gestire gli allarmi (sistema legacy) . . . 111
  - Riferimento allarmi (sistema legacy) . . . 132
- Riferimenti ai file di log . . . 159
  - Riferimento ai file di log: Panoramica . . . 159
  - Log del software StorageGRID . . . 161
  - Log di implementazione e manutenzione . . . 167
  - Registri per software di terze parti . . . 168

A proposito di bycast.log . . . 169
Configurare le destinazioni dei messaggi di controllo e del registro . . . 178
Considerazioni sull'utilizzo di un server syslog esterno . . . 178
Configurare i messaggi di controllo e il server syslog esterno . . . 183
Utilizzare il monitoraggio SNMP . . . 192
USA monitoraggio SNMP: Panoramica . . . 192
Configurare l'agente SNMP . . . 193
Aggiornare l'agente SNMP . . . 200
Accedere ai file MIB . . . 201
Raccogliere dati StorageGRID aggiuntivi . . . 204
Utilizzare grafici e grafici . . . 204
Utilizzare report di testo . . . 215
Monitorare L'EFFICIENZA e OTTENERE le performance . . . 219
Monitorare le operazioni di verifica degli oggetti . . . 220
Monitorare gli eventi . . . 222
Esaminare i messaggi di audit . . . 226
Raccogliere i file di log e i dati di sistema . . . 227
Attivare manualmente un pacchetto AutoSupport . . . 229
Visualizzare l'albero topologia griglia . . . 230
Rivedere le metriche di supporto . . . 231
Eseguire la diagnostica . . . 233
Creare applicazioni di monitoraggio personalizzate . . . 237

Monitorare il sistema StorageGRID

Monitorare un sistema StorageGRID: Panoramica

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

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

A proposito di questa attività

Queste istruzioni descrivono come:

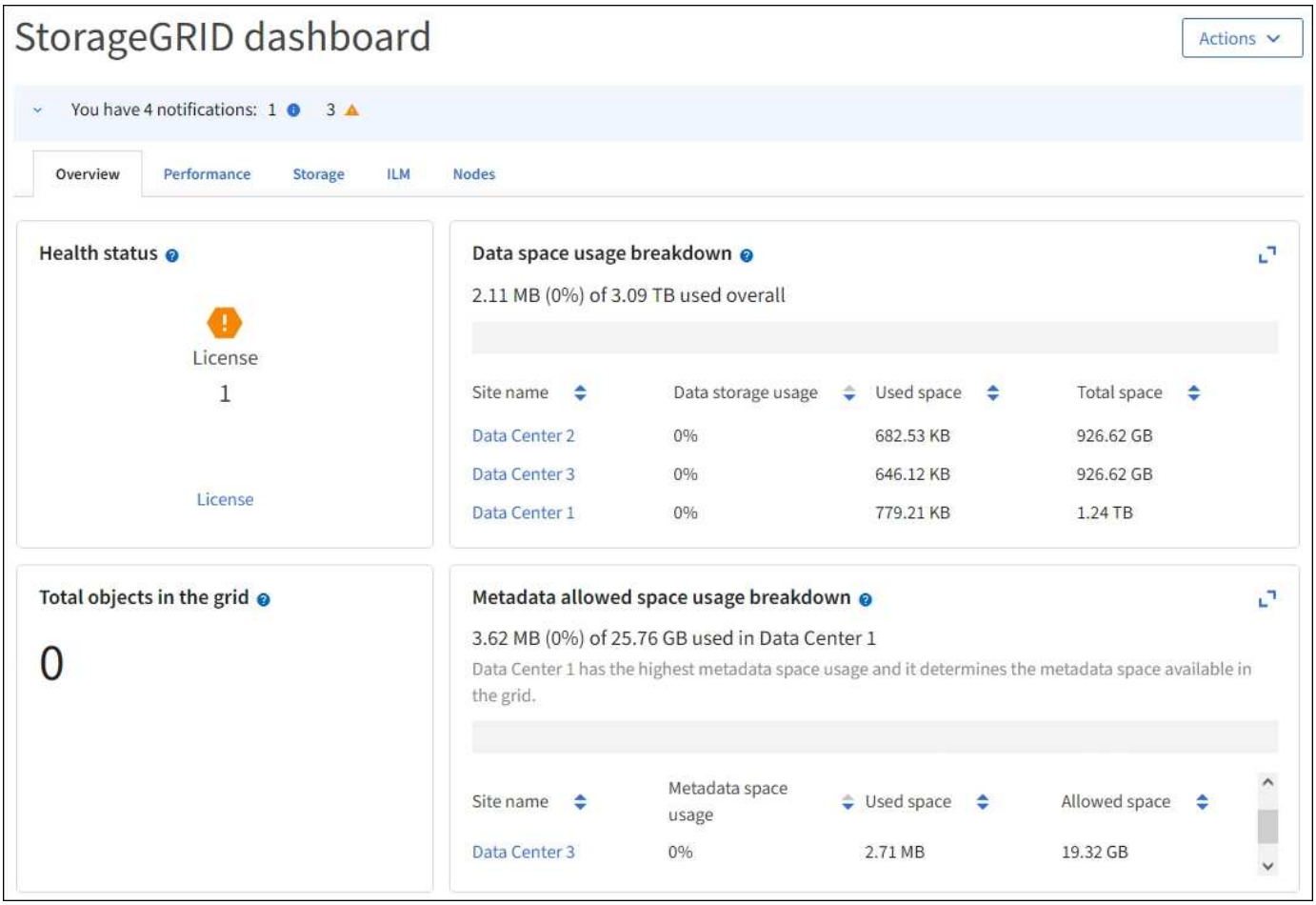
- "Visualizzare e gestire la dashboard"
- "Visualizzare la pagina nodi"
- "Monitorare regolarmente questi aspetti del sistema:"
  - "Stato del sistema"
  - "Capacità dello storage"
  - "Gestione del ciclo di vita delle informazioni"
  - "Risorse di rete e di sistema"
  - "Attività del tenant"
  - "Operazioni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

Visualizzare e gestire la dashboard

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

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

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



Visualizza la dashboard

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

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

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

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

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

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

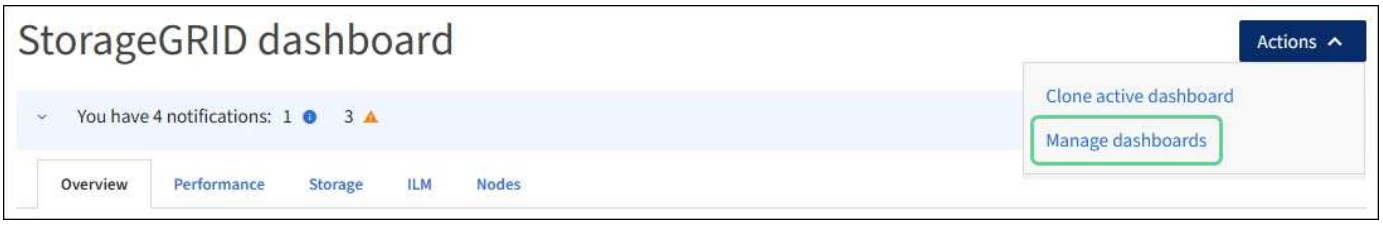
Gestire i dashboard

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

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

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

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



Configurare i dashboard

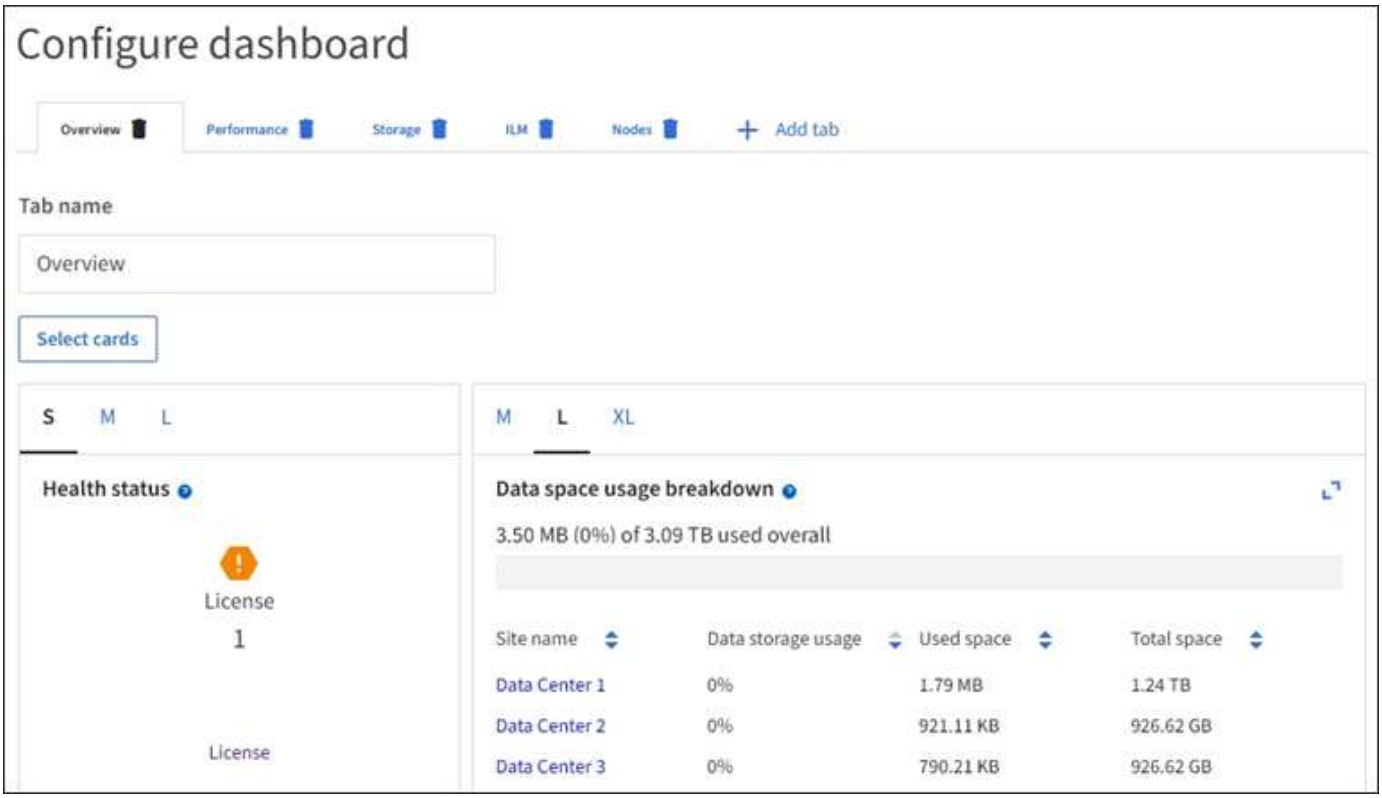
Per creare una nuova dashboard clonando la dashboard attiva, selezionare **azioni** > **Clona dashboard attiva**.

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

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

Durante la configurazione di una dashboard, è possibile:

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



Visualizzare la pagina nodi

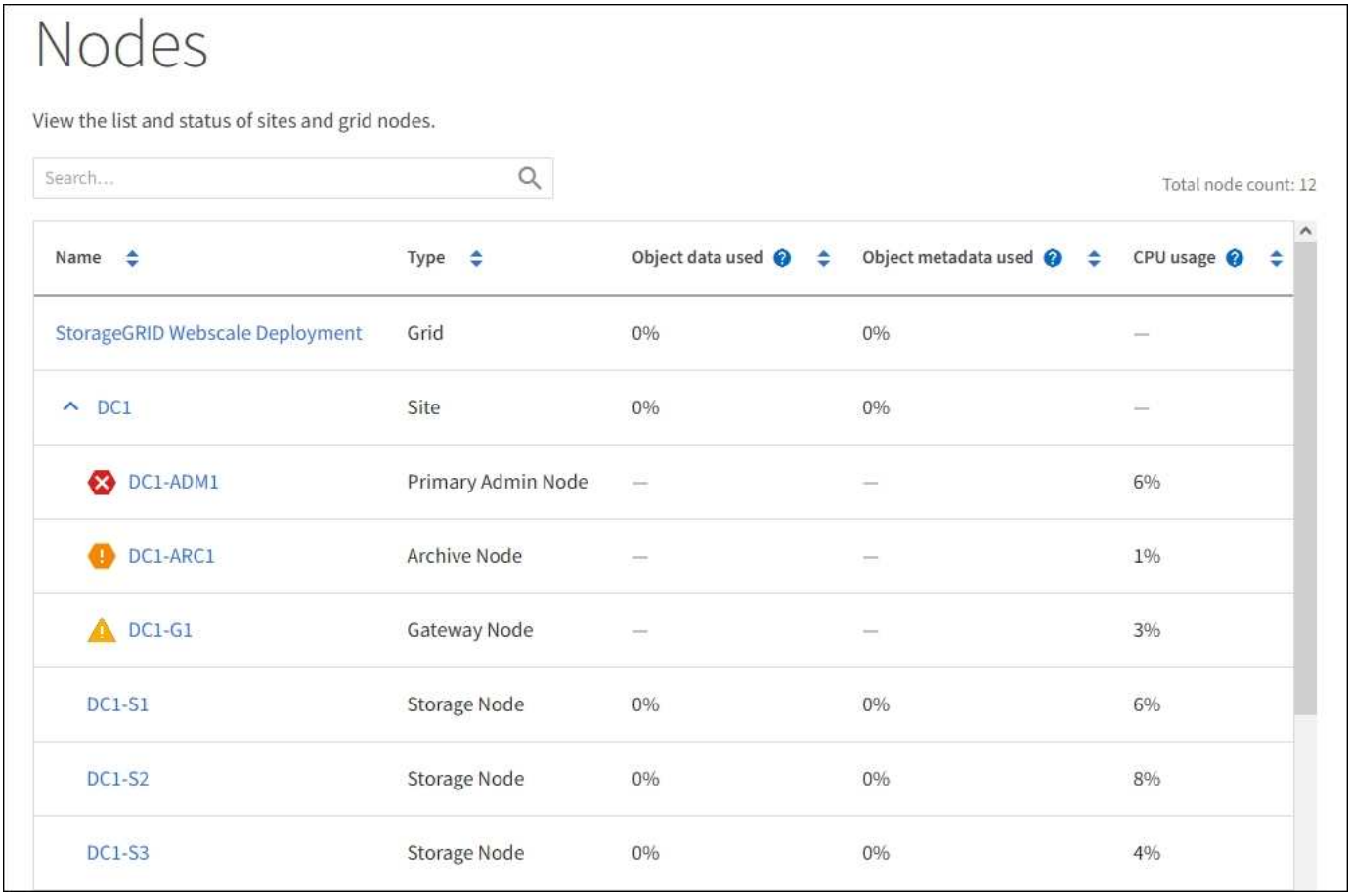
Visualizza la pagina nodi: Panoramica

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

La tabella Nodes (nodi) elenca informazioni riepilogative per l'intera griglia, ciascun sito e ciascun nodo. Se un nodo è disconnesso o presenta un avviso attivo, viene visualizzata un'icona accanto al nome del nodo. Se il nodo è connesso e non sono presenti avvisi attivi, non viene visualizzata alcuna icona.

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

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



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

Se un nodo è disconnesso dalla griglia, potrebbe essere presente un avviso sottostante, ma viene visualizzata solo l'icona "non connesso". Per visualizzare gli avvisi attivi per un nodo, selezionare il nodo.

Icone di avviso

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

Critico: Si verifica una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. È necessario risolvere immediatamente il problema sottostante. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.

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

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

Visualizza i dettagli di un sistema, sito o nodo

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

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

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

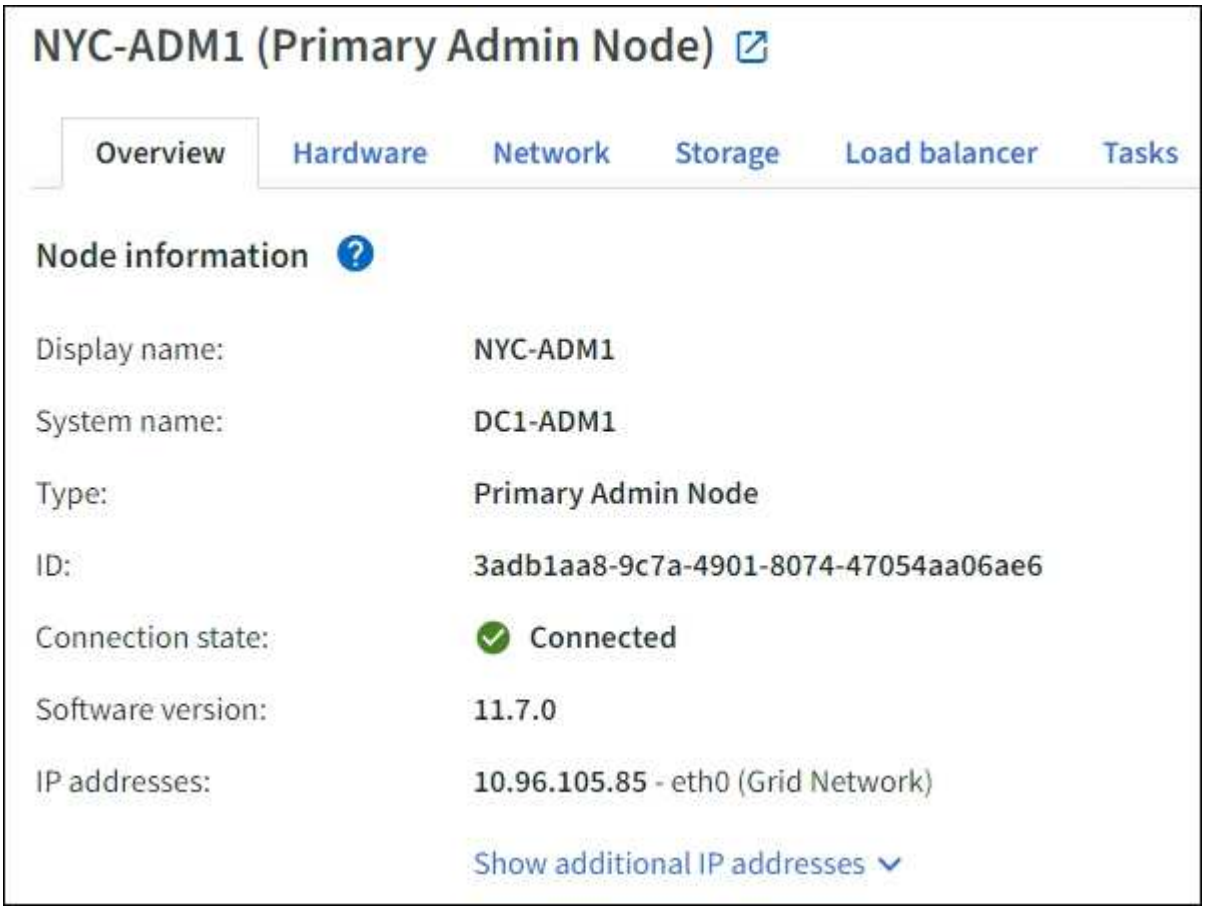
Visualizzare la scheda Panoramica

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

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

Informazioni sul nodo

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



Le informazioni generali per un nodo includono quanto segue:

- **Nome visualizzato** (visualizzato solo se il nodo è stato rinominato): Il nome visualizzato corrente per il nodo. Utilizzare "Rinominare la griglia, i siti e i nodi" procedura per aggiornare questo valore.
- **Nome sistema**: Il nome immesso per il nodo durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni StorageGRID interne e non possono essere modificati.
- **Type**: Il tipo di nodo — Admin Node, Primary Admin Node, Storage Node, Gateway Node o Archive Node.

> Il supporto per i nodi di archiviazione è obsoleto e verrà rimosso in una release futura. Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità.

- **ID**: Identificatore univoco del nodo, chiamato anche UUID.
- **Stato connessione**: Uno dei tre stati. Viene visualizzata l'icona dello stato più grave.
  - **Sconosciuto** : Per un motivo sconosciuto, il nodo non è connesso alla rete o uno o più servizi sono inaspettatamente fuori servizio. Ad esempio, la connessione di rete tra i nodi è stata persa, l'alimentazione è inattiva o un servizio è inattivo. Potrebbe essere attivato anche l'avviso **Impossibile comunicare con il nodo**. Potrebbero essere attivi anche altri avvisi. Questa situazione richiede un'attenzione immediata.

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

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

Avvisi

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

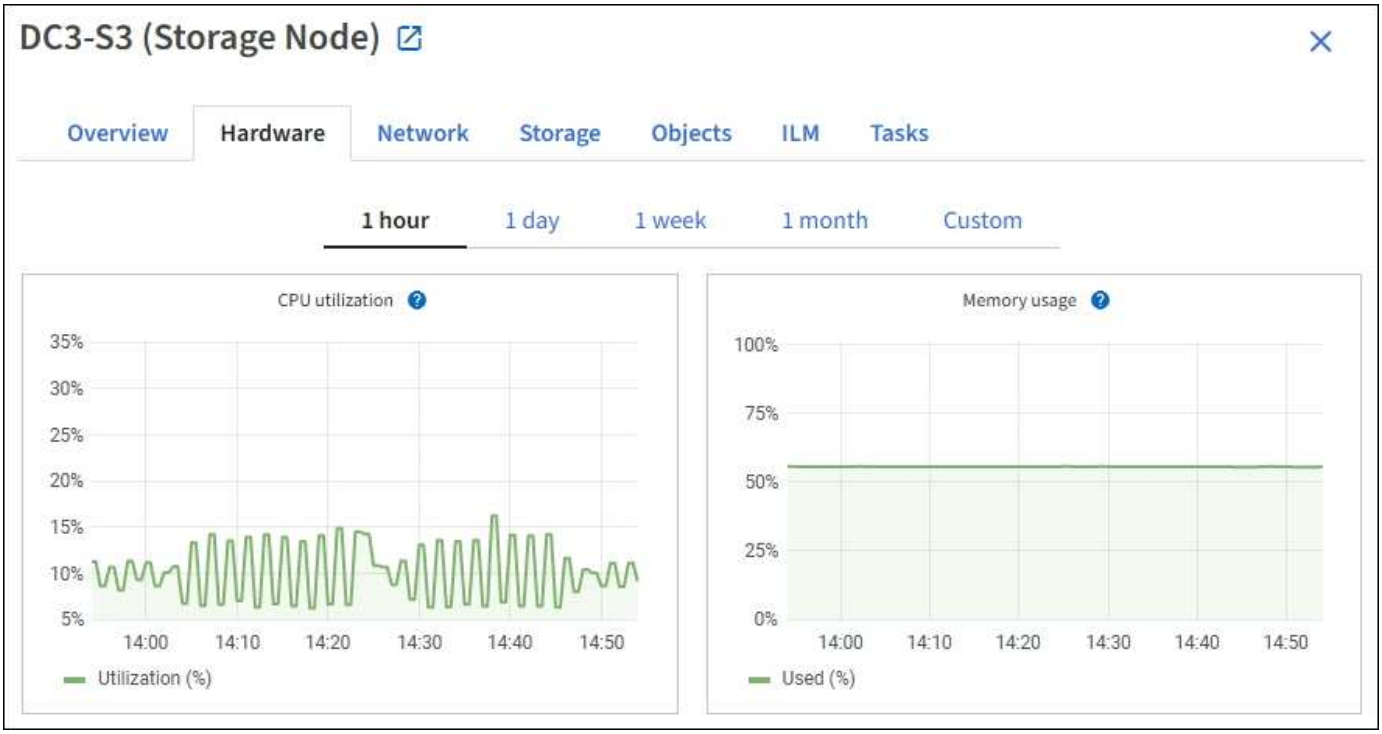
Sono inclusi anche gli avvisi per "stati di connessione del nodo".

Visualizzare la scheda hardware

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

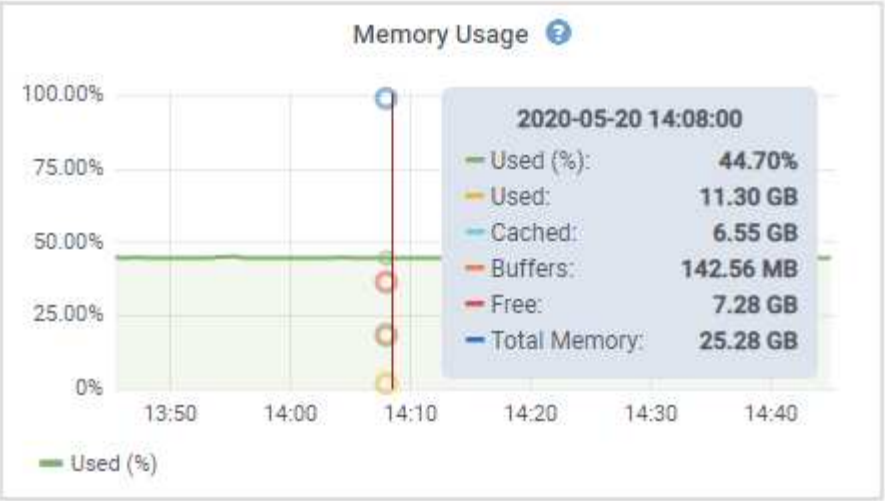
> Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio di questa pagina.

Viene visualizzata la scheda hardware per tutti i nodi.



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

Per visualizzare i dettagli relativi all'utilizzo della CPU e della memoria, posizionare il cursore su ciascun grafico.



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

Visualizza informazioni sui nodi di storage dell'appliance

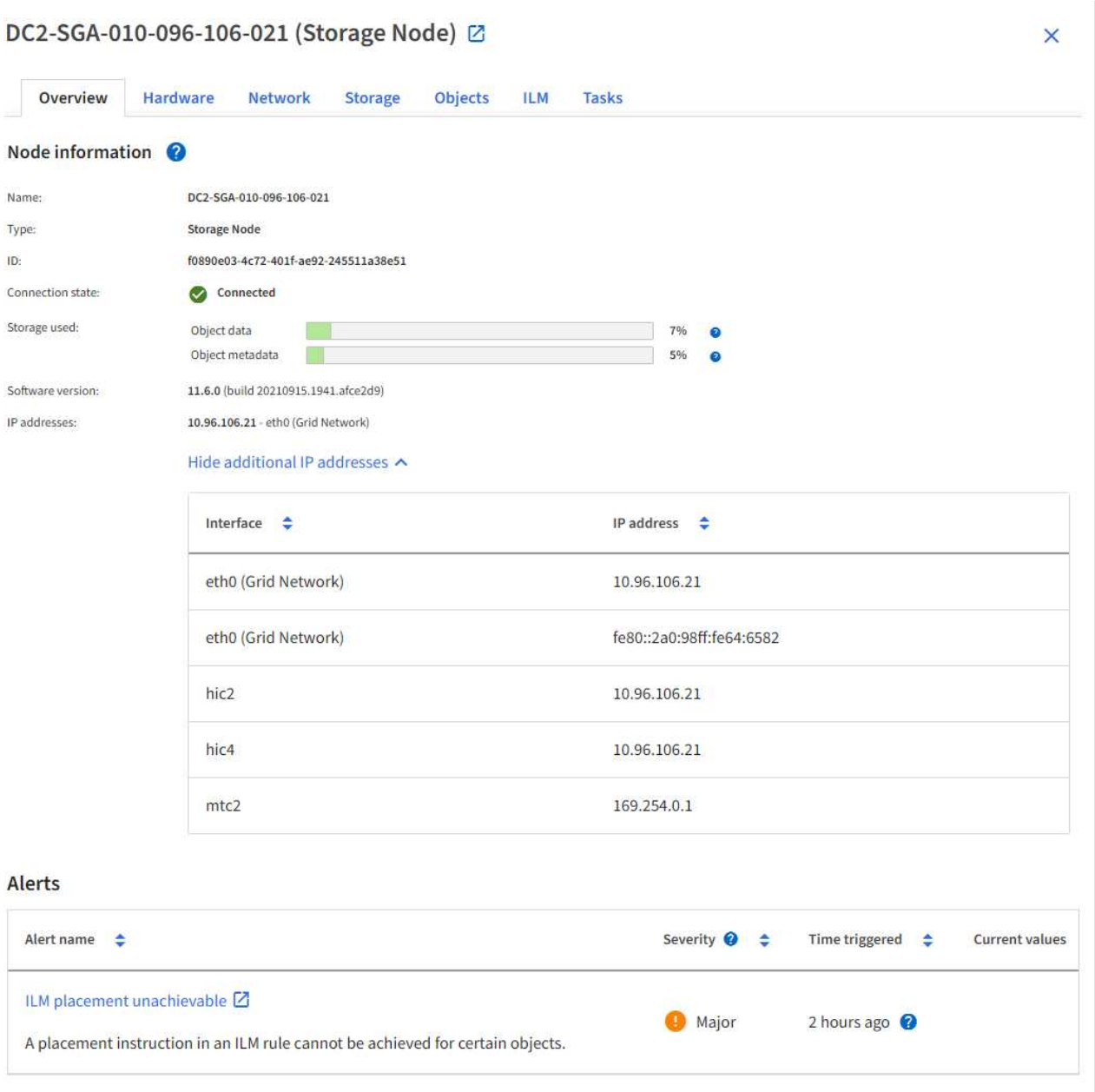
La pagina Nodes (nodi) elenca le informazioni sullo stato di salute del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ciascun nodo di storage dell'appliance. È inoltre possibile visualizzare memoria, hardware di storage, versione del firmware del controller, risorse di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

Fasi

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

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

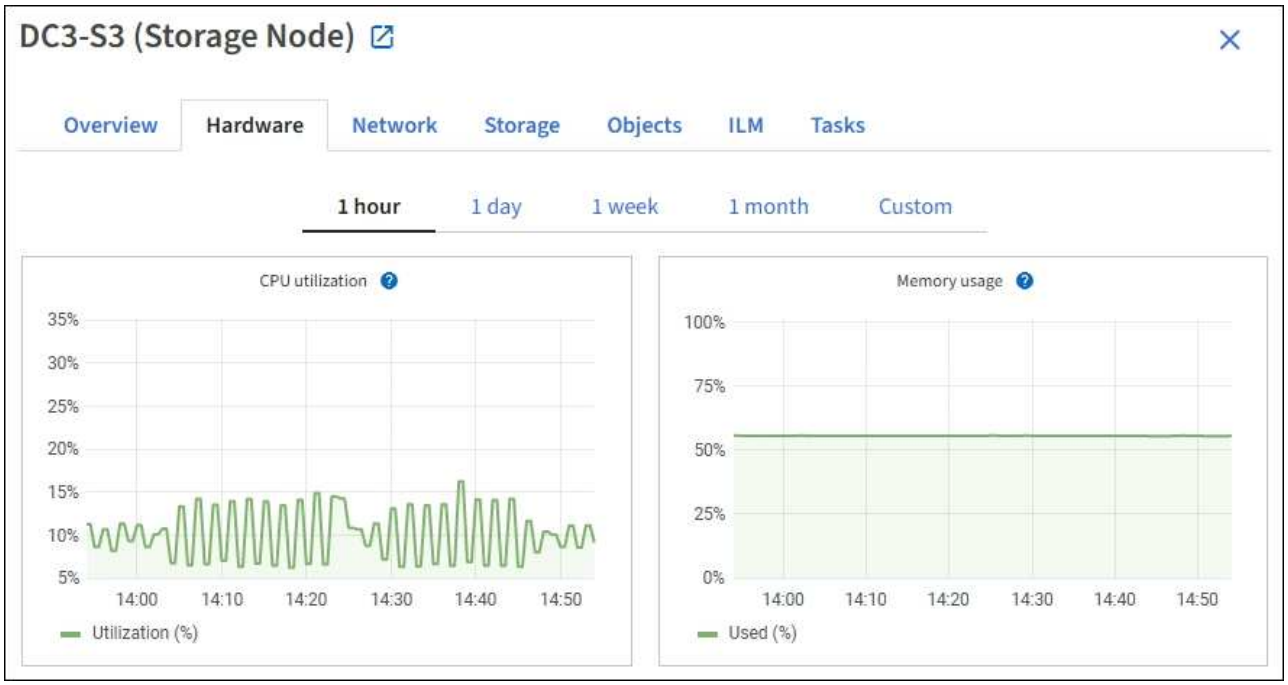
   - **eth**: Rete griglia, rete amministrativa o rete client.
   - **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
   - **mtc**: Una delle porte 1 GbE fisiche dell'appliance.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



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

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

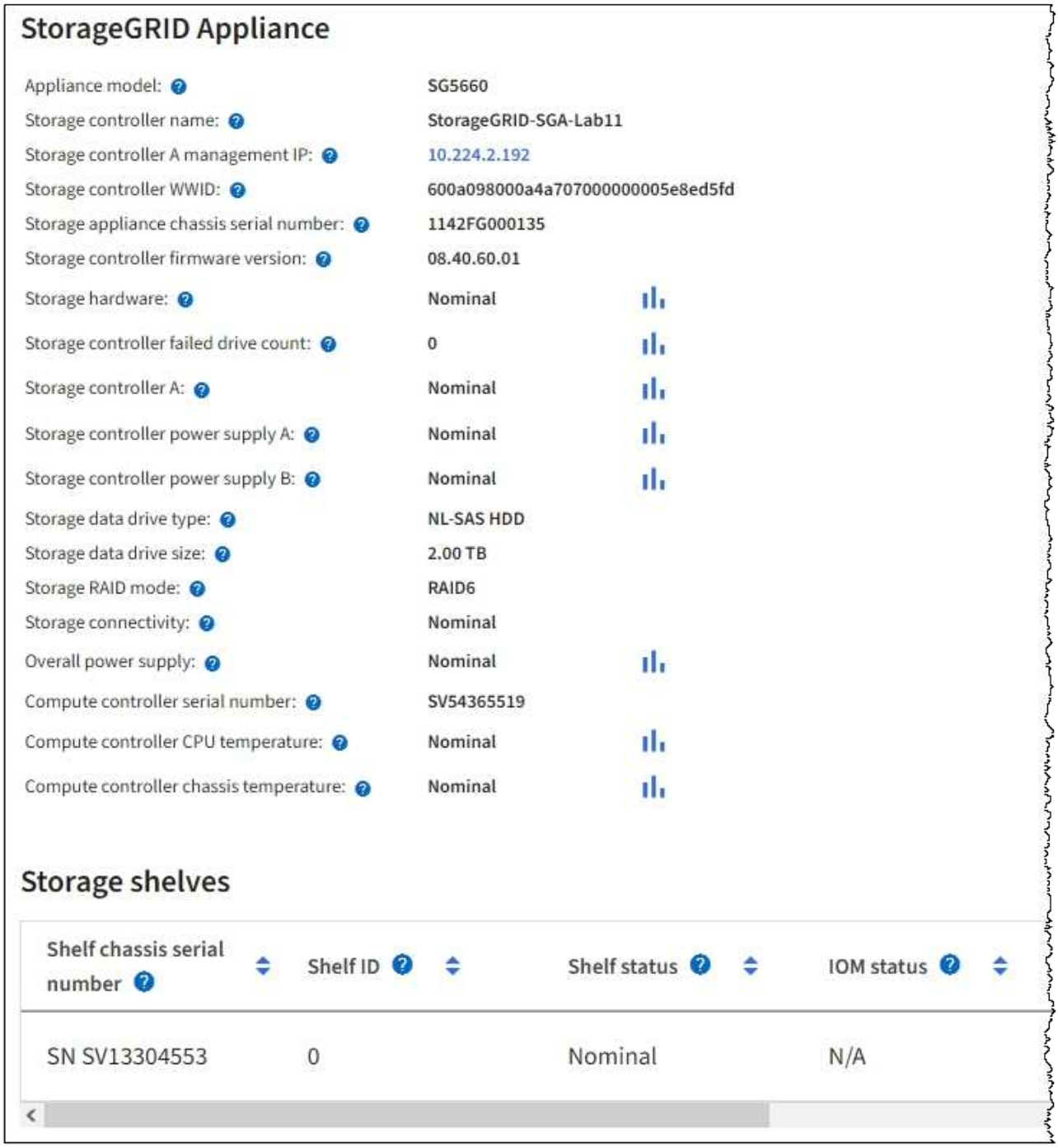
   a. Visualizzare i grafici relativi all'utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni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



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

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

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



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

Nella tabella Appliance	Descrizione
IP di gestione dello storage controller B.	Indirizzo IP per la porta di gestione 1 sul controller di storage B. Questo IP viene utilizzato per accedere al sistema operativo SANtricity e risolvere i problemi di storage. Alcuni modelli di appliance non dispongono di un controller di storage B.
WWID dello storage controller	L'identificatore mondiale dello storage controller mostrato in SANtricity OS.
Numero di serie dello chassis dell'appliance di storage	Il numero di serie dello chassis dell'appliance.
Versione del firmware del controller di storage	La versione del firmware del controller di storage per l'appliance.
Hardware per lo storage	Lo stato generale dell'hardware del controller dello storage. Se Gestore di sistema di SANtricity riporta lo stato di intervento richiesto per l'hardware di storage, anche il sistema StorageGRID riporta questo valore. Se lo stato è "richiede attenzione", controllare prima lo storage controller utilizzando il sistema operativo SANtricity. Quindi, assicurarsi che non esistano altri allarmi applicabili al controller di calcolo.
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Controller dello storage A	Lo stato dello storage controller A.
Controller dello storage B	Lo stato dello storage controller B. Alcuni modelli di appliance non dispongono di un controller di storage B.
Alimentazione a del controller storage	Lo stato dell'alimentatore A per il controller dello storage.
Alimentazione controller storage B	Lo stato dell'alimentazione B del controller di storage.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).
Dimensioni del disco per i dati di storage	Le dimensioni effettive di un'unità dati. **Nota**: Per i nodi con shelf di espansione, utilizzare Dimensioni del disco dati per ogni shelf invece. Le dimensioni effettive del disco potrebbero differire in base allo shelf.

Nella tabella Appliance	Descrizione
Storage RAID mode (modalità RAID storage)	La modalità RAID configurata per l'appliance.
Connettività dello storage	Lo stato di connettività dello storage.
Alimentatore generale	Lo stato di tutti gli alimentatori dell'apparecchio.
IP BMC del controller di calcolo	L'indirizzo IP della porta BMC (Baseboard Management Controller) nel controller di calcolo. Questo IP viene utilizzato per connettersi all'interfaccia BMC per monitorare e diagnosticare l'hardware dell'appliance. Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.
Hardware di calcolo	Lo stato dell'hardware del controller di calcolo. Questo campo non viene visualizzato per i modelli di appliance che non dispongono di hardware di calcolo e storage separati.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di calcolo.
Temperatura dello chassis del controller di calcolo	Lo stato della temperatura del controller di calcolo.

+

Nella tabella Storage shelf	Descrizione
Numero di serie dello shelf chassis	Il numero di serie dello chassis dello shelf di storage.
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 scaffali di espansione si applicano solo ai modelli SG6060 e SG6160.
Stato dello shelf	Lo stato generale dello shelf di storage.

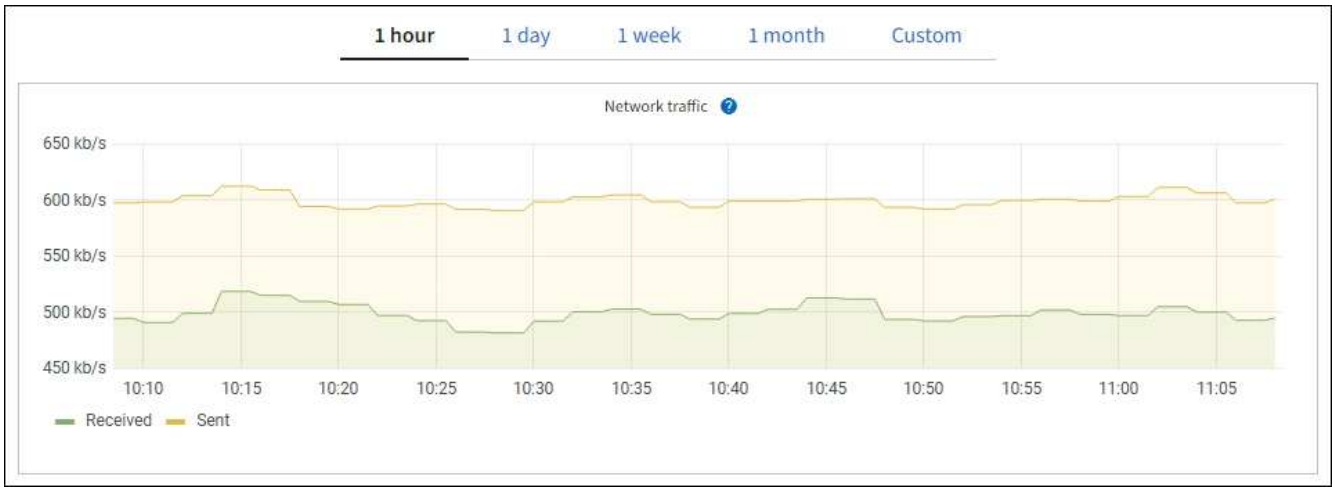
Nella tabella Storage shelf	Descrizione
Stato IOM	Lo stato dei moduli di input/output (IOM) in qualsiasi shelf di espansione. N/D se non si tratta di uno shelf di espansione.
Stato dell'alimentatore	Lo stato generale degli alimentatori per lo shelf di storage.
Stato del cassetto	Lo stato dei cassetti nello shelf di archiviazione. N/D se il ripiano non contiene cassetti.
Stato della ventola	Lo stato generale delle ventole di raffreddamento nello shelf di storage.
Slot per dischi	Il numero totale di slot per dischi nello shelf di storage.
Dischi dati	Il numero di dischi nello shelf di storage utilizzati per lo storage dei dati.
dimensione del disco dati	La dimensione effettiva di un'unità dati nello shelf di storage.
Dischi cache	Il numero di dischi nello shelf di storage utilizzati come cache.
Dimensione dell'unità cache	La dimensione dell'unità cache più piccola nello shelf di storage. Normalmente, le unità cache sono tutte delle stesse dimensioni.
Stato della configurazione	Lo stato di configurazione dello shelf di storage.

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

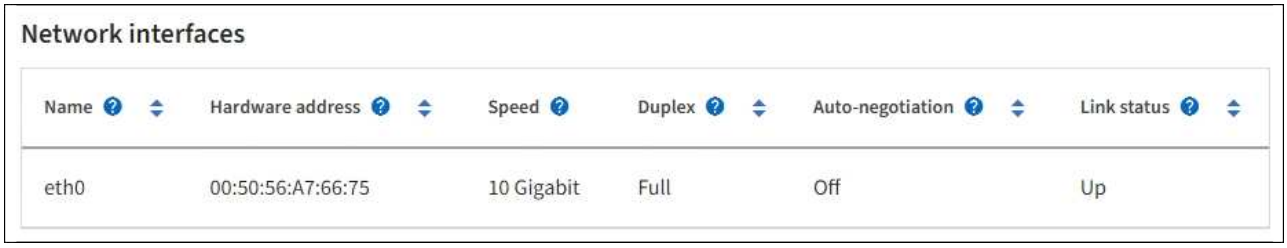
   Se uno stato non è "nominale", esaminare eventuali avvisi correnti. Puoi anche utilizzare Gestione di sistema di SANtricity per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

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

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



a. Consultare la sezione interfacce di rete.



Network interfaces

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

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

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

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

Vedere "Configurare i collegamenti di rete" Per ulteriori informazioni sulla configurazione delle porte 10/25-GbE.

b. Consultare la sezione comunicazione di rete.

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

Network communication

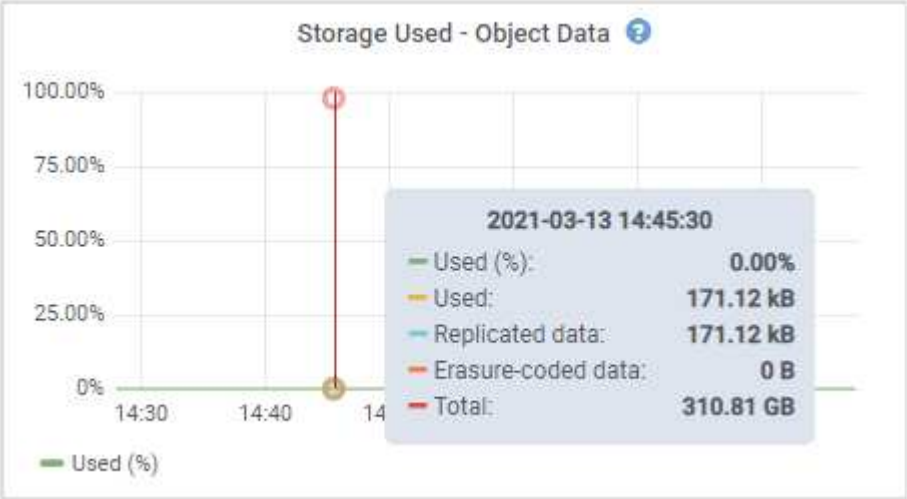
Receive

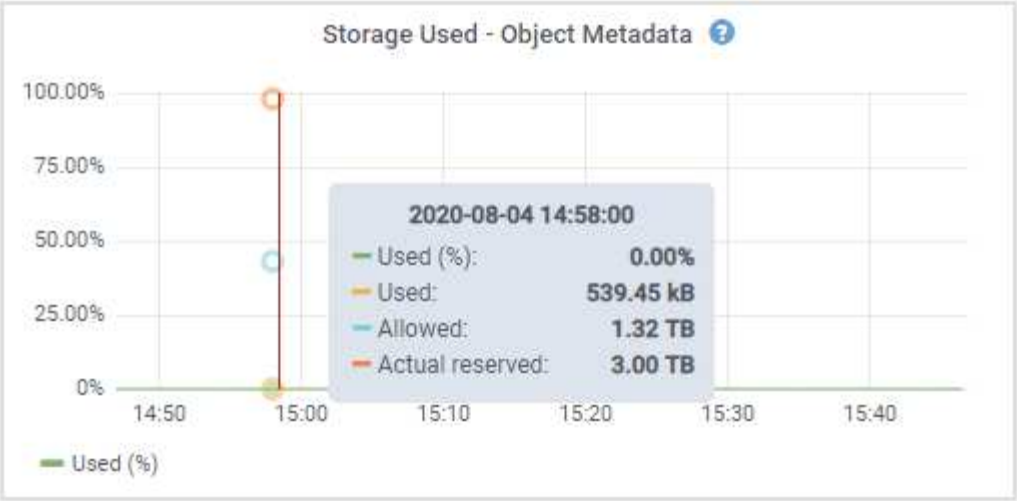
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

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

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





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

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

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

Disk devices

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

Volumes

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

Object stores

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

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

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

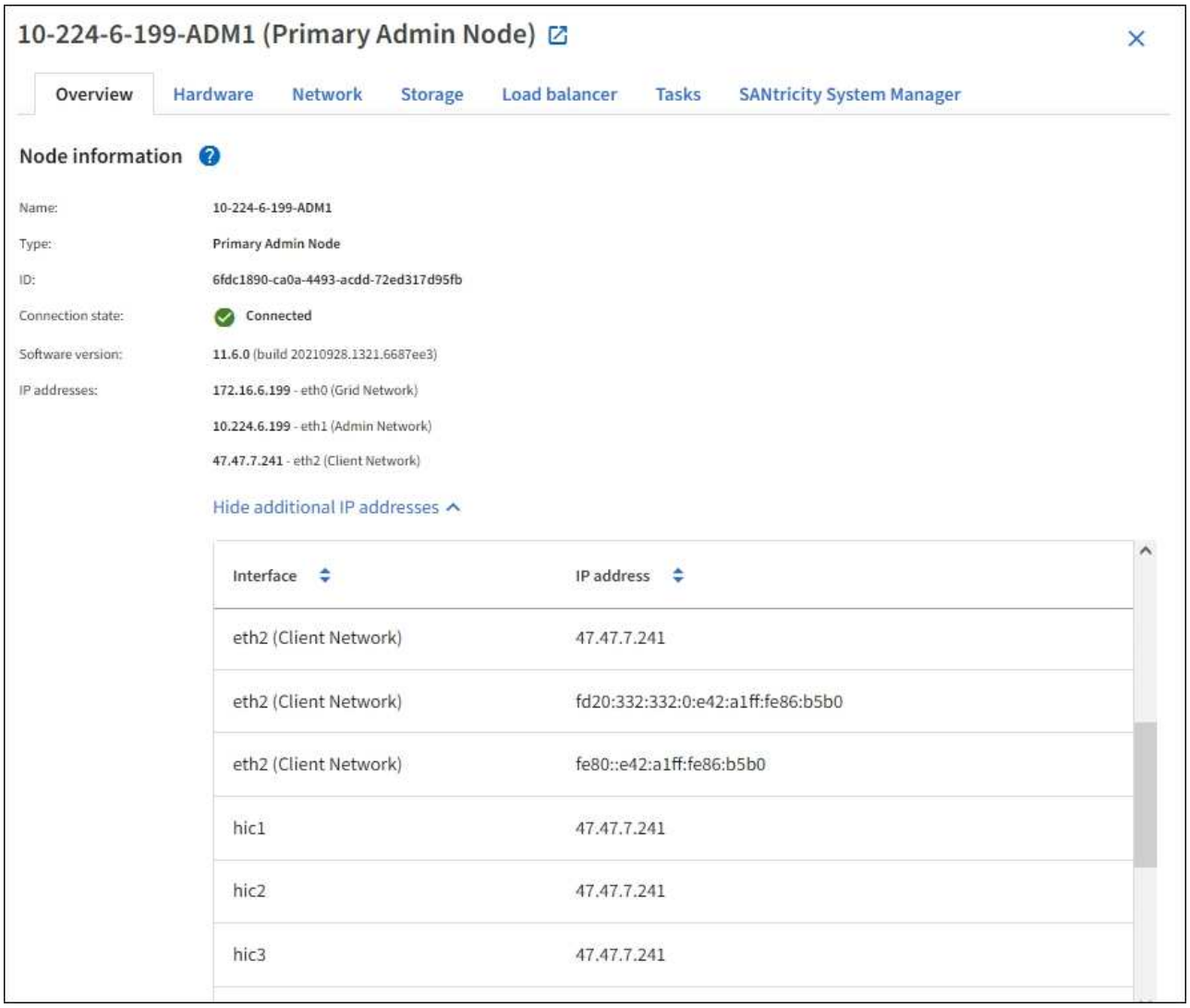
Fasi

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

   La sezione Node information (informazioni nodo) della scheda Overview (Panoramica) visualizza

informazioni riepilogative per il nodo, ad esempio il nome, il tipo, l'ID e lo stato di connessione del nodo. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

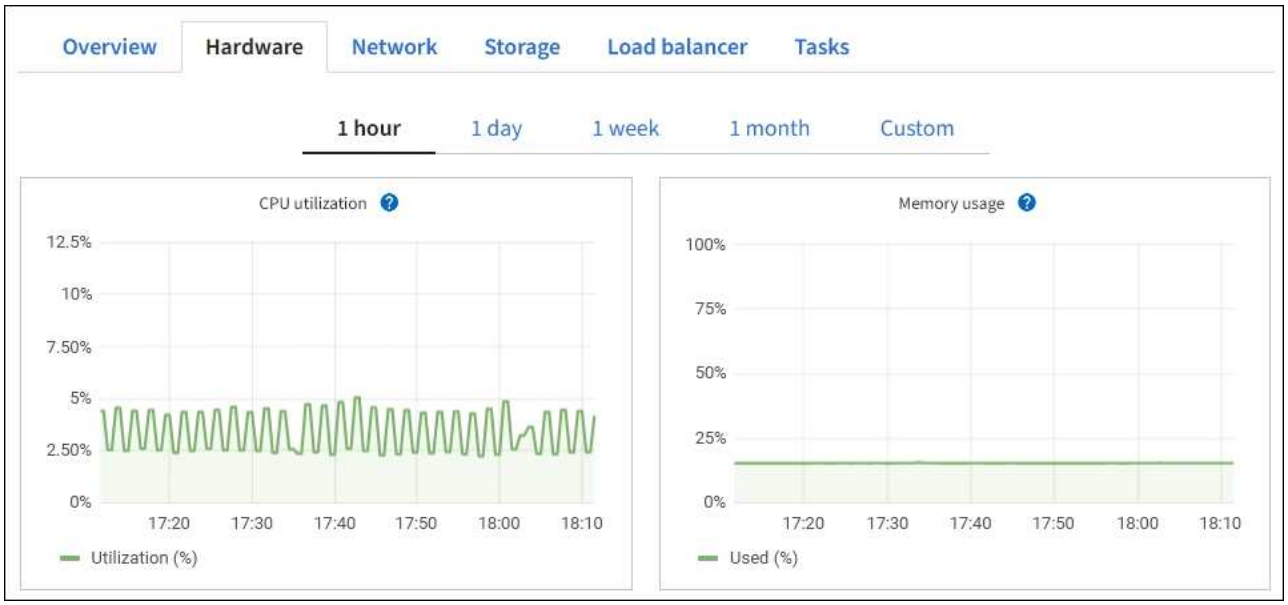
- **Adllb** e **adlli**: Visualizzato se si utilizza il bonding Active/backup per l'interfaccia di Admin Network
- **eth**: Rete griglia, rete amministrativa o rete client.
- **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla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



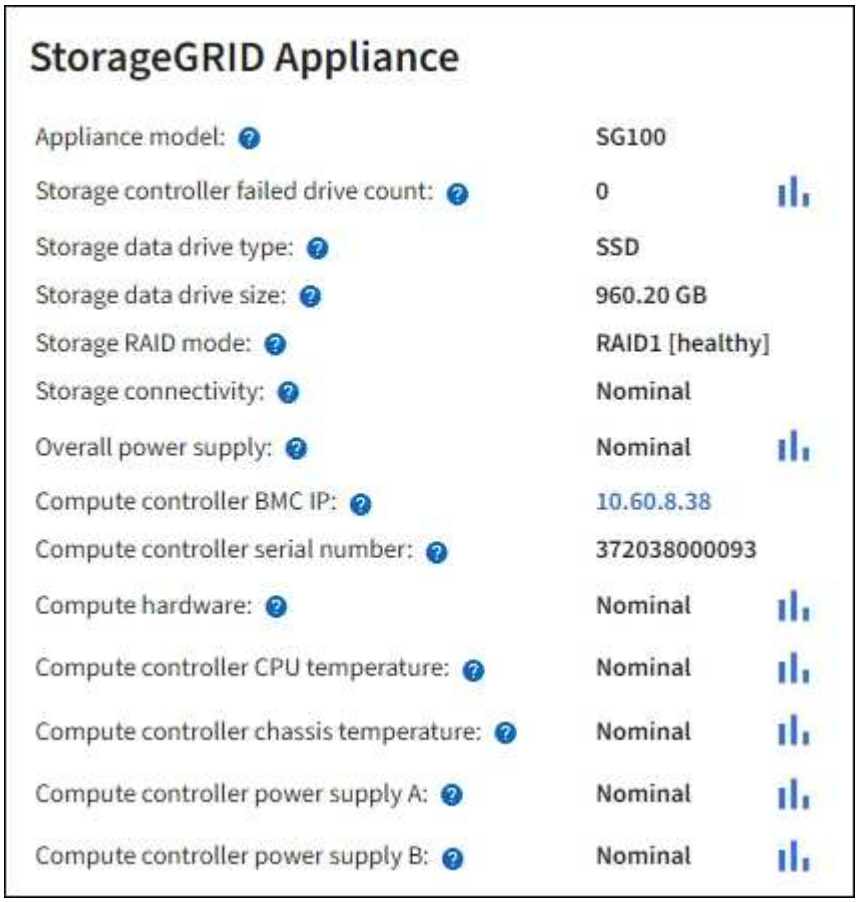
La sezione Avvisi della scheda Panoramica visualizza gli avvisi attivi per il nodo.

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

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



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



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

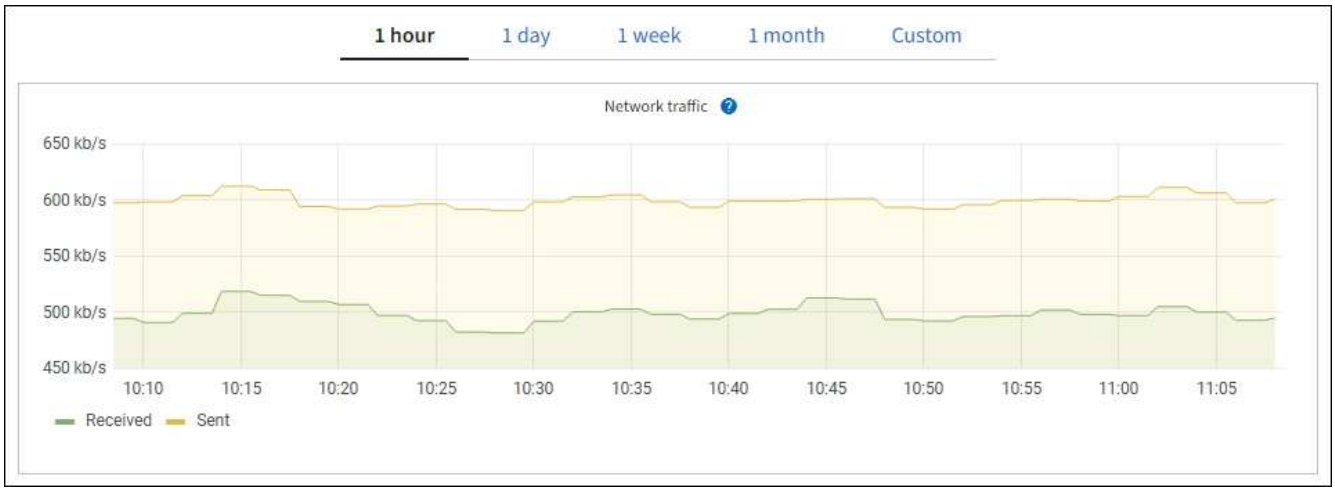
Nella tabella Appliance	Descrizione
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).
Dimensioni del disco per i dati di storage	Le dimensioni effettive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

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

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

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

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



a. Consultare la sezione interfacce di rete.

Network interfaces

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

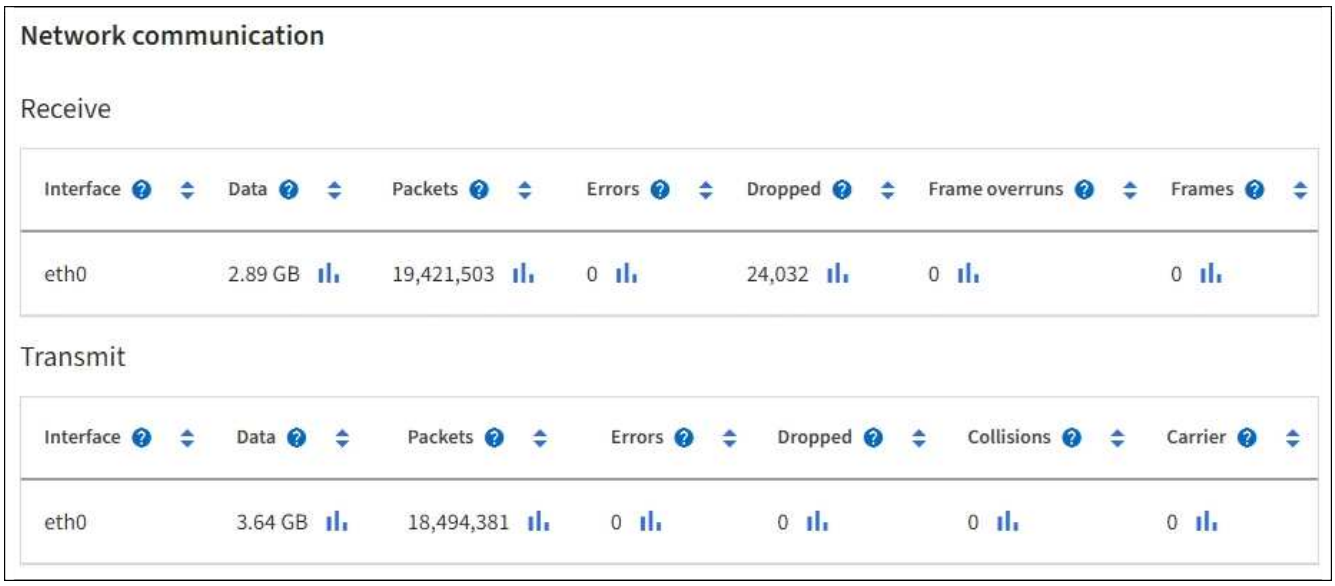
Utilizzare la seguente tabella con i valori nella colonna **Speed** della tabella Network Interfaces (interfacce di rete) per determinare se le quattro porte di rete 40/100-GbE dell'appliance sono state configurate per l'utilizzo della modalità Active/backup o LACP.

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

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

b. Consultare la sezione comunicazione di rete.

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



5. Selezionare **Storage** per visualizzare le informazioni relative ai dischi e ai volumi sull'appliance di servizi.

DO-REF-DC1-GW1 (Gateway Node)

Overview | Hardware | Network | Storage | Load balancer | Tasks

Disk devices

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

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.63 GB	Unknown

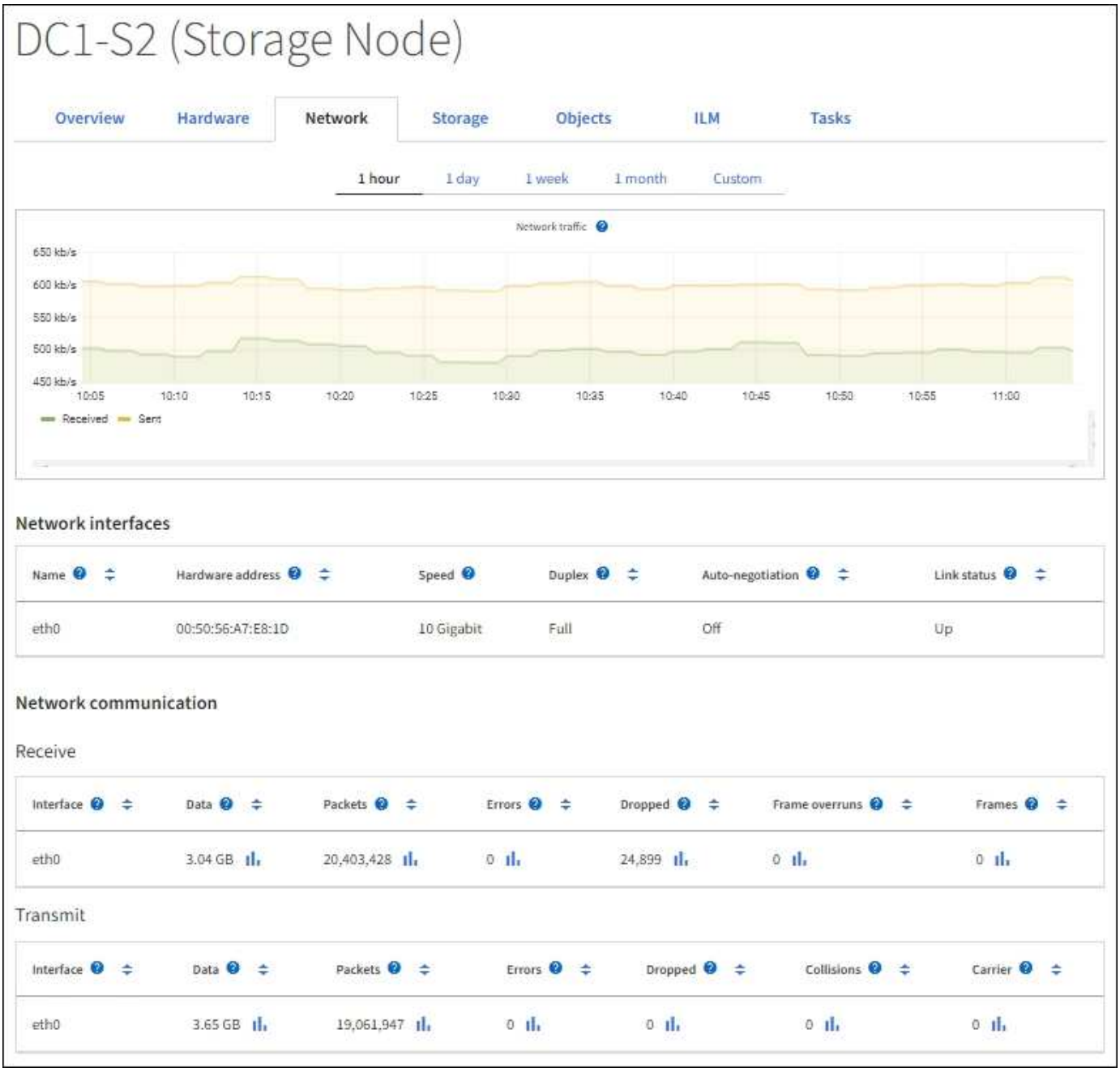
Visualizzare la scheda rete

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

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

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

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



Informazioni correlate

"Monitorare le connessioni di rete e le performance"

Visualizzare la scheda Storage (archiviazione)

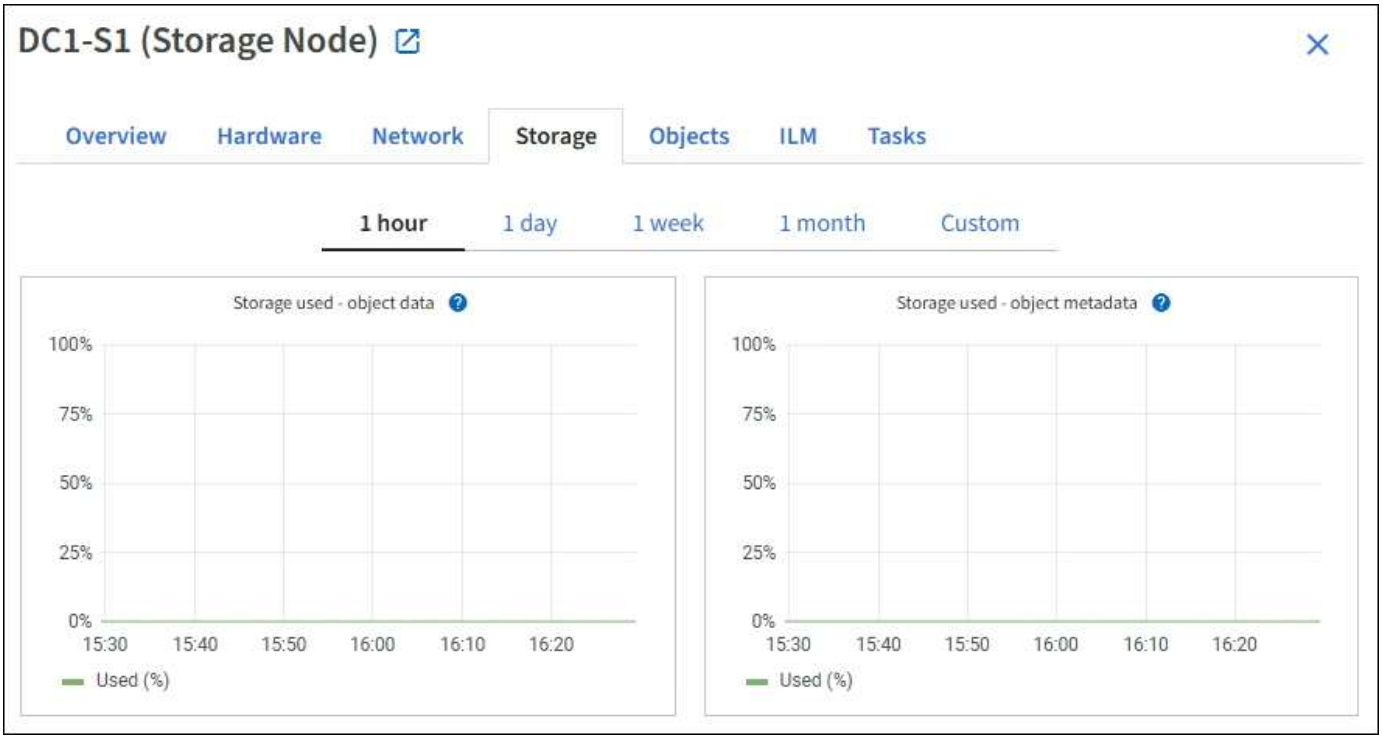
La scheda Storage riepiloga la disponibilità dello storage e altre metriche di storage.

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

Grafici utilizzati per lo storage

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

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



Dischi, volumi e tabelle di archiviazione degli oggetti

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

Disk devices

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

Volumes

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

Object stores

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

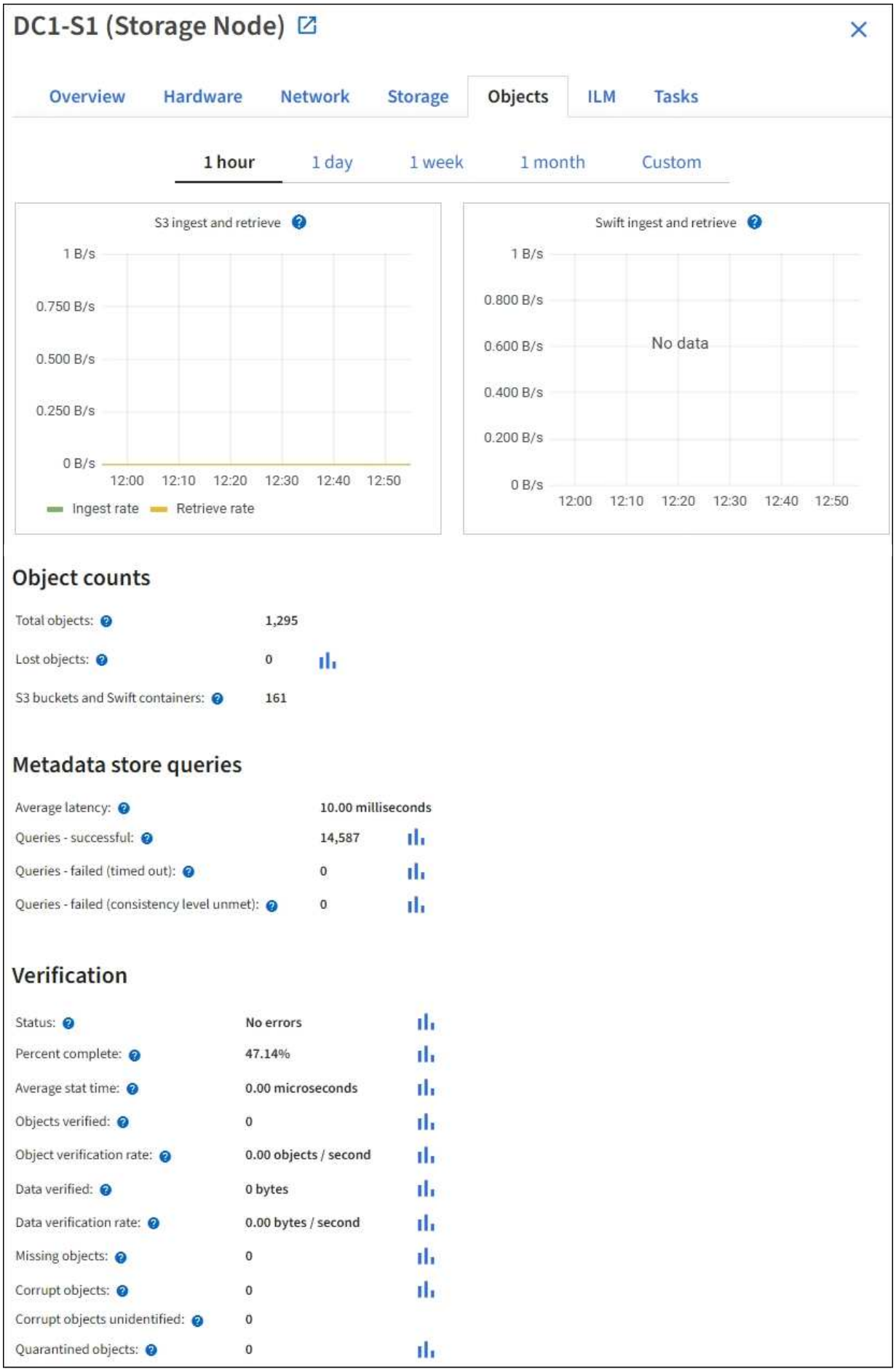
Informazioni correlate

"Monitorare la capacità dello storage"

Visualizzare la scheda oggetti

La scheda oggetti fornisce informazioni su "S3" e. "Rapido" velocità di acquisizione e recupero.

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

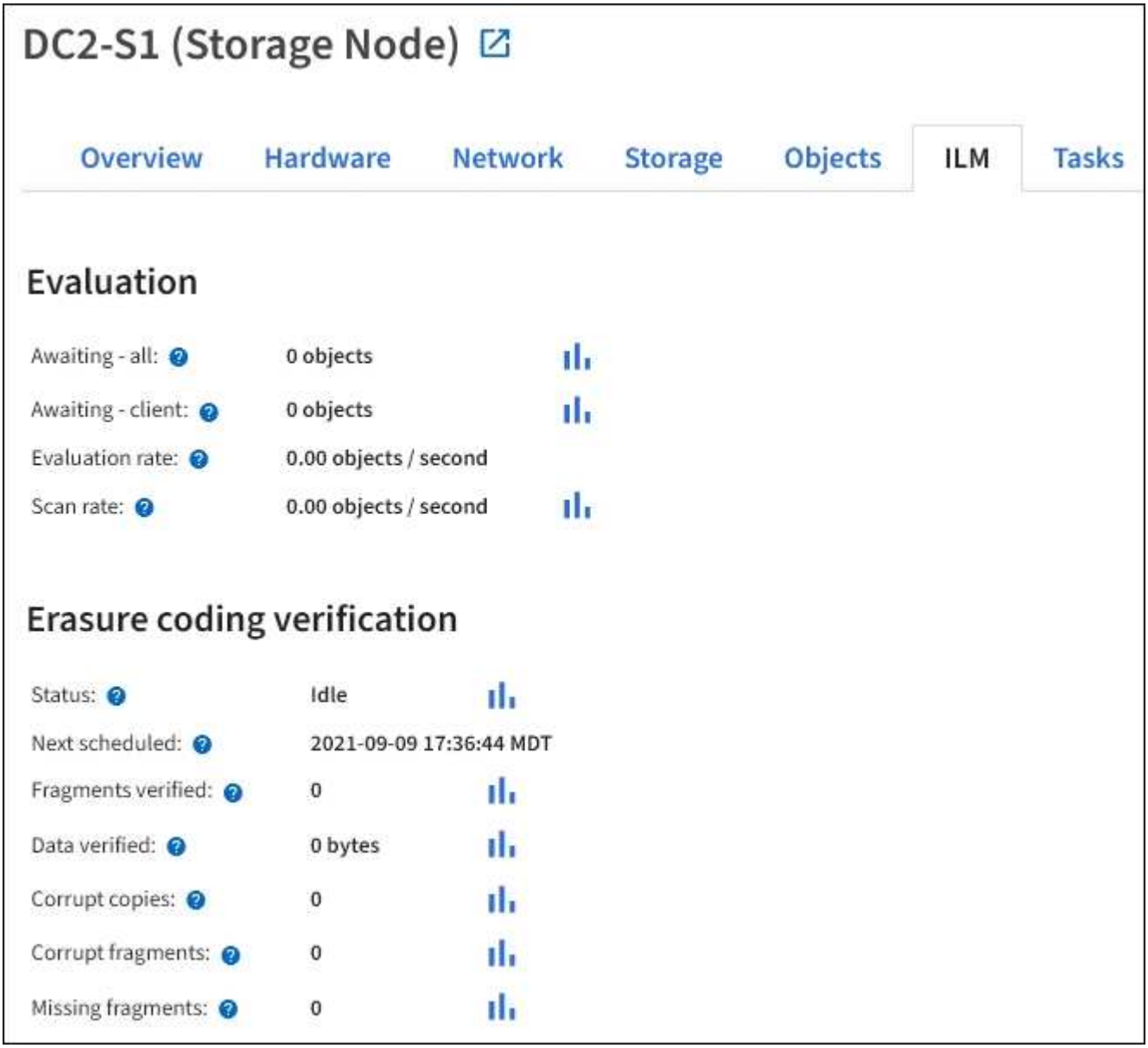

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 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

Visualizzare la scheda ILM

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

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

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



Informazioni correlate

"Monitorare la gestione del ciclo di vita delle informazioni"

"Amministrare StorageGRID"

Utilizzare la scheda attività

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

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

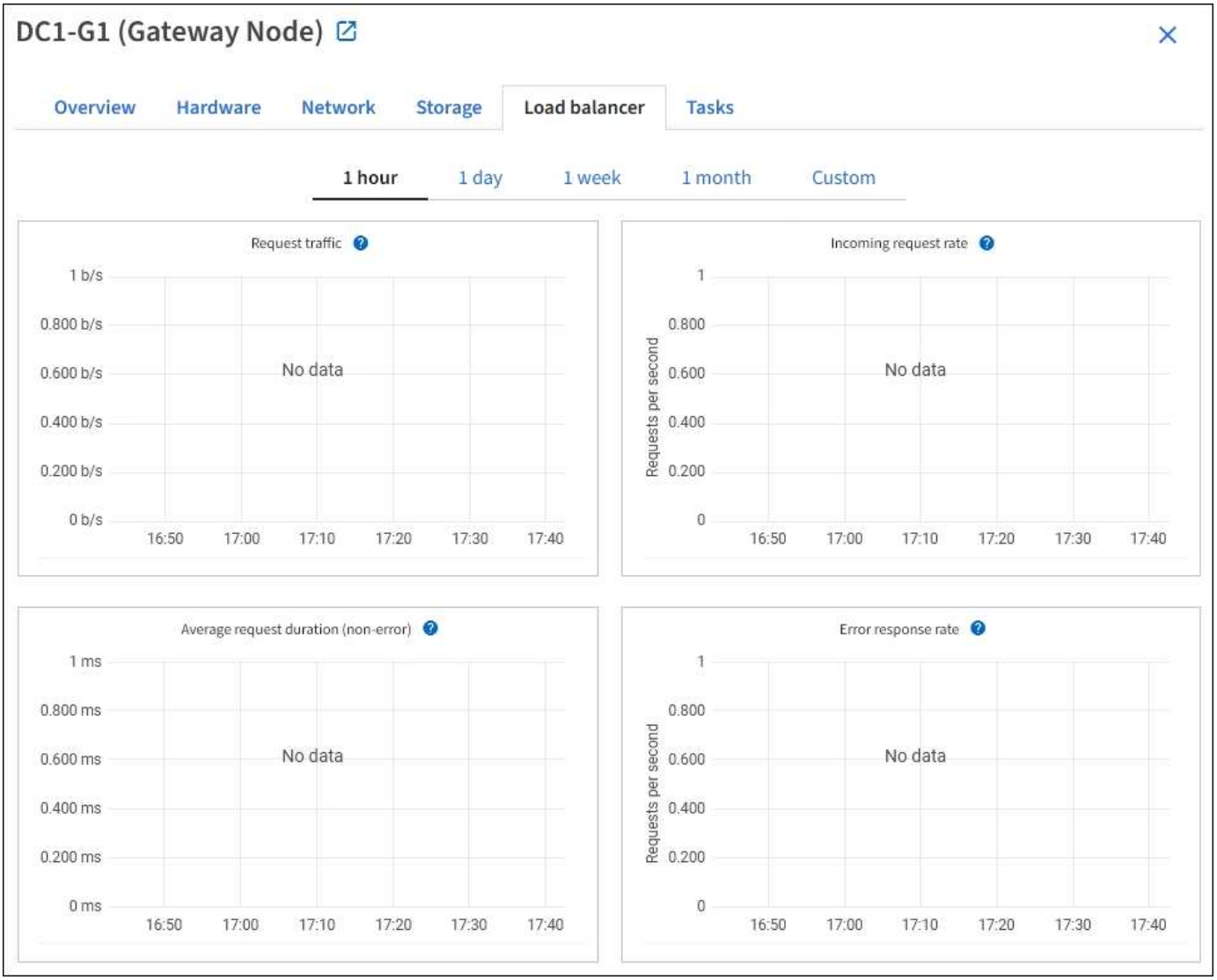
- "Rinominare la griglia, i siti e i nodi"
- "Nodo di reboot grid"
- "Impostare l'apparecchio in modalità di manutenzione"

Visualizzare la scheda bilanciamento del carico

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

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

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



Richiesta di traffico

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

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

Tasso di richiesta in entrata

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

Durata media della richiesta (non errore)

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

Tasso di risposta agli errori

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

Informazioni correlate

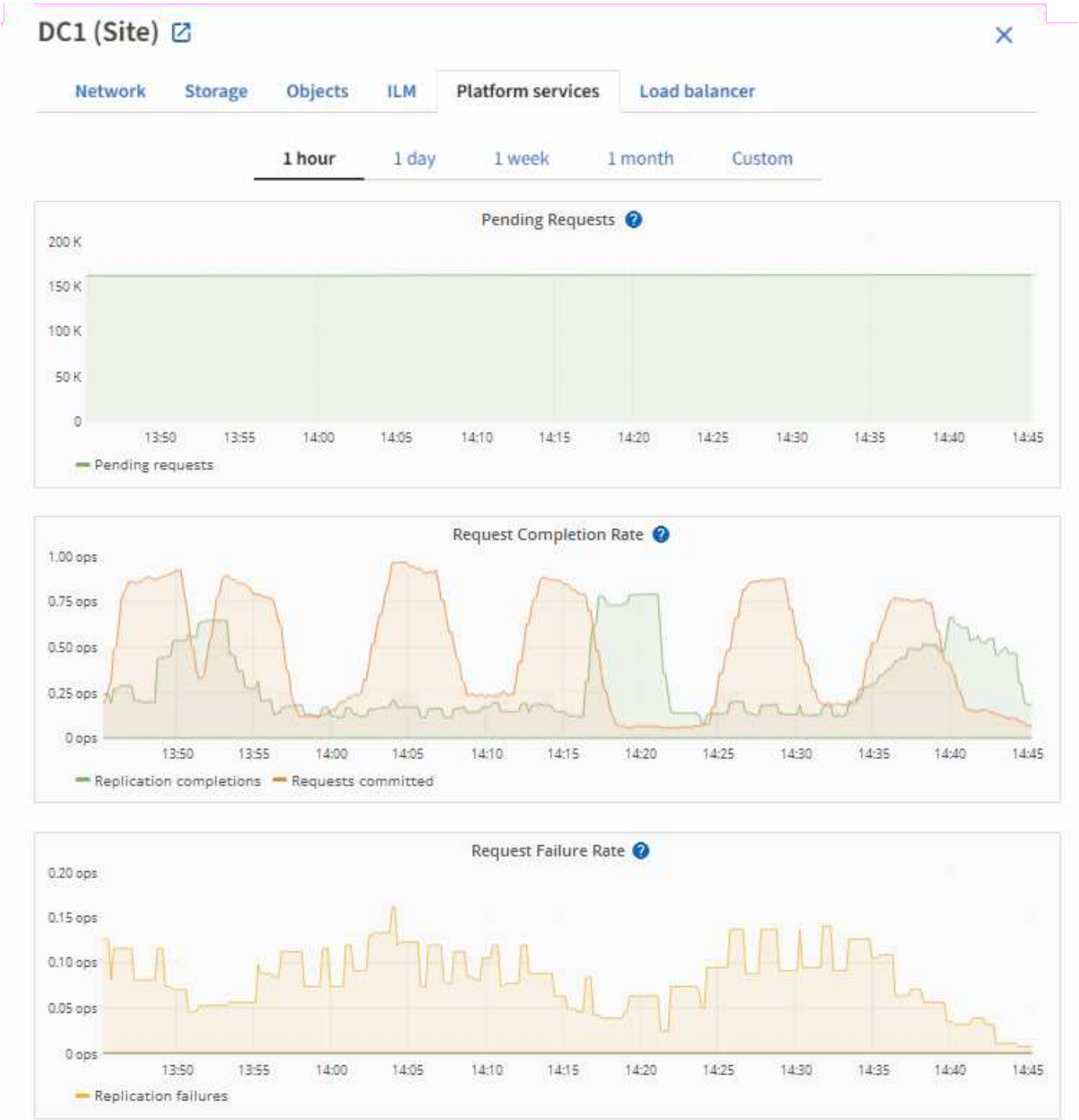
"Monitorare le operazioni di bilanciamento del carico"

"Amministrare StorageGRID"

Visualizzare la scheda Platform Services (servizi piattaforma)

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

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



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

Visualizza la scheda Gestisci unità (solo SGF6112)

La scheda Manage Drives (Gestisci dischi) consente di accedere ai dettagli ed eseguire le attività di troubleshooting e manutenzione dei dischi dell'appliance SGF6112.

> La scheda Gestisci dischi è disponibile solo per SGF6112 nodi di appliance di storage.

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

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

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

Per informazioni sull'utilizzo della scheda Gestisci unità, vedere "Utilizzare la scheda Gestisci unità".

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

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

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

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

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

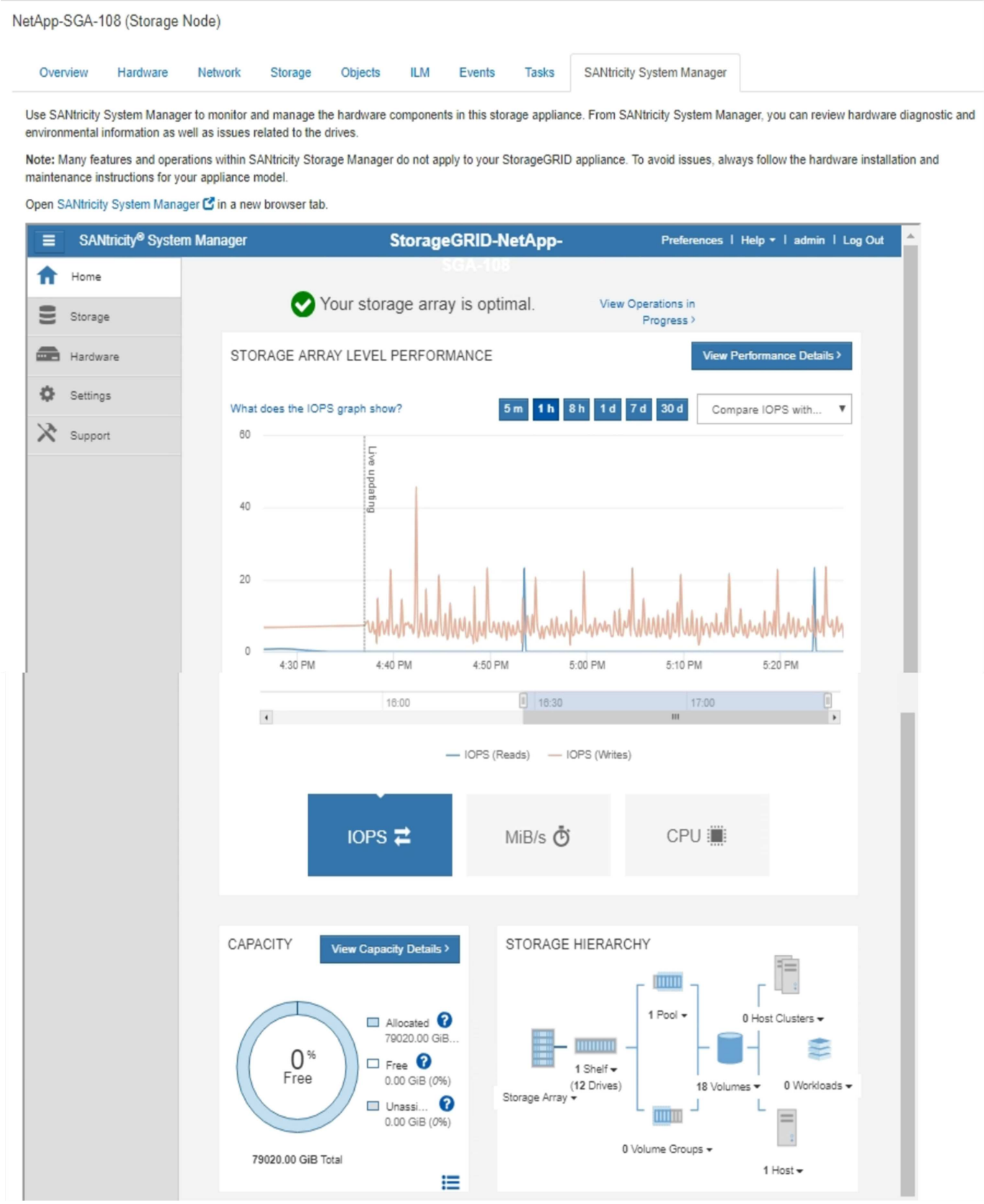
> Per utilizzare Gestione di sistema di SANtricity per configurare un proxy per e-Series AutoSupport, vedere "Invio dei pacchetti e-Series AutoSupport tramite StorageGRID".

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

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

> L'accesso a Gestione di sistema SANtricity da Gestione griglia è generalmente destinato solo al monitoraggio dell'hardware dell'appliance e alla configurazione di e-Series AutoSupport. Molte funzionalità e operazioni di Gestione sistema di SANtricity, come l'aggiornamento del firmware, non si applicano al monitoraggio dell'appliance StorageGRID. Per evitare problemi, seguire sempre le istruzioni per la manutenzione dell'hardware dell'apparecchio.

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



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

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

posizionare il cursore su ciascun grafico.

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

Informazioni da monitorare regolarmente

Cosa e quando monitorare

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Informazioni sulle attività di monitoraggio

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

Cosa monitorare	Frequenza
"Stato di salute del sistema"	Ogni giorno
Valuta a quale "Capacità di metadati e oggetti del nodo di storage" è in corso di consumo	Settimanale
"Operazioni di gestione del ciclo di vita delle informazioni"	Settimanale
"Risorse di rete e di sistema"	Settimanale
"Attività del tenant"	Settimanale
"Operazioni dei client S3 e Swift"	Settimanale
"Operazioni di bilanciamento del carico"	Dopo la configurazione iniziale e dopo eventuali modifiche alla configurazione
"Connessioni a federazione di griglie"	Settimanale
"Capacità del sistema storage di archiviazione esterno"	Settimanale

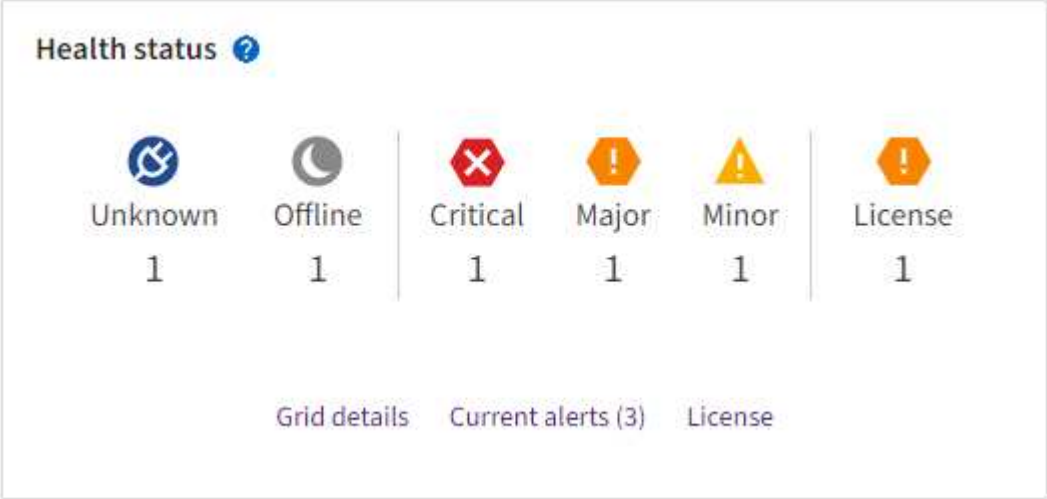
Monitorare lo stato del sistema

Monitorare quotidianamente lo stato di salute generale del sistema StorageGRID.

A proposito di questa attività

Il sistema StorageGRID può continuare a funzionare quando le parti della griglia non sono disponibili. I potenziali problemi indicati da avvisi o allarmi (sistema legacy) non sono necessariamente problemi con le operazioni del sistema. Esaminare i problemi riepilogati nella scheda di stato dello stato di salute del pannello di controllo di Grid Manager.

Per ricevere notifiche di avvisi non appena vengono attivati, è possibile "imposta le notifiche via email per gli avvisi" oppure "Configurare i trap SNMP".



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

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

Monitorare gli stati di connessione del nodo

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

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

Visualizzare gli avvisi correnti e risolti

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

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

Facoltativamente, hai guardato il video: "Video: Panoramica degli avvisi per StorageGRID 11,8"

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

Intestazione di colonna	Descrizione
Nome o titolo	Il nome dell'avviso e la relativa descrizione.

Intestazione di colonna	Descrizione
Severità	La severità dell'avviso. Per gli avvisi correnti, se sono raggruppati più avvisi, la riga del titolo mostra il numero di istanze di tale avviso che si verificano a ogni livello di gravità. **Critico**: Si verifica una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. È necessario risolvere immediatamente il problema sottostante. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati. **Major**: Si verifica una condizione anomala che influisce sulle operazioni correnti o si avvicina alla soglia per un avviso critico. È necessario analizzare gli avvisi principali e risolvere eventuali problemi sottostanti per assicurarsi che le condizioni anomale non interrompano il normale funzionamento di un nodo o servizio StorageGRID. **Minore**: Il sistema funziona normalmente, ma esiste una condizione anomala che potrebbe influire sulla capacità di funzionamento del sistema se continua. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per garantire che non causino problemi più gravi.
Tempo di attivazione	**Current alerts** (Avvisi correnti): La data e l'ora in cui l'avviso è stato attivato nell'ora locale e in UTC. Se vengono raggruppati più avvisi, la riga del titolo mostra l'ora dell'istanza più recente dell'avviso (*NEST*) e l'istanza più vecchia dell'avviso (*OLDEST*). **Resolved alerts** (Avvisi risolti): Quanto tempo fa è stato attivato l'avviso.
Sito/nodo	Il nome del sito e del nodo in cui si è verificato o si è verificato l'avviso.
Stato	Se l'avviso è attivo, tacitato o risolto. Se vengono raggruppati più avvisi e nell'elenco a discesa viene selezionato **tutti gli avvisi**, la riga del titolo mostra quante istanze di tale avviso sono attive e quante istanze sono state tacitati.
Tempo risolto (solo avvisi risolti)	Quanto tempo fa l'avviso è stato risolto.
Valori correnti o *valori di dati*	Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso **Low Object Data Storage** includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata. **Nota:** se vengono raggruppati più avvisi correnti, 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 causato l'attivazione dell'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso **Low Object Data Storage** includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.

Fasi

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

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

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

     La pagina degli avvisi correnti viene aggiornata ogni due minuti.

2. Per espandere i gruppi di avvisi, selezionare il cart inferiore ⌄. Per chiudere i singoli avvisi in un gruppo, selezionare il caret up ⌃oppure selezionare il nome del gruppo.
3. Per visualizzare singoli avvisi invece di gruppi di avvisi, deselezionare la casella di controllo **Group alerts** (Avvisi di gruppo).
4. Per ordinare gli avvisi o i gruppi di avvisi correnti, selezionare le frecce su/giù ⇅ in ogni intestazione di colonna.
   - Quando si seleziona **Group alerts** (Avvisi di gruppo), vengono ordinati sia i gruppi di avvisi che i singoli avvisi all'interno di ciascun gruppo. Ad esempio, è possibile ordinare gli avvisi in un gruppo in base all'ora * attivata per trovare l'istanza più recente di un avviso specifico.
   - Quando l'opzione **Group alerts** (Avvisi di gruppo) viene deselezionata, viene ordinato l'intero elenco di avvisi. Ad esempio, è possibile ordinare tutti gli avvisi in base a **nodo/sito** per visualizzare tutti gli avvisi relativi a un nodo specifico.
5. Per filtrare gli avvisi correnti in base allo stato (**tutti gli avvisi**, **attivi** o **silenziati**, utilizzare il menu a discesa nella parte superiore della tabella.

   Vedere "Tacitare le notifiche di avviso".

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

7. Per visualizzare i dettagli di un avviso specifico, selezionarlo. Una finestra di dialogo fornisce dettagli e azioni consigliate per l'avviso selezionato.
8. (Facoltativo) per un avviso specifico, selezionare Silence this alert (tacita questo avviso) per tacitare la regola che ha causato l'attivazione dell'avviso.

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

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

9. Per visualizzare le condizioni correnti della regola di avviso:
   a. Dai dettagli dell'avviso, selezionare **View conditions** (Visualizza condizioni).

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

   b. Per chiudere la finestra a comparsa, fare clic in un punto qualsiasi all'esterno della finestra a comparsa.
10. Facoltativamente, selezionare **Edit rule** (Modifica regola) per modificare la regola di avviso che ha causato l'attivazione dell'avviso.

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

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

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

Monitorare la capacità dello storage

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

StorageGRID memorizza i dati degli oggetti e i metadati degli oggetti separatamente e riserva una quantità specifica di spazio per un database Cassandra distribuito che contiene metadati degli oggetti. Monitorare la quantità totale di spazio consumata per gli oggetti e per i metadati degli oggetti, nonché le tendenze della quantità di spazio consumata per ciascuno di essi. Ciò consente di pianificare in anticipo l'aggiunta di nodi ed evitare interruzioni del servizio.

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

Monitorare la capacità di storage per l'intero grid

Monitorare la capacità di storage complessiva del grid per garantire che rimanga spazio libero adeguato per i dati degli oggetti e i metadati degli oggetti. Comprendere come la capacità dello storage cambia nel tempo può

aiutarti a pianificare l'aggiunta di nodi o volumi di storage prima che la capacità dello storage utilizzabile del grid venga consumata.

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

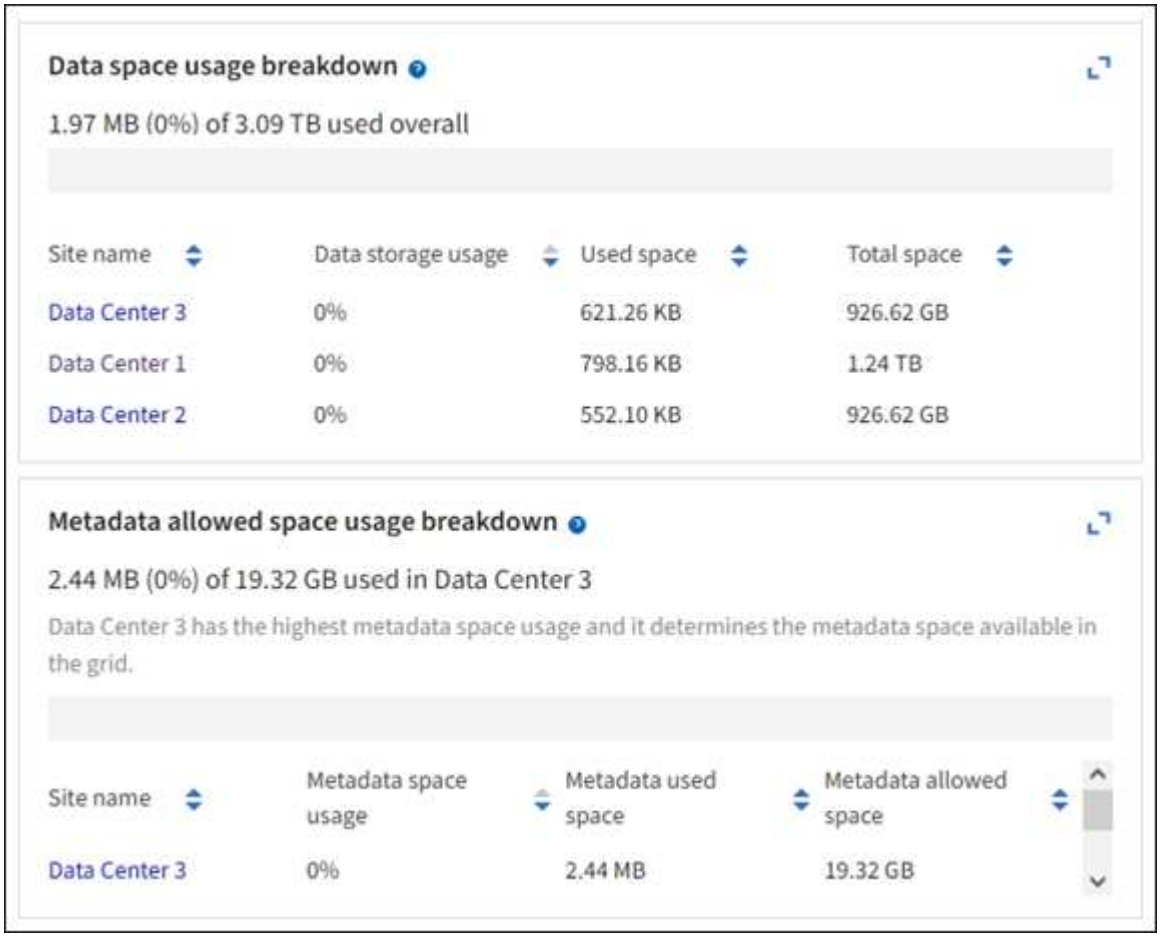
Fasi

1. Valutare la quantità di storage disponibile per l'intero grid e per ciascun data center.

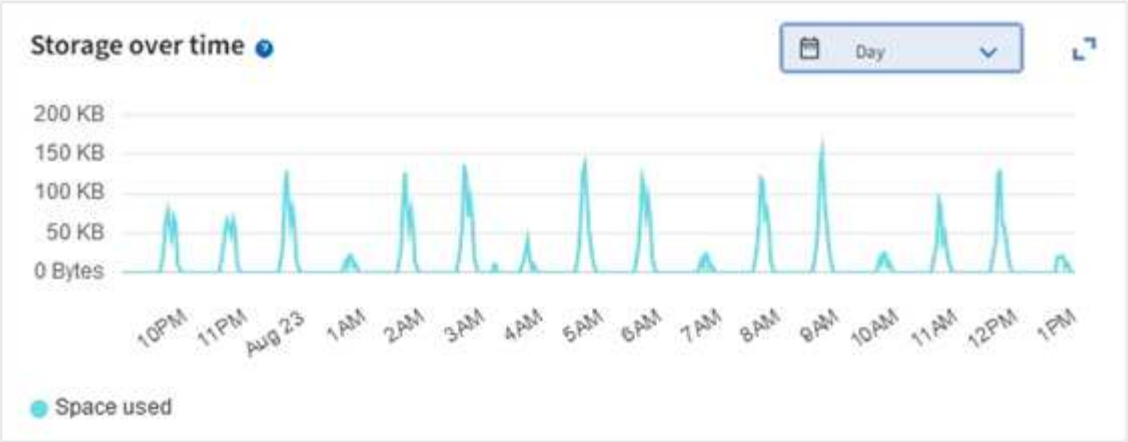
   a. Selezionare **Dashboard > Overview**.

   b. Prendere nota dei valori riportati nelle schede di analisi dell'utilizzo dello spazio dati e delle schede di analisi dell'utilizzo dello spazio consentito dai metadati. Ciascuna scheda elenca una percentuale di utilizzo dello storage, la capacità dello spazio utilizzato e lo spazio totale disponibile o consentito dal sito.

   > Il riepilogo non include i supporti di archiviazione.



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



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

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

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

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

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

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

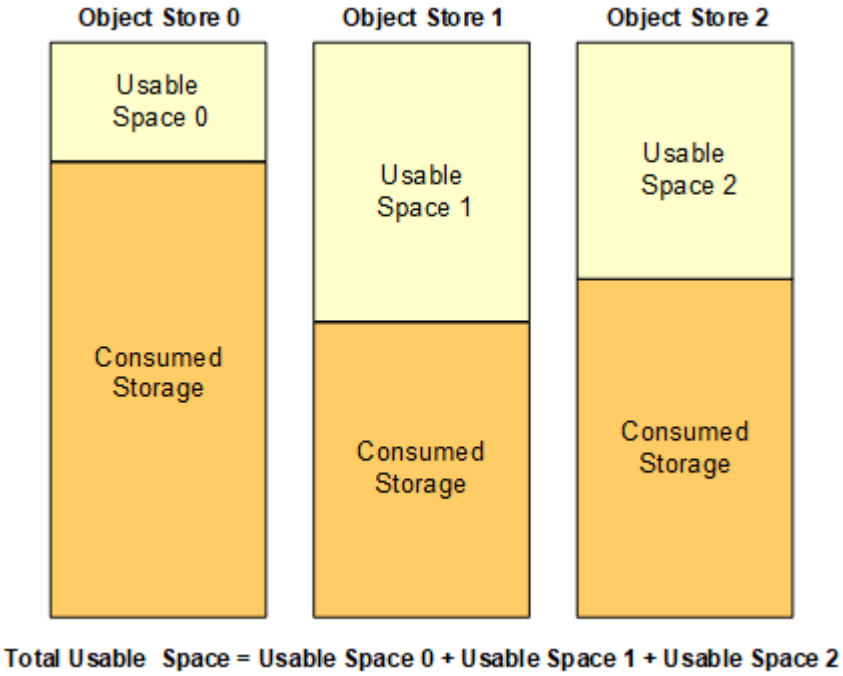
Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, consultare "Istruzioni per espandere StorageGRID".

Monitorare la capacità di storage per ciascun nodo di storage

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

A proposito di questa attività

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



Fasi

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

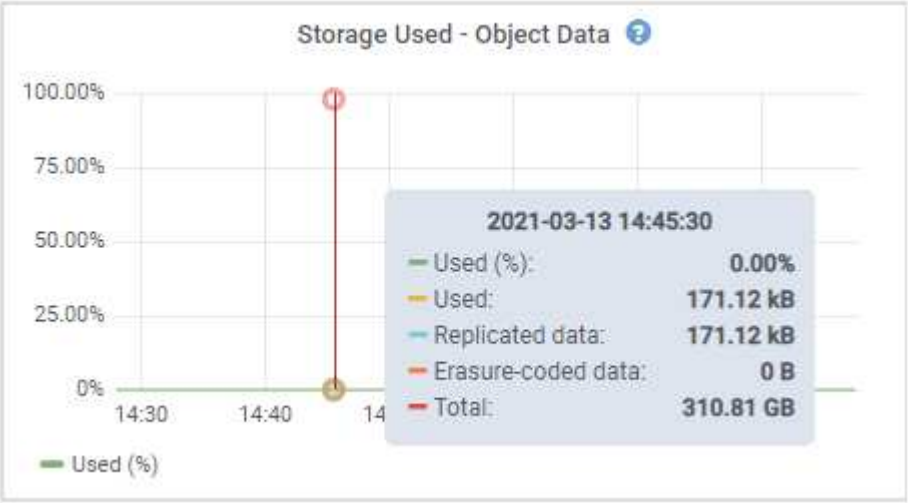
   Vengono visualizzati i grafici e le tabelle del nodo.

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

   Vengono visualizzati i seguenti valori:

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

- **Total**: Quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è `storagegrid_storage_utilization_data_bytes` metrico.



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

> Per visualizzare i grafici di questi valori, fare clic sulle icone del grafico Nelle colonne disponibili.

Disk devices

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

Volumes

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

Object stores

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

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

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

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

   Per ulteriori informazioni sulla pianificazione di un'espansione dello storage, consultare "Istruzioni per espandere StorageGRID".

Il "Storage dei dati a oggetti basso" L'avviso viene attivato quando rimane spazio insufficiente per memorizzare i dati dell'oggetto su un nodo di storage.

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

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

A proposito di questa attività

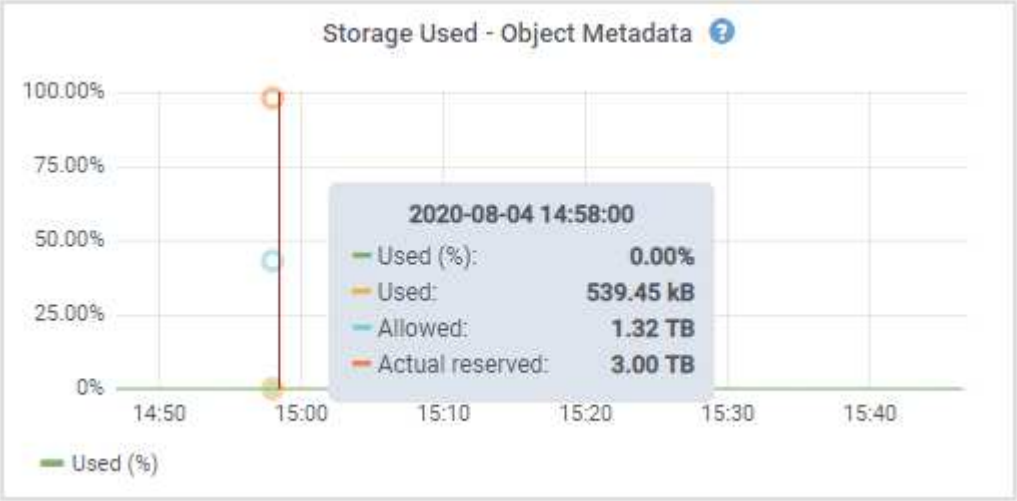
StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di storage di ogni sito utilizzando lo spazio riservato ai metadati sul volume di storage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

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

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

Fasi

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



Utilizzato (%)

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

Metriche Prometheus: `storagegrid_storage_utilization_metadata_bytes` e. `storagegrid_storage_utilization_metadata_allowed_bytes`

Utilizzato

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

Metrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Consentito

Lo spazio consentito per i metadati dell'oggetto su questo nodo di storage. Per informazioni su come determinare questo valore per ciascun nodo di storage, vedere "Descrizione completa dello spazio consentito per i metadati".

Metrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Riservato

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

La metrica Prometheus verrà aggiunta in una release futura.

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

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

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

Quando si aggiungono nuovi nodi, il sistema ribilancia automaticamente i metadati degli oggetti in tutti i nodi di storage all'interno del sito. Vedere "Istruzioni per espandere un sistema StorageGRID".

Monitorare le previsioni di utilizzo dello spazio

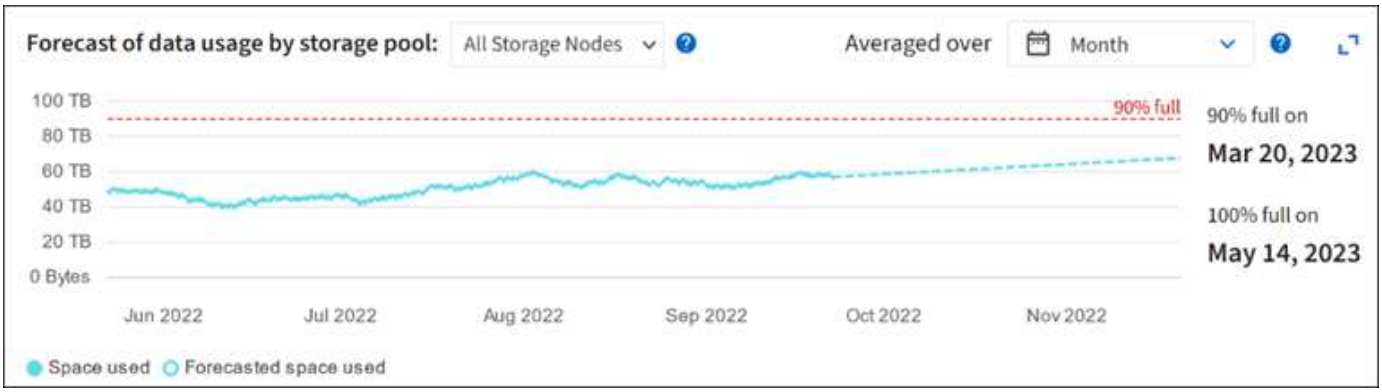
Monitorare le previsioni di utilizzo dello spazio per i dati utente e i metadati per stimare quando sarà necessario "espandere una griglia".

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

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

Fasi

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



Monitorare la gestione del ciclo di vita delle informazioni

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

A proposito di questa attività

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

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

USA la scheda del pannello di controllo di Grid Manager

Fasi

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

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

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

Utilizzare la pagina NODI

Fasi

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

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

1. Selezionare **NODI**.

2. Selezionare ***grid name*** > **ILM**.
3. Posizionare il cursore sul grafico della coda ILM per visualizzare il valore dei seguenti attributi in un determinato momento:
   - **Oggetti accodati (da operazioni client)**: Il numero totale di oggetti in attesa di valutazione ILM a causa delle operazioni del client (ad esempio, acquisizione).
   - **Oggetti accodati (da tutte le operazioni)**: Il numero totale di oggetti in attesa di valutazione ILM.
   - **Scan rate (objects/sec)**: La velocità con cui gli oggetti nella griglia vengono sottoposti a scansione e messi in coda per ILM.
   - **Evaluation rate (objects/sec)**: La velocità corrente alla quale gli oggetti vengono valutati rispetto alla policy ILM nella griglia.
4. Nella sezione ILM Queue (coda ILM), esaminare i seguenti attributi.

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

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

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

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

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

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

Monitorare le risorse di rete e di sistema

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

Monitorare le connessioni di rete e le performance

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

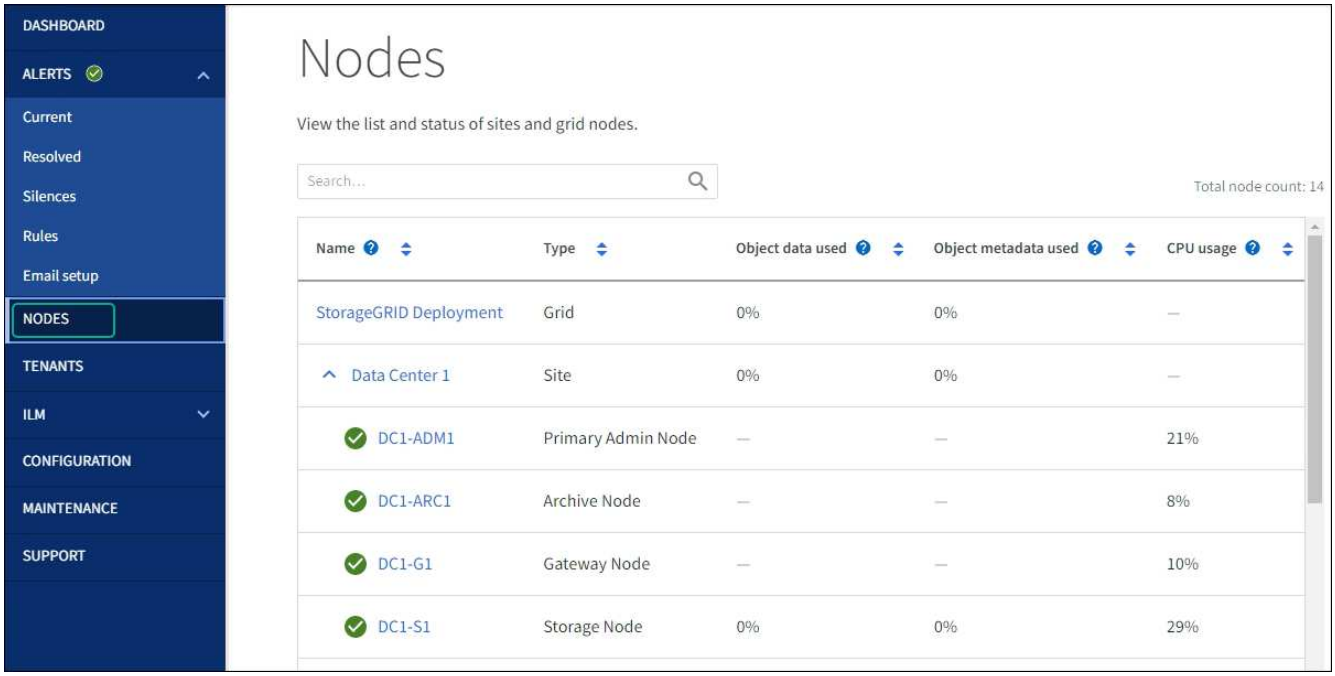
Utilizza Grid Manager per monitorare la connettività e le performance di rete, in modo da poter risolvere tempestivamente qualsiasi problema.

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

Fasi

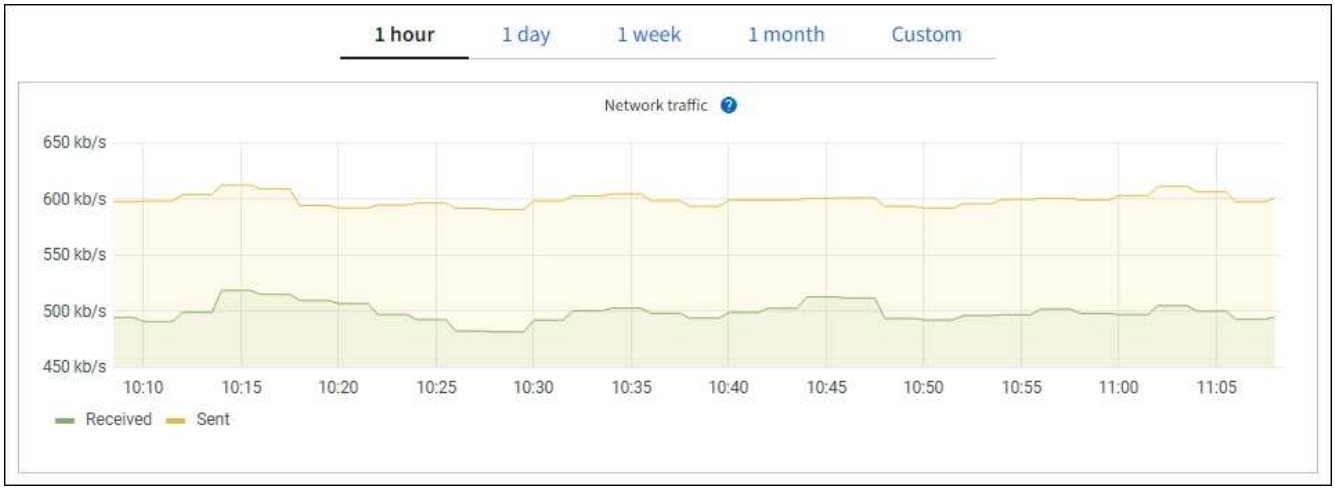
1. Selezionare **NODI**.

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



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

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



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

Network interfaces

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

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

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

Network communication

Receive

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

Transmit

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

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

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

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

Traffic Classification Policies

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

+ Create | Edit | Remove | Metrics

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

Displaying 2 traffic classification policies.

a. Per visualizzare i grafici che mostrano le metriche di rete associate a un criterio, selezionare il pulsante di opzione a sinistra del criterio, quindi fare clic su **metriche**.

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

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

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

Informazioni correlate

"Visualizzare la scheda rete"

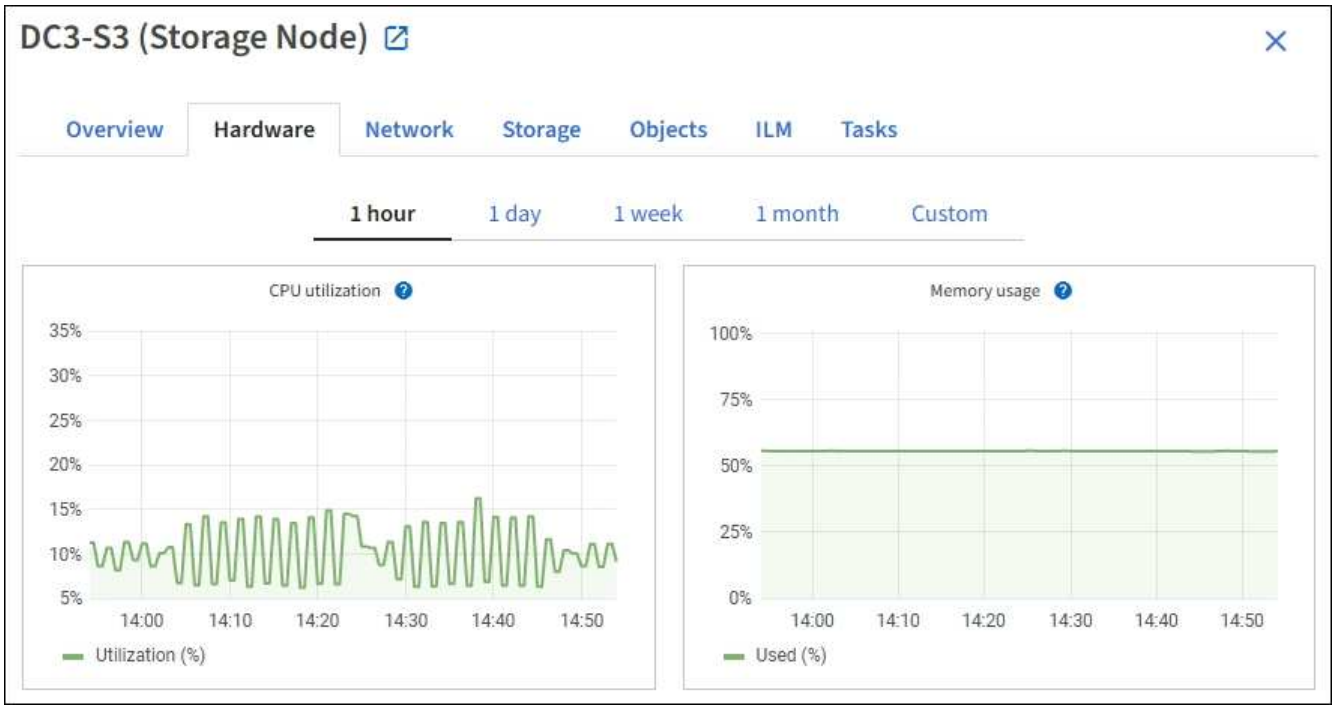
"Monitorare gli stati di connessione del nodo"

Monitorare le risorse a livello di nodo

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

Fasi

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



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

Informazioni correlate

"Visualizza informazioni sui nodi di storage dell'appliance"

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

Monitorare l'attività del tenant

Tutte le attività dei client S3 e Swift sono associate agli account del tenant StorageGRID. È possibile utilizzare Grid Manager per monitorare l'utilizzo dello storage o il traffico di rete di tutti i tenant o di uno specifico tenant. È possibile utilizzare il registro di controllo o le dashboard Grafana per ottenere informazioni più dettagliate sull'utilizzo di StorageGRID da parte dei tenant.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".

Visualizza tutti i tenant

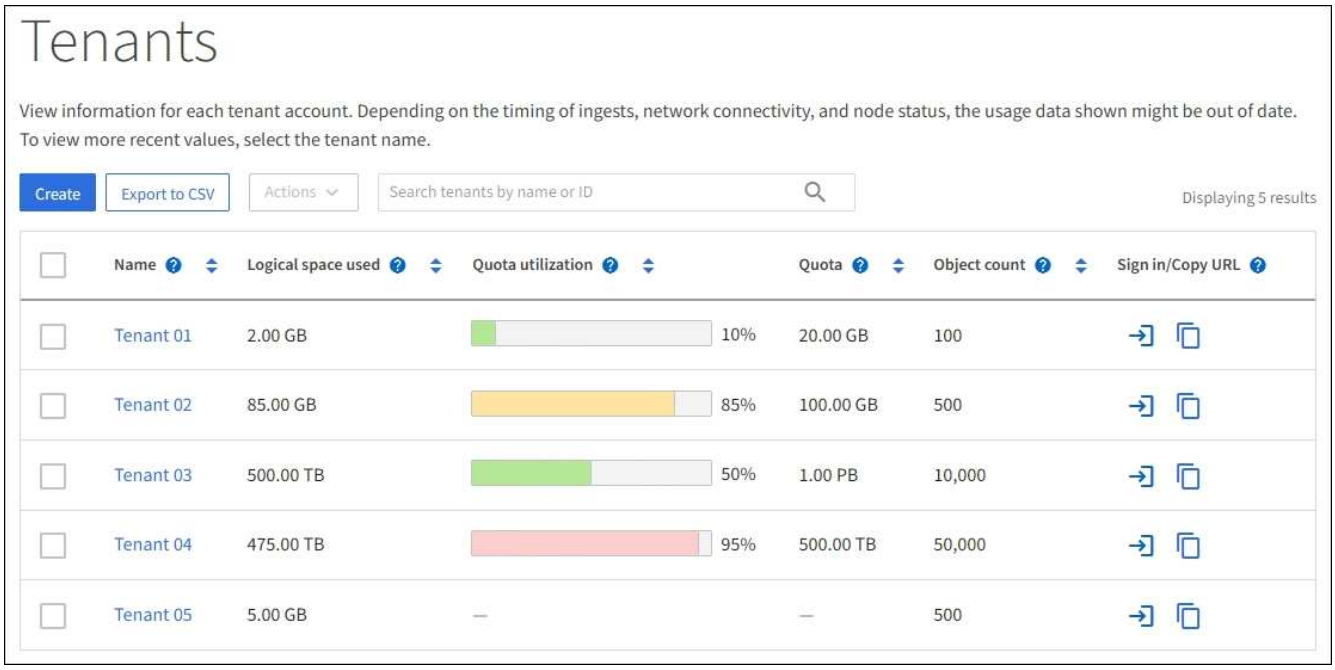
La pagina tenant mostra le informazioni di base per tutti gli account tenant correnti.

Fasi

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

   Per ogni tenant vengono elencati lo spazio logico utilizzato, l'utilizzo della quota, la quota e il numero di oggetti. Se non viene impostata una quota per un tenant, i campi relativi all'utilizzo della quota e alla quota contengono un trattino (& 8212;).

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



3. Se lo si desidera, accedere a un account tenant selezionando il collegamento di accesso Nella colonna **URL di accesso/copia**.
4. Se si desidera, copiare l'URL della pagina di accesso del tenant selezionando il collegamento URL della copia Nella colonna **URL di accesso/copia**.

5. In alternativa, selezionare **Export to CSV** (Esporta in CSV) per visualizzare ed esportare un `.csv` file contenente i valori di utilizzo per tutti i tenant.

   Viene richiesto di aprire o salvare `.csv` file.

   Il contenuto di `.csv` il file è simile al seguente esempio:

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

   È possibile aprire `.csv` file in un'applicazione per fogli di calcolo o utilizzarlo in automazione.

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

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

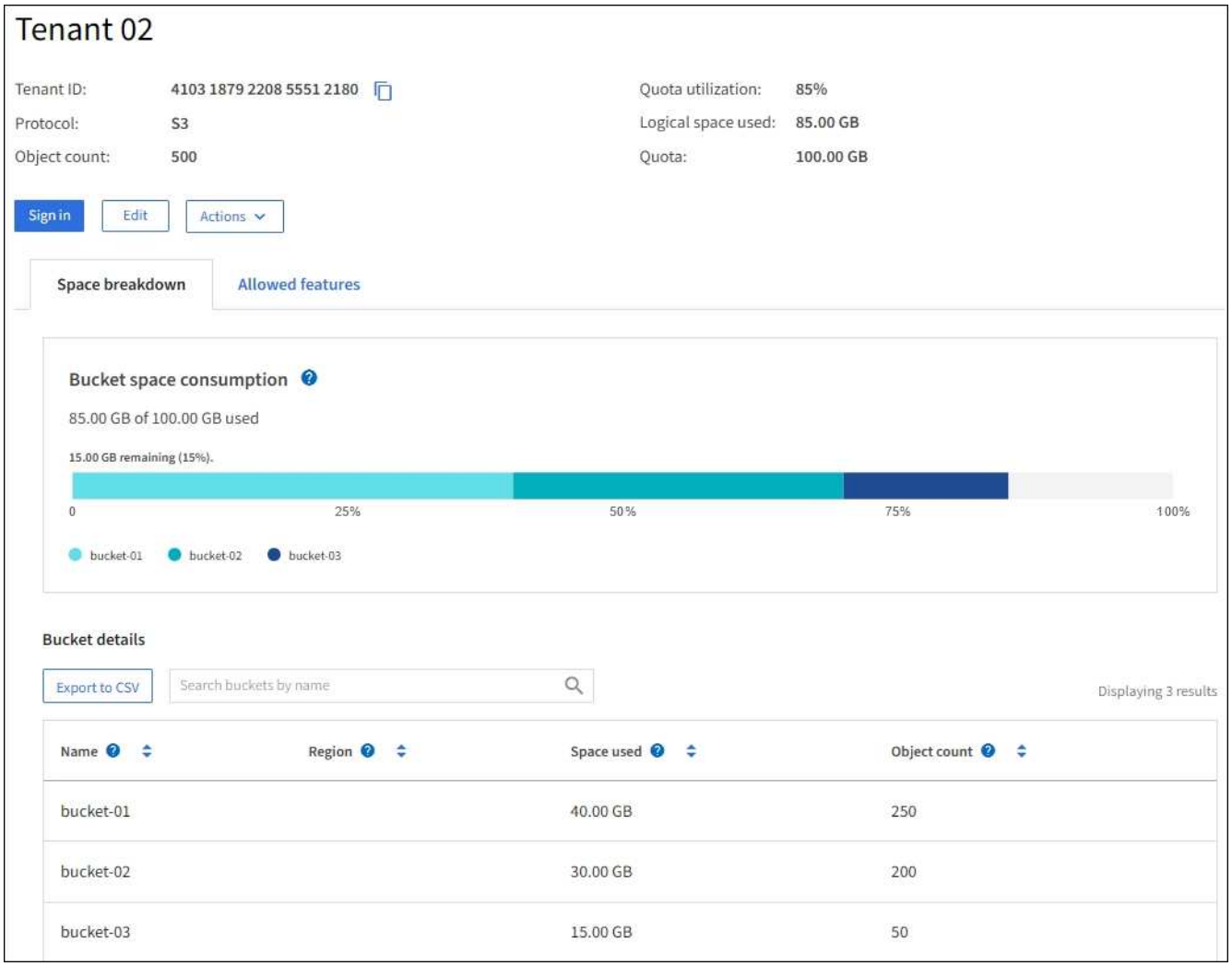
Visualizzare un tenant specifico

È possibile visualizzare i dettagli di un tenant specifico.

Fasi

1. Selezionare il nome del tenant dalla pagina tenant.

   Viene visualizzata la pagina dei dettagli del tenant.



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

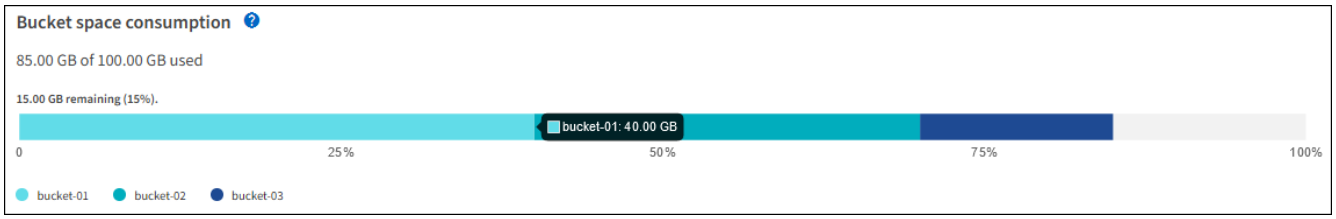
   Questa sezione della pagina dei dettagli fornisce informazioni riepilogative per il tenant, tra cui il numero di oggetti del tenant, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

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

   Questo grafico mostra il consumo totale di spazio per tutti i bucket S3 (o container Swift) del tenant.

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

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



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

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

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

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

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

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

   Il contenuto di un singolo tenant S3 `.csv` il file è simile al seguente esempio:

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

   È possibile aprire `.csv` file in un'applicazione per fogli di calcolo o utilizzarlo in automazione.

6. Se si desidera, selezionare la scheda **funzioni consentite** per visualizzare un elenco delle autorizzazioni e delle funzionalità attivate per il tenant. Vedere "Modificare l'account tenant" se è necessario modificare una di queste impostazioni.
7. Se il tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, selezionare la scheda **federazione griglia** per ulteriori informazioni sulla connessione.

   Vedere "Che cos'è la federazione di griglie?" e. "Gestire i tenant consentiti per la federazione di grid".

Visualizzare il traffico di rete

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

Fasi

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

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

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

Vedere "Gestire le policy di classificazione del traffico" per ulteriori informazioni.

Utilizzare il registro di controllo

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

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

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

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

Vedere "Esaminare i registri di audit" per ulteriori informazioni.

Utilizza le metriche Prometheus

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

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

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

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

Vedere "Rivedere le metriche di supporto" per ulteriori informazioni.

Monitoraggio di operazioni client S3 e Swift

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

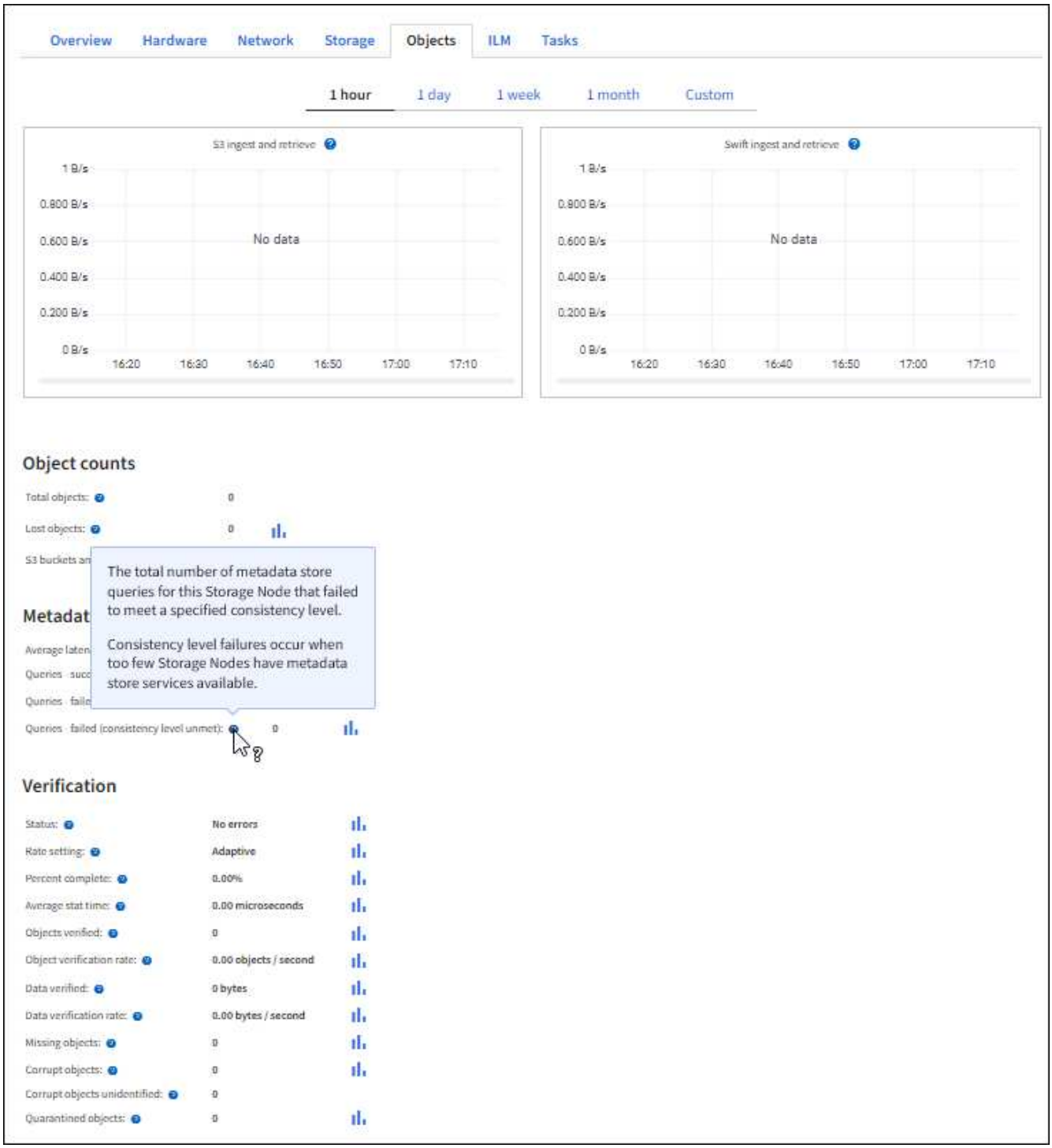
Fasi

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

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

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

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



Monitorare le operazioni di bilanciamento del carico

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

A proposito di questa attività

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

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

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

Per ulteriori informazioni, vedere "Configurare le connessioni client S3 e Swift".

Fasi

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

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

   d. Per ogni nodo che deve distribuire attivamente le richieste client, selezionare "Scheda bilanciamento del carico".
   e. Esaminare il grafico del traffico di richiesta del bilanciamento del carico dell'ultima settimana per assicurarsi che il nodo stia distribuendo attivamente le richieste.

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

   f. Esaminare il grafico del tasso di richiesta in entrata del bilanciamento del carico dell'ultima settimana per esaminare il throughput degli oggetti del nodo.
   g. Ripetere questi passaggi per ogni nodo amministratore o nodo gateway nel sistema StorageGRID.
   h. Facoltativamente, utilizzare le policy di classificazione del traffico per visualizzare un'analisi più dettagliata del traffico fornito dal servizio Load Balancer.
2. Verificare che queste richieste vengano distribuite uniformemente ai nodi di storage.
   a. Selezionare ***Storage Node*** > **LDR** > **HTTP**.
   b. Esaminare il numero di **sessioni in entrata attualmente stabilite**.
   c. Ripetere l'operazione per ogni nodo di storage nella griglia.

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

Monitorare le connessioni a federazione di griglie

È possibile monitorare le informazioni di base su tutti "connessioni a federazione di griglie", Informazioni dettagliate su una connessione specifica o metriche Prometheus sulle operazioni di replica cross-grid. È possibile monitorare una connessione da entrambe le griglie.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su una delle griglie utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per la griglia a cui si è effettuato l'accesso.

Visualizza tutte le connessioni

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

Fasi

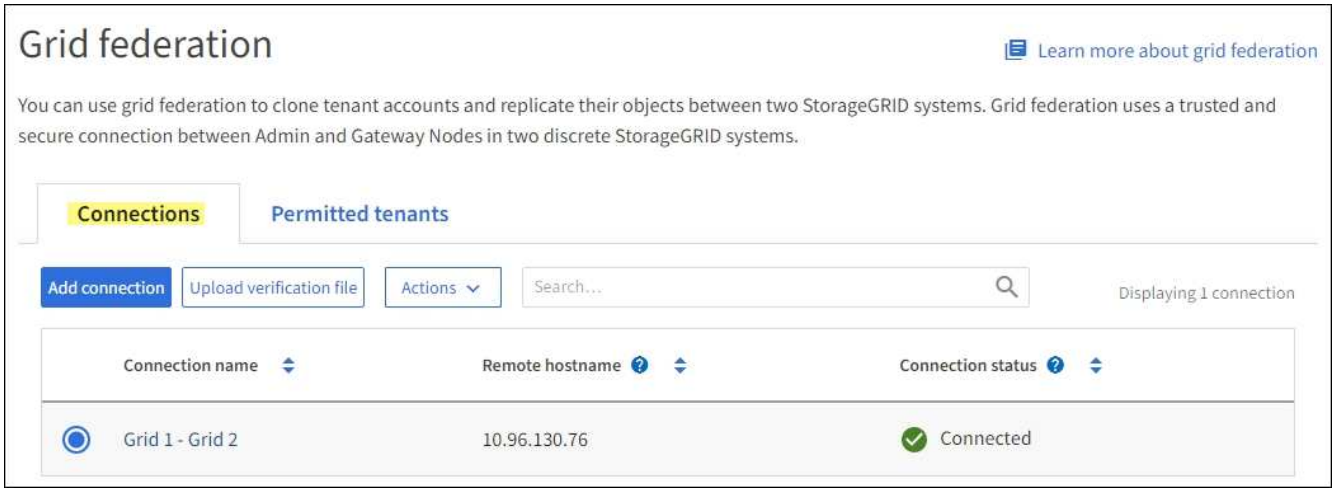
1. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.

   Viene visualizzata la pagina Grid Federation.

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

   Da questa scheda è possibile:

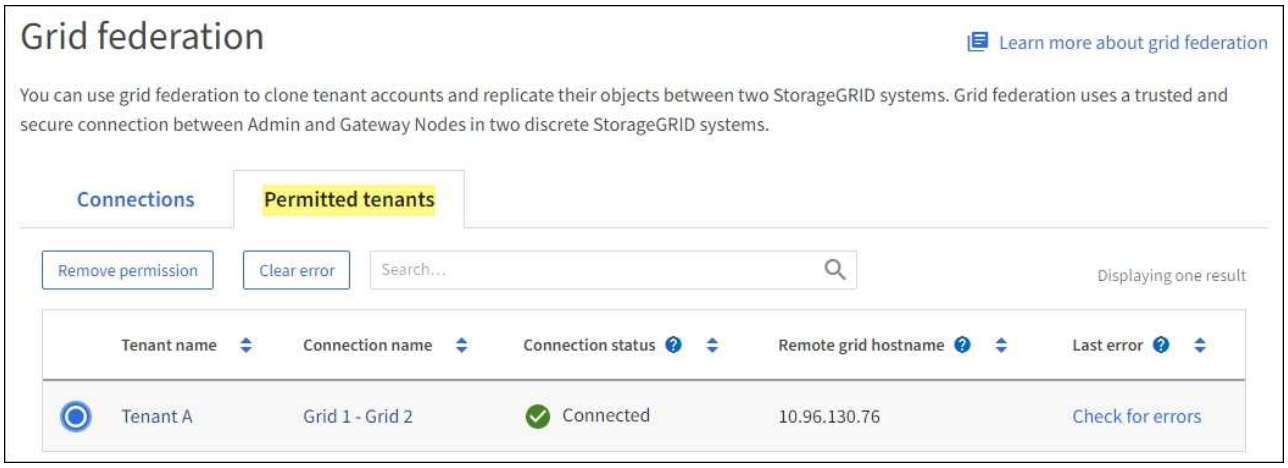
   - "Creare una nuova connessione".
   - Selezionare una connessione esistente a. "modifica o verifica".



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

   Da questa scheda è possibile:

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



Visualizza una connessione specifica

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

Fasi

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

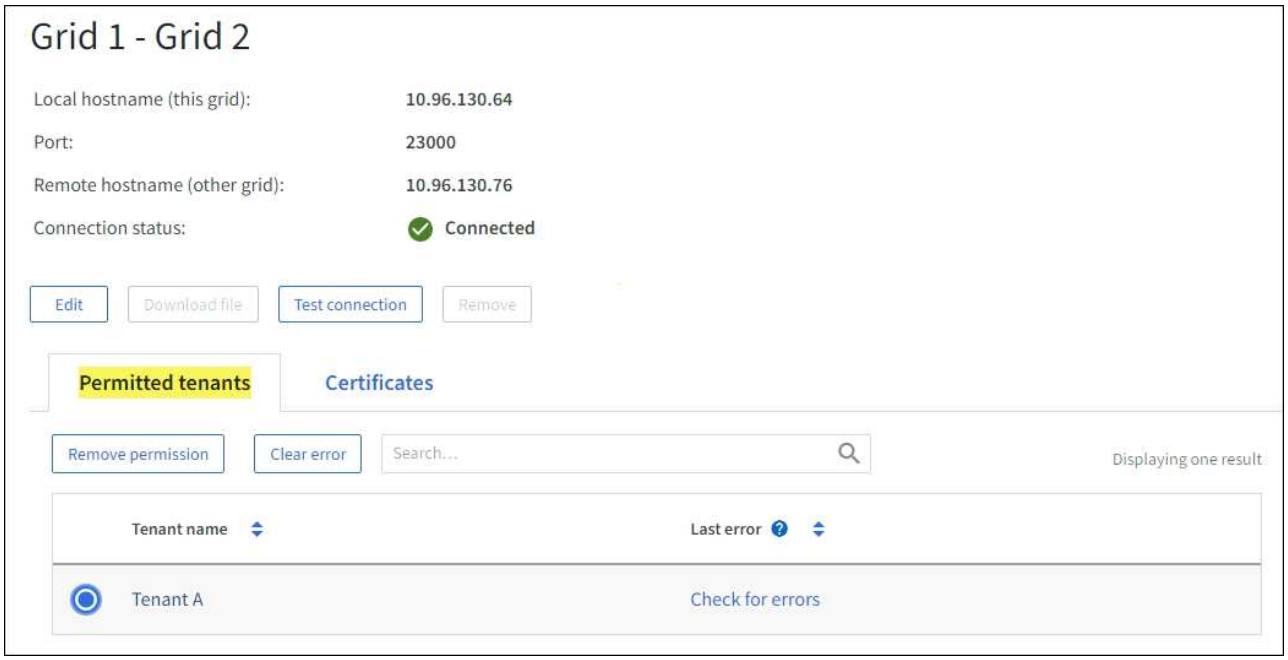
   Dalla pagina dei dettagli per la connessione, è possibile:

   - Consultare le informazioni di base sullo stato della connessione, inclusi i nomi host locali e remoti, la porta e lo stato della connessione.
   - Selezionare una connessione a. "modifica, verifica o rimozione".

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

   Da questa scheda è possibile:

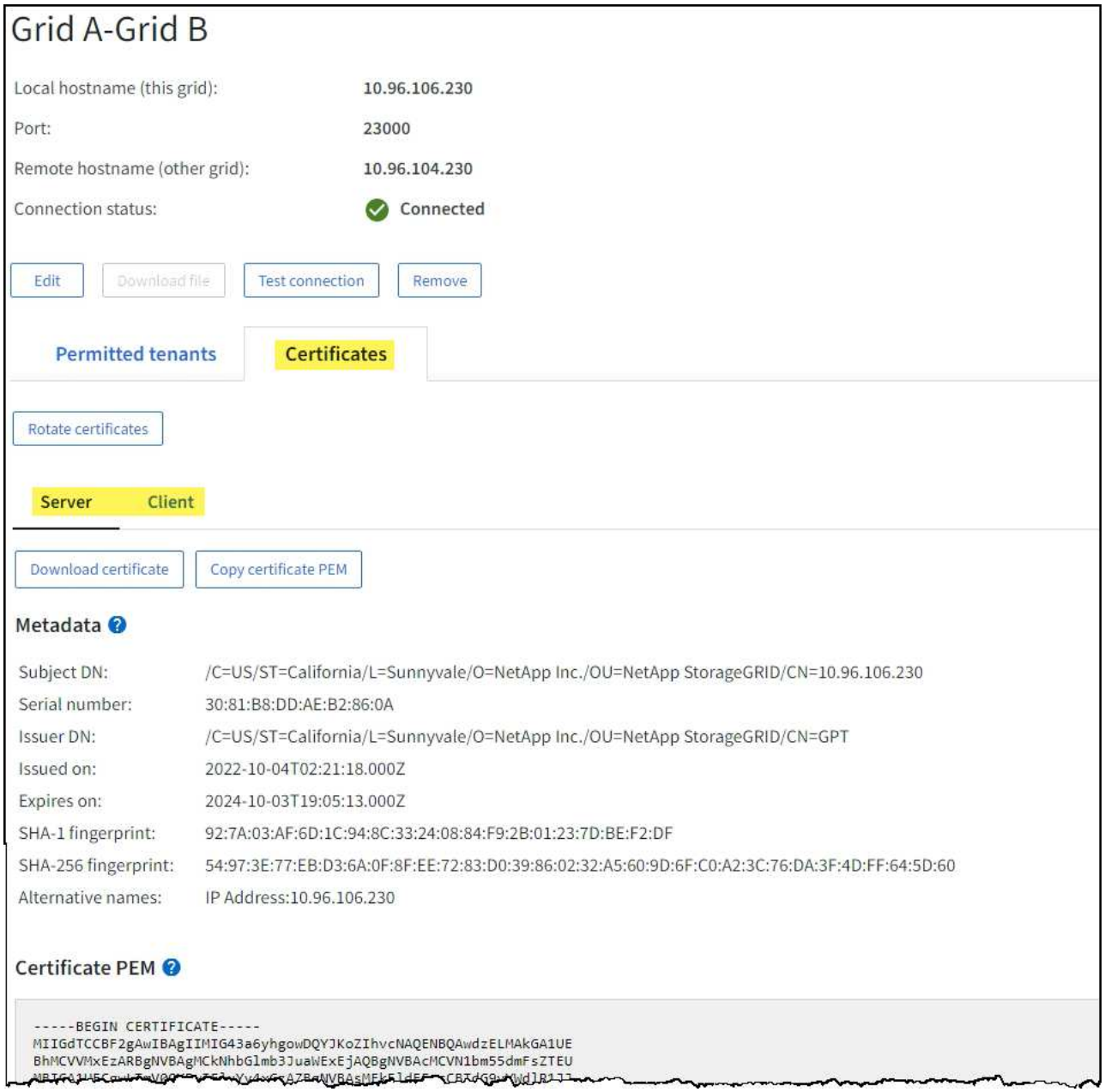
   - "Visualizza la pagina dei dettagli per ciascun tenant consentito".
   - "Rimuovere l'autorizzazione di un tenant" per utilizzare la connessione.
   - Verificare la presenza di errori di replica tra griglie e cancellare l'ultimo errore. Vedere "Risolvere i problemi relativi agli errori di federazione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



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

   Da questa scheda è possibile:

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



Analisi delle metriche di replica cross-grid

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

Fasi

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

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

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

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

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

Monitorare la capacità di archiviazione

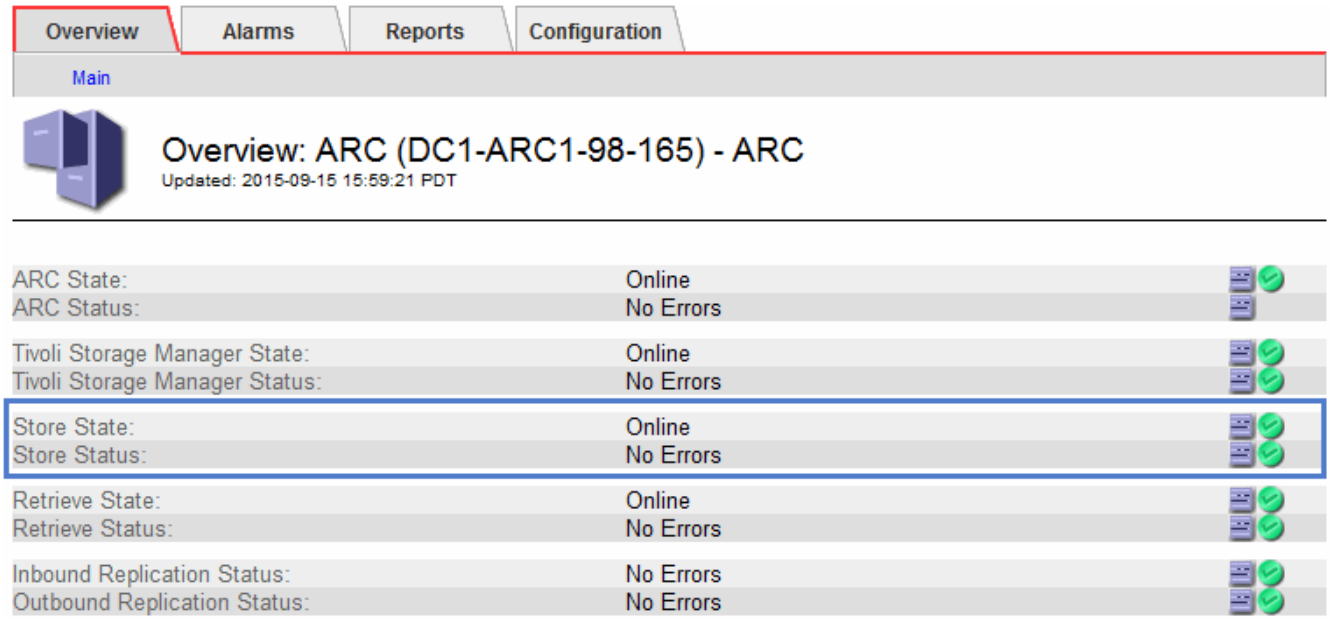
Non è possibile monitorare direttamente la capacità di un sistema storage di archiviazione esterno attraverso il sistema StorageGRID. Tuttavia, è possibile controllare se il nodo di archiviazione può ancora inviare i dati degli oggetti alla destinazione di archiviazione, il che potrebbe indicare che è necessaria un'espansione dei supporti di archiviazione.

A proposito di questa attività

È possibile monitorare il componente Store per verificare se il nodo di archiviazione è ancora in grado di inviare i dati dell'oggetto al sistema di storage di archiviazione di destinazione. L'allarme Store Failures (ARVF) potrebbe anche indicare che il sistema storage di archiviazione di destinazione ha raggiunto la capacità e non può più accettare i dati degli oggetti.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC> Overview> Main**.
3. Controllare gli attributi Store state (Stato archiviazione) e Store Status (Stato archiviazione) per verificare che il componente Store sia online senza errori.



Un componente offline Store o un componente con errori potrebbe indicare che il sistema storage di archiviazione di destinazione non può più accettare dati a oggetti perché ha raggiunto la capacità.

Avvisi e allarmi

Gestire avvisi e allarmi: Panoramica

Il sistema di allerta StorageGRID è progettato per informare l'utente sui problemi operativi

che richiedono attenzione. Il sistema di allarme legacy è obsoleto.

Sistema di allerta

Il sistema di allerta è progettato per essere lo strumento principale per il monitoraggio di eventuali problemi che potrebbero verificarsi nel sistema StorageGRID. Il sistema di allerta fornisce un'interfaccia di facile utilizzo per rilevare, valutare e risolvere i problemi.

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

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

Sistema di allarme legacy

Analogamente agli avvisi, gli allarmi vengono attivati a livelli di severità specifici quando gli attributi raggiungono valori di soglia definiti. Tuttavia, a differenza degli avvisi, vengono attivati molti allarmi per gli eventi che è possibile ignorare in modo sicuro, il che potrebbe causare un numero eccessivo di notifiche e-mail o SNMP.

> Il sistema di allarme è obsoleto e verrà rimosso in una versione futura. Se si utilizzano ancora allarmi legacy, è necessario passare completamente al sistema di allarme il prima possibile.

Quando viene attivato un allarme, si verificano le seguenti azioni:

- L'allarme viene visualizzato nella pagina **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.
- Viene inviata una notifica via email, a condizione che sia stato configurato un server SMTP e siano state configurate una o più mailing list.
- È possibile che venga inviata una notifica SNMP, purché sia stato configurato l'agente SNMP di StorageGRID. (Le notifiche SNMP non vengono inviate per tutti gli allarmi o le gravità degli allarmi).

Confrontare avvisi e allarmi

Esistono diverse analogie tra il sistema di allarme e il sistema di allarme legacy, ma il sistema di allarme offre notevoli vantaggi ed è più semplice da utilizzare.

Fare riferimento alla seguente tabella per informazioni su come eseguire operazioni simili.

	Avvisi	Allarmi (sistema precedente)
Come si visualizzano gli avvisi o gli allarmi attivi?	• Selezionare il collegamento **Current alerts** (Avvisi correnti) nella dashboard. • Selezionare l'avviso nella pagina **NODI** > **Panoramica**. • Selezionare **ALERTS** > **current**. "Visualizzare gli avvisi correnti"	Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**. "Gestire gli allarmi (sistema legacy)"
Cosa causa l'attivazione di un allarme o di un allarme?	Gli avvisi vengono attivati quando un'espressione Prometheus in una regola di avviso valuta true per la condizione di attivazione e la durata specifiche. "Visualizzare le regole degli avvisi"	Gli allarmi vengono attivati quando un attributo StorageGRID raggiunge un valore di soglia. "Gestire gli allarmi (sistema legacy)"
Se viene attivato un allarme o un allarme, come si risolve il problema sottostante?	Le azioni consigliate per un avviso sono incluse nelle notifiche e-mail e sono disponibili nelle pagine Avvisi di Grid Manager. Come richiesto, ulteriori informazioni sono fornite nella documentazione di StorageGRID. "Riferimenti agli avvisi"	Per informazioni su un allarme, selezionare il nome dell'attributo oppure cercare un codice di allarme nella documentazione di StorageGRID. "Riferimento allarmi (sistema legacy)"
Dove è possibile visualizzare un elenco di avvisi o allarmi risolti?	Selezionare **ALERTS** > **resolved**. "Visualizzare gli avvisi correnti e risolti"	Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi storici**. "Gestire gli allarmi (sistema legacy)"
Dove posso gestire le impostazioni?	Selezionare **ALERTS** > **Rules**. "Gestire gli avvisi"	Selezionare **SUPPORT**. Quindi, utilizzare le opzioni nella sezione **Allarmi (legacy)** del menu. "Gestire gli allarmi (sistema legacy)"

	Avvisi	Allarmi (sistema precedente)
Quali autorizzazioni di gruppo utenti sono necessarie?	• Chiunque possa accedere a Grid Manager può visualizzare gli avvisi correnti e risolti. • È necessario disporre dell'autorizzazione Manage alerts (Gestisci avvisi) per gestire silenzi, notifiche di avviso e regole di avviso. "Amministrare StorageGRID"	• Chiunque possa accedere a Grid Manager può visualizzare gli allarmi legacy. • Per riconoscere gli allarmi, è necessario disporre dell'autorizzazione di riconoscimento degli allarmi. • Per gestire gli allarmi globali e le notifiche e-mail, è necessario disporre sia della configurazione della pagina topologia griglia che di altre autorizzazioni di configurazione griglia. "Amministrare StorageGRID"
Come si gestiscono le notifiche e-mail?	Selezionare **ALERTS** > **email setup**. **Nota:** poiché gli allarmi e gli avvisi sono sistemi indipendenti, la configurazione dell'e-mail utilizzata per le notifiche di allarme e AutoSupport non viene utilizzata per le notifiche di avviso. Tuttavia, è possibile utilizzare lo stesso server di posta per tutte le notifiche. "Imposta le notifiche via email per gli avvisi"	Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**. "Gestire gli allarmi (sistema legacy)"
Come si gestiscono le notifiche SNMP?	Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**. "Utilizzare il monitoraggio SNMP"	*Non supportato*
Come posso controllare chi riceve le notifiche?	1. Selezionare **ALERTS** > **email setup**. 2. Nella sezione **destinatari**, immettere un indirizzo e-mail per ciascun elenco o persona che deve ricevere un'e-mail quando si verifica un avviso. "Imposta le notifiche via email per gli avvisi"	1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**. 2. Creazione di una mailing list. 3. Selezionare **Notifiche**. 4. Selezionare la mailing list. "Gestire gli allarmi (sistema legacy)"

	Avvisi	Allarmi (sistema precedente)
Quali nodi di amministrazione inviano notifiche?	Un singolo nodo Admin (il mittente preferito). "Che cos'è un nodo amministratore?"	Un singolo nodo Admin (il mittente preferito). "Che cos'è un nodo amministratore?"
Come posso eliminare alcune notifiche?	1. Selezionare **ALERTS** > **silences**. 2. Selezionare la regola di avviso che si desidera disattivare. 3. Specificare la durata del silenzio. 4. Selezionare il livello di gravità dell'avviso che si desidera disattivare. 5. Selezionare per applicare il silenzio all'intera griglia, a un singolo sito o a un singolo nodo. **Nota**: Se è stato attivato l'agente SNMP, le silenzi sopprimono anche i trap SNMP e informano. "Tacitare le notifiche di avviso"	1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**. 2. Selezionare **Notifiche**. 3. Selezionare una mailing list e selezionare **Sospendi**. "Gestire gli allarmi (sistema legacy)"
Come posso eliminare tutte le notifiche?	Selezionare **ALERTS** > **silences**.quindi, selezionare **All rules**. **Nota**: Se è stato attivato l'agente SNMP, le silenzi sopprimono anche i trap SNMP e informano. "Tacitare le notifiche di avviso"	*Non supportato*
Come si personalizzano le condizioni e i trigger?	1. Selezionare **ALERTS** > **Rules**. 2. Selezionare una regola predefinita da modificare oppure selezionare **Crea regola personalizzata**. "Modificare le regole degli avvisi" "Creare regole di avviso personalizzate"	1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**. 2. Creare un allarme personalizzato globale per ignorare un allarme predefinito o per monitorare un attributo che non ha un allarme predefinito. "Gestire gli allarmi (sistema legacy)"

	Avvisi	Allarmi (sistema precedente)
Come si disattiva un singolo avviso o allarme?	1. Selezionare **ALERTS** > **Rules**. 2. Selezionare la regola e selezionare **Modifica regola**. 3. Deselezionare la casella di controllo **Enabled**. "Disattiva le regole di avviso"	1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**. 2. Selezionare la regola e l'icona Modifica. 3. Deselezionare la casella di controllo **Enabled**. "Gestire gli allarmi (sistema legacy)"

Gestire gli avvisi

Gestisci avvisi: Panoramica

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

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

Per saperne di più:

- Guarda il video: "Video: Panoramica degli avvisi per StorageGRID 11,8"
- Guarda il video: "Video: Utilizzo delle metriche per creare avvisi personalizzati in StorageGRID 11,8"
- Vedere "Riferimenti agli avvisi".

Visualizzare le regole degli avvisi

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

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".
- Facoltativamente, hai guardato il video: "Video: Panoramica degli avvisi per StorageGRID 11,8"

Fasi

1. Selezionare **ALERTS** > **Rules**.

Viene visualizzata la pagina regole di avviso.

Alert Rules Learn more

Alert rules define which conditions trigger specific alerts.

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

Create custom rule | Edit rule | Remove custom rule

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

Displaying 62 alert rules.

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

Intestazione di colonna	Descrizione
Nome	Nome univoco e descrizione della regola di avviso. Vengono elencate per prime le regole di avviso personalizzate, seguite dalle regole di avviso predefinite. Il nome della regola di avviso è l'oggetto delle notifiche e-mail.

Intestazione di colonna	Descrizione
Condizioni	Le espressioni Prometheus che determinano quando viene attivato questo avviso. Un avviso può essere attivato in uno o più dei seguenti livelli di severità, ma non è richiesta alcuna condizione per ogni severità. • **Critico** : Si verifica una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. È necessario risolvere immediatamente il problema sottostante. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati. • **Maggiore** : Si verifica una condizione anomala che influisce sulle operazioni correnti o si avvicina alla soglia per un avviso critico. È necessario analizzare gli avvisi principali e risolvere eventuali problemi sottostanti per assicurarsi che le condizioni anomale non interrompano il normale funzionamento di un nodo o servizio StorageGRID. • **Minore** : Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe influire sulla capacità di funzionamento del sistema se continua a funzionare. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per garantire che non causino problemi più gravi.
Tipo	Il tipo di regola di avviso: • **Default**: Una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificare le condizioni e la durata di una regola di avviso predefinita. Non è possibile rimuovere una regola di avviso predefinita. • **Default***: Una regola di avviso predefinita che include una condizione o una durata modificate. Se necessario, è possibile ripristinare facilmente le impostazioni predefinite originali di una condizione modificata. • **Personalizzato**: Una regola di avviso creata dall'utente. È possibile disattivare, modificare e rimuovere regole di avviso personalizzate.
Stato	Se questa regola di avviso è attualmente attivata o disattivata. Le condizioni per le regole di avviso disabilitate non vengono valutate, quindi non vengono attivati avvisi.

Creare regole di avviso personalizzate

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".
- Conosci già "Metriche Prometheus comunemente utilizzate".

- Hai capito "Sintassi delle query Prometheus".
- Facoltativamente, hai guardato il video: "Video: Utilizzo delle metriche per creare avvisi personalizzati in StorageGRID 11,8".

A proposito di questa attività

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

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

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

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

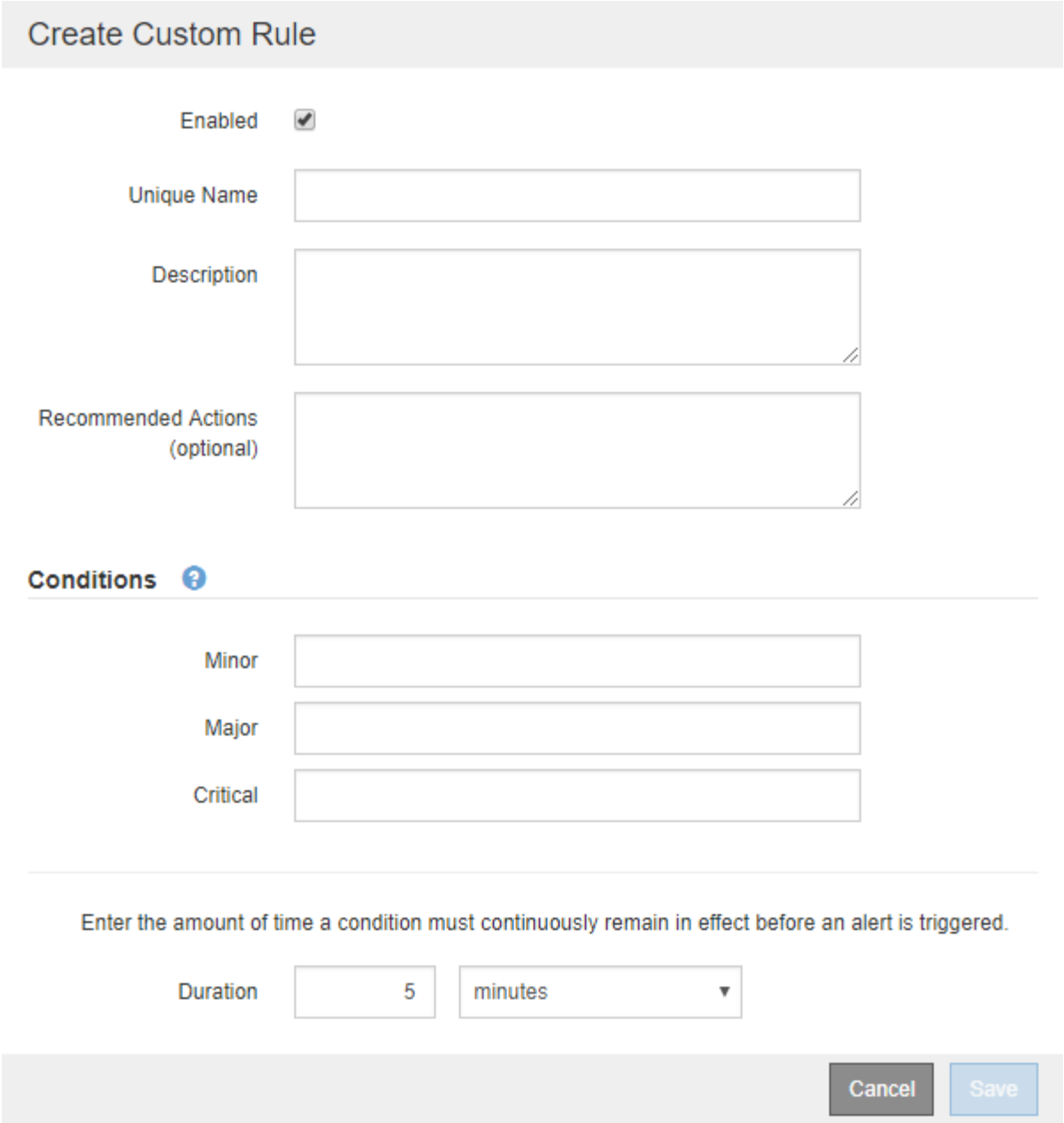
Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

2. Selezionare **Crea regola personalizzata**.

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



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

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

4. Inserire le seguenti informazioni:

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

Campo	Descrizione
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1,024 caratteri.

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

   Un'espressione di base è in genere della forma:

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

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

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

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Per visualizzare le metriche disponibili e verificare le espressioni Prometheus, selezionare l'icona della guida ? E segui il link alla sezione metriche dell'API Grid Management.

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

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

   L'impostazione predefinita è 5 minuti.

7. Selezionare **Salva**.

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

Modificare le regole degli avvisi

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

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

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

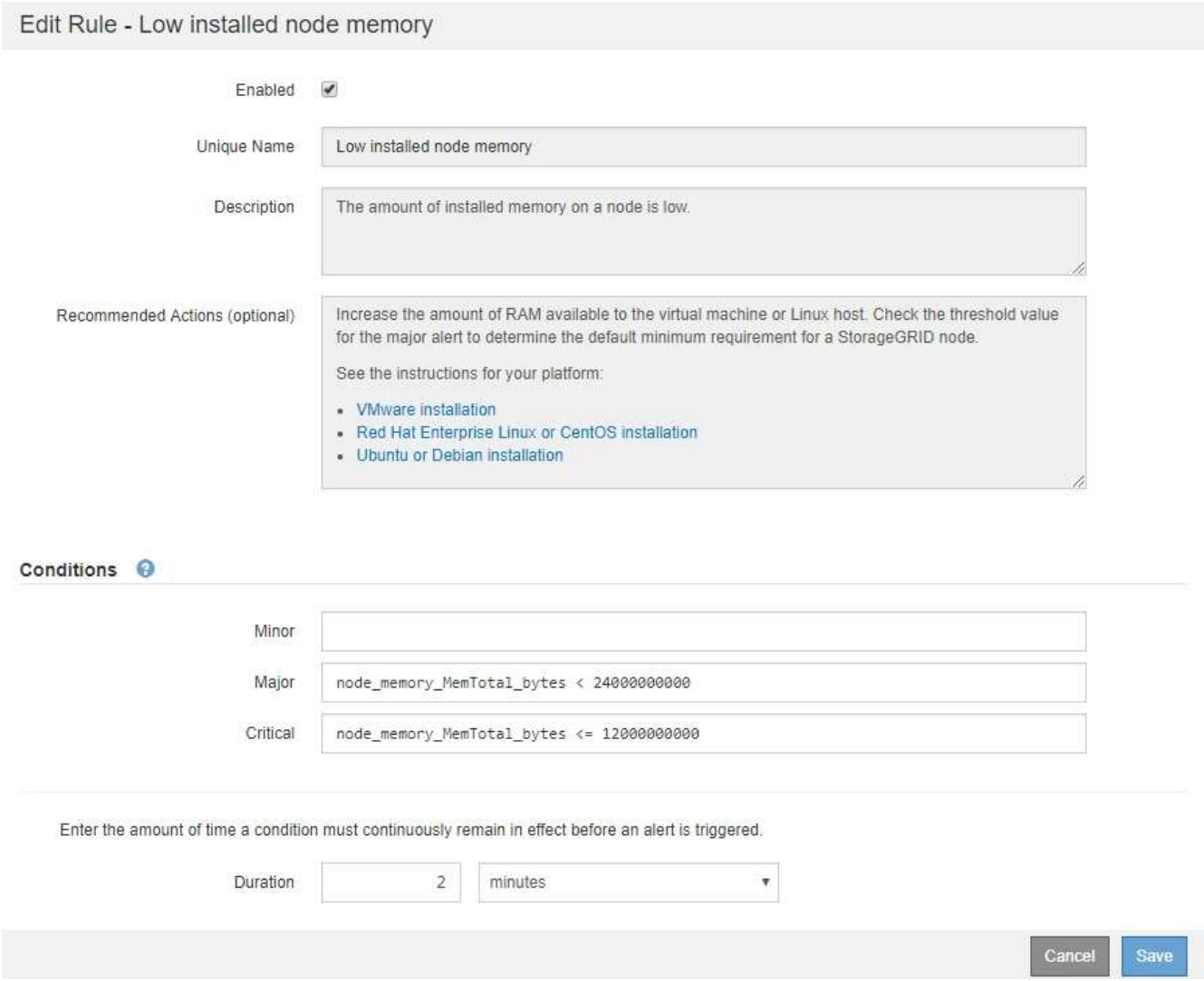
Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

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

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



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

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

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

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

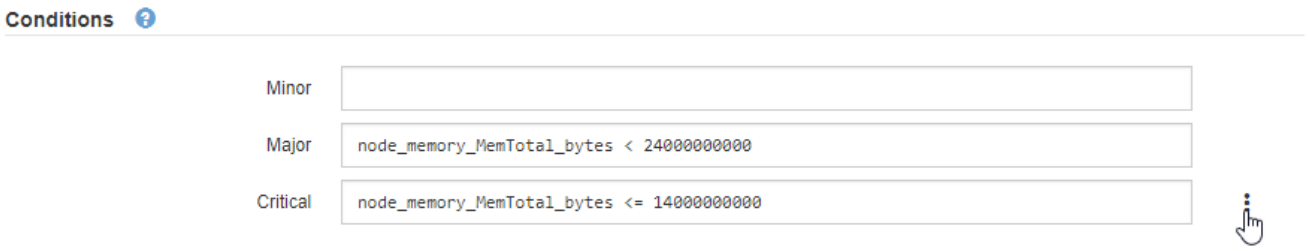
5. Per le regole di avviso personalizzate, aggiornare le seguenti informazioni secondo necessità.

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

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche e-mail. I nomi delle regole di avviso possono essere compresi tra 1 e 64 caratteri.
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1,024 caratteri.

6. Nella sezione Condizioni, immettere o aggiornare l'espressione Prometheus per uno o più livelli di gravità dell'avviso.

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



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

Un'espressione di base è in genere della forma:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

   L'impostazione predefinita è 5 minuti.

8. Selezionare **Salva**.

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

Disattiva le regole di avviso

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

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

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

Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

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

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

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

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

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

5. Selezionare **Salva**.

   Disabled viene visualizzato nella colonna **Status**.

Rimuovere le regole di avviso personalizzate

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

Fasi

1. Selezionare **ALERTS** > **Rules**.

   Viene visualizzata la pagina regole di avviso.

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

   Non è possibile rimuovere una regola di avviso predefinita.

3. Selezionare **Rimuovi regola personalizzata**.

   Viene visualizzata una finestra di dialogo di conferma.

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

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

Gestire le notifiche di avviso

Impostare le notifiche SNMP per gli avvisi

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

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

Per informazioni sulla configurazione dell'agente SNMP, vedere "Utilizzare il monitoraggio SNMP".

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

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

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

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

Imposta le notifiche via email per gli avvisi

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

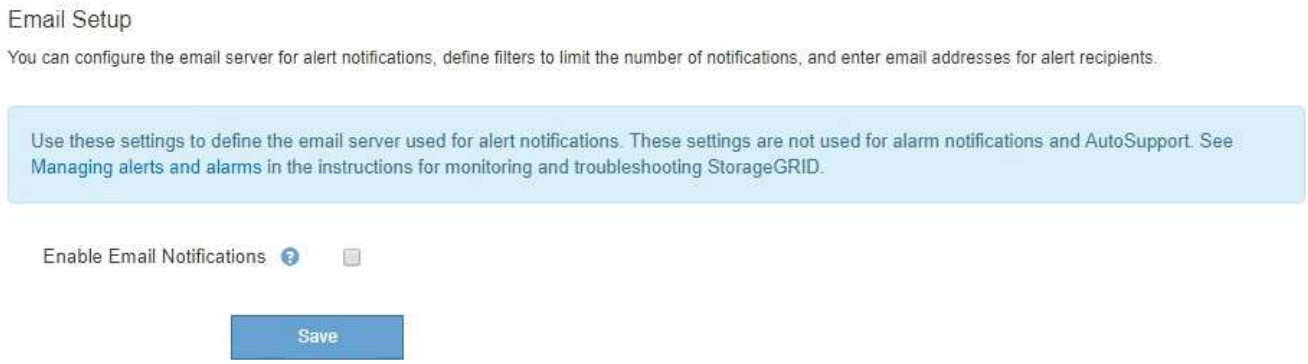
Poiché gli allarmi e gli avvisi sono sistemi indipendenti, la configurazione e-mail utilizzata per le notifiche di avviso non viene utilizzata per le notifiche di allarme e i pacchetti AutoSupport. Tuttavia, è possibile utilizzare lo stesso server di posta elettronica per tutte le notifiche.

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

Fasi

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

   Viene visualizzata la pagina Configurazione e-mail.



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

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

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

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

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

4. Nella sezione indirizzi e-mail, immettere gli indirizzi e-mail per il mittente e per ciascun destinatario.

   a. Per **Sender Email Address**, specificare un indirizzo e-mail valido da utilizzare come indirizzo da per le notifiche degli avvisi.

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

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

   Selezionare l'icona più ➕ per aggiungere destinatari.

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

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

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

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

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

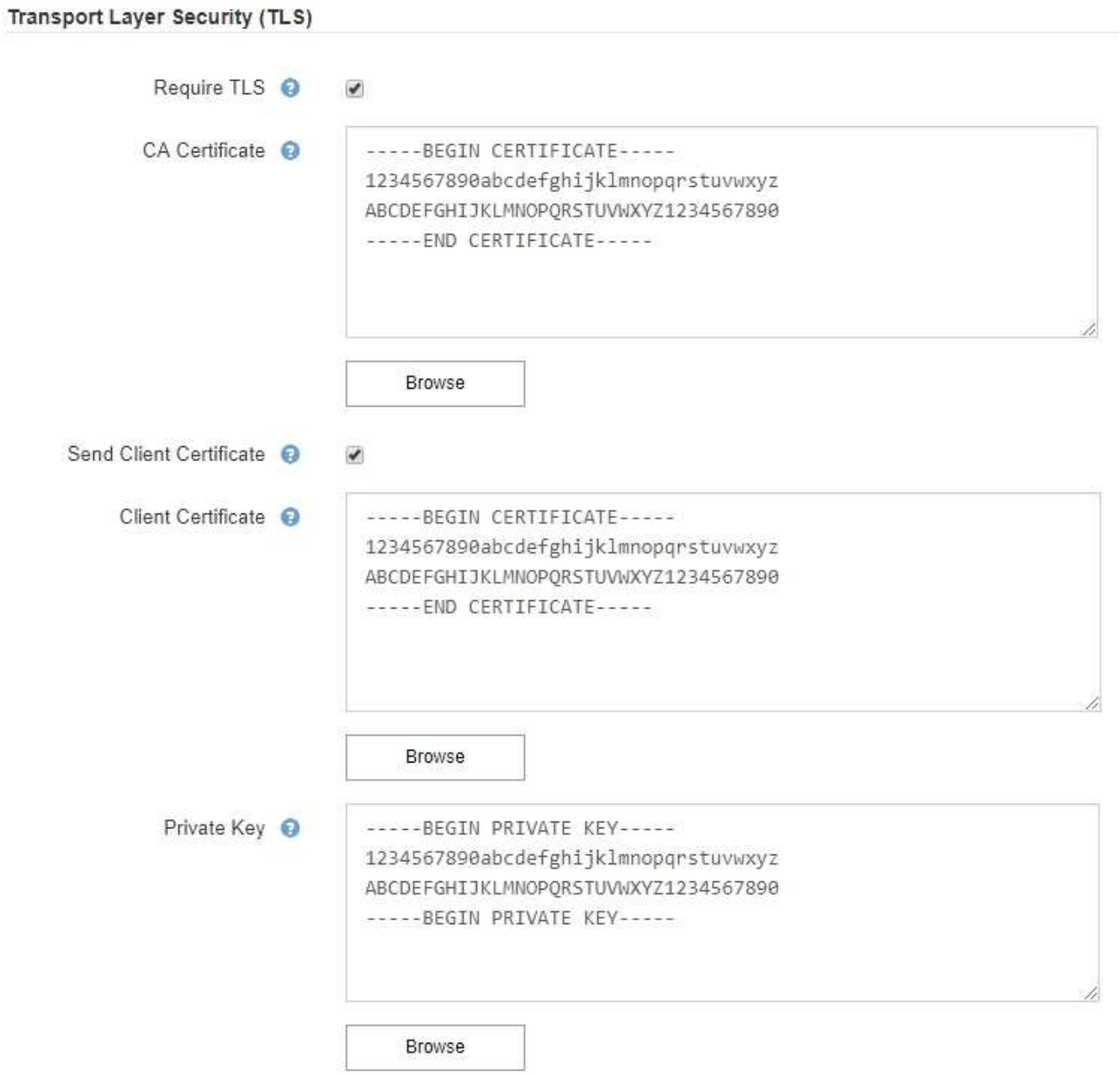
   c. Nel campo **certificato client**, fornire il certificato client con codifica PEM da inviare al server SMTP.

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

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

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

> Se si desidera modificare la configurazione dell'e-mail, selezionare l'icona a forma di matita per aggiornare questo campo.



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

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

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

7. Quando si è pronti a verificare le impostazioni e-mail, attenersi alla seguente procedura:
   a. Selezionare **Invia email di prova**.

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

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

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

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

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

8. Selezionare **Salva**.

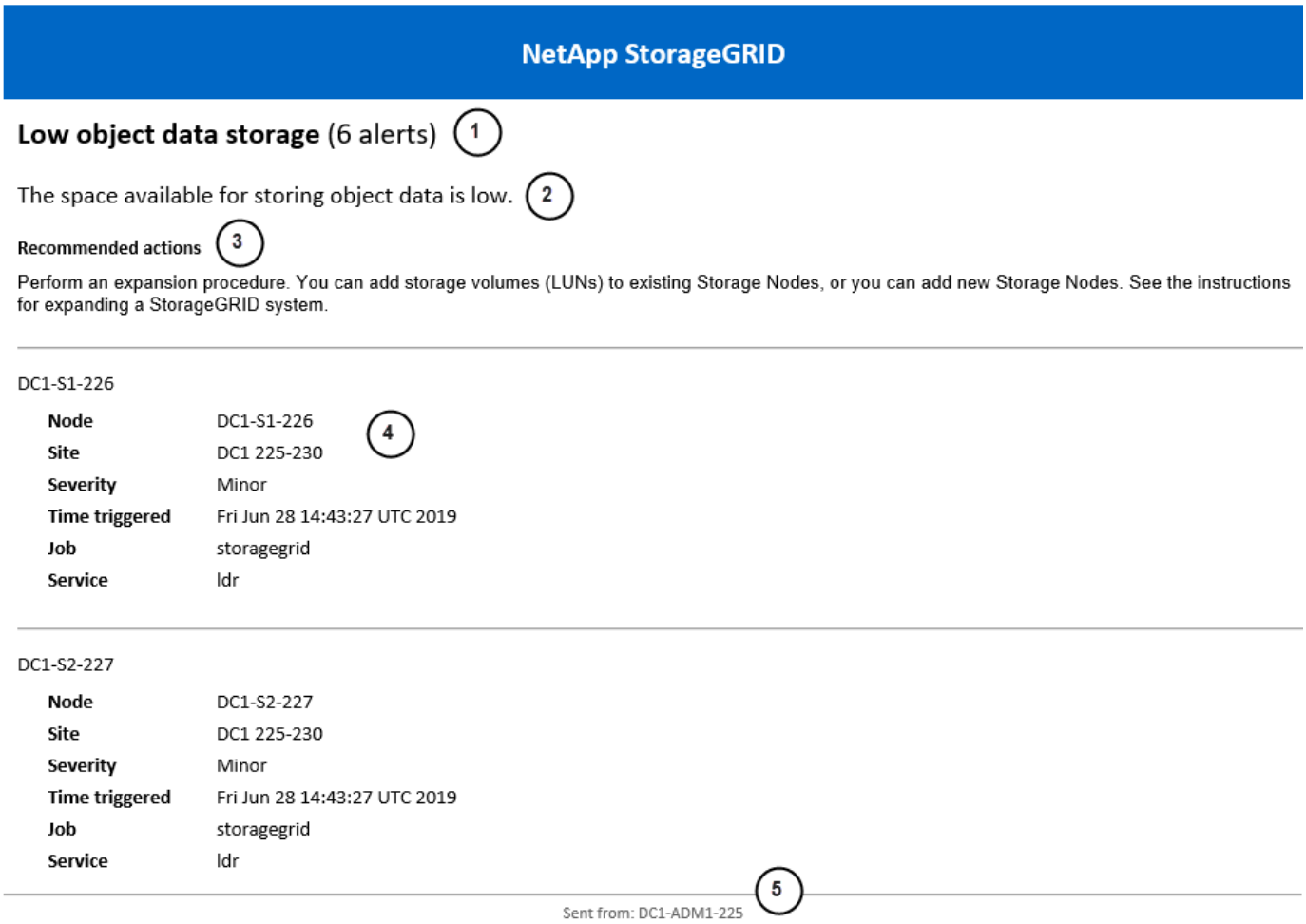
   L'invio di un'e-mail di prova non salva le impostazioni. Selezionare **Salva**.

   Le impostazioni e-mail vengono salvate.

Informazioni incluse nelle notifiche e-mail di avviso

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

Le notifiche e-mail includono le seguenti informazioni:



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

Modalità di raggruppamento degli avvisi

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

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

Comportamento	Esempio
Ogni notifica di avviso si applica solo agli avvisi con lo stesso nome. Se vengono attivati contemporaneamente due avvisi con nomi diversi, vengono inviate due notifiche e-mail.	• L'avviso A viene attivato su due nodi contemporaneamente. Viene inviata una sola notifica. • L'allarme A viene attivato sul nodo 1 e l'allarme B viene attivato contemporaneamente sul nodo 2. Vengono inviate due notifiche, una per ogni avviso.
Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di una severità, viene inviata una notifica solo per l'avviso più grave.	• Viene attivato l'allarme A e vengono raggiunte le soglie di allarme minore, maggiore e critico. Viene inviata una notifica per l'avviso critico.
La prima volta che viene attivato un avviso, StorageGRID attende 2 minuti prima di inviare una notifica. Se durante questo periodo vengono attivati altri avvisi con lo stesso nome, StorageGRID raggruppa tutti gli avvisi nella notifica iniziale.	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 (gli avvisi correnti che non sono stati tacitati), anche se precedentemente segnalati.	1. L'allarme A viene attivato sul nodo 1 alle 08:00. Viene inviata una notifica alle ore 08:02. 2. L'allarme A viene attivato sul nodo 2 alle 08:05. Una seconda notifica viene inviata alle 08:15 (10 minuti dopo). Vengono segnalati entrambi i nodi.
Se sono presenti più avvisi correnti con lo stesso nome e uno di questi viene risolto, non viene inviata una nuova notifica se l'avviso si ripresenta sul nodo per il quale l'avviso è stato risolto.	1. Viene attivato l'avviso A per il nodo 1. Viene inviata una notifica. 2. L'avviso A viene attivato per il nodo 2. Viene inviata una seconda notifica. 3. L'avviso A è stato risolto per il nodo 2, ma rimane attivo per il nodo 1. 4. L'avviso A viene nuovamente attivato per il nodo 2. Non viene inviata alcuna nuova notifica perché l'avviso è ancora attivo per il nodo 1.
StorageGRID continua a inviare notifiche via email ogni 7 giorni fino a quando tutte le istanze dell'avviso non vengono risolte o la regola dell'avviso non viene tacitata.	1. L'allarme A viene attivato per il nodo 1 l'8 marzo. Viene inviata una notifica. 2. L'avviso A non viene risolto o tacitato. Ulteriori notifiche verranno inviate il 15 marzo, il 22 marzo, il 29 marzo e così via.

Risolvere i problemi relativi alle notifiche email di avviso

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

Fasi

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

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

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

Tacitare le notifiche di avviso

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Gestire gli avvisi o l'autorizzazione di accesso principale".

A proposito di questa attività

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

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

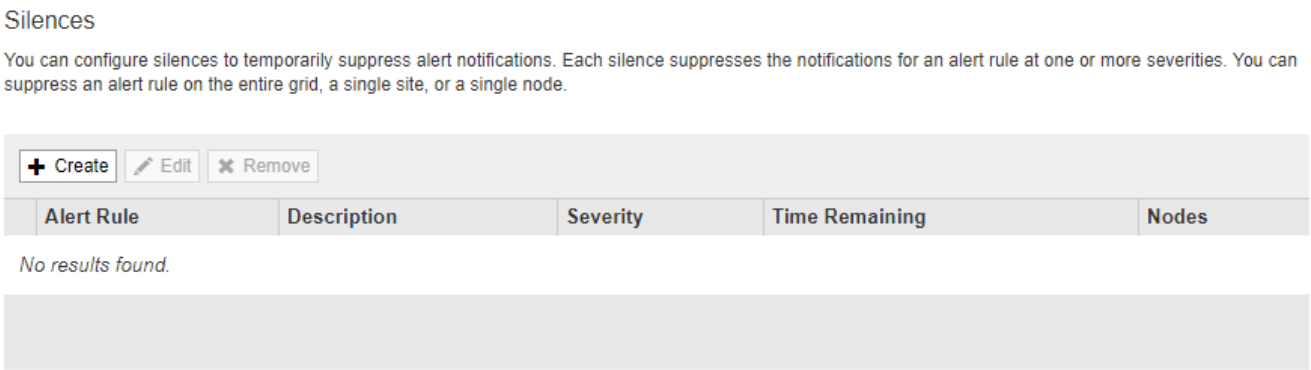
> Prestare attenzione quando si decide di tacitare una regola di avviso. Se si tacita un avviso, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

> Poiché gli allarmi e gli avvisi sono sistemi indipendenti, non è possibile utilizzare questa funzionalità per eliminare le notifiche di allarme.

Fasi

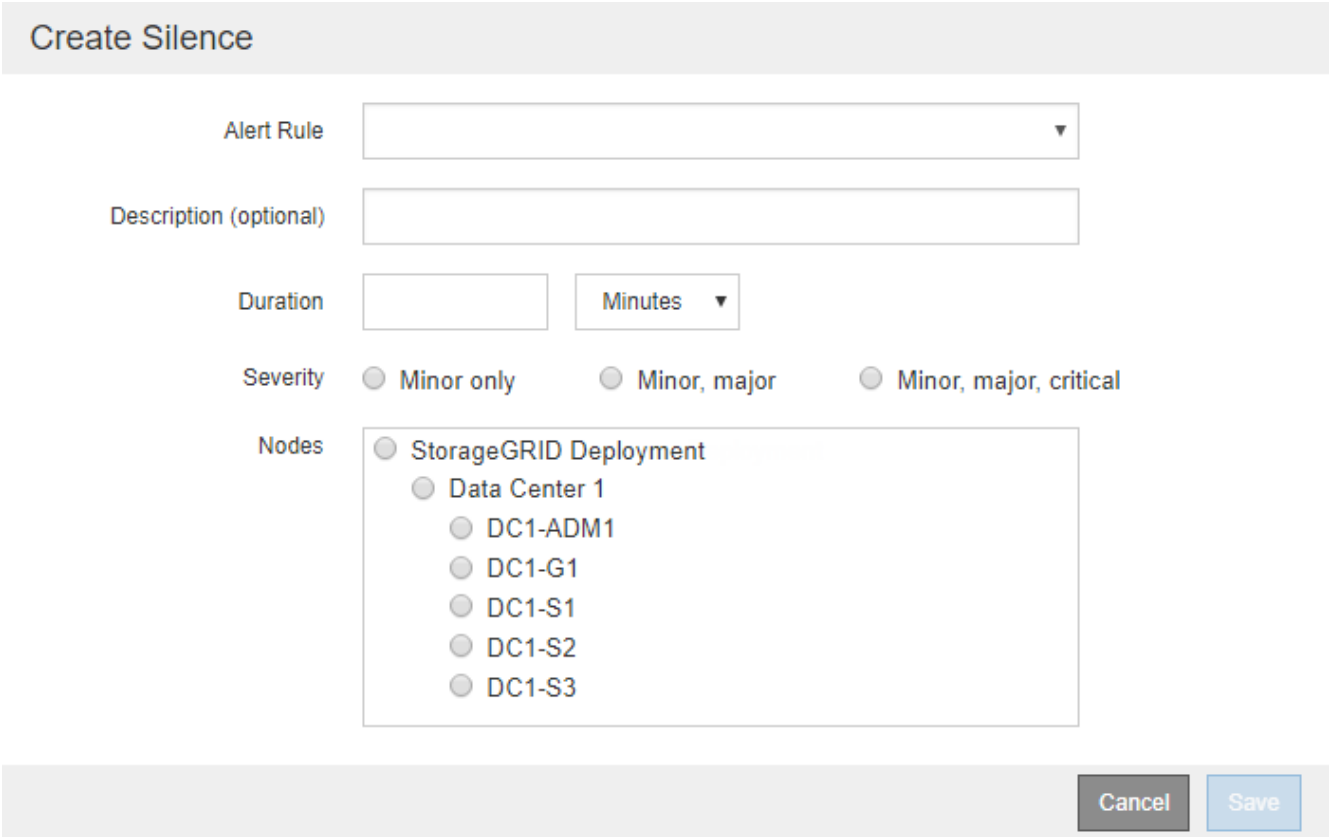
1. Selezionare **ALERTS** > **silences**.

   Viene visualizzata la pagina Silences (silenzi).



2. Selezionare **Crea**.

   Viene visualizzata la finestra di dialogo Crea silenzio.



3. Selezionare o inserire le seguenti informazioni:

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

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

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

Opzione	Descrizione
Modificare un silenzio	a. Selezionare **ALERTS** > **silences**. b. Dalla tabella, selezionare il pulsante di opzione relativo al silenzio che si desidera modificare. c. Selezionare **Modifica**. d. Modificare la descrizione, il tempo rimanente, le severità selezionate o il nodo interessato. e. Selezionare **Salva**.

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

Informazioni correlate

- "Configurare l'agente SNMP"

Riferimenti agli avvisi

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

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

Alcuni degli avvisi predefiniti vengono utilizzati "Metriche Prometheus".

Avvisi sull'appliance

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

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

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

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

Avvisi di audit e syslog

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

Avvisi bucket

Nome dell'avviso	Descrizione
Il bucket FabricPool ha un'impostazione di coerenza del bucket non supportata	Un bucket FabricPool utilizza il livello di coerenza disponibile o di sito sicuro, che non è supportato.

Avvisi Cassandra

Nome dell'avviso	Descrizione
Errore compattatore automatico Cassandra	Si è verificato un errore nel compattatore automatico Cassandra.
Metriche del compattatore automatico Cassandra non aggiornate	Le metriche che descrivono il compattatore automatico Cassandra non sono aggiornate.
Errore di comunicazione Cassandra	I nodi che eseguono il servizio Cassandra hanno problemi di comunicazione tra loro.
Le compaction di Cassandra sono sovraccaricate	Il processo di compattazione Cassandra è sovraccarico.
Errore di scrittura Cassandra oversize	Un processo StorageGRID interno ha inviato a Cassandra una richiesta di scrittura troppo grande.
Metriche di riparazione Cassandra non aggiornate	Le metriche che descrivono i lavori di riparazione Cassandra non sono aggiornate.
Il processo di riparazione di Cassandra è lento	Il progresso delle riparazioni del database Cassandra è lento.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione Cassandra non è disponibile.
Tabella Cassandra corrotta	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva la corruzione della tabella.

Avvisi Cloud Storage Pool

Nome dell'avviso	Descrizione
Errore di connettività del pool di cloud storage	Il controllo dello stato di salute dei Cloud Storage Pools ha rilevato uno o più nuovi errori.

Avvisi di replica cross-grid

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

Avvisi DHCP

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

Avvisi di debug e traccia

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

Avvisi e-mail e AutoSupport

Nome dell'avviso	Descrizione
Impossibile inviare il messaggio AutoSupport	Impossibile inviare il messaggio AutoSupport più recente.
Errore di notifica e-mail	Impossibile inviare la notifica via email per un avviso.

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

Nome dell'avviso	Descrizione
Errore di ribilanciamento EC	La procedura di ribilanciamento EC non è riuscita o è stata interrotta.
Errore di riparazione EC	Un intervento di riparazione per i dati EC non è riuscito o è stato interrotto.

Nome dell'avviso	Descrizione
Riparazione EC in stallo	Un intervento di riparazione per i dati EC si è bloccato.

Scadenza degli avvisi relativi ai certificati

Nome dell'avviso	Descrizione
Scadenza certificato CA proxy amministratore	Uno o più certificati nel pacchetto CA del server proxy amministratore stanno per scadere.
Scadenza del certificato client	Uno o più certificati client stanno per scadere.
Scadenza del certificato server globale per S3 e Swift	Il certificato server globale per S3 e Swift sta per scadere.
Scadenza del certificato endpoint del bilanciamento del carico	Uno o più certificati endpoint per il bilanciamento del carico stanno per scadere.
Scadenza del certificato del server per l'interfaccia di gestione	Il certificato del server utilizzato per l'interfaccia di gestione sta per scadere.
Scadenza del certificato CA syslog esterno	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server syslog esterno sta per scadere.
Scadenza del certificato client syslog esterno	Il certificato client per un server syslog esterno sta per scadere.
Scadenza del certificato del server syslog esterno	Il certificato del server presentato dal server syslog esterno sta per scadere.

Avvisi Grid Network

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

Avvisi di federazione delle griglie

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

Avvisi di utilizzo elevato o latenza elevata

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

Avvisi di Identity Federation

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

Avvisi ILM (Information Lifecycle Management)

Nome dell'avviso	Descrizione
Posizionamento ILM non raggiungibile	Non è possibile ottenere un'istruzione di posizionamento in una regola ILM per determinati oggetti.
Periodo di scansione ILM troppo lungo	Il tempo necessario per eseguire la scansione, la valutazione e l'applicazione di ILM agli oggetti è troppo lungo.
Velocità di scansione ILM bassa	La velocità di scansione ILM è impostata su un valore inferiore a 100 oggetti/secondo.

Avvisi del server di gestione delle chiavi (KMS)

Nome dell'avviso	Descrizione
Scadenza del certificato CA KMS	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server di gestione delle chiavi (KMS) sta per scadere.
Scadenza del certificato client KMS	Il certificato client per un server di gestione delle chiavi sta per scadere
Impossibile caricare la configurazione KMS	La configurazione per il server di gestione delle chiavi esiste ma non è riuscita a caricarsi.
Errore di connettività KMS	Un nodo appliance non è riuscito a connettersi al server di gestione delle chiavi del proprio sito.

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

Avvisi di offset dell'orologio locale

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

Avvisi di memoria insufficiente o spazio insufficiente

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

Nome dell'avviso	Descrizione
Override del watermark di sola lettura bassa	L'override filigrana di sola lettura soft del volume di storage è inferiore al watermark ottimizzato minimo per un nodo di storage.
Bassa capacità del disco root	Lo spazio disponibile sul disco root è insufficiente.
Bassa capacità dei dati di sistema	Lo spazio disponibile per /var/local è basso. Se questa condizione non viene risolta, le operazioni S3 o Swift potrebbero non riuscire.
Spazio libero nella directory tmp basso	Lo spazio disponibile nella directory /tmp è insufficiente.

Avvisi di rete di nodi o nodi

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

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

Nome dell'avviso	Descrizione
Nodo di storage non nello stato di storage desiderato	Il servizio LDR su un nodo di archiviazione non può passare allo stato desiderato a causa di un errore interno o di un problema relativo al volume
Utilizzo della connessione TCP	Il numero di connessioni TCP su questo nodo si avvicina al numero massimo che è possibile tenere traccia.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono o non è possibile raggiungere il nodo.
Riavvio del nodo imprevisto	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore.

Avvisi a oggetti

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

Avvisi sui servizi della piattaforma

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

Avvisi sul volume di storage

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

Nome dell'avviso	Descrizione
Il volume di storage deve essere ripristinato	Un volume di storage è stato ripristinato e deve essere ripristinato.
Volume di storage offline	Un volume di storage è rimasto offline per più di 5 minuti, probabilmente perché il nodo è stato riavviato durante la fase di formattazione del volume.
Ripristino volume non riuscito ad avviare la riparazione dei dati replicati	Impossibile avviare automaticamente la riparazione dei dati replicati per un volume riparato.

Avvisi dei servizi StorageGRID

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

Avvisi del tenant

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

Metriche Prometheus comunemente utilizzate

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

Puoi anche farlo ottenere un elenco completo di tutte le metriche.

Per ulteriori informazioni sulla sintassi delle query Prometheus, vedere "Interrogazione di Prometheus".

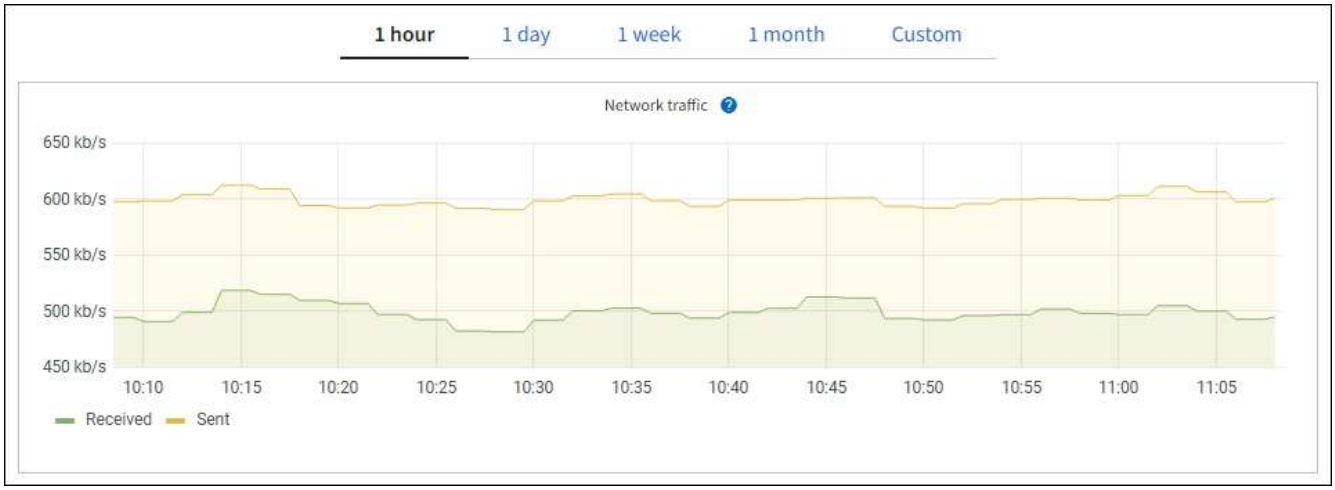
Quali sono le metriche Prometheus?

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

Dove vengono utilizzate le metriche Prometheus?

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

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



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

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

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

> Alcune funzioni e voci di menu della pagina metriche sono intenzionalmente non funzionali e sono soggette a modifiche.

Elenco delle metriche più comuni

Il seguente elenco contiene le metriche Prometheus più comunemente utilizzate.

> Le metriche che includono *private* nei loro nomi sono solo per uso interno e sono soggette a modifiche senza preavviso tra le release di StorageGRID.

alertmanager_notifications_failed_total

Il numero totale di notifiche di avviso non riuscite.

node_filesystem_avail_bytes

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

Node_Memory_MemAvailable_Bytes

Campo delle informazioni sulla memoria MemAvailable_Bytes.

node_network_carrier

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

node_network_receive_errs_total

Statistiche sui dispositivi di rete `receive_errs`.

node_network_transmit_errs_total

Statistiche sui dispositivi di rete `transmit_errs`.

storagegrid_administively_down

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

storagegrid_appliance_compute_controller_hardware_status

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

storagegrid_appliance_failed_disks

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

storagegrid_appliance_storage_controller_hardware_status

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

storagegrid_content_bucket_and_containers

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

storagegrid_content_objects

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

storagegrid_content_objects_lost

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

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

storagegrid_http_sessions_incoming_tented

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

storagegrid_http_sessions_incoming_currently_established

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

storagegrid_http_sessions_incoming_failed

Il numero totale di sessioni HTTP che non sono riuscite a completare correttamente, a causa di una richiesta HTTP non valida o di un errore durante l'elaborazione di un'operazione.

storagegrid_http_sessions_incoming_successful

Il numero totale di sessioni HTTP completate correttamente.

storagegrid_ilm_waiting_background_objects

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

storagegrid_ilm_waiting_client_evaluation_objects_per_second

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

storagegrid_ilm_waiting_client_objects

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

storagegrid_ilm_waiting_total_objects

Il numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_objects_per_second

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

storagegrid_ilm_scan_period_estimated_minutes

Il tempo stimato per completare una scansione ILM completa su questo nodo.

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

storagegrid_load_balancer_endpoint_cert_expiry_time

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

storagegrid_metadata_queries_average_latency_millisecondi

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

storagegrid_network_received_bytes

La quantità totale di dati ricevuti dall'installazione.

storagegrid_network_transmitted_bytes

La quantità totale di dati inviati dall'installazione.

storagegrid_node_cpu_utilization_percent

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

storagegrid_ntp_chouged_time_source_offset_millisecondi

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

storagegrid_ntp_locked

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

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

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

storagegrid_s3_operations_failed

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

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_non autorizzato

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

storagegrid_servercertificate_management_interface_cert_expiry_days

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

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

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

storagegrid_service_cpu_seconds

La quantità di tempo cumulativa in cui la CPU è stata utilizzata da questo servizio dopo l'installazione.

storagegrid_service_memory_usage_bytes

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

storagegrid_service_network_received_bytes

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

storagegrid_service_network_transmitted_bytes

La quantità totale di dati inviati da questo servizio.

storagegrid_service_reavvies

Il numero totale di riavvii del servizio.

storagegrid_service_runtime_seconds

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

storagegrid_service_uptime_seconds

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

storagegrid_storage_state_current

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

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

storagegrid_storage_status

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

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

storagegrid_storage_utilization_data_bytes

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

storagegrid_storage_utilization_metadata_allowed_bytes

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

storagegrid_storage_utilization_metadata_bytes

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

storagegrid_storage_utilization_total_space_bytes

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

storagegrid_storage_utilization_usable_space_bytes

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

storagegrid_swift_data_transfers_bytes_ingested

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

storagegrid_swift_data_transfers_bytes_retrieved

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

storagegrid_swift_operations_failed

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

storagegrid_swift_operations_successful

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

storagegrid_swift_operations_inhautorizzata

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

storagegrid_tenant_usage_data_bytes

La dimensione logica di tutti gli oggetti per il tenant.

storagegrid_tenant_usage_object_count

Il numero di oggetti per il tenant.

storagegrid_tenant_usage_quota_byte

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

Ottieni un elenco di tutte le metriche

per ottenere l'elenco completo delle metriche, utilizza l'API Grid Management.

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

Gestire gli allarmi (sistema legacy)

Gestire gli allarmi (sistema legacy)

Il sistema di allarme StorageGRID è il sistema legacy utilizzato per identificare i punti di errore che talvolta si verificano durante il normale funzionamento.

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Classi di allarme (sistema legacy)

Un allarme legacy può appartenere a una delle due classi di allarme che si escludono a vicenda.

- Gli allarmi predefiniti vengono forniti con ogni sistema StorageGRID e non possono essere modificati. Tuttavia, è possibile disattivare gli allarmi predefiniti o ignorarli definendo gli allarmi personalizzati globali.
- Gli allarmi personalizzati globali monitorano lo stato di tutti i servizi di un determinato tipo nel sistema StorageGRID. È possibile creare un allarme Global Custom per ignorare un allarme Default. È inoltre possibile creare un nuovo allarme Global Custom. Ciò può essere utile per monitorare qualsiasi condizione personalizzata del sistema StorageGRID.

Logica di attivazione degli allarmi (sistema legacy)

Un allarme legacy viene attivato quando un attributo StorageGRID raggiunge un valore di soglia che viene valutato come true rispetto a una combinazione di classe di allarme (predefinita o personalizzata globale) e livello di gravità dell'allarme.

Icona	Colore	Severità degli allarmi	Significato
	Giallo	Avviso	Il nodo è connesso alla rete, ma esiste una condizione insolita che non influisce sulle normali operazioni.
	Arancione chiaro	Minore	Il nodo è collegato alla rete, ma esiste una condizione anomala che potrebbe influire sul funzionamento in futuro. È necessario indagare per evitare l'escalation.
	Arancione scuro	Maggiore	Il nodo è collegato alla rete, ma esiste una condizione anomala che attualmente influisce sul funzionamento. Ciò richiede una rapida attenzione per evitare l'escalation.
	Rosso	Critico	Il nodo è connesso alla rete, ma esiste una condizione anomala che ha interrotto le normali operazioni. Il problema deve essere risolto immediatamente.

È possibile impostare la severità dell'allarme e il valore di soglia corrispondente per ogni attributo numerico. Il servizio NMS su ciascun nodo di amministrazione monitora continuamente i valori degli attributi correnti in base alle soglie configurate. Quando viene attivato un allarme, viene inviata una notifica a tutto il personale designato.

Si noti che un livello di severità normale non attiva un allarme.

I valori degli attributi vengono valutati in base all'elenco di allarmi abilitati definito per tale attributo. L'elenco degli allarmi viene controllato nel seguente ordine per individuare la prima classe di allarme con un allarme definito e attivato per l'attributo:

1. Allarmi personalizzati globali con livelli di interruzione degli allarmi da critici a avvisi.
2. Allarmi predefiniti con livelli di gravità degli allarmi da critico a Avviso.

Dopo che un allarme abilitato per un attributo viene trovato nella classe di allarme superiore, il servizio NMS valuta solo all'interno di tale classe. Il servizio NMS non valuterà le altre classi con priorità inferiore. In altri termini, se per un attributo è attivato un allarme Global Custom, il servizio NMS valuta solo il valore dell'attributo rispetto agli allarmi Global Custom. Gli allarmi predefiniti non vengono valutati. Pertanto, un allarme predefinito abilitato per un attributo può soddisfare i criteri necessari per attivare un allarme, ma non verrà attivato perché è attivato un allarme personalizzato globale (che non soddisfa i criteri specificati) per lo stesso attributo. Non viene attivato alcun allarme e non viene inviata alcuna notifica.

Esempio di attivazione degli allarmi

È possibile utilizzare questo esempio per comprendere come vengono attivati gli allarmi Global Custom e Default.

Nell'esempio seguente, un attributo ha un allarme Global Custom e un allarme Default definiti e attivati come mostrato nella tabella seguente.

	Soglia di allarme Global Custom (abilitata)	**Soglia di allarme predefinita (attivata)**
Avviso	>= 1500	>= 1000
Minore	>= 15.000	>= 1000
Maggiore	>=150,000	>= 250.000

Se l'attributo viene valutato quando il suo valore è 1000, non viene attivato alcun allarme e non viene inviata alcuna notifica.

L'allarme Global Custom ha la precedenza sull'allarme Default. Un valore di 1000 non raggiunge il valore di soglia di alcun livello di severità per l'allarme Global Custom. Di conseguenza, il livello di allarme viene valutato come normale.

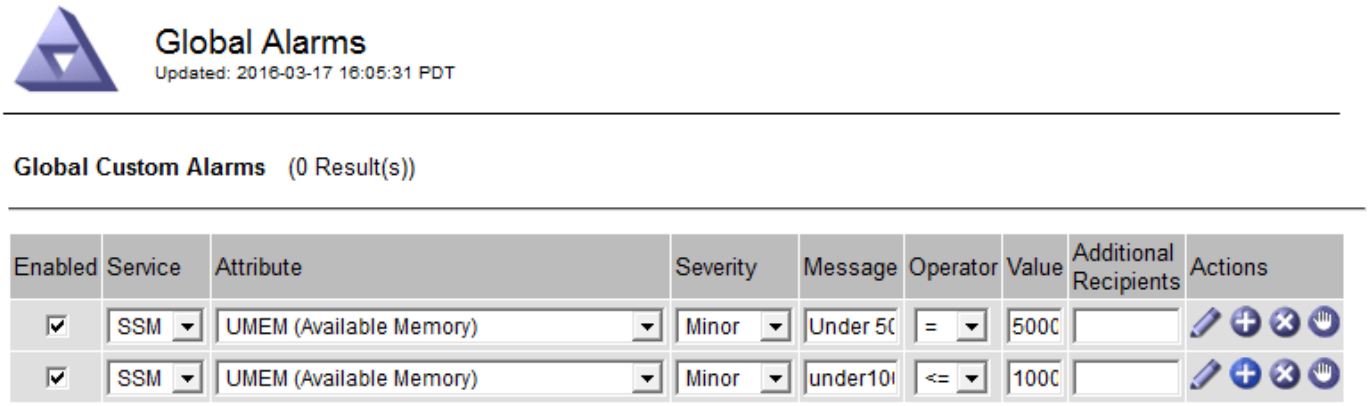
Dopo lo scenario precedente, se l'allarme Global Custom è disattivato, non cambia nulla. Il valore dell'attributo deve essere rivalutato prima che venga attivato un nuovo livello di allarme.

Se l'allarme Global Custom è disattivato, quando il valore dell'attributo viene rivalutato, il valore dell'attributo viene valutato in base ai valori di soglia per l'allarme Default. Il livello di allarme attiva un allarme di livello Notice e viene inviata una notifica via email al personale designato.

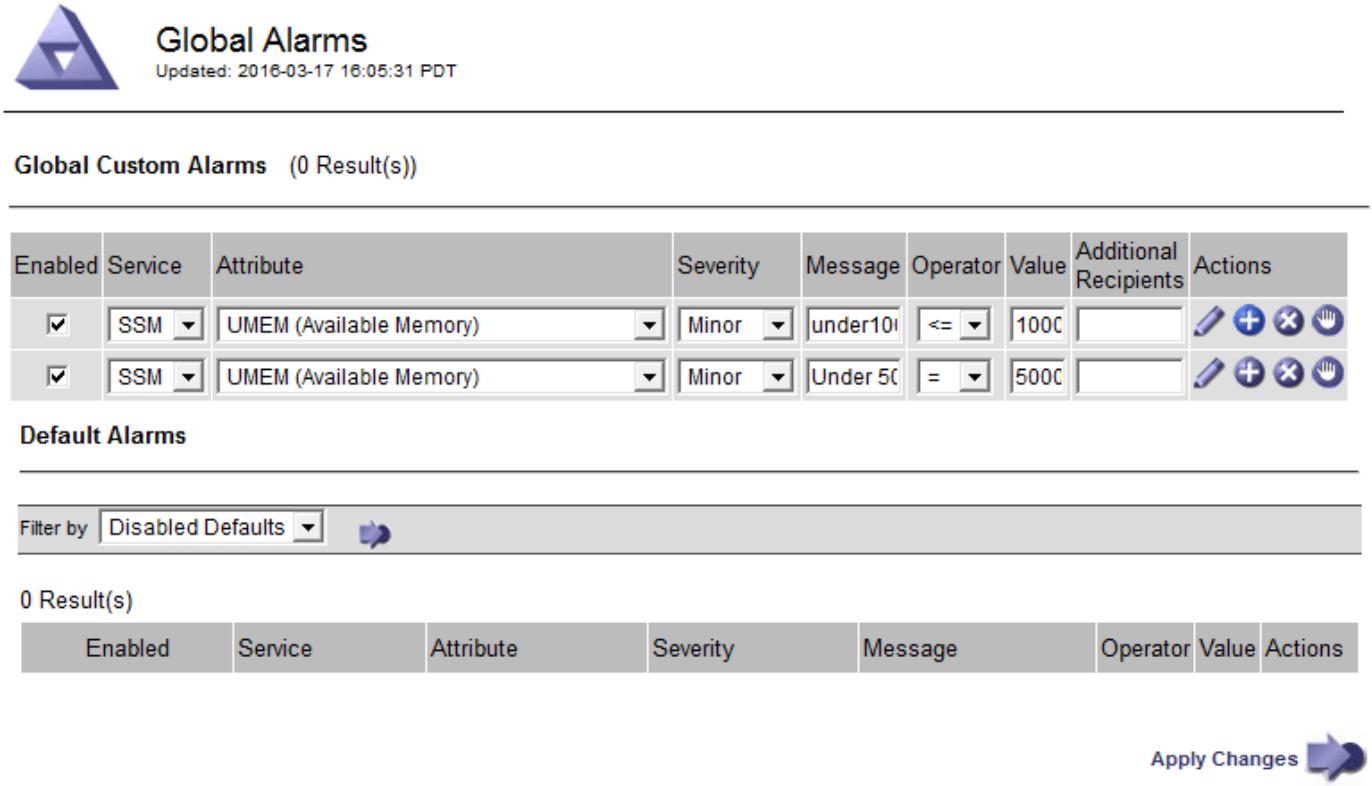
Allarmi della stessa severità

Se due allarmi personalizzati globali per lo stesso attributo hanno lo stesso livello di gravità, gli allarmi vengono valutati con una priorità "dall'alto verso il basso".

Ad esempio, se l'UMEM scende a 50 MB, viene attivato il primo allarme (= 50000000), ma non quello sottostante (⇐100000000).



Se l'ordine viene invertito, quando l'UMEM scende a 100 MB, viene attivato il primo allarme (⇐100000000), ma non quello sottostante (= 50000000).



Notifiche

Una notifica indica il verificarsi di un allarme o il cambiamento di stato di un servizio. Le notifiche di allarme possono essere inviate tramite e-mail o SNMP.

Per evitare l'invio di più allarmi e notifiche quando viene raggiunto un valore di soglia di allarme, la gravità dell'allarme viene controllata in base alla gravità corrente dell'attributo. Se non si verificano modifiche, non viene intrapresa alcuna azione. Ciò significa che mentre il servizio NMS continua a monitorare il sistema, genera un allarme e invia notifiche solo la prima volta che rileva una condizione di allarme per un attributo. Se viene raggiunta e rilevata una nuova soglia di valore per l'attributo, la gravità dell'allarme cambia e viene inviata una nuova notifica. Gli allarmi vengono cancellati quando le condizioni tornano al livello normale.

Il valore di attivazione visualizzato nella notifica di uno stato di allarme viene arrotondato a tre cifre decimali. Pertanto, un valore di attributo 1.9999 attiva un allarme la cui soglia è inferiore a (<) 2.0, anche se la notifica di allarme mostra il valore di attivazione come 2.0.

Nuovi servizi

Man mano che i nuovi servizi vengono aggiunti tramite l'aggiunta di nuovi nodi o siti della griglia, ereditano gli allarmi predefiniti e gli allarmi personalizzati globali.

Allarmi e tabelle

Gli attributi degli allarmi visualizzati nelle tabelle possono essere disattivati a livello di sistema. Non è possibile disattivare gli allarmi per singole righe di una tabella.

Ad esempio, la tabella seguente mostra due allarmi VMFI (Critical Entries Available). (Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare ***Storage Node*** > **SSM** > **Resources**.)

È possibile disattivare l'allarme VMFI in modo che l'allarme VMFI di livello critico non venga attivato (entrambi gli allarmi attualmente critici vengono visualizzati in verde nella tabella); Tuttavia, non è possibile disattivare un

singolo allarme in una riga di tabella in modo che un allarme VMFI venga visualizzato come allarme di livello critico mentre l'altro rimane verde.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Riconoscere gli allarmi correnti (sistema precedente)

Gli allarmi legacy vengono attivati quando gli attributi di sistema raggiungono i valori di soglia degli allarmi. Se si desidera ridurre o cancellare l'elenco degli allarmi legacy, è possibile confermarli.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- È necessario disporre dell'autorizzazione di riconoscimento degli allarmi.

A proposito di questa attività

Poiché il sistema di allarme legacy continua a essere supportato, l'elenco degli allarmi legacy nella pagina Allarmi correnti aumenta ogni volta che si verifica un nuovo allarme. In genere, è possibile ignorare gli allarmi (in quanto forniscono una migliore visualizzazione del sistema) oppure riconoscere gli allarmi.

> In alternativa, una volta eseguita la transizione completa al sistema di allerta, è possibile disattivare ciascun allarme legacy per evitare che venga attivato e aggiunto al numero di allarmi legacy.

Quando si riconosce un allarme, questo non viene più elencato nella pagina Current Alarms (Allarmi correnti) di Grid Manager, a meno che l'allarme non venga attivato al livello di severità successivo o venga risolto e riattivato.

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms
Last Refreshed: 2020-05-27 09:41:39 MDT

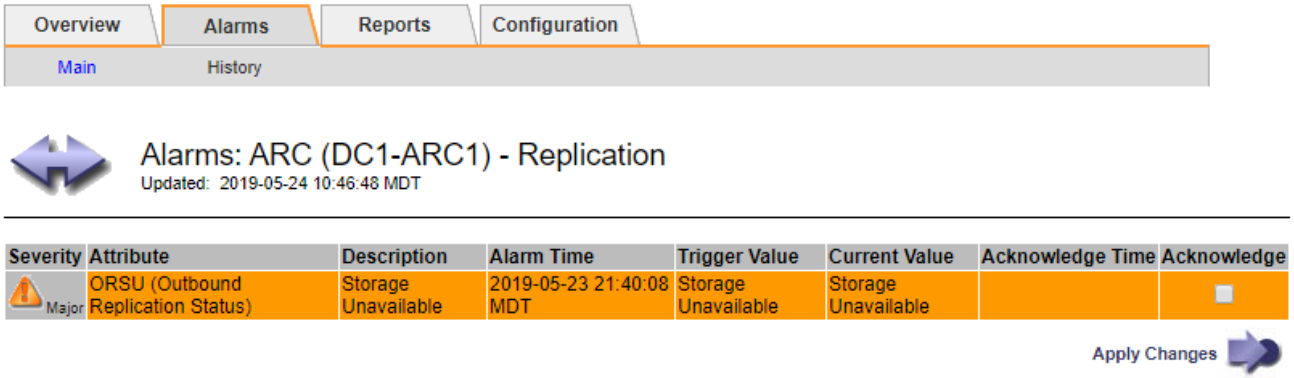
Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show 50 Records Per Page Refresh Previous « 1 » Next

2. Selezionare il nome del servizio nella tabella.

   Viene visualizzata la scheda Allarmi per il servizio selezionato (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarms**).



3. Selezionare la casella di controllo **Acknowledge** (Conferma) per l'allarme e fare clic su **Apply Changes** (Applica modifiche).

   L'allarme non viene più visualizzato nella dashboard o nella pagina Allarmi correnti.

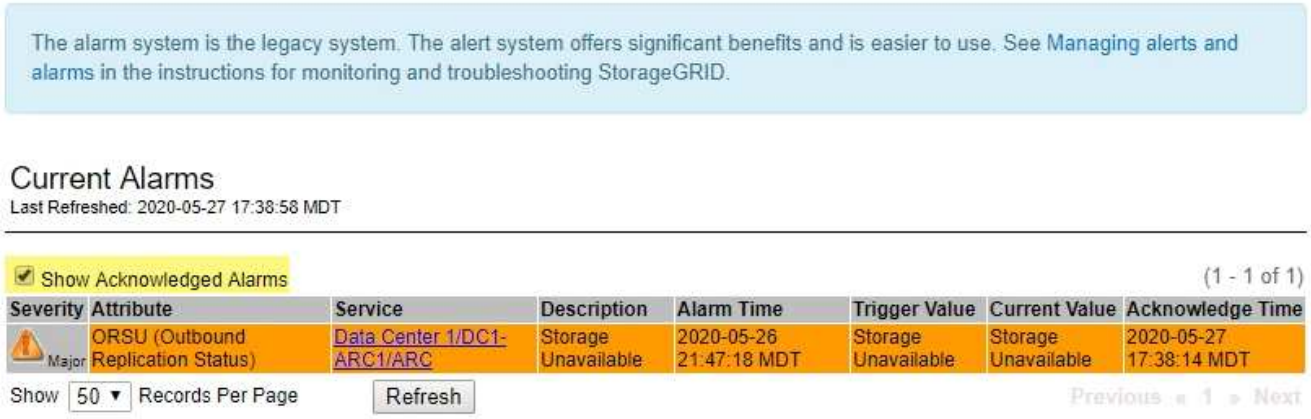
   > Quando si riconosce un allarme, la conferma non viene copiata in altri nodi di amministrazione. Per questo motivo, se si visualizza la dashboard da un altro nodo di amministrazione, è possibile continuare a visualizzare l'allarme attivo.

4. Se necessario, visualizzare gli allarmi confermati.

   a. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.

   b. Selezionare **Mostra allarmi confermati**.

      Vengono visualizzati tutti gli allarmi confermati.



Visualizza allarmi predefiniti (sistema legacy)

È possibile visualizzare l'elenco di tutti gli allarmi legacy predefiniti.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".

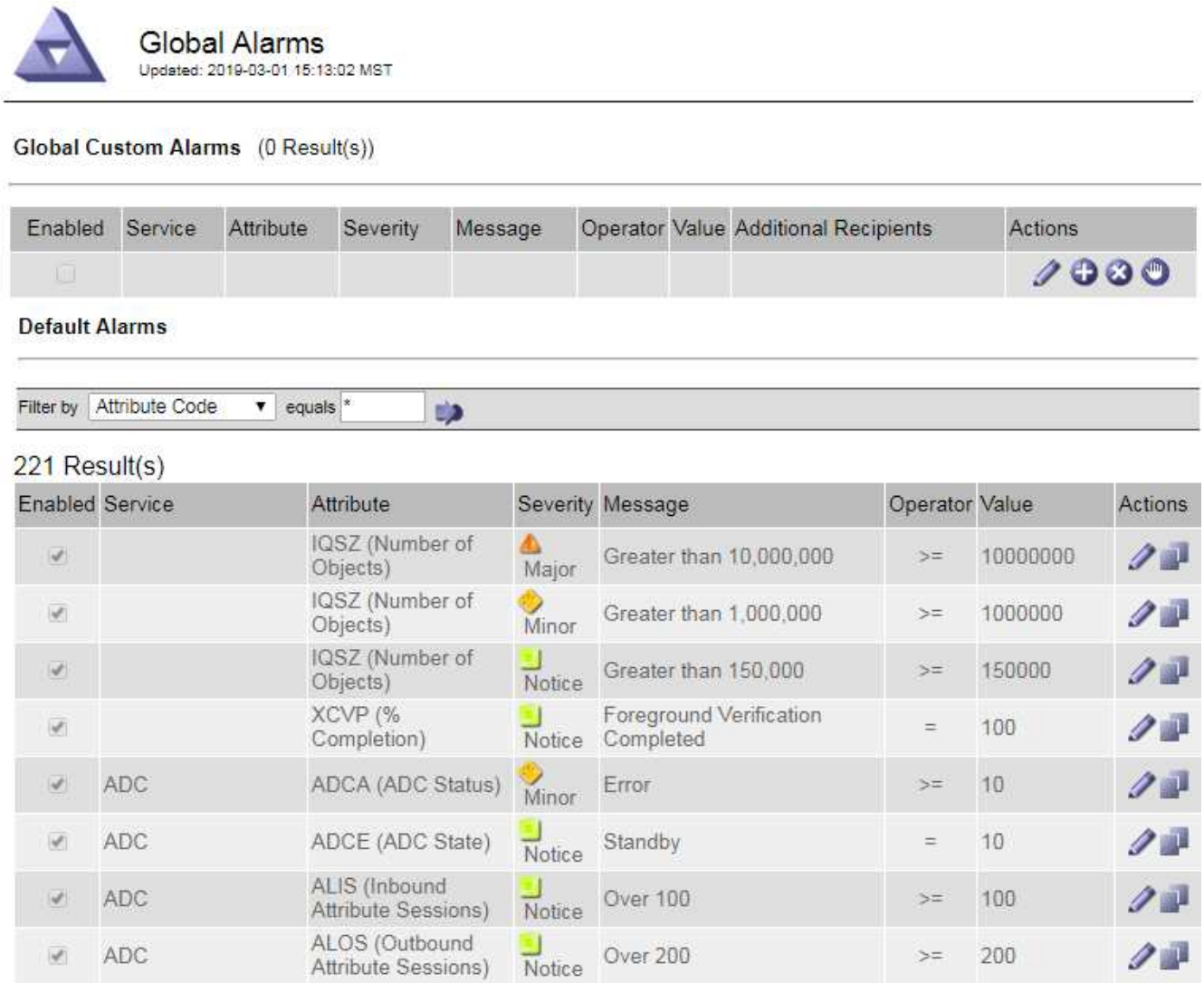
- Lo hai fatto "autorizzazioni di accesso specifiche".

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Per Filtra per, selezionare **Codice attributo** o **Nome attributo**.
3. Per uguale, inserire un asterisco: *
4. Fare clic sulla freccia Oppure premere **Invio**.

   Vengono elencati tutti gli allarmi predefiniti.



Rivedere la cronologia degli allarmi e la frequenza degli allarmi (sistema precedente)

Durante la risoluzione di un problema, è possibile verificare la frequenza con cui un allarme legacy è stato attivato in passato.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Fasi

1. Seguire questa procedura per ottenere un elenco di tutti gli allarmi attivati in un determinato periodo di tempo.
   a. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi storici**.
   b. Effettuare una delle seguenti operazioni:
      - Fare clic su uno dei periodi di tempo.
      - Immettere un intervallo personalizzato e fare clic su **Custom Query** (Query personalizzata).
2. Seguire questa procedura per scoprire la frequenza con cui sono stati attivati gli allarmi per un determinato attributo.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***grid node*** > ***service o component*** > **Alarms** > **History**.
   c. Selezionare l'attributo dall'elenco.
   d. Effettuare una delle seguenti operazioni:
      - Fare clic su uno dei periodi di tempo.
      - Immettere un intervallo personalizzato e fare clic su **Custom Query** (Query personalizzata).

        Gli allarmi sono elencati in ordine cronologico inverso.
   e. Per tornare al modulo di richiesta della cronologia degli allarmi, fare clic su **Cronologia**.

Creazione di allarmi personalizzati globali (sistema legacy)

È possibile che siano stati utilizzati gli allarmi Global Custom per il sistema legacy per soddisfare specifici requisiti di monitoraggio. Gli allarmi Global Custom potrebbero avere livelli di allarme che prevalgono sugli allarmi predefiniti oppure potrebbero monitorare attributi che non hanno un allarme predefinito.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

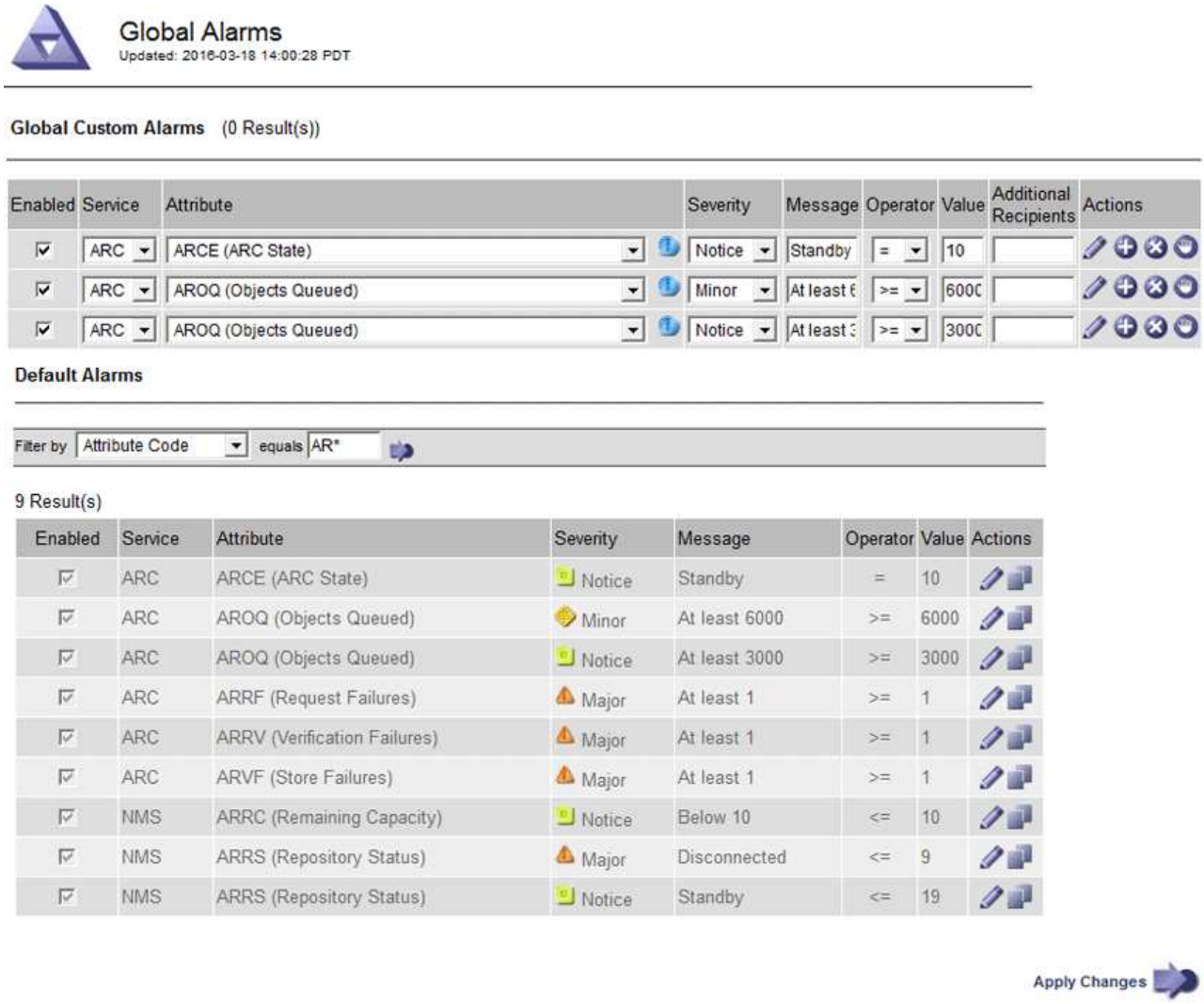
> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Gli allarmi Global Custom prevalgono sugli allarmi predefiniti. Non modificare i valori di allarme predefiniti, a meno che non sia assolutamente necessario. Modificando gli allarmi predefiniti, si corre il rischio di nascondere problemi che potrebbero altrimenti attivare un allarme.

> Prestare attenzione se si modificano le impostazioni della sveglia. Ad esempio, se si aumenta il valore di soglia per un allarme, potrebbe non essere rilevato un problema sottostante. Discutere le modifiche proposte con il supporto tecnico prima di modificare l'impostazione di un allarme.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Aggiungere una nuova riga alla tabella Global Custom Alarms (Allarmi personalizzati globali):
   - Per aggiungere un nuovo allarme, fare clic su **Edit** (Modifica) (Se si tratta della prima voce) o **Insert**.



   - Per modificare un allarme predefinito, cercare l'allarme predefinito.
     i. In Filtra per, selezionare **Codice attributo** o **Nome attributo**.
     ii. Digitare una stringa di ricerca.

     Specificare quattro caratteri o utilizzare caratteri jolly (Ad esempio, A???? O AB*). Gli asterischi (*) rappresentano più caratteri e punti interrogativi (?) rappresenta un singolo carattere.

     iii. Fare clic sulla freccia Oppure premere **Invio**.
     iv. Nell'elenco dei risultati, fare clic su **Copia** accanto all'allarme che si desidera modificare.

     L'allarme predefinito viene copiato nella tabella Global Custom Alarms (Allarmi personalizzati globali).

3. Apportare le modifiche necessarie alle impostazioni degli allarmi Global Custom:

Intestazione	Descrizione
Attivato	Selezionare o deselezionare la casella di controllo per attivare o disattivare l'allarme.
Attributo	Selezionare il nome e il codice dell'attributo monitorato dall'elenco di tutti gli attributi applicabili al servizio o al componente selezionato. Per visualizzare le informazioni relative all'attributo, fare clic su **Info** accanto al nome dell'attributo.
Severità	L'icona e il testo che indicano il livello dell'allarme.
Messaggio	Il motivo dell'allarme (connessione persa, spazio di storage inferiore al 10% e così via).
Operatore	Operatori per il test del valore dell'attributo corrente rispetto alla soglia del valore: • = uguale • > maggiore di • < meno di • >= maggiore o uguale a. • ⇐ minore o uguale a. • ≠ non uguale a.
Valore	Il valore di soglia dell'allarme utilizzato per eseguire il test in base al valore effettivo dell'attributo utilizzando l'operatore. La voce può essere un singolo numero, un intervallo di numeri specificato con due punti (1:3) o un elenco di numeri e intervalli delimitati da virgole.
Destinatari aggiuntivi	Un elenco supplementare di indirizzi e-mail da notificare quando viene attivato l'allarme. Oltre alla mailing list configurata nella pagina **Allarmi** > **Configurazione e-mail**. Gli elenchi sono delimitati da virgole. **Nota:** le mailing list richiedono la configurazione del server SMTP per funzionare. Prima di aggiungere mailing list, verificare che SMTP sia configurato. Le notifiche per gli allarmi personalizzati possono ignorare le notifiche degli allarmi Global Custom o Default.
Azioni	Pulsanti di controllo per: Modificare una riga + Inserire una riga + Eliminare una riga + Trascinare una riga verso l'alto o verso il basso + Copiare una riga

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

Disattivazione degli allarmi (sistema legacy)

Gli allarmi nel sistema di allarme legacy sono attivati per impostazione predefinita, ma è possibile disattivarli che non sono necessari. È inoltre possibile disattivare gli allarmi legacy dopo la completa transizione al nuovo sistema di allerta.

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Disattivazione di un allarme predefinito (sistema legacy)

È possibile disattivare uno degli allarmi predefiniti legacy per l'intero sistema.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

La disattivazione di un allarme per un attributo per il quale è attualmente attivato un allarme non cancella l'allarme corrente. L'allarme verrà disattivato al successivo superamento della soglia di allarme da parte dell'attributo oppure sarà possibile eliminare l'allarme attivato.

> Non disattivare gli allarmi legacy fino a quando non si è passati completamente al nuovo sistema di allarme. In caso contrario, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si è impedito il completamento di un'operazione critica.

Fasi

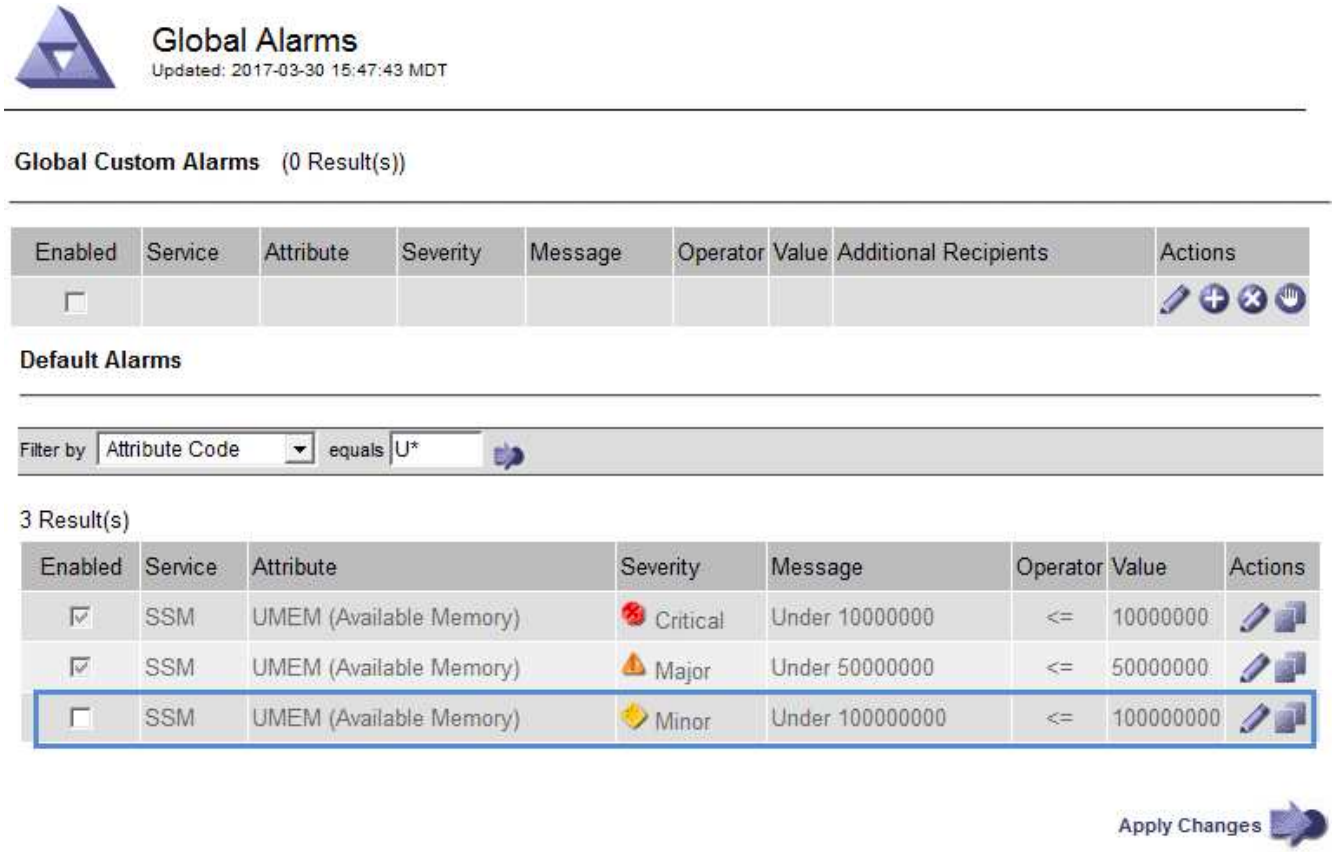
1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Cercare l'allarme predefinito da disattivare.
   a. Nella sezione Allarmi predefiniti, selezionare **Filtra per** > **Codice attributo** o **Nome attributo**.
   b. Digitare una stringa di ricerca.

      Specificare quattro caratteri o utilizzare caratteri jolly (Ad esempio, A???? O AB*). Gli asterischi (*) rappresentano più caratteri e punti interrogativi (?) rappresenta un singolo carattere.

   c. Fare clic sulla freccia Oppure premere **Invio**.

      > Selezionando **Disabled Defaults** (Impostazioni predefinite disabilitate) viene visualizzato un elenco di tutti gli allarmi predefiniti attualmente disattivati.

3. Nella tabella dei risultati della ricerca, fare clic sull'icona Modifica per la sveglia che si desidera disattivare.



La casella di controllo **Enabled** dell'allarme selezionato diventa attiva.

4. Deselezionare la casella di controllo **Enabled**.
5. Fare clic su **Applica modifiche**.

   L'allarme predefinito è disattivato.

Disattiva allarmi Global Custom (sistema legacy)

È possibile disattivare un allarme Global Custom legacy per l'intero sistema.

Prima di iniziare

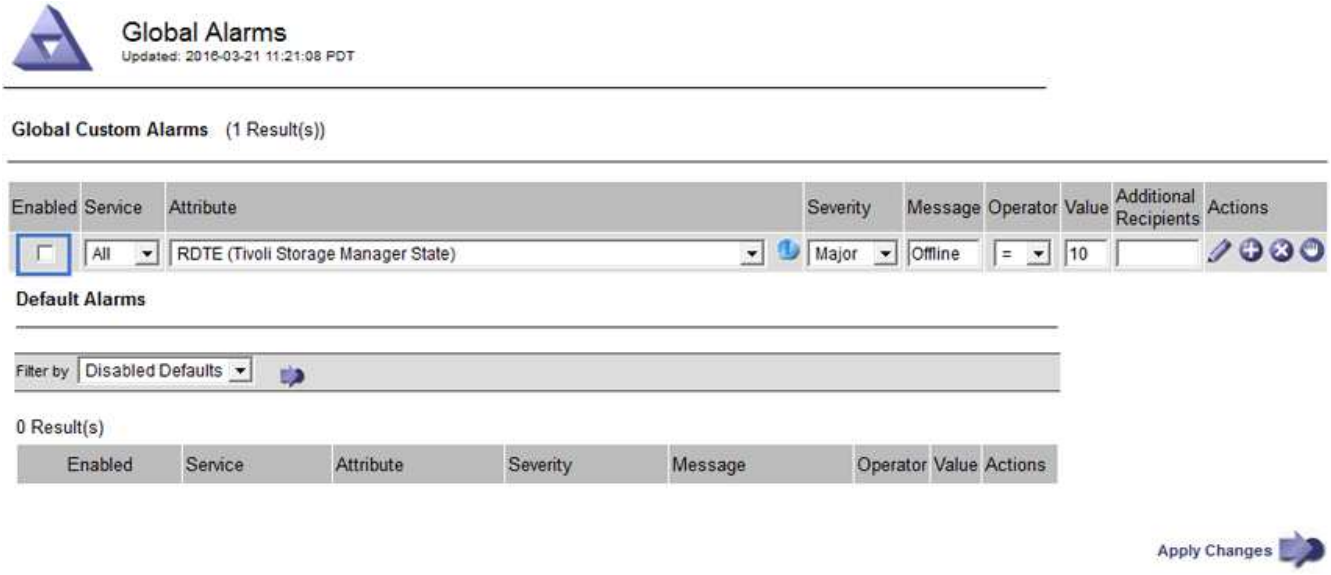
- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

La disattivazione di un allarme per un attributo per il quale è attualmente attivato un allarme non cancella l'allarme corrente. L'allarme verrà disattivato al successivo superamento della soglia di allarme da parte dell'attributo oppure sarà possibile eliminare l'allarme attivato.

Fasi

1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi globali**.
2. Nella tabella Global Custom Alarms (Allarmi personalizzati globali), fare clic su **Edit** (Modifica) accanto all'allarme che si desidera disattivare.
3. Deselezionare la casella di controllo **Enabled**.



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

   L'allarme Global Custom è disattivato.

Cancellazione degli allarmi attivati (sistema precedente)

Se viene attivato un allarme legacy, è possibile cancellarlo invece di confermarlo.

Prima di iniziare

- È necessario disporre di `Passwords.txt` file.

La disattivazione di un allarme per un attributo per il quale è attualmente attivato un allarme non cancella l'allarme. L'allarme verrà disattivato alla successiva modifica dell'attributo. È possibile riconoscere l'allarme oppure, se si desidera annullare immediatamente l'allarme anziché attendere la modifica del valore dell'attributo (con conseguente modifica dello stato dell'allarme), è possibile annullare l'allarme attivato. Questa operazione potrebbe essere utile se si desidera eliminare immediatamente un allarme in relazione a un attributo il cui valore non cambia spesso (ad esempio, gli attributi di stato).

1. Disattiva l'allarme.
2. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: *`ssh admin@primary_Admin_Node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
3. Riavviare il servizio NMS: `service nms restart`
4. Disconnettersi dal nodo di amministrazione: `exit`

   L'allarme viene cancellato.

Configurazione delle notifiche per gli allarmi (sistema legacy)

Il sistema StorageGRID può inviare automaticamente e-mail e. "Notifiche SNMP" quando viene attivato un allarme o quando cambia lo stato di servizio.

Per impostazione predefinita, le notifiche e-mail di allarme non vengono inviate. Per le notifiche e-mail, è necessario configurare il server e-mail e specificare i destinatari. Per le notifiche SNMP, è necessario configurare l'agente SNMP.

Tipi di notifiche di allarme (sistema legacy)

Quando viene attivato un allarme legacy, il sistema StorageGRID invia due tipi di notifiche di allarme: Livello di severità e stato del servizio.

Notifiche del livello di severità

Quando viene attivato un allarme legacy a un livello di severità selezionato, viene inviata una notifica via email:

- Avviso
- Minore
- Maggiore
- Critico

Una mailing list riceve tutte le notifiche relative all'allarme per la severità selezionata. Quando l'allarme esce dal livello di allarme, viene inviata una notifica tramite risoluzione o immissione di un livello di gravità diverso.

Notifiche dello stato del servizio

Viene inviata una notifica dello stato del servizio quando un servizio (ad esempio, il servizio LDR o il servizio NMS) entra nello stato del servizio selezionato e lascia lo stato del servizio selezionato. Le notifiche dello stato del servizio vengono inviate quando un servizio entra o lascia uno dei seguenti stati del servizio:

- Sconosciuto
- Amministrazione non disponibile

Una mailing list riceve tutte le notifiche relative ai cambiamenti nello stato selezionato.

Configurare le impostazioni del server di posta elettronica per gli allarmi (sistema legacy)

Se si desidera che StorageGRID invii notifiche e-mail quando viene attivato un allarme legacy, è necessario specificare le impostazioni del server di posta SMTP. Il sistema StorageGRID invia solo e-mail; non può ricevere e-mail.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Utilizzare queste impostazioni per definire il server SMTP utilizzato per le notifiche e-mail di allarme legacy e i messaggi e-mail AutoSupport. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

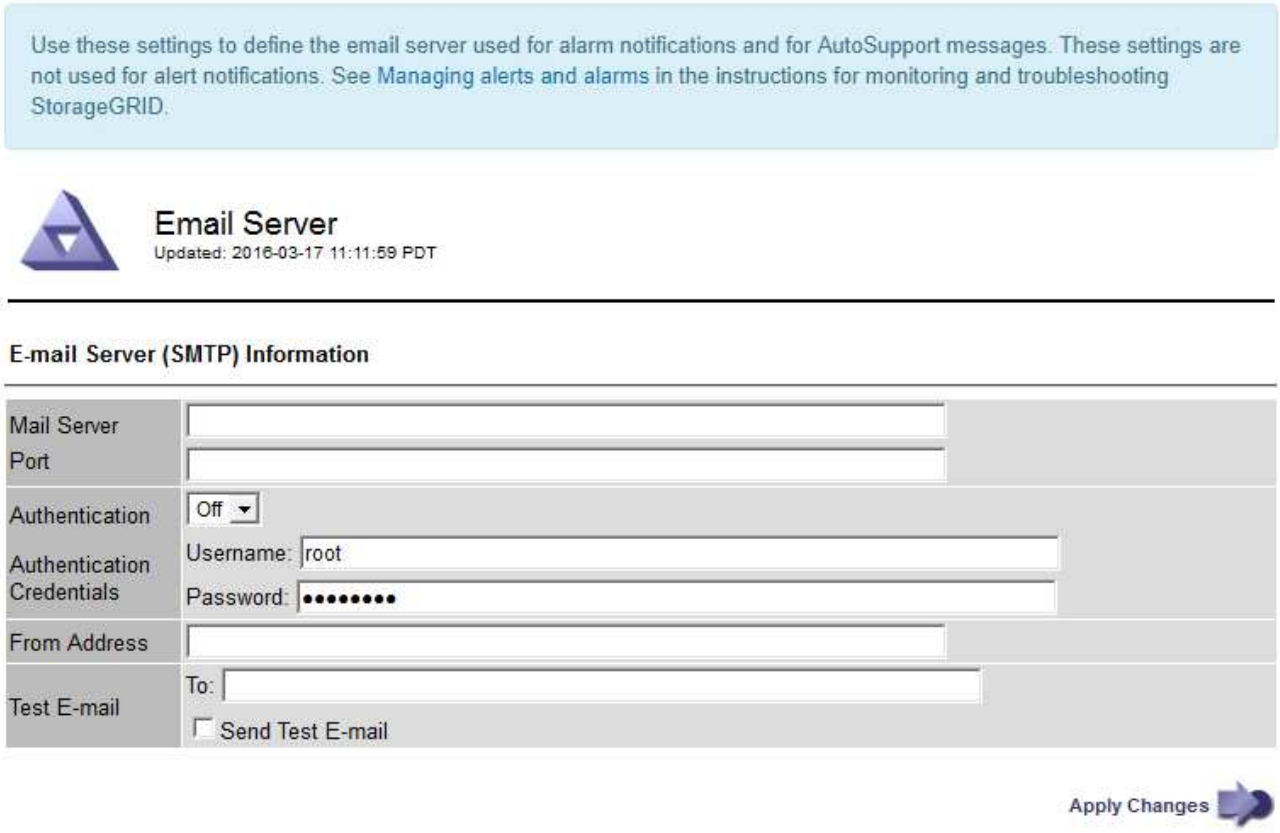
Se si utilizza SMTP come protocollo per i pacchetti AutoSupport, è possibile che sia già stato configurato un server di posta SMTP. Lo stesso server SMTP viene utilizzato per le notifiche e-mail di allarme, pertanto è possibile saltare questa procedura. Vedere "Istruzioni per l'amministrazione di StorageGRID".

SMTP è l'unico protocollo supportato per l'invio di e-mail.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Server**.

   Viene visualizzata la pagina Server di posta elettronica. Questa pagina viene utilizzata anche per configurare il server di posta elettronica per i pacchetti AutoSupport.



3. Aggiungere le seguenti impostazioni del server di posta SMTP:

Elemento	Descrizione
Server di posta	Indirizzo IP del server di posta SMTP. È possibile inserire un nome host anziché un indirizzo IP se in precedenza sono state configurate le impostazioni DNS nel nodo di amministrazione.
Porta	Numero di porta per accedere al server di posta SMTP.
Autenticazione	Consente l'autenticazione del server di posta SMTP. Per impostazione predefinita, l'autenticazione è disattivata.

Elemento	Descrizione
Credenziali di autenticazione	Nome utente e password del server di posta SMTP. Se l'opzione Authentication (autenticazione) è impostata su on, è necessario fornire un nome utente e una password per accedere al server di posta SMTP.

4. Sotto **Indirizzo mittente**, immettere un indirizzo e-mail valido che il server SMTP riconoscerà come indirizzo e-mail di invio. Indirizzo e-mail ufficiale da cui viene inviato il messaggio e-mail.
5. Facoltativamente, inviare un'e-mail di prova per confermare che le impostazioni del server di posta SMTP sono corrette.
   a. Nella casella **e-mail di prova** > **a**, aggiungere uno o più indirizzi ai quali è possibile accedere.

      È possibile inserire un singolo indirizzo e-mail o un elenco di indirizzi e-mail delimitati da virgole. Poiché il servizio NMS non conferma l'esito positivo o negativo dell'invio di un'e-mail di prova, è necessario controllare la posta in arrivo del destinatario del test.

   b. Selezionare **Invia e-mail di prova**.
6. Fare clic su **Applica modifiche**.

   Le impostazioni del server di posta SMTP vengono salvate. Se sono state inserite informazioni per un'e-mail di prova, tale e-mail viene inviata. I messaggi di posta elettronica di prova vengono inviati immediatamente al server di posta e non attraverso la coda delle notifiche. In un sistema con più nodi di amministrazione, ogni nodo di amministrazione invia un'email. La ricezione dell'email di prova conferma che le impostazioni del server di posta SMTP sono corrette e che il servizio NMS si sta connettendo correttamente al server di posta. Un problema di connessione tra il servizio NMS e il server di posta attiva l'allarme MIN legacy (NMS Notification Status) al livello di gravità minore.

Creazione di modelli e-mail di allarme (sistema legacy)

I modelli e-mail consentono di personalizzare l'intestazione, il piè di pagina e l'oggetto di una notifica e-mail di allarme legacy. È possibile utilizzare i modelli e-mail per inviare notifiche univoche contenenti lo stesso corpo del testo a diverse mailing list.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

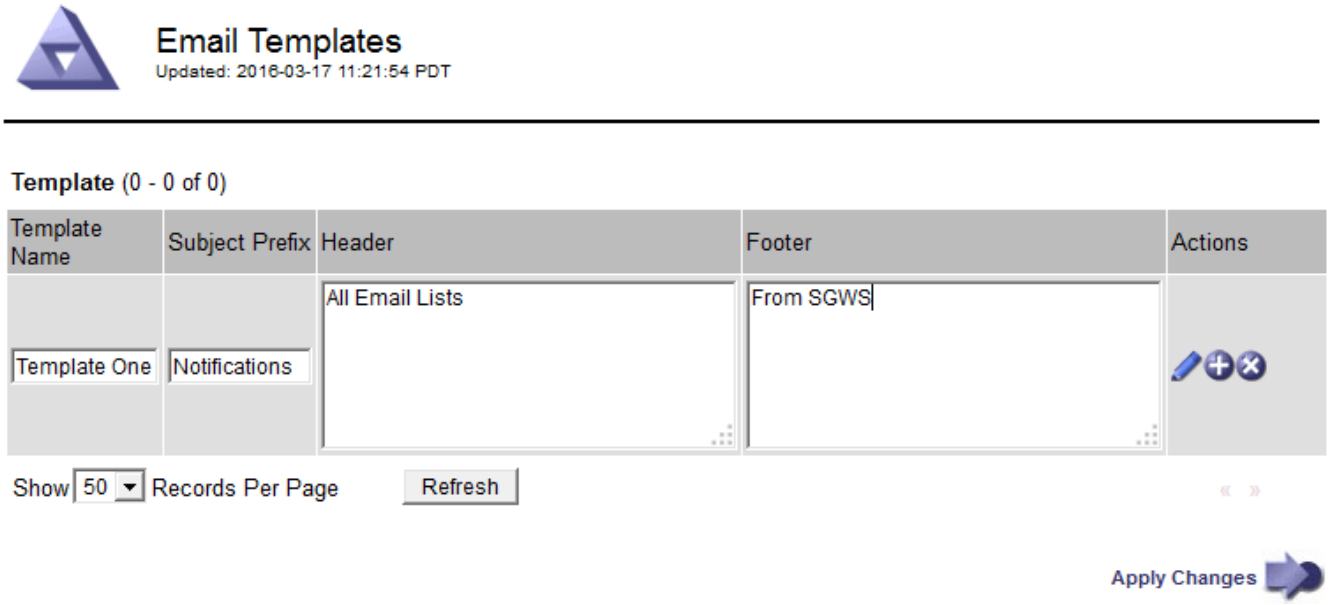
A proposito di questa attività

Utilizzare queste impostazioni per definire i modelli e-mail utilizzati per le notifiche di allarme legacy. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

Diverse mailing list potrebbero richiedere informazioni di contatto diverse. I modelli non includono il corpo del messaggio e-mail.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **modelli**.
3. Fare clic su **Edit** (Modifica) (O **Inserisci** se questo non è il primo modello).



4. Nella nuova riga aggiungere quanto segue:

Elemento	Descrizione
Nome modello	Nome univoco utilizzato per identificare il modello. I nomi dei modelli non possono essere duplicati.
Prefisso soggetto	Opzionale. Prefisso che verrà visualizzato all'inizio dell'oggetto dell'e-mail. I prefissi possono essere utilizzati per configurare facilmente i filtri e-mail e organizzare le notifiche.
Intestazione	Opzionale. Testo dell'intestazione visualizzato all'inizio del corpo del messaggio di posta elettronica. Il testo dell'intestazione può essere utilizzato per anteporre al contenuto del messaggio di posta elettronica informazioni quali nome e indirizzo della società.
Piè di pagina	Opzionale. Testo a piè di pagina visualizzato alla fine del corpo del messaggio di posta elettronica. Il testo a piè di pagina può essere utilizzato per chiudere il messaggio e-mail con informazioni di promemoria come un numero di telefono di un contatto o un collegamento a un sito Web.

5. Fare clic su **Applica modifiche**.

   Viene aggiunto un nuovo modello per le notifiche.

Creare mailing list per le notifiche di allarme (sistema legacy)

Le mailing list consentono di notificare ai destinatari quando viene attivato un allarme legacy o quando cambia lo stato di un servizio. È necessario creare almeno una mailing list prima di poter inviare notifiche di allarme via email. Per inviare una notifica a un singolo destinatario, creare una mailing list con un indirizzo e-mail.

Prima di iniziare

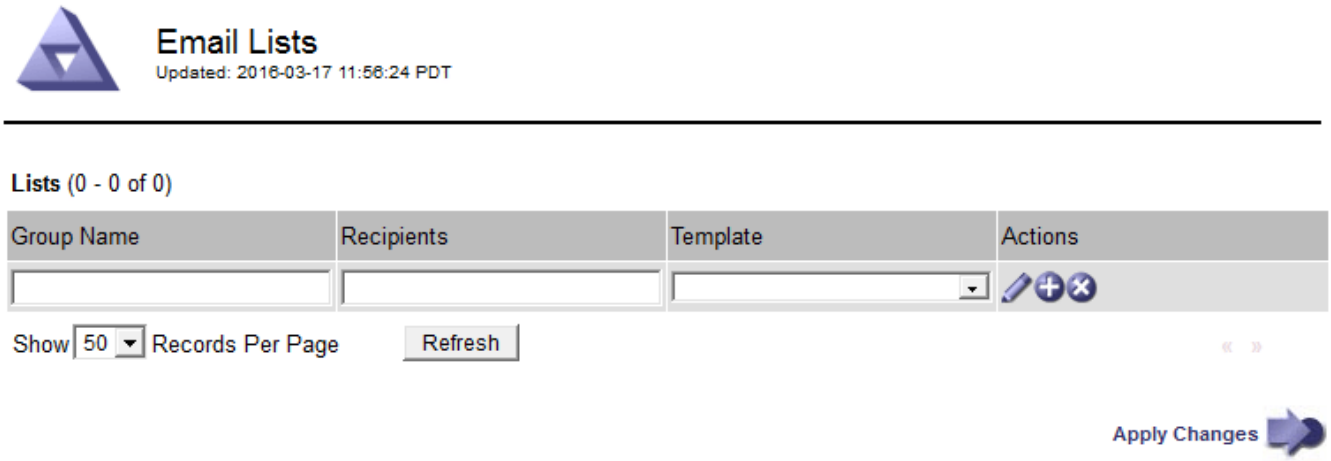
- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Se si desidera specificare un modello e-mail per la mailing list (intestazione personalizzata, piè di pagina e oggetto), è necessario aver già creato il modello.

A proposito di questa attività

Utilizzare queste impostazioni per definire le mailing list utilizzate per le notifiche e-mail di allarme legacy. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Liste**.
3. Fare clic su **Edit** (Modifica) (O *Inserisci* se questa non è la prima mailing list).



4. Nella nuova riga, aggiungere quanto segue:

Elemento	Descrizione
Nome gruppo	Nome univoco utilizzato per identificare la mailing list. I nomi delle mailing list non possono essere duplicati. **Nota:** se si modifica il nome di una mailing list, la modifica non viene propagata alle altre posizioni che utilizzano il nome della mailing list. È necessario aggiornare manualmente tutte le notifiche configurate per utilizzare il nuovo nome della mailing list.
Destinatari	Singolo indirizzo e-mail, una mailing list precedentemente configurata o un elenco di indirizzi e-mail e mailing list delimitati da virgole a cui verranno inviate le notifiche. **Nota:** se un indirizzo e-mail appartiene a più mailing list, viene inviata solo una notifica e-mail quando si verifica un evento di attivazione della notifica.

Elemento	Descrizione
Modello	Se si desidera, selezionare un modello e-mail per aggiungere un'intestazione, un piè di pagina e una riga dell'oggetto univoci alle notifiche inviate a tutti i destinatari della mailing list.

5. Fare clic su **Applica modifiche**.

   Viene creata una nuova mailing list.

Configurazione delle notifiche e-mail per gli allarmi (sistema legacy)

Per ricevere notifiche via email per il sistema di allarme legacy, i destinatari devono essere membri di una mailing list e tale elenco deve essere aggiunto alla pagina Notifiche. Le notifiche sono configurate in modo da inviare e-mail ai destinatari solo quando viene attivato un allarme con un livello di gravità specificato o quando cambia lo stato di un servizio. Pertanto, i destinatari ricevono solo le notifiche necessarie.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario aver configurato un elenco e-mail.

A proposito di questa attività

Utilizzare queste impostazioni per configurare le notifiche per gli allarmi legacy. Queste impostazioni non vengono utilizzate per le notifiche degli avvisi.

Se un indirizzo e-mail (o un elenco) appartiene a più mailing list, viene inviata una sola notifica e-mail quando si verifica un evento di attivazione della notifica. Ad esempio, un gruppo di amministratori all'interno dell'organizzazione può essere configurato per ricevere notifiche per tutti gli allarmi, indipendentemente dalla gravità. Un altro gruppo potrebbe richiedere notifiche solo per gli allarmi con un livello di gravità critico. È possibile appartenere a entrambi gli elenchi. Se viene attivato un allarme critico, si riceve una sola notifica.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Notifiche**.
3. Fare clic su **Edit** (Modifica) (O *Inserisci* se questa non è la prima notifica).
4. In elenco e-mail, selezionare la mailing list.
5. Selezionare uno o più livelli di severità degli allarmi e stati del servizio.
6. Fare clic su **Applica modifiche**.

   Le notifiche vengono inviate alla mailing list quando vengono attivati o modificati gli allarmi con il livello di gravità dell'allarme o lo stato di servizio selezionato.

Eliminazione delle notifiche di allarme per una mailing list (sistema legacy)

È possibile eliminare le notifiche di allarme per una mailing list quando non si desidera più ricevere le notifiche relative agli allarmi. Ad esempio, è possibile eliminare le notifiche relative agli allarmi legacy dopo la transizione all'utilizzo delle notifiche e-mail di avviso.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Utilizzare queste impostazioni per eliminare le notifiche e-mail per il sistema di allarme legacy. Queste impostazioni non si applicano alle notifiche e-mail di avviso.

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Fasi

1. Selezionare **SUPPORT** > **Alarms (legacy)** > **Legacy email setup**.
2. Dal menu e-mail, selezionare **Notifiche**.
3. Fare clic su **Edit** (Modifica) accanto alla mailing list per la quale si desidera eliminare le notifiche.
4. In Sospendi, selezionare la casella di controllo accanto alla mailing list che si desidera sospendere oppure selezionare **Sospendi** nella parte superiore della colonna per eliminare tutte le mailing list.
5. Fare clic su **Applica modifiche**.

   Le notifiche di allarme legacy vengono soppresse per le mailing list selezionate.

Visualizzare gli allarmi legacy

Gli allarmi (sistema legacy) vengono attivati quando gli attributi di sistema raggiungono i valori di soglia degli allarmi. È possibile visualizzare gli allarmi attualmente attivi dalla pagina Allarmi correnti.

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".

Fasi

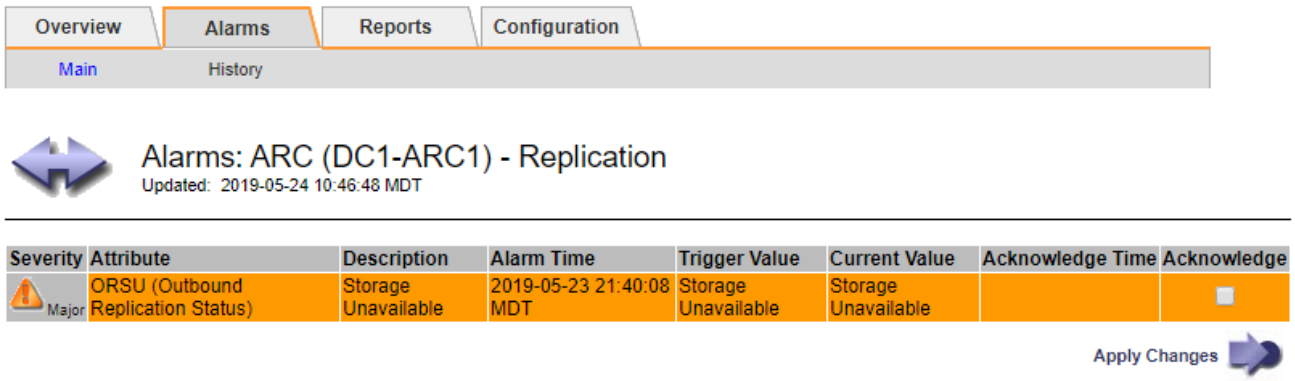
1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Allarmi correnti**.

L'icona di allarme indica la gravità di ciascun allarme, come indicato di seguito:

Icona	Colore	Severità degli allarmi	Significato
	Giallo	Avviso	Il nodo è connesso alla rete, ma esiste una condizione insolita che non influisce sulle normali operazioni.
	Arancione chiaro	Minore	Il nodo è collegato alla rete, ma esiste una condizione anomala che potrebbe influire sul funzionamento in futuro. È necessario indagare per evitare l'escalation.
	Arancione scuro	Maggiore	Il nodo è collegato alla rete, ma esiste una condizione anomala che attualmente influisce sul funzionamento. Ciò richiede una rapida attenzione per evitare l'escalation.
	Rosso	Critico	Il nodo è connesso alla rete, ma esiste una condizione anomala che ha interrotto le normali operazioni. Il problema deve essere risolto immediatamente.

2. Per informazioni sull'attributo che ha causato l'attivazione dell'allarme, fare clic con il pulsante destro del mouse sul nome dell'attributo nella tabella.
3. Per visualizzare ulteriori dettagli su un allarme, fare clic sul nome del servizio nella tabella.

   Viene visualizzata la scheda Allarmi per il servizio selezionato (**SUPPORT** > **Tools** > **Grid topology** > ***Grid Node*** > ***Service*** > **Alarms**).



4. Se si desidera azzerare il conteggio degli allarmi correnti, è possibile eseguire le seguenti operazioni:
   - Riconoscere l'allarme. Un allarme confermato non viene più incluso nel conteggio degli allarmi legacy a meno che non venga attivato al livello di severità successivo o venga risolto e si verifichi di nuovo.
   - Disattivare un particolare allarme predefinito o Global Custom per l'intero sistema per evitare che venga attivato nuovamente.

Informazioni correlate

"Riferimento allarmi (sistema legacy)"

"Riconoscere gli allarmi correnti (sistema precedente)"

"Disattivazione degli allarmi (sistema legacy)"

Riferimento allarmi (sistema legacy)

La tabella seguente elenca tutti gli allarmi predefiniti legacy. Se viene attivato un allarme, è possibile cercare il codice di allarme in questa tabella per individuare le azioni consigliate.

> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Codice	Nome	Servizio	Azione consigliata
ABRL	Relè attributi disponibili	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Ripristinare la connettività a un servizio (un servizio ADC) che esegue un Attribute Relay Service il prima possibile. Se non sono presenti relay di attributi connessi, il nodo della griglia non può riportare i valori di attributo al servizio NMS. Pertanto, il servizio NMS non può più monitorare lo stato del servizio o aggiornare gli attributi del servizio. Se il problema persiste, contattare il supporto tecnico.
ACMS	Servizi metadati disponibili	BARC, BLDR, BCMN	Viene attivato un allarme quando un servizio LDR o ARC perde la connessione a un servizio DDS. In questo caso, le transazioni di acquisizione o recupero non possono essere elaborate. Se l'indisponibilità dei servizi DDS è solo un breve problema transitorio, le transazioni possono essere ritardate. Controllare e ripristinare le connessioni a un servizio DDS per annullare questo allarme e ripristinare il servizio alla funzionalità completa.
ATTI	Stato del servizio di tiering cloud	ARCO	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Cloud Tiering - Simple Storage Service (S3). Se l'attributo ACTS per il nodo di archiviazione è impostato su sola lettura abilitata o lettura/scrittura disabilitata, è necessario impostare l'attributo su lettura/scrittura abilitata. Se viene attivato un allarme grave a causa di un errore di autenticazione, verificare le credenziali associate al bucket di destinazione e aggiornare i valori, se necessario. Se viene attivato un allarme grave per qualsiasi altro motivo, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
ADCA	Stato ADC	ADC	Se viene attivato un allarme, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **ADC** > **Overview** > **Main** e **ADC** > **Alarms** > **Main** per determinare la causa dell'allarme. Se il problema persiste, contattare il supporto tecnico.
ADCE	Stato ADC	ADC	Se il valore di ADC state (Stato ADC) è Standby, continuare il monitoraggio del servizio e, se il problema persiste, contattare il supporto tecnico. Se il valore di Stato ADC è offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
AITE	Recupera stato	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore Retrieve state (Stato recupero) è Waiting for Target (in attesa di destinazione), controllare il server middleware TSM e assicurarsi che funzioni correttamente. Se il nodo di archiviazione è stato appena aggiunto al sistema StorageGRID, assicurarsi che la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione sia configurata correttamente. Se il valore di Archive Retrieve state (Stato recupero archivio) è Offline (non in linea), provare ad aggiornare lo stato in Online. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Archive Retrieve state** > **Online** e fare clic su **Apply Changes**. Se il problema persiste, contattare il supporto tecnico.
AITU	Recupera stato	BARC	Se il valore di Recupera stato è Target Error (errore di destinazione), verificare la presenza di errori nel sistema di storage di archiviazione esterno di destinazione. Se il valore di Archive Retrieve Status (Stato recupero archivio) è Session Lost (sessione persa), controllare il sistema di storage di archiviazione esterno di destinazione per assicurarsi che sia online e funzioni correttamente. Verificare la connessione di rete con la destinazione. Se il valore di Archive Retrieve Status (Stato recupero archivio) è Unknown Error (errore sconosciuto), contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
ALIS	Sessioni di attributi inbound	ADC	Se il numero di sessioni di attributi in entrata su un relay di attributi aumenta troppo, può essere un'indicazione che il sistema StorageGRID è diventato sbilanciato. In condizioni normali, le sessioni degli attributi devono essere distribuite uniformemente tra i servizi ADC. Uno squilibrio può causare problemi di performance. Se il problema persiste, contattare il supporto tecnico.
ALOS	Sessioni di attributi in uscita	ADC	Il servizio ADC ha un numero elevato di sessioni di attributi e sta diventando sovraccarico. Se questo allarme viene attivato, contattare il supporto tecnico.
ALUR	Repository di attributi non raggiungibili	ADC	Verificare la connettività di rete con il servizio NMS per assicurarsi che il servizio possa contattare il repository degli attributi. Se questo allarme viene attivato e la connettività di rete è buona, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
AMQS	Messaggi di controllo in coda	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se i messaggi di audit non possono essere inoltrati immediatamente a un relay di audit o a un repository, i messaggi vengono memorizzati in una coda di dischi. Se la coda dei dischi si esaurisce, possono verificarsi interruzioni. Per consentire di rispondere in tempo per evitare un'interruzione, gli allarmi AMQS vengono attivati quando il numero di messaggi nella coda del disco raggiunge le seguenti soglie: • Avviso: Più di 100,000 messaggi • Minore: Almeno 500,000 messaggi • Maggiore: Almeno 2,000,000 messaggi • Critico: Almeno 5,000,000 messaggi Se viene attivato un allarme AMQS, controllare il carico sul sistema. Se si è verificato un numero significativo di transazioni, l'allarme dovrebbe risolversi automaticamente nel tempo. In questo caso, è possibile ignorare l'allarme. Se l'allarme persiste e aumenta di severità, visualizzare un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, il carico di audit ha probabilmente superato la capacità di audit del sistema. Ridurre la velocità operativa del client o diminuire il numero di messaggi di audit registrati cambiando il livello di audit in Error (errore) o Off (Disattivato). Vedere "Configurare i messaggi di audit e le destinazioni dei log".
AOTE	Store state (Stato archiviazione)	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore di Store state è in attesa di Target, controllare il sistema di storage di archiviazione esterno e assicurarsi che funzioni correttamente. Se il nodo di archiviazione è stato appena aggiunto al sistema StorageGRID, assicurarsi che la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione sia configurata correttamente. Se il valore di Store state è offline, controlla il valore di Store Status. Correggere eventuali problemi prima di riportare lo stato dello store in linea.

Codice	Nome	Servizio	Azione consigliata
AOTU	Stato del negozio	BARC	Se il valore di Store Status (Stato negozio) è Session Lost (sessione persa), verificare che il sistema di storage di archiviazione esterno sia connesso e online. Se il valore di Target Error (errore di destinazione), verificare la presenza di errori nel sistema di storage di archiviazione esterno. Se il valore di Stato negozio è Unknown Error, contattare il supporto tecnico.
APM	Connettività storage multipath	SSM	Se l'allarme di stato multipercorso viene visualizzato come "danneggiato" (selezionare **SUPPORTO** > **Strumenti** > **topologia griglia**, quindi selezionare ***sito*** > ***nodo griglia*** > **SSM** > **Eventi**), procedere come segue: 1. Collegare o sostituire il cavo che non visualizza spie luminose. 2. Attendere da uno a cinque minuti. Non scollegare l'altro cavo fino a cinque minuti dopo aver collegato il primo cavo. Se si scollega troppo presto, il volume root può diventare di sola lettura, il che richiede il riavvio dell'hardware. 3. Tornare alla pagina **SSM** > **risorse** e verificare che lo stato del multipath "degradato" sia stato modificato in "nominale" nella sezione hardware di archiviazione.
ARCE	ARC state (Stato ARCO)	ARCO	Il servizio ARC ha uno stato di standby fino all'avvio di tutti i componenti ARC (Replication, Store, Retrieve, Target). Passa quindi a Online. Se il valore dello stato ARC non passa da Standby a Online, controllare lo stato dei componenti ARC. Se il valore di ARC state (Stato arco) è Offline (non in linea), riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
AROQ	Oggetti in coda	ARCO	Questo allarme può essere attivato se il dispositivo di storage rimovibile è lento a causa di problemi con il sistema di storage di archiviazione esterno di destinazione o se si verificano errori di lettura multipli. Verificare la presenza di errori nel sistema di storage di archiviazione esterno e assicurarsi che funzioni correttamente. In alcuni casi, questo errore può verificarsi a causa di un elevato numero di richieste di dati. Monitorare il numero di oggetti accodati quando l'attività di sistema diminuisce.
ARRF	Errori della richiesta	ARCO	Se un recupero dal sistema di storage di archiviazione esterno di destinazione non riesce, il nodo di archiviazione tenta di nuovo il recupero in quanto l'errore può essere dovuto a un problema transitorio. Tuttavia, se i dati dell'oggetto sono corrotti o sono stati contrassegnati come indisponibili in modo permanente, il recupero non avrà esito negativo. Invece, il nodo di archiviazione tenta continuamente il recupero e il valore di Request Failures continua ad aumentare. Questo allarme può indicare che il supporto di memorizzazione contenente i dati richiesti è corrotto. Controllare il sistema di storage di archiviazione esterno per diagnosticare ulteriormente il problema. Se si determina che i dati dell'oggetto non sono più presenti nell'archivio, l'oggetto dovrà essere rimosso dal sistema StorageGRID. Per ulteriori informazioni, contatta il supporto tecnico. Una volta risolto il problema che ha attivato questo allarme, ripristinare il conteggio degli errori. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Reset Request Failure Count** e fare clic su **Apply Changes**.

Codice	Nome	Servizio	Azione consigliata
ARRV	Errori di verifica	ARCO	Per diagnosticare e correggere questo problema, contattare il supporto tecnico. Dopo aver risolto il problema che ha generato questo allarme, azzerare il conteggio dei guasti. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Reset Verification Failure Count** e fare clic su **Apply Changes**.
ARVF	Guasti del negozio	ARCO	Questo allarme può verificarsi in seguito a errori del sistema di storage di archiviazione esterno di destinazione. Verificare la presenza di errori nel sistema di storage di archiviazione esterno e assicurarsi che funzioni correttamente. Una volta risolto il problema che ha attivato questo allarme, ripristinare il conteggio degli errori. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **ARC** > **Recupera** > **Configurazione** > **principale**, selezionare **Reset Store Failure Count** e fare clic su **Apply Changes**.
ASXP	Controlla le condivisioni	AMS	Viene attivato un allarme se il valore di Audit shares è Unknown (Sconosciuto). Questo allarme può indicare un problema con l'installazione o la configurazione del nodo di amministrazione. Se il problema persiste, contattare il supporto tecnico.
AUMA	Stato AMS	AMS	Se il valore di AMS Status (Stato AMS) è DB Connectivity Error (errore di connettività DB), riavviare il nodo Grid. Se il problema persiste, contattare il supporto tecnico.
AUME	Stato AMS	AMS	Se il valore di AMS state (Stato AMS) è Standby, continuare il monitoraggio del sistema StorageGRID. Se il problema persiste, contattare il supporto tecnico. Se il valore di AMS state è Offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
AUXS	Audit Export Status (Stato esportazione audit)	AMS	Se viene attivato un allarme, correggere il problema sottostante, quindi riavviare il servizio AMS. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
BADD	Storage Controller Failed Drive Count (Conteggio dischi guasto	SSM	Questo allarme viene attivato quando uno o più dischi di un'appliance StorageGRID si sono guastati o non sono ottimali. Sostituire le unità secondo necessità.
BASE	Identificatori di oggetti disponibili	CMN	Quando viene eseguito il provisioning di un sistema StorageGRID, al servizio CMN viene assegnato un numero fisso di identificatori di oggetti. Questo allarme viene attivato quando il sistema StorageGRID inizia a esaurire la fornitura di identificatori di oggetti. Per assegnare altri identificatori, contattare il supporto tecnico.
BASSI	Stato allocazione blocco identificatore	CMN	Per impostazione predefinita, viene attivato un allarme quando non è possibile allocare gli identificatori degli oggetti perché non è possibile raggiungere il quorum ADC. L'allocazione del blocco di identificatori sul servizio CMN richiede che un quorum (50% + 1) dei servizi ADC sia online e connesso. Se il quorum non è disponibile, il servizio CMN non è in grado di allocare nuovi blocchi identificatori fino a quando non viene ristabilita il quorum ADC. In caso di perdita del quorum ADC, in genere non vi è alcun impatto immediato sul sistema StorageGRID (i client possono ancora acquisire e recuperare il contenuto), in quanto circa un mese di fornitura di identificatori viene memorizzato nella cache altrove nella griglia; Tuttavia, se la condizione persiste, il sistema StorageGRID perderà la capacità di acquisire nuovi contenuti. Se viene attivato un allarme, esaminare il motivo della perdita del quorum ADC (ad esempio, potrebbe trattarsi di un guasto di rete o del nodo di storage) e intraprendere un'azione correttiva. Se il problema persiste, contattare il supporto tecnico.
BRDT	Temperatura dello chassis del controller di calcolo	SSM	Viene attivato un allarme se la temperatura del controller di calcolo in un'appliance StorageGRID supera una soglia nominale. Controllare i componenti hardware e i problemi ambientali per verificare la presenza di condizioni di surriscaldamento. Se necessario, sostituire il componente.

Codice	Nome	Servizio	Azione consigliata
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Viene attivato un allarme se il tempo di servizio (secondi) differisce significativamente dall'ora del sistema operativo. In condizioni normali, il servizio dovrebbe risincronizzarsi. Se il tempo di servizio è troppo lontano dall'ora del sistema operativo, le operazioni del sistema potrebbero risentirne. Verificare che l'origine dell'ora del sistema StorageGRID sia corretta. Se il problema persiste, contattare il supporto tecnico.
BTSE	Stato del clock	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Viene attivato un allarme se l'ora del servizio non è sincronizzata con l'ora tracciata dal sistema operativo. In condizioni normali, il servizio dovrebbe risincronizzarsi. Se il tempo si disasse troppo dall'ora del sistema operativo, le operazioni del sistema potrebbero risentirne. Verificare che l'origine dell'ora del sistema StorageGRID sia corretta. Se il problema persiste, contattare il supporto tecnico.
CAHP	Percentuale di utilizzo di Java Heap	DDS	Viene attivato un allarme se Java non è in grado di eseguire la garbage collection a una velocità tale da consentire al sistema di funzionare correttamente. Un allarme potrebbe indicare un carico di lavoro dell'utente che supera le risorse disponibili nel sistema per l'archivio di metadati DDS. Controllare l'attività ILM nella dashboard oppure selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***site*** > ***grid node*** > **DDS** > **Resources** > **Overview** > **Main**. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
CASA	Data Store Status (Stato archivio dati)	DDS	Viene generato un allarme se l'archivio di metadati Cassandra non è più disponibile. Controllare lo stato di Cassandra: 1. Nel nodo di storage, accedere come admin e. `su` Per eseguire l'root utilizzando la password elencata nel file Passwords.txt. 2. Inserire: `service cassandra status` 3. Se Cassandra non è in esecuzione, riavviarlo: `service cassandra restart` Questo allarme potrebbe anche indicare che l'archivio di metadati (database Cassandra) per un nodo di storage deve essere ricostruito. Consultare le informazioni relative alla risoluzione dei problemi relativi all'allarme Services: Status - Cassandra (SVST) in "Risolvere i problemi relativi ai metadati". Se il problema persiste, contattare il supporto tecnico.
CASO	Data Store state (Stato archivio dati)	DDS	Questo allarme viene attivato durante l'installazione o l'espansione per indicare che un nuovo archivio di dati si sta unendo alla griglia.
CCNA	Hardware di calcolo	SSM	Questo allarme viene attivato se lo stato dell'hardware del controller di calcolo in un'appliance StorageGRID richiede attenzione.

Codice	Nome	Servizio	Azione consigliata
CDLP	Spazio utilizzato metadati (percentuale)	DDS	Questo allarme viene attivato quando lo spazio effettivo dei metadati (CEMS) raggiunge il 70% di pieno (allarme minore), il 90% di pieno (allarme maggiore) e il 100% di pieno (allarme critico). Se questo allarme raggiunge la soglia del 90%, viene visualizzato un avviso sul dashboard in Grid Manager. È necessario eseguire una procedura di espansione per aggiungere nuovi nodi di storage il prima possibile. Vedere "Espandere una griglia". Se questo allarme raggiunge la soglia del 100%, è necessario interrompere l'acquisizione di oggetti e aggiungere nodi di storage immediatamente. Cassandra richiede una certa quantità di spazio per eseguire operazioni essenziali come la compattazione e la riparazione. Queste operazioni saranno influenzate se i metadati dell'oggetto utilizzano più del 100% dello spazio consentito. Possono verificarsi risultati indesiderati. **Nota**: Se non si riesce ad aggiungere nodi di storage, contattare il supporto tecnico. Una volta aggiunti nuovi nodi di storage, il sistema ribilancia automaticamente i metadati degli oggetti in tutti i nodi di storage e l'allarme viene cancellato. Inoltre, consultare le informazioni sulla risoluzione dei problemi relativi all'avviso di storage con metadati bassi in "Risolvere i problemi relativi ai metadati". Se il problema persiste, contattare il supporto tecnico.
CMNA	Stato CMN	CMN	Se il valore di CMN Status (Stato CMN) è Error (errore), selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***Site*** > ***Grid node*** > **CMN** > **Overview** > **Main** e **CMN** > **Alarms** > **Main** per determinare la causa dell'errore e risolvere il problema. Viene attivato un allarme e il valore di CMN Status (Stato CMN) è No Online CMN (Nessuna CMN online) durante un aggiornamento hardware del nodo di amministrazione primario quando vengono commutate le CMN (il valore del vecchio stato CMN è Standby e il nuovo è Online). Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
CPRC	Capacità rimanente	NMS	Viene attivato un allarme se la capacità rimanente (numero di connessioni disponibili che è possibile aprire nel database NMS) scende al di sotto della gravità dell'allarme configurata. Se viene attivato un allarme, contattare il supporto tecnico.
CPSA	Alimentatore a del controller di calcolo	SSM	Viene attivato un allarme in caso di problemi con l'alimentazione A nel controller di calcolo di un'appliance StorageGRID. Se necessario, sostituire il componente.
CPSB	Alimentatore del controller di calcolo B	SSM	Viene attivato un allarme in caso di problemi con l'alimentazione B nel controller di calcolo di un'appliance StorageGRID. Se necessario, sostituire il componente.
CPUT	Temperatura CPU del controller di calcolo	SSM	Viene attivato un allarme se la temperatura della CPU nel controller di calcolo di un'appliance StorageGRID supera una soglia nominale. Se il nodo di storage è un'appliance StorageGRID, il sistema StorageGRID indica che il controller richiede attenzione. Controllare i componenti hardware e i problemi ambientali per verificare la presenza di condizioni di surriscaldamento. Se necessario, sostituire il componente.
DNST	DNS Status (Stato DNS)	SSM	Al termine dell'installazione, viene attivato un allarme DNST nel servizio SSM. Una volta configurato il DNS e le nuove informazioni sul server raggiungono tutti i nodi della griglia, l'allarme viene annullato.

Codice	Nome	Servizio	Azione consigliata
ECCD	Rilevati frammenti corrotti	LDR	Un allarme viene attivato quando il processo di verifica in background rileva un frammento danneggiato sottoposto a erasure coding. Se viene rilevato un frammento corrotto, si tenta di ricostruire il frammento. Ripristinare i frammenti danneggiati rilevati e copiare gli attributi Lost su zero e monitorarli per verificare se i conteggi si rialzano. Se il numero aumenta, potrebbe esserci un problema con lo storage sottostante del nodo di storage. Una copia dei dati oggetto sottoposti a erasure coding non viene considerata mancante fino a quando il numero di frammenti persi o corrotti non viola la tolleranza di errore del codice di cancellazione; pertanto, è possibile avere un frammento corrotto e poter recuperare l'oggetto. Se il problema persiste, contattare il supporto tecnico.
ECST	Stato di verifica	LDR	Questo allarme indica lo stato corrente del processo di verifica in background per i dati oggetto con erasure coding su questo nodo di storage. In caso di errore nel processo di verifica in background, viene attivato un allarme grave.
FOPN	Aprire file Descriptor	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Il FOPN può diventare grande durante le attività di picco. Se non diminuisce durante i periodi di attività lenta, contattare il supporto tecnico.
HSTE	HTTP state (Stato HTTP)	BLDR	Consultare le azioni consigliate per HSTU.

Codice	Nome	Servizio	Azione consigliata
HSTU	HTTP Status (Stato HTTP)	BLDR	HSTE e HSTU sono correlati a HTTP per tutto il traffico LDR, inclusi S3, Swift e altro traffico StorageGRID interno. Un allarme indica che si è verificata una delle seguenti situazioni: • HTTP è stato portato offline manualmente. • L'attributo HTTP Auto-Start è stato disattivato. • Chiusura del servizio LDR in corso. L'attributo HTTP Auto-Start è attivato per impostazione predefinita. Se questa impostazione viene modificata, HTTP potrebbe rimanere offline dopo un riavvio. Se necessario, attendere il riavvio del servizio LDR. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Storage Node*** > **LDR** > **Configuration**. Se HTTP non è in linea, metterlo in linea. Verificare che l'attributo Avvio automatico HTTP sia attivato. Se HTTP rimane offline, contattare il supporto tecnico.
HTA	Avvio automatico HTTP	LDR	Specifica se avviare automaticamente i servizi HTTP all'avvio. Questa è un'opzione di configurazione specificata dall'utente.
IRSU	Stato della replica in entrata	BLDR, BARC	Un allarme indica che la replica in entrata è stata disattivata. Confermare le impostazioni di configurazione: Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**.
LATA	Latenza media	NMS	Verificare la presenza di problemi di connettività. Controllare l'attività del sistema per verificare che l'attività del sistema aumenti. Un aumento dell'attività di sistema determinerà un aumento dell'attributo dell'attività dei dati. L'aumento dell'attività comporterà un ritardo nell'elaborazione dei dati degli attributi. Si tratta di un'attività normale del sistema che verrà a trovarsi in una posizione secondaria. Verificare la presenza di più allarmi. Un aumento dei tempi di latenza medi può essere indicato da un numero eccessivo di allarmi attivati. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
DRE	Stato LDR	LDR	Se il valore dello stato LDR è Standby, continuare a monitorare la situazione e, se il problema persiste, contattare il supporto tecnico. Se il valore di stato LDR è Offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
PERSO	Oggetti persi	DDS, LDR	Viene attivato quando il sistema StorageGRID non riesce a recuperare una copia dell'oggetto richiesto da qualsiasi punto del sistema. Prima che venga attivato un allarme LOST (Lost Objects), il sistema tenta di recuperare e sostituire un oggetto mancante da un'altra parte del sistema. Gli oggetti persi rappresentano una perdita di dati. L'attributo Lost Objects viene incrementato ogni volta che il numero di posizioni di un oggetto scende a zero senza che il servizio DDS purifichi intenzionalmente il contenuto per soddisfare la policy ILM. Esaminare immediatamente gli allarmi PERSI (oggetti SMARRITI). Se il problema persiste, contattare il supporto tecnico. "Risolvere i problemi relativi ai dati degli oggetti persi e mancanti"
MCEP	Scadenza del certificato dell'interfaccia di gestione	CMN	Viene attivato quando il certificato utilizzato per accedere all'interfaccia di gestione sta per scadere. 1. Da Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**. 2. Nella scheda **Global**, selezionare **Management interface certificate**. 3. "Caricare un nuovo certificato dell'interfaccia di gestione."
MINQ	Notifiche e-mail in coda	NMS	Controllare le connessioni di rete dei server che ospitano il servizio NMS e il server di posta esterno. Verificare inoltre che la configurazione del server di posta elettronica sia corretta. "Configurare le impostazioni del server di posta elettronica per gli allarmi (sistema legacy)"

Codice	Nome	Servizio	Azione consigliata
MIN	Email Notifications Status (Stato notifiche e-mail)	BNMS	Se il servizio NMS non riesce a connettersi al server di posta, viene attivato un allarme minore. Controllare le connessioni di rete dei server che ospitano il servizio NMS e il server di posta esterno. Verificare inoltre che la configurazione del server di posta elettronica sia corretta. "Configurare le impostazioni del server di posta elettronica per gli allarmi (sistema legacy)"
SIG.NA	Stato del motore di interfaccia NMS	BNMS	Viene attivato un allarme se il motore di interfaccia NMS sul nodo di amministrazione che raccoglie e genera il contenuto dell'interfaccia viene disconnesso dal sistema. Controllare Server Manager per determinare se la singola applicazione del server non è disponibile.
NANG	Network Auto Negotiate (negoziazione automatica di rete	SSM	Controllare la configurazione della scheda di rete. L'impostazione deve corrispondere alle preferenze dei router e degli switch di rete. Un'impostazione errata può avere un impatto grave sulle prestazioni del sistema.
NUP	Impostazione fronte/retro di rete	SSM	Controllare la configurazione della scheda di rete. L'impostazione deve corrispondere alle preferenze dei router e degli switch di rete. Un'impostazione errata può avere un impatto grave sulle prestazioni del sistema.
NLNK	Network link Detect (rilevamento collegamento di rete	SSM	Controllare i collegamenti dei cavi di rete sulla porta e sullo switch. Controllare le configurazioni di router, switch e adattatori di rete. Riavviare il server. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
NRER	Errori di ricezione	SSM	Di seguito sono riportate le cause degli allarmi NRER: • Mancata corrispondenza FEC (Forward Error Correction) • Mancata corrispondenza tra porta dello switch e MTU della scheda NIC • Elevati tassi di errore di collegamento • Buffer di anello NIC scaduto Consultare le informazioni relative alla risoluzione dei problemi relativi all'allarme NRER (Network Receive Error) in "Risolvere i problemi di rete, hardware e piattaforma".
NRLY	Relè di audit disponibili	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Se i relè di audit non sono connessi ai servizi ADC, non è possibile segnalare gli eventi di audit. Vengono messi in coda e non disponibili per gli utenti fino al ripristino della connessione. Ripristinare la connettività a un servizio ADC il prima possibile. Se il problema persiste, contattare il supporto tecnico.
NSCA	Stato NMS	NMS	Se il valore di NMS Status (Stato NMS) è DB Connectivity Error (errore di connettività DB), riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
NSCE	Stato NMS	NMS	Se il valore di NMS state (Stato NMS) è Standby, continuare il monitoraggio e, se il problema persiste, contattare il supporto tecnico. Se il valore di NMS state (Stato NMS) è Offline, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
NSPD	Velocità	SSM	Ciò può essere causato da problemi di connettività di rete o di compatibilità dei driver. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
NTBR	Spazio tabella libero	NMS	Se viene attivato un allarme, verificare la velocità di modifica dell'utilizzo del database. Un calo improvviso (invece di un cambiamento graduale nel tempo) indica una condizione di errore. Se il problema persiste, contattare il supporto tecnico. La regolazione della soglia di allarme consente di gestire in modo proattivo quando è necessario allocare ulteriore storage. Se lo spazio disponibile raggiunge una soglia bassa (vedere soglia di allarme), contattare il supporto tecnico per modificare l'allocazione del database.
NTER.A.	Errori di trasmissione	SSM	Questi errori possono essere azzerati senza essere reimpostati manualmente. In caso contrario, controllare l'hardware di rete. Verificare che l'hardware e il driver della scheda siano installati e configurati correttamente per funzionare con i router e gli switch di rete. Una volta risolto il problema sottostante, azzerare il contatore. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **Main**, selezionare **Reset Transmit Error Count** e fare clic su **Apply Changes**.
NTFQ	Offset frequenza NTP	SSM	Se l'offset di frequenza supera la soglia configurata, è probabile che si sia verificato un problema hardware con l'orologio locale. Se il problema persiste, contattare il supporto tecnico per richiedere la sostituzione.
NTLK	Blocco NTP	SSM	Se il daemon NTP non è bloccato su una fonte di tempo esterna, controllare la connettività di rete alle fonti di tempo esterne designate, la loro disponibilità e la loro stabilità.
NTOF	Offset ora NTP	SSM	Se l'offset temporale supera la soglia configurata, è probabile che si sia verificato un problema hardware con l'oscillatore del clock locale. Se il problema persiste, contattare il supporto tecnico per richiedere la sostituzione.

Codice	Nome	Servizio	Azione consigliata
NTSJ	Jitter di origine temporale selezionato	SSM	Questo valore indica l'affidabilità e la stabilità dell'origine temporale utilizzata da NTP sul server locale come riferimento. Se viene attivato un allarme, può essere un'indicazione che l'oscillatore dell'origine del tempo è difettoso o che si è verificato un problema con il collegamento WAN all'origine del tempo.
NTSU	NTP Status (Stato NTP)	SSM	Se il valore NTP Status (Stato NTP) non è in esecuzione, contattare il supporto tecnico.
OPST	Stato generale dell'alimentazione	SSM	Viene attivato un allarme se l'alimentazione di un apparecchio StorageGRID non rientra nella tensione di esercizio consigliata. Controllare lo stato dell'alimentatore A o B per determinare quale alimentatore funziona in modo anomalo. Se necessario, sostituire l'alimentatore.
OQRT	Oggetti in quarantena	LDR	Dopo il ripristino automatico degli oggetti da parte del sistema StorageGRID, è possibile rimuovere gli oggetti in quarantena dalla directory di quarantena. 1. Selezionare **SUPPORT** > **Tools** > **Grid topology**. 2. Selezionare **sito** > **nodo di storage** > **LDR** > **verifica** > **Configurazione** > **principale**. 3. Selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena). 4. Fare clic su **Applica modifiche**. Gli oggetti in quarantena vengono rimossi e il conteggio viene azzerato.
ORSU	Stato della replica in uscita	BLDR, BARC	Un allarme indica che la replica in uscita non è possibile: Lo storage si trova in uno stato in cui gli oggetti non possono essere recuperati. Viene attivato un allarme se la replica in uscita viene disattivata manualmente. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration**. Viene attivato un allarme se il servizio LDR non è disponibile per la replica. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Storage**.

Codice	Nome	Servizio	Azione consigliata
OSLF	Stato dello shelf	SSM	Viene attivato un allarme se lo stato di uno dei componenti dello shelf di storage di un'appliance di storage è degradato. I componenti dello shelf di storage includono gli IOM, le ventole, gli alimentatori e i cassetti delle unità. Se viene attivato questo allarme, consultare le istruzioni di manutenzione dell'apparecchio.
PMEM	Utilizzo della memoria di servizio (percentuale)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Può avere un valore superiore a Y% di RAM, dove Y rappresenta la percentuale di memoria utilizzata dal server. I valori inferiori al 80% sono normali. Oltre il 90% è considerato un problema. Se l'utilizzo della memoria è elevato per un singolo servizio, monitorare la situazione e analizzare. Se il problema persiste, contattare il supporto tecnico.
PSA	Power Supply A Status (Stato alimentatore A)	SSM	Viene attivato un allarme se l'alimentazione A di un apparecchio StorageGRID non rientra nella tensione di esercizio consigliata. Se necessario, sostituire l'alimentatore A.
PSB	Stato dell'alimentatore B.	SSM	Viene attivato un allarme se l'alimentazione B di un apparecchio StorageGRID si discosta dalla tensione di esercizio consigliata. Se necessario, sostituire l'alimentatore B.
RDTE	Stato di Tivoli Storage Manager	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore di Tivoli Storage Manager state (Stato di Tivoli Storage Manager) è offline, controllare lo stato di Tivoli Storage Manager e risolvere eventuali problemi. Riportare il componente online. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **ARC** > **Target** > **Configuration** > **Main**, selezionare **Tivoli Storage Manager state** > **Online** e fare clic su **Apply Changes**.

Codice	Nome	Servizio	Azione consigliata
RDTU	Stato di Tivoli Storage Manager	BARC	Disponibile solo per i nodi di archiviazione con un tipo di destinazione di Tivoli Storage Manager (TSM). Se il valore dello stato di Tivoli Storage Manager è errore di configurazione e il nodo di archiviazione è stato appena aggiunto al sistema StorageGRID, assicurarsi che il server middleware TSM sia configurato correttamente. Se il valore di Stato di Tivoli Storage Manager è errore di connessione o errore di connessione, Riprova, controllare la configurazione di rete sul server middleware TSM e la connessione di rete tra il server middleware TSM e il sistema StorageGRID. Se il valore di Stato di Tivoli Storage Manager è errore di autenticazione o errore di autenticazione, riconnessione, il sistema StorageGRID può connettersi al server middleware TSM, ma non può autenticare la connessione. Verificare che il server middleware TSM sia configurato con l'utente, la password e le autorizzazioni corretti, quindi riavviare il servizio. Se il valore di Tivoli Storage Manager Status (Stato di Tivoli Storage Manager) è Session Failure (errore di sessione), una sessione stabilita è stata persa inaspettatamente. Verificare la connessione di rete tra il server middleware TSM e il sistema StorageGRID. Verificare la presenza di errori nel server middleware. Se il valore di Tivoli Storage Manager Status (Stato di Tivoli Storage Manager) è Unknown Error (errore sconosciuto), contattare il supporto tecnico.
RRF	Repliche in entrata — non riuscite	BLDR, BARC	Un allarme Inbound Replications — Failed (repliche in entrata) può verificarsi in periodi di carico elevato o interruzioni temporanee della rete. Una volta ridotta l'attività del sistema, questo allarme dovrebbe essere disattivato. Se il numero di repliche non riuscite continua ad aumentare, cercare i problemi di rete e verificare che i servizi LDR e ARC di origine e destinazione siano online e disponibili. Per azzerare il conteggio, selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***Site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**. Selezionare **Reset Inbound Replication Failure Count**, quindi fare clic su **Apply Changes** (Applica modifiche).

Codice	Nome	Servizio	Azione consigliata
RIRQ	Repliche inbound — in coda	BLDR, BARC	Gli allarmi possono verificarsi in periodi di carico elevato o interruzione temporanea della rete. Una volta ridotta l'attività del sistema, questo allarme dovrebbe essere disattivato. Se il numero di repliche in coda continua ad aumentare, cercare i problemi di rete e verificare che i servizi LDR e ARC di origine e destinazione siano online e disponibili.
RORQ	Repliche in uscita — in coda	BLDR, BARC	La coda di replica in uscita contiene i dati oggetto copiati per soddisfare le regole ILM e gli oggetti richiesti dai client. Un allarme può verificarsi in seguito a un sovraccarico del sistema. Attendere per verificare se l'allarme viene cancellato quando l'attività del sistema diminuisce. Se l'allarme si ripete, aggiungere capacità aggiungendo nodi di storage.
SAVP	Spazio totale utilizzabile (percentuale)	LDR	Se lo spazio utilizzabile raggiunge una soglia bassa, le opzioni includono l'espansione del sistema StorageGRID o lo spostamento dei dati dell'oggetto nell'archivio attraverso un nodo di archiviazione.
SCA	Stato	CMN	Se il valore di Status (Stato) per l'attività della griglia attiva è Error (errore), cercare il messaggio Grid task (attività griglia). Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***Site*** > ***Grid node*** > **CMN** > **Grid Tasks** > **Overview** > **Main**. Il messaggio dell'attività griglia visualizza informazioni sull'errore (ad esempio, "controllo non riuscito sul nodo 12130011"). Dopo aver esaminato e corretto il problema, riavviare l'attività Grid. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Configuration** > **Main** e selezionare **Actions** > **Run**. Se il valore Stato per un'attività di griglia interrotta è Error, riprovare a terminare l'attività di griglia. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
SCEP	Scadenza del certificato per gli endpoint del servizio API di storage	CMN	Viene attivato quando il certificato utilizzato per l'accesso agli endpoint API dello storage sta per scadere. 1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**. 2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**. 3. "Caricare un nuovo certificato API S3 e Swift."
SCHR	Stato	CMN	Se il valore di Status (Stato) per l'attività della griglia storica viene interrotto, esaminare il motivo ed eseguire nuovamente l'attività, se necessario. Se il problema persiste, contattare il supporto tecnico.
SCSA	Controller dello storage A	SSM	Viene attivato un allarme in caso di problemi con lo storage controller A in un'appliance StorageGRID. Se necessario, sostituire il componente.
SCSB	Controller dello storage B	SSM	Viene attivato un allarme in caso di problemi con lo storage controller B in un'appliance StorageGRID. Se necessario, sostituire il componente. Alcuni modelli di appliance non dispongono di un controller di storage B.
SHLH	Salute	LDR	Se il valore di Health per un archivio di oggetti è Error (errore), controllare e correggere: • problemi con il volume montato • errori del file system
SLSA	Media carico CPU	SSM	Maggiore è il valore, maggiore è il numero di componenti del sistema. Se la media del carico della CPU persiste a un valore elevato, è necessario esaminare il numero di transazioni nel sistema per determinare se ciò sia dovuto a un carico pesante in quel momento. Visualizza un grafico della media di carico della CPU: Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **SSM** > **Resources** > **Reports** > **Charts**. Se il carico sul sistema non è elevato e il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
SMST	Log Monitor state (Stato monitoraggio registro) non è connesso per un periodo di tempo persistente, contattare il supporto tecnico.	SSM	Se il valore Log Monitor state (Stato monitoraggio registro) non è connesso per un periodo di tempo persistente, contattare il supporto tecnico.
SMTT	Eventi totali	SSM	Se il valore di Total Events (Eventi totali) è maggiore di zero, controllare se la causa può essere la presenza di eventi noti (come gli errori di rete). A meno che questi errori non siano stati cancellati (ovvero, il conteggio è stato reimpostato su 0), possono essere attivati gli allarmi Total Events (Eventi totali). Una volta risolto il problema, azzerare il contatore per eliminare l'allarme. Selezionare **NODI** > ***sito*** > ***nodo griglia*** > **Eventi** > **Ripristina conteggi eventi**. Per reimpostare i conteggi degli eventi, è necessario disporre dell'autorizzazione di configurazione della pagina topologia griglia. Se il valore di Total Events (Eventi totali) è zero o il numero aumenta e il problema persiste, contattare il supporto tecnico.
SNST	Stato	CMN	Un allarme indica che si è verificato un problema nella memorizzazione dei bundle di attività della griglia. Se il valore Stato è errore del punto di controllo o quorum non raggiunto, verificare che la maggior parte dei servizi ADC sia connessa al sistema StorageGRID (50% più uno), quindi attendere alcuni minuti. Se il problema persiste, contattare il supporto tecnico.
SOSS	Stato del sistema operativo per lo storage	SSM	Un allarme viene attivato se SANtricity OS indica che un componente di un'apparecchiatura StorageGRID presenta un problema di "intervento richiesto". Selezionare **NODI**. Quindi selezionare **Appliance Storage Node** > **hardware**. Scorrere verso il basso per visualizzare lo stato di ciascun componente. In SANtricity OS, controllare gli altri componenti dell'appliance per isolare il problema.

Codice	Nome	Servizio	Azione consigliata
SSMA	Stato SSM	SSM	Se il valore di SSM Status (Stato SSM) è Error (errore), selezionare **SUPPORT** > **Tools** > **Grid topology**, quindi selezionare ***Site*** > ***Grid node*** > **SSM** > **Overview** > **Main** e **SSM** > **Overview** > **Alarms** per determinare la causa dell'allarme. Se il problema persiste, contattare il supporto tecnico.
SSME	Stato SSM	SSM	Se il valore di SSM state (Stato SSM) è Standby, continuare il monitoraggio e, se il problema persiste, contattare il supporto tecnico. Se il valore di SSM state (Stato SSM) è Offline (non in linea), riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.
SST	Stato dello storage	BLDR	Se il valore di Storage Status (Stato storage) è Insufficient usable Space (spazio utilizzabile insufficiente), lo storage disponibile sul nodo di storage non è più disponibile e i dati acquisiti vengono reindirizzati ad altri nodi di storage disponibili. Le richieste di recupero possono continuare ad essere inviate da questo nodo della griglia. È necessario aggiungere ulteriore storage. Non influisce sulla funzionalità dell'utente finale, ma l'allarme persiste fino a quando non viene aggiunto ulteriore storage. Se il valore di Storage Status (Stato storage) è Volume(i) Unavailable (volumi non disponibili), una parte dello storage non è disponibile. Lo storage e il recupero da questi volumi non sono possibili. Per ulteriori informazioni, controllare lo stato di salute del volume: Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. Lo stato di salute del volume è elencato in archivi di oggetti. Se il valore dello stato dello storage è Error (errore), contattare il supporto tecnico. "Risolvere i problemi relativi all'allarme Storage Status (SST)"

Codice	Nome	Servizio	Azione consigliata
SVST	Stato	SSM	Questo allarme viene cancellato quando vengono risolti altri allarmi relativi a un servizio non in esecuzione. Tenere traccia degli allarmi di manutenzione della sorgente per ripristinare il funzionamento. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **SSM** > **servizi** > **Panoramica** > **principale**. Quando lo stato di un servizio viene visualizzato come non in esecuzione, il suo stato è amministrativamente inattivo. Lo stato del servizio può essere indicato come non in esecuzione per i seguenti motivi: • Il servizio è stato arrestato manualmente (`/etc/init.d/<service\> stop`). • Si è verificato un problema con il database MySQL e Server Manager arresta IL servizio MI. • È stato aggiunto un nodo Grid, ma non è stato avviato. • Durante l'installazione, un nodo Grid non è ancora connesso al nodo Admin. Se un servizio viene visualizzato come non in esecuzione, riavviarlo (`/etc/init.d/<service\> restart`). Questo allarme potrebbe anche indicare che l'archivio di metadati (database Cassandra) per un nodo di storage deve essere ricostruito. Se il problema persiste, contattare il supporto tecnico. "Risolvere i problemi relativi all'allarme Services: Status - Cassandra (SVST)"
TMEM	Memoria installata	SSM	I nodi in esecuzione con meno di 24 GB di memoria installata possono causare problemi di performance e instabilità del sistema. La quantità di memoria installata nel sistema deve essere aumentata ad almeno 24 GiB.
TPOP	Operazioni in sospeso	ADC	Una coda di messaggi può indicare che il servizio ADC è sovraccarico. È possibile collegare al sistema StorageGRID un numero troppo basso di servizi ADC. In un'implementazione di grandi dimensioni, il servizio ADC può richiedere l'aggiunta di risorse di calcolo oppure il sistema può richiedere servizi ADC aggiuntivi.

Codice	Nome	Servizio	Azione consigliata
UMEM	Memoria disponibile	SSM	Se la RAM disponibile si sta esaurendo, determinare se si tratta di un problema hardware o software. Se non si tratta di un problema hardware o se la memoria disponibile scende al di sotto di 50 MB (soglia di allarme predefinita), contattare il supporto tecnico.
VMFI	Voci disponibili	SSM	Ciò indica che è necessario uno storage aggiuntivo. Contattare il supporto tecnico.
VMFR	Spazio disponibile	SSM	Se il valore di spazio disponibile diventa troppo basso (vedi soglie di allarme), occorre verificare se ci sono file di log che crescono fuori proporzione o oggetti che occupano troppo spazio su disco (vedi soglie di allarme) che devono essere ridotti o cancellati. Se il problema persiste, contattare il supporto tecnico.
VMST	Stato	SSM	Viene attivato un allarme se il valore di Status (Stato) per il volume montato è Unknown (Sconosciuto). Il valore Unknown (Sconosciuto) o Offline (non in linea) indica che non è possibile montare o accedere al volume a causa di un problema con il dispositivo di storage sottostante.
VPRI	Priorità di verifica	BLDR, BARC	Per impostazione predefinita, il valore della priorità di verifica è Adaptive. Se la priorità di verifica è impostata su alta, viene attivato un allarme perché la verifica dello storage può rallentare le normali operazioni del servizio.
VSTU	Stato di verifica dell'oggetto	BLDR	Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. Controllare il sistema operativo per verificare la presenza di eventuali errori relativi a dispositivi a blocchi o file system. Se il valore di Stato verifica oggetto è Unknown Error (errore sconosciuto), di solito indica un problema di file system o hardware di basso livello (errore i/o) che impedisce all'attività di verifica dello storage di accedere al contenuto memorizzato. Contattare il supporto tecnico.
XAMS	Repository di audit non raggiungibili	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Verificare la connettività di rete al server che ospita il nodo di amministrazione. Se il problema persiste, contattare il supporto tecnico.

Riferimenti ai file di log

Riferimento ai file di log: Panoramica

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

I log sono classificati come segue:

- "Log del software StorageGRID"
- "Log di implementazione e manutenzione"
- "Registri per software di terze parti"
- "A proposito di bycast.log"

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

Accedere ai registri

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

1. Immettere il seguente comando: `ssh admin@grid_node_IP`
2. Immettere la password elencata in `Passwords.txt` file.
3. Immettere il seguente comando per passare a root: `su -`
4. Immettere la password elencata in `Passwords.txt` file.

Categorie di file di log

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

Percorso di archiviazione	Descrizione
audit	Messaggi di audit generati durante il normale funzionamento del sistema.
log-sistema-di-base	Informazioni di base sul sistema operativo, incluse le versioni delle immagini StorageGRID.
bundle	Informazioni sulla configurazione globale (bundle).

Percorso di archiviazione	Descrizione
cassandra	Informazioni sul database Cassandra e registri di riparazione Reaper.
ce	Informazioni sui VCSs relative al nodo corrente e informazioni sul gruppo EC in base all'ID del profilo.
griglia	Log di griglia generali, incluso il debug (`bycast.log`) e. `servermanager` registri.
grid.xml	File di configurazione della griglia condiviso tra tutti i nodi.
hagroup	Metriche e registri dei gruppi ad alta disponibilità.
installare	`Gdu-server` e installare i log.
lumberjack.log	Messaggi di debug relativi alla raccolta dei log.
Arbitro lambda	Registri relativi alla richiesta del proxy S3 Select.
Metriche	Log di servizio per Grafana, Jaeger, node esporter e Prometheus.
errore	Accesso Miscd e log degli errori.
mysql	La configurazione del database MariaDB e i relativi log.
netto	Log generati da script correlati alla rete e dal servizio Dynip.
nginx	File e log di configurazione del bilanciamento del carico e della federazione di griglie. Include anche i log di traffico di Grid Manager e Tenant Manager.
nginx-gw	File e log di configurazione del bilanciamento del carico e della federazione di griglie.
ntp	File di configurazione NTP e registri.
sistema operativo	File di stato del nodo e della griglia, inclusi i servizi `pid`.
altro	File di log in `/var/local/log` che non vengono raccolte in altre cartelle.
perf	Informazioni sulle prestazioni per CPU, rete e i/o del disco
prometheus-data	Metriche Prometheus correnti, se la raccolta di log include i dati Prometheus.

Percorso di archiviazione	Descrizione
provisioning	Log relativi al processo di provisioning della griglia.
zattera	Log dal cluster Raft utilizzato nei servizi della piattaforma.
ssh	Registri relativi alla configurazione e al servizio SSH.
snmp	Configurazione dell'agente SNMP e elenchi di allow/deny degli allarmi utilizzati per l'invio di notifiche SNMP.
socket-dati	Dati socket per il debug di rete.
system-commands.txt	Output dei comandi del container StorageGRID. Contiene informazioni di sistema, ad esempio le reti e l'utilizzo del disco.

Log del software StorageGRID

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

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

Log StorageGRID generali

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

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

Log relativi alla crittografia

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

Log della federazione di griglie

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

Registri NMS

Nome del file	Note	Trovato in
/var/local/log/nms.log	• Acquisisce le notifiche da Grid Manager e Tenant Manager. • Acquisisce gli eventi correlati al funzionamento del servizio NMS, ad esempio l'elaborazione degli allarmi, le notifiche e-mail e le modifiche alla configurazione. • Contiene gli aggiornamenti del bundle XML risultanti dalle modifiche di configurazione apportate nel sistema. • Contiene messaggi di errore relativi al downsampling degli attributi eseguito una volta al giorno. • Contiene messaggi di errore del server Web Java, ad esempio errori di generazione pagina e errori HTTP Status 500.	Nodi di amministrazione
/var/local/log/nms.errlog	Contiene messaggi di errore relativi agli aggiornamenti del database MySQL. Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.	Nodi di amministrazione
/var/local/log/nms.requestlog	Contiene informazioni sulle connessioni in uscita dall'API di gestione ai servizi StorageGRID interni.	Nodi di amministrazione

Log di Server Manager

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

Log dei servizi StorageGRID

Nome del file	Note	Trovato in
/var/local/log/acct.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/adc.errlog	Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.	Nodi di storage che eseguono il servizio ADC
/var/local/log/ams.errlog		Nodi di amministrazione
/var/local/log/arc.errlog		Nodi di archiviazione
/var/local/log/cassandra/system.log	Informazioni per l'archivio di metadati (database Cassandra) che possono essere utilizzate se si verificano problemi durante l'aggiunta di nuovi nodi di storage o se l'attività di riparazione nodetool si blocca.	Nodi di storage
/var/local/log/cassandra-reaper.log	Informazioni per il servizio Cassandra Reaper, che esegue la riparazione dei dati nel database Cassandra.	Nodi di storage
/var/local/log/cassandra-reaper.errlog	Informazioni sugli errori per il servizio Cassandra Reaper.	Nodi di storage
/var/local/log/chunk.errlog		Nodi di storage
/var/local/log/cmn.errlog		Nodi di amministrazione
/var/local/log/cms.errlog	Questo file di log potrebbe essere presente sui sistemi che sono stati aggiornati da una versione precedente di StorageGRID. Contiene informazioni legacy.	Nodi di storage
/var/local/log/cts.errlog	Questo file di log viene creato solo se il tipo di destinazione è **Cloud Tiering - Simple Storage Service (S3).**	Nodi di archiviazione
/var/local/log/dds.errlog		Nodi di storage
/var/local/log/dmv.errlog		Nodi di storage

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

Nome del file	Note	Trovato in
/var/local/log/nginx/*.log	Contiene i log per il servizio nginx, che funge da meccanismo di autenticazione e comunicazione sicura per diversi servizi grid (come Prometheus e Dynip) per poter comunicare con servizi su altri nodi tramite API HTTPS.	Tutti i nodi
/var/local/log/nginx-gw/*.log	Contiene i log generali relativi al servizio nginx-gw, inclusi i log degli errori e i log per le porte amministrative limitate sui nodi di amministrazione.	Nodi di amministrazione e nodi gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene log di accesso relativi al traffico di replica cross-grid.	Nodi di amministrazione, nodi gateway o entrambi, in base alla configurazione della federazione di griglie. Trovato solo nella griglia di destinazione per la replica cross-grid.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene i log di accesso per il servizio Load Balancer, che fornisce il bilanciamento del carico del traffico S3 e Swift dai client ai nodi di storage.	Nodi di amministrazione e nodi gateway
/var/local/log/persistence*	Contiene i log per il servizio di persistenza, che gestisce i file sul disco root che devono persistere durante un riavvio.	Tutti i nodi
/var/local/log/prometheus.log	Per tutti i nodi, contiene il log del servizio dell'esportatore di nodi e il log del servizio di metriche dell'esportatore. Per i nodi di amministrazione, contiene anche i registri per i servizi Prometheus e Alert Manager.	Tutti i nodi
/var/local/log/raft.log	Contiene l'output della libreria utilizzata dal servizio RSM per il protocollo Raft.	Nodi storage con servizio RSM
/var/local/log/rms.errlog	Contiene i registri per il servizio RSM (Replicated state Machine Service), utilizzato per i servizi della piattaforma S3.	Nodi storage con servizio RSM
/var/local/log/ssm.errlog		Tutti i nodi

Nome del file	Note	Trovato in
/var/local/log/update-s3vs-domains.log	Contiene i registri relativi all'elaborazione degli aggiornamenti per la configurazione dei nomi di dominio host virtuali S3.vedere le istruzioni per l'implementazione delle applicazioni client S3.	Nodi Admin e Gateway
/var/local/log/update-snmp-firewall.*	Contiene i registri relativi alle porte firewall gestite per SNMP.	Tutti i nodi
/var/local/log/update-sysl.log	Contiene i registri relativi alle modifiche apportate alla configurazione syslog del sistema.	Tutti i nodi
/var/local/log/update-traffic-classes.log	Contiene i registri relativi alle modifiche apportate alla configurazione dei classificatori del traffico.	Nodi Admin e Gateway
/var/local/log/update-utcn.log	Contiene i registri relativi alla modalità di rete client non attendibile su questo nodo.	Tutti i nodi

Informazioni correlate

"A proposito di bycast.log"

"UTILIZZARE L'API REST S3"

Log di implementazione e manutenzione

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

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

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

Registri per software di terze parti

È possibile utilizzare i registri del software di terze parti per risolvere i problemi.

Categoria	Nome del file	Note	Trovato in
Archiviazione	/var/local/log/dsierror.log	Informazioni sugli errori per le API del client TSM.	Nodi di archiviazione
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	File di log generati da MySQL. `mysql.err` acquisisce errori e eventi del database, come avvii e arresti. `mysql-slow.log` (Log di query lento) acquisisce le istruzioni SQL che hanno richiesto più di 10 secondi per l'esecuzione.	Nodi di amministrazione
Sistema operativo	/var/local/log/messages	Questa directory contiene i file di log per il sistema operativo. Gli errori contenuti in questi log vengono visualizzati anche in Grid Manager. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare **topologia** > ***Sito*** > ***nodo*** > **SSM** > **Eventi**.	Tutti i nodi

Categoria	Nome del file	Note	Trovato in
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	`/var/local/log/ntp.log` Contiene il file di log per i messaggi di errore NTP. `/var/lib/ntp/var/log/ntpstats/` La directory contiene le statistiche di tempo NTP. `loopstats` registra le informazioni statistiche del filtro loop. `peerstats` registra le informazioni delle statistiche peer.	Tutti i nodi

A proposito di bycast.log

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 del nodo della griglia.

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

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

Rotazione del file per bycast.log

Quando il `bycast.log` Il 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 denominato `bycast.log`. Quando il nuovo `bycast.log` Raggiunge 1 GB, `bycast.log.1` viene rinominato e compresso come `bycast.log.2.gz`, e. `bycast.log` viene rinominato `bycast.log.1`.

Il limite di rotazione per `bycast.log` è di 21 file. Quando la ventiduesima versione di `bycast.log` il file viene creato, il file meno recente viene cancellato.

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

> Se un file di log è stato compresso, non è necessario decomprimerlo nella stessa posizione in cui è stato scritto. La decompressione del file nella stessa posizione può interferire con gli script di rotazione del log.

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

Informazioni correlate

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

Messaggi nel bycast.log

Messaggi in `bycast.log` Sono scritti da ADE (Asynchronous Distributed Environment). ADE è l'ambiente di runtime utilizzato dai servizi di ciascun nodo di rete.

Esempio di messaggio ADE:

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

I messaggi ADE contengono le seguenti informazioni:

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

Severità dei messaggi nel bycast.log

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

Ad esempio:

- **NOTA** — si è verificato un evento da registrare. La maggior parte dei messaggi di log è a questo livello.
- **ATTENZIONE** — si è verificata una condizione imprevista.
- **ERRORE** — si è verificato un errore grave che ha un impatto sulle operazioni.
- **CRITICO** — si è verificata una condizione anomala che ha interrotto le normali operazioni. È necessario risolvere immediatamente la condizione sottostante. I messaggi critici vengono visualizzati anche in Grid Manager. Selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi selezionare **Sito** > **nodo** > **SSM** >

Eventi.

Codici di errore in `bycast.log`

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

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

Codice di errore	Significato
SUC	Nessun errore
GERR	Sconosciuto
CANC	Annullato
ABRT	Interrotto
TOUT	Timeout
INVL	Non valido
NFND	Non trovato
VERS	Versione
CONF	Configurazione
NON RIUSCITO	Non riuscito
ICPL	Incompleto
FATTO	Fatto
SUNV	Servizio non disponibile

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

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

Numero di errore	Codice di errore	Significato
004	EINTR	Chiamata di sistema interrotta
005	EIO	Errore i/O.
006	ENXIO	Nessun dispositivo o indirizzo di questo tipo
007	E2BIG	Elenco di argomenti troppo lungo
008	ENOEXEC	Errore di formato Exec
009	EBADF	Numero di file errato
010	ECHILD	Nessun processo figlio
011	EAGAIN	Riprovare
012	ENOMEM	Memoria esaurita
013	EACCES	Permesso negato
014	EFAULT	Indirizzo non valido
015	ENOTBLK	Dispositivo a blocchi richiesto
016	EBUSY	Periferica o risorsa occupata
017	EEXIST	Il file esiste
018	ESCLUDI	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo di questo tipo
020	ENOTDIR	Non una directory
021	EISDIR	È una directory
022	EINVAL	Argomento non valido
023	ENFILE	Overflow della tabella dei file
024	EMFILE	Troppi file aperti

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 non disponibile sul dispositivo
029	ESPIPE	Ricerca illegale
030	EROFS	File system di sola lettura
031	EMSINK	Troppi collegamenti
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dominio della funzione
034	ERANGE	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un deadlock delle risorse
036	ENAMETOLONG	Nome file troppo lungo
037	ENOLCK	Nessun blocco di record disponibile
038	ENOSYS	Funzione non implementata
039	ENOTEMPTY	Directory non vuota
040	ELOOP	Sono stati rilevati troppi collegamenti simbolici
041		
042	ENOMSG	Nessun messaggio del tipo desiderato
043	EIDRM	Identificatore rimosso
044	ECHRNG	Numero di canale fuori intervallo
045	EL2NSYNC	Livello 2 non sincronizzato

Numero di errore	Codice di errore	Significato
046	EL3HLT	Livello 3 interrotto
047	EL3RST	Ripristino livello 3
048	ELNRNG	Numero di collegamento fuori intervallo
049	EUNATCH	Driver del protocollo non collegato
050	ENOCSI	Nessuna struttura CSI disponibile
051	EL2HLT	Livello 2 arrestato
052	EBADE	Scambio non valido
053	EBADR	Descrittore della richiesta non valido
054	ESCLUDI	Exchange pieno
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato del file di font non valido
060	ENOSTR	Il dispositivo non è un flusso
061	ENODATA	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse out of Streams
064	ENONET	La macchina non è in rete
065	ENOPKG	Pacchetto non installato
066	EREMOTE	L’oggetto è remoto

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

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

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

Numero di errore	Codice di errore	Significato
129	EKEYREJECTED	Chiave rifiutata dal servizio
130	EOWNERDEAD	Per i mutex più forti: Il proprietario è morto
131	ENOTRECOVERABILE	Per mutex affidabili: Stato non ripristinabile

Configurare le destinazioni dei messaggi di controllo e del registro

Considerazioni sull'utilizzo di un server syslog esterno

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

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

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

Quando utilizzare un server syslog esterno

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

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

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

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

Come configurare un server syslog esterno

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

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

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

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

Come valutare le dimensioni del server syslog esterno

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

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

Utilizzare le operazioni S3 al secondo nelle formule di stima

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

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

Formule di stima per i log di audit

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

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

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

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

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

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

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

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione di Storage, Che è impostato su Error):

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

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

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

Formule di stima per livelli di audit non predefiniti

Le formule fornite per i registri di controllo presuppongono l'utilizzo delle impostazioni predefinite del livello di controllo (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore). Non sono disponibili formule dettagliate per la stima del tasso e della dimensione media dei messaggi di audit per le impostazioni del livello di audit non predefinite. Tuttavia, la seguente tabella può essere utilizzata per effettuare una stima approssimativa del tasso; è possibile utilizzare la formula delle dimensioni medie fornita per i registri di controllo, ma è probabile che si verifichi una sovrastima perché i messaggi di controllo "extra" sono, in media, più piccoli dei messaggi di controllo predefiniti.

Condizione	Formula
Replica: Tutti i livelli di controllo sono impostati su Debug o Normal	Tasso del registro di controllo = 8 x S3 tasso di operazioni
Erasure coding (codifica erasure): I livelli di audit sono tutti impostati su Debug o Normal (normale)	Utilizzare la stessa formula utilizzata per le impostazioni predefinite

Formule di stima per gli eventi di sicurezza

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

Formule di stima per i log delle applicazioni

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

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

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

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

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

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

Stime di dimensionamento di esempio

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

- Replica
- Erasure coding

Se si utilizza la replica per la protezione dei dati

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

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

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

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

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket e i nomi degli oggetti sono in media di 90 byte, il server syslog esterno deve essere dimensionato in modo da supportare 1800 log delle applicazioni al secondo, E riceverà (e in genere memorizzerà) i dati delle applicazioni a una velocità di 0.5 MB al secondo.

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

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

Sia K la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il

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

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

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

Ad esempio, se il grid è dimensionato per 1.000 S3 operazioni al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket mentre i nomi degli oggetti hanno una media di 90 byte, il server syslog esterno dovrebbe essere dimensionato in modo da supportare 2.250 registri delle applicazioni al secondo e dovrebbe essere in grado di ricevere (e generalmente archiviare) dati delle applicazioni a una velocità di 0,6 MB al secondo.

Configurare i messaggi di controllo e il server syslog esterno

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

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

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Se si prevede di configurare un server syslog esterno, è stata esaminata la "considerazioni sull'utilizzo di un server syslog esterno" e ha assicurato che il server abbia capacità sufficiente per ricevere e memorizzare i file di registro.
- Se si intende configurare un server syslog esterno utilizzando il protocollo TLS o RELP/TLS, si dispone della CA del server e dei certificati client richiesti e della chiave privata del client.

Modificare i livelli dei messaggi di controllo

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

di audit:

Categoria di audit	Impostazione predefinita	Ulteriori informazioni
Sistema	Normale	"Messaggi di audit del sistema"
Storage	Errore	"Messaggi di audit dello storage a oggetti"
Gestione	Normale	"Messaggio di audit della gestione"
Letture del client	Normale	"Messaggi di audit in lettura del client"
Il client scrive	Normale	"Messaggi di audit di scrittura del client"
ILM	Normale	"Messaggi di controllo ILM"
Replica cross-grid	Errore	"CGRR: Richiesta di replica cross-grid"

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

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

Fasi

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

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

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

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

3. Selezionare **Salva**.

   Un banner verde indica che la configurazione è stata salvata.

Definire le intestazioni delle richieste HTTP

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

Fasi

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

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

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

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

   > Le intestazioni delle richieste del protocollo di audit vengono registrate solo se il livello di audit per **letture client** o **scritture client** non è **disattivato**.

3. Selezionare **Salva**

   Un banner verde indica che la configurazione è stata salvata.

Usa un server syslog esterno

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

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

> Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili da soddisfare le proprie esigenze, è possibile applicare ulteriori opzioni di configurazione utilizzando `audit-destinations` Endpoint, che si trovano nella sezione API privata di "API di Grid Management". Ad esempio, è possibile utilizzare l'API se si desidera utilizzare server syslog diversi per diversi gruppi di nodi.

Inserire le informazioni di syslog

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

Fasi

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

   Viene visualizzata la procedura guidata Configura server syslog esterno.

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

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

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

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

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

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

7. Selezionare **continua**.

Gestire il contenuto syslog

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

Fasi

1. Per la fase **Gestisci contenuto syslog** della procedura guidata, selezionare ogni tipo di informazione di audit che si desidera inviare al server syslog esterno.
   - **Invia log di audit**: Invia eventi StorageGRID e attività di sistema
   - **Invia eventi di sicurezza**: Invia eventi di sicurezza, ad esempio quando un utente non autorizzato tenta di effettuare l'accesso o un utente accede come root
   - **Send application logs**: Invia file di log utili per la risoluzione dei problemi, tra cui:
     - `bycast-err.log`

- `bycast.log`
- `jaeger.log`
- `nms.log` (Solo nodi di amministrazione)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

Per informazioni sui registri del software StorageGRID, vedere "Log del software StorageGRID".

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

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

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

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

Severità	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di gravità di quando è stato registrato localmente sul nodo: • Per i registri di controllo, la gravità è "info". • Per gli eventi di sicurezza, i valori di gravità sono generati dalla distribuzione Linux sui nodi. • Per i registri delle applicazioni, i livelli di gravità variano tra "info" e "avviso", a seconda del problema. Ad esempio, aggiungendo un server NTP e configurando un gruppo ha si ottiene il valore "info", mentre arrestando intenzionalmente il servizio SSM o RSM si ottiene il valore "avviso".
0	Emergenza: Il sistema non è utilizzabile
1	Attenzione: L'azione deve essere eseguita immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore
4	Avvertenza: Condizioni di avviso
5	Avviso: Condizione normale ma significativa
6	Informativo: Messaggi informativi

Severità	Descrizione
7	Debug: Messaggi a livello di debug

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

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

Struttura	Descrizione

Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di struttura di quando è stato collegato localmente al nodo:
	• Per i registri di controllo, la struttura inviata al server syslog esterno è "local7".
	• Per gli eventi di sicurezza, i valori della struttura vengono generati dalla distribuzione linux sui nodi.
	• Per i registri delle applicazioni, i registri delle applicazioni inviati al server syslog esterno presentano i seguenti valori di struttura:
	  ◦ `bycast.log`: utente o daemon
	  ◦ `bycast-err.log`: utente, daemon, local3 o local4
	  ◦ `jaeger.log`: local2
	  ◦ `nms.log`: local3
	  ◦ `prometheus.log`: local4
	  ◦ `raft.log`: local5
	  ◦ `hagroups.log`: local6

0	kern (messaggi kernel)
1	utente (messaggi a livello utente)
2	mail
3	daemon (daemon di sistema)
4	auth (messaggi di sicurezza/autorizzazione)
5	syslog (messaggi generati internamente da syslogd)
6	lpr (sottosistema di stampanti di linea)
7	news (sottosistema notizie di rete)

Struttura	Descrizione
8	UUCP
9	cron (daemon di clock)
10	sicurezza (messaggi di sicurezza/autorizzazione)
11	FTP
12	NTP
13	logaudit (audit del log)
14	logalert (avviso di log)
15	clock (daemon di clock)
16	local0
17	locale1
18	locale2
19	locale3
20	locale4
21	locale5
22	locale6
23	locale7

3. Selezionare **continua**.

Inviare messaggi di test

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

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

Fasi

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

   Un banner verde indica che la configurazione è stata salvata.

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

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

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

   Vedere "Risolvere i problemi di un server syslog esterno" per risolvere eventuali errori.

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

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

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

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

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

Selezionare le destinazioni delle informazioni di audit

È possibile specificare la posizione dei registri di controllo, dei registri eventi di protezione e. "Log del software StorageGRID" vengono inviati.

> StorageGRID utilizza per impostazione predefinita le destinazioni di controllo dei nodi locali e memorizza le informazioni di controllo in `/var/local/log/localaudit.log`.
>
> Quando si utilizza `/var/local/log/localaudit.log`, le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione. È possibile individuare il nodo con le voci più recenti utilizzando il `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` comando.
>
> Alcune destinazioni sono disponibili solo se è stato configurato un server syslog esterno.

Fasi

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

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

Opzione	Descrizione
Solo nodi locali (impostazione predefinita)	I messaggi di controllo, i registri degli eventi di protezione e i registri delle applicazioni non vengono inviati ai nodi amministrativi. Vengono invece salvati solo sui nodi che li hanno generati ("nodo locale"). Le informazioni di controllo generate su ogni nodo locale sono memorizzate in `/var/local/log/localaudit.log`. **Nota**: StorageGRID rimuove periodicamente i log locali in una rotazione per liberare spazio. Quando il file di log di un nodo raggiunge 1 GB, il file esistente viene salvato e viene avviato un nuovo file di log. Il limite di rotazione per il log è di 21 file. Quando viene creata la ventiduesima versione del file di log, il file di log più vecchio viene cancellato. In media, su ciascun nodo vengono memorizzati circa 20 GB di dati di log.
Nodi amministrativi/nodi locali	I messaggi di controllo vengono inviati al registro di controllo sui nodi Admin, mentre i registri degli eventi di protezione e i registri delle applicazioni vengono memorizzati sui nodi che li hanno generati. Le informazioni di controllo sono memorizzate nei seguenti file: • 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, ad esempio una copia aggiuntiva di alcuni messaggi.
Server syslog esterno	Le informazioni di controllo vengono inviate a un server syslog esterno e salvate sui nodi locali (`/var/local/log/localaudit.log`). Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.
Nodo di amministrazione e server syslog esterno	I messaggi di controllo vengono inviati al registro di controllo (`/var/local/audit/export/audit.log`) sui nodi Admin e le informazioni di controllo vengono inviate al server syslog esterno e salvate sul nodo locale (`/var/local/log/localaudit.log`. Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.

2. Selezionare **Salva**.

   Viene visualizzato un messaggio di avviso.

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

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

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

Utilizzare il monitoraggio SNMP

USA monitoraggio SNMP: Panoramica

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

- "Configurare l'agente SNMP"
- "Aggiornare l'agente SNMP"

Funzionalità

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

Vedere "Accedere ai file MIB" Se si desidera scaricare i file MIB sui nodi della griglia.

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

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

Trappole

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

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

Informa

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

Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche trap e inform vengono inviate nei seguenti casi:

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

  Ogni avviso viene associato a uno dei tre tipi di trap in base al livello di gravità dell'avviso: ActiveMinorAlert, activeMajorAlert e activeCriticalAlert. Per un elenco degli avvisi che possono attivare questi trap, vedere "Riferimenti agli avvisi".

- Certo "allarmi (sistema legacy)" vengono attivati a livelli di gravità specificati o superiori.

> Le notifiche SNMP non vengono inviate per ogni allarme o per ogni severità di allarme.

Supporto della versione SNMP

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

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

Limitazioni

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

Configurare l'agente SNMP

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

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

Tutti i nodi nella griglia utilizzano la stessa configurazione SNMP.

Specificare la configurazione di base

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

Fasi

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

   Viene visualizzata la pagina SNMP Agent.

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

Campo	Descrizione
Contatto per il sistema	Opzionale. Il contatto principale per il sistema StorageGRID, che viene restituito nei messaggi SNMP come sysContact. In genere, il contatto di sistema è un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID. **Il contatto di sistema** può contenere al massimo 255 caratteri.
Ubicazione del sistema	Opzionale. La posizione del sistema StorageGRID, che viene restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere una qualsiasi informazione utile per identificare la posizione del sistema StorageGRID. Ad esempio, è possibile utilizzare l'indirizzo di una struttura. Questo valore si applica a tutti i nodi nel sistema StorageGRID. **La posizione del sistema** può contenere al massimo 255 caratteri.
Attivare le notifiche dell'agente SNMP	• Se selezionata, l'agente SNMP StorageGRID invia notifiche trap e inform. • Se questa opzione non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.
Abilita trap di autenticazione	Se selezionata, l'agente SNMP StorageGRID invia trap di autenticazione se riceve messaggi di protocollo autenticati in modo errato.

Immettere le stringhe di comunità

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

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

Fasi

1. Per **comunità di sola lettura**, è possibile immettere una stringa di comunità per consentire l'accesso MIB di sola lettura agli indirizzi di agenti IPv4 e IPv6.

   > Per garantire la sicurezza del sistema StorageGRID, non utilizzare "public" come stringa di comunità. Se questo campo viene lasciato vuoto, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa di comunità.

   Ogni stringa di community può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

2. Selezionare **Aggiungi un'altra stringa di comunità** per aggiungere altre stringhe.

   Sono consentite fino a cinque stringhe.

creare destinazioni trap

Utilizzare la scheda destinazioni trap nella sezione altre configurazioni per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

Fasi

1. Per il campo **Comunità trap predefinita**, è possibile immettere la stringa di comunità predefinita che si desidera utilizzare per le destinazioni trap SNMPv1 o SNMPv2.

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

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

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

SNMPv1

Se si seleziona SNMPv1 come versione, completare questi campi.

Campo	Descrizione
Tipo	Deve essere trap per SNMPv1.
Host	Un indirizzo IPv4 o IPv6 o un nome di dominio completo (FQDN) per ricevere il trap.
Porta	Utilizzare 162, quale porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv2c

Se si seleziona SNMPv2c come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv3

Se si seleziona SNMPv3 come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Utente USM	L'utente USM che verrà utilizzato per l'autenticazione. • Se si seleziona **Trap**, vengono visualizzati solo gli utenti USM senza ID motore autorevoli. • Se si seleziona **inform**, vengono visualizzati solo gli utenti USM con ID motore autorevoli. • Se non viene visualizzato alcun utente: i. Creare e salvare la destinazione trap. ii. Passare a. Creare utenti USM e creare l'utente. iii. Tornare alla scheda Destinazioni trap, selezionare la destinazione salvata dalla tabella e selezionare **Modifica**. iv. Selezionare l'utente.

5. Selezionare **Crea**.

   La destinazione trap viene creata e aggiunta alla tabella.

Creare gli indirizzi degli agenti

Facoltativamente, utilizzare la scheda indirizzi agente nella sezione altre configurazioni per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

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

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

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

Campo	Descrizione
Protocollo di trasporto	Se questo indirizzo utilizza UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
Rete StorageGRID	La rete StorageGRID su cui l'agente ascolta. • Grid, Admin e Client Networks (reti Grid, Admin e Client): L'agente SNMP è in attesa di query su tutte e tre le reti. • Grid Network • Admin Network (rete amministrativa) • Rete client **Nota**: Se si utilizza la rete client per i dati non protetti e si crea un indirizzo agente per la rete client, tenere presente che anche il traffico SNMP non sarà sicuro.
Porta	Facoltativamente, il numero di porta su cui l'agente SNMP deve essere in attesa. La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta inutilizzato. **Nota**: Quando si salva l'agente SNMP, StorageGRID apre automaticamente le porte degli indirizzi dell'agente sul firewall interno. È necessario assicurarsi che tutti i firewall esterni consentano l'accesso a queste porte.

3. Selezionare **Crea**.

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

creare utenti USM

Se si utilizza SNMPv3, utilizzare la scheda utenti USM nella sezione altre configurazioni per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

> SNMPv3 *inform* le destinazioni devono avere utenti con ID motore. SNMPv3 la destinazione *trap* non può avere utenti con ID motore.

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

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

Campo	Descrizione
Nome utente	Un nome univoco per questo utente USM. I nomi utente possono avere un massimo di 32 caratteri e non possono contenere spazi vuoti. Il nome utente non può essere modificato dopo la creazione dell'utente.
Accesso MIB di sola lettura	Se selezionata, l'opzione consente all'utente di accedere in sola lettura al MIB.
ID motore autorevole	Se l'utente verrà utilizzato in una destinazione inform, l'ID motore autorevole per questo utente. Inserire da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è necessario per gli utenti USM che verranno selezionati nelle destinazioni trap per gli informa. Questo valore non è consentito per gli utenti USM che verranno selezionati nelle destinazioni trap per trap. **Nota**: Questo campo non viene visualizzato se si seleziona **accesso MIB di sola lettura** perché gli utenti USM che hanno accesso MIB di sola lettura non possono avere ID motore.
Livello di sicurezza	Il livello di sicurezza per l'utente USM: • **Authprim**: Questo utente comunica con autenticazione e privacy (crittografia). È necessario specificare un protocollo di autenticazione e una password, nonché un protocollo e una password per la privacy. • **AuthNoPriv**: Questo utente comunica con autenticazione e senza privacy (senza crittografia). Specificare un protocollo di autenticazione e una password.
Protocollo di autenticazione	Impostare sempre su SHA, che è l'unico protocollo supportato (HMAC-SHA-96).
Password	La password che l'utente utilizzerà per l'autenticazione.
Protocollo di privacy	Visualizzato solo se si seleziona **authviv** e si imposta sempre su AES, che è l'unico protocollo di privacy supportato.
Password	Visualizzato solo se è stato selezionato **authviv**. La password che l'utente utilizzerà per la privacy.

3. Selezionare **Crea**.

   L'utente USM viene creato e aggiunto alla tabella.

4. Una volta completata la configurazione dell'agente SNMP, selezionare **Salva**.

La nuova configurazione dell'agente SNMP diventa attiva.

Aggiornare l'agente SNMP

È possibile disattivare le notifiche SNMP, aggiornare le stringhe di comunità o aggiungere o rimuovere indirizzi di agenti, utenti USM e destinazioni trap.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

Vedere "Configurare l'agente SNMP" Per informazioni dettagliate su ciascun campo nella pagina dell'agente SNMP. È necessario selezionare **Salva** nella parte inferiore della pagina per confermare le modifiche apportate in ciascuna scheda.

Fasi

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

   Viene visualizzata la pagina SNMP Agent.

2. Per disattivare l'agente SNMP su tutti i nodi della griglia, deselezionare la casella di controllo **attiva SNMP** e selezionare **Salva**.

   Se si riattiva l'agente SNMP, tutte le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Se si desidera, aggiornare le informazioni nella sezione Configurazione di base:
   a. Se necessario, aggiornare **System contact** e **System location**.
   b. In alternativa, selezionare o deselezionare la casella di controllo **attiva notifiche agente SNMP** per controllare se l'agente SNMP StorageGRID invia notifiche trap e inform.

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

   c. Facoltativamente, selezionare o deselezionare la casella di controllo **Abilita trap di autenticazione** per controllare se l'agente SNMP di StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo autenticati in modo errato.
4. Se si utilizza SNMPv1 o SNMPv2c, è possibile aggiornare o aggiungere una comunità **di sola lettura** nella sezione Community Strings (stringhe comunità).
5. Per aggiornare le destinazioni trap, selezionare la scheda destinazioni trap nella sezione altre configurazioni.

   Utilizzare questa scheda per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

   Per informazioni dettagliate su cosa immettere, vedere "Creare destinazioni trap".

   - Facoltativamente, aggiornare o rimuovere la comunità trap predefinita.

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

- Per aggiungere una destinazione trap, selezionare **Crea**.
- Per modificare una destinazione trap, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere una destinazione trap, selezionare il pulsante di opzione e selezionare **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

6. Per aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

   Utilizzare questa scheda per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

   Per informazioni dettagliate su cosa immettere, vedere "Creare gli indirizzi degli agenti".

   - Per aggiungere un indirizzo agente, selezionare **Crea**.
   - Per modificare l'indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Modifica**.
   - Per rimuovere un indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Rimuovi**.
   - Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

7. Per aggiornare gli utenti USM, selezionare la scheda utenti USM nella sezione altre configurazioni.

   Utilizzare questa scheda per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

   Per informazioni dettagliate su cosa immettere, vedere "Creare utenti USM".

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

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

     > Se si aggiunge o si rimuove l'ID motore autorevole di un utente e tale utente è attualmente selezionato per una destinazione, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

   - Per rimuovere un utente USM, selezionare il pulsante di opzione e selezionare **Rimuovi**.

     > Se l'utente rimosso è attualmente selezionato per una destinazione trap, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

   - Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

8. Una volta aggiornata la configurazione dell'agente SNMP, selezionare **Salva**.

Accedere ai file MIB

I file MIB contengono definizioni e informazioni sulle proprietà delle risorse e dei servizi

gestiti per i nodi della griglia. È possibile accedere ai file MIB che definiscono gli oggetti e le notifiche per StorageGRID. Questi file possono essere utili per il monitoraggio della griglia.

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

Accedere ai file MIB

Per accedere ai file MIB, procedere come segue.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **SNMP Agent**.
2. Nella pagina dell'agente SNMP, selezionare il file che si desidera scaricare:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definisce la tabella degli avvisi e le notifiche (trap) accessibili su tutti i nodi di amministrazione.
   - **ES-NETAPP-06-MIB.mib**: Definisce gli oggetti e le notifiche per le appliance basate su e-Series.
   - **MIB_1_10.zip**: Definisce gli oggetti e le notifiche per le appliance con un'interfaccia BMC.

   > È inoltre possibile accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID StorageGRID dal file MIB:

   a. Ottenere l'OID della directory principale del MIB StorageGRID:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Risultato: `.1.3.6.1.4.1.789.28669` (`28669` È sempre l'OID per StorageGRID)

   a. Grep per l'OID di StorageGRID nell'intero albero (usando `paste` per unire le linee):

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

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

Contenuto del file MIB

Tutti gli oggetti si trovano sotto l'OID StorageGRID.

Nome dell'oggetto	ID oggetto (OID)	Descrizione
iso.org.dod.internet. private.enterprise. netapp.storagegrid		Il modulo MIB per le entità NetApp StorageGRID.

Oggetti MIB

Nome dell'oggetto	ID oggetto (OID)	Descrizione
ActiveAlertCount	**1.3.6.1.4.1.** 789.28669.1.3	Il numero di avvisi attivi in activeAlertTable.
ActiveAlertTable	**1.3.6.1.4.1.** 789.28669.1.4	Tabella degli avvisi attivi in StorageGRID.
ActiveAlertId	**1.3.6.1.4.1.** 789.28669.1.4.1.1	L'ID dell'avviso. Unico solo nel set corrente di avvisi attivi.
ActiveAlertName	**1.3.6.1.4.1.** 789.28669.1.4.1.2	Il nome dell'avviso.
ActiveAlertInstance	**1.3.6.1.4.1.** 789.28669.1.4.1.3	Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
ActiveAlertSeverity	**1.3.6.1.4.1.** 789.28669.1.4.1.4	La severità dell'avviso.
ActiveAlertStartTime	**1.3.6.1.4.1.** 789.28669.1.4.1.5	La data e l'ora di attivazione dell'avviso.

Tipi di notifica (trap)

Tutte le notifiche includono le seguenti variabili come varbind:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo di notifica	ID oggetto (OID)	Descrizione
ActiveMinorAlert	**1.3.6.1.4.1.** 789.28669.0.6	Un avviso con un livello di severità minore
ActiveMajorAlert	**1.3.6.1.4.1.** 789.28669.0.7	Un avviso con severità maggiore

Tipo di notifica	ID oggetto (OID)	Descrizione
ActiveCriticalAlert	**1.3.6.1.4.1.** 789.28669.0.8	Un avviso con severità critica

Raccogliere dati StorageGRID aggiuntivi

Utilizzare grafici e grafici

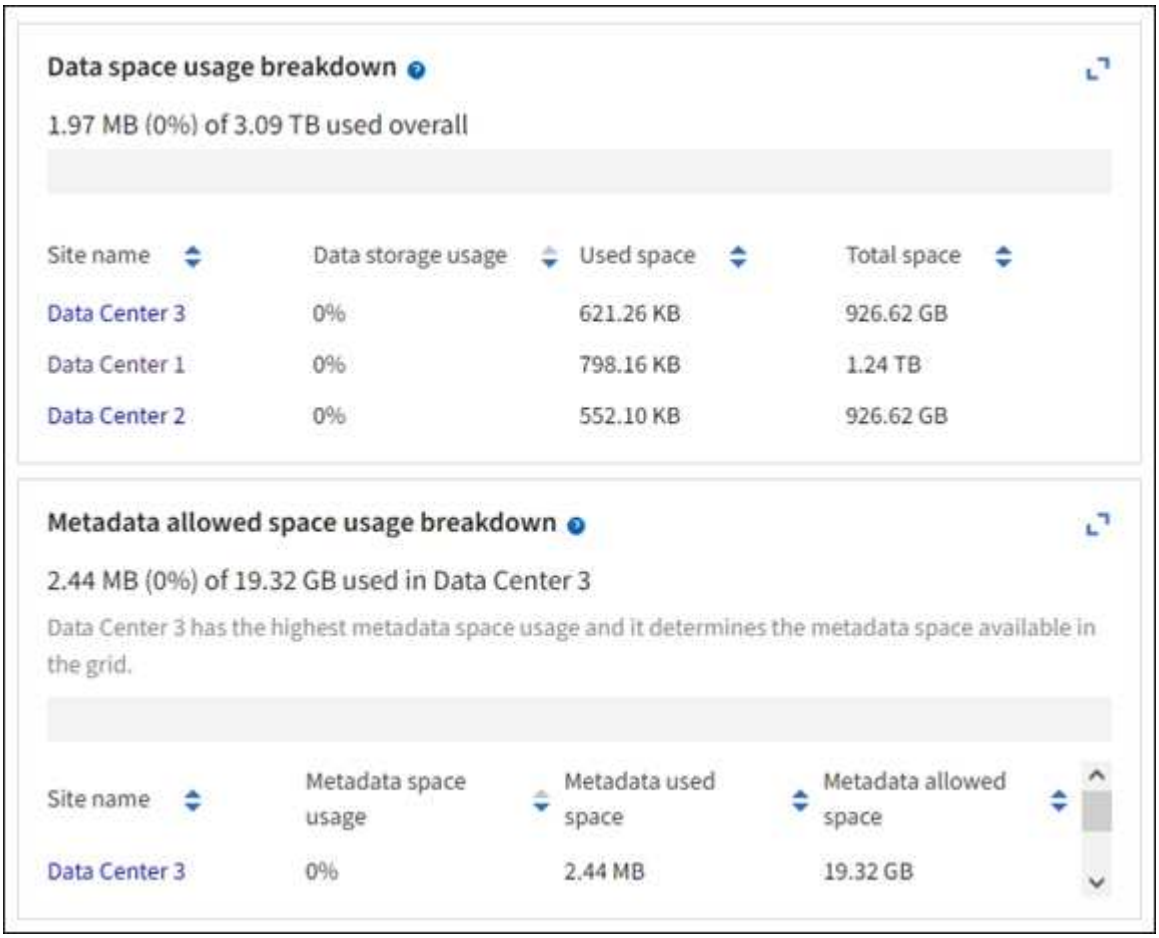
È possibile utilizzare grafici e report per monitorare lo stato del sistema StorageGRID e risolvere i problemi.

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

Tipi di grafici

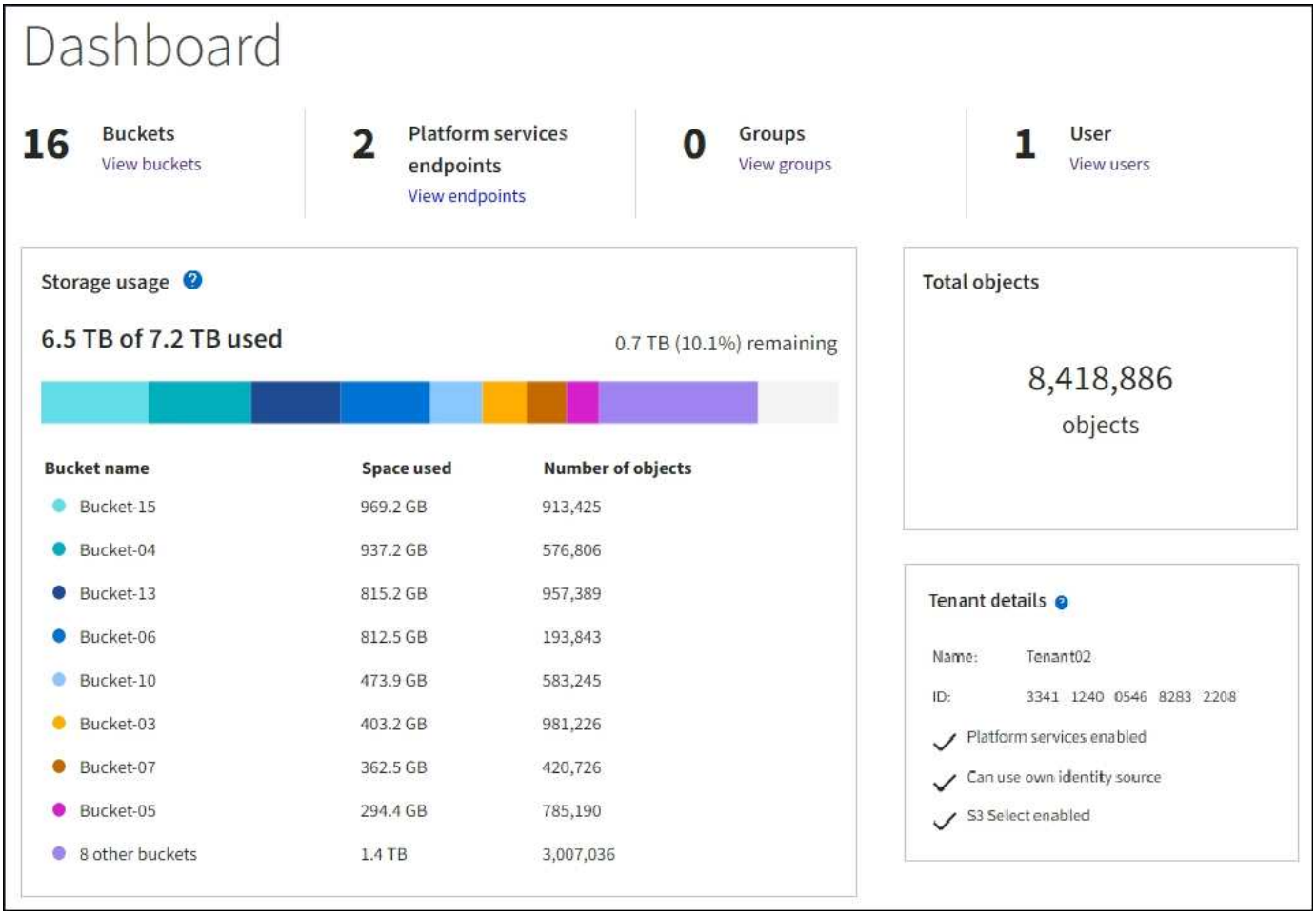
I grafici e i grafici riassumono i valori delle metriche e degli attributi specifici di StorageGRID.

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



Il pannello Storage Use (utilizzo storage) della dashboard di Tenant Manager visualizza quanto segue:

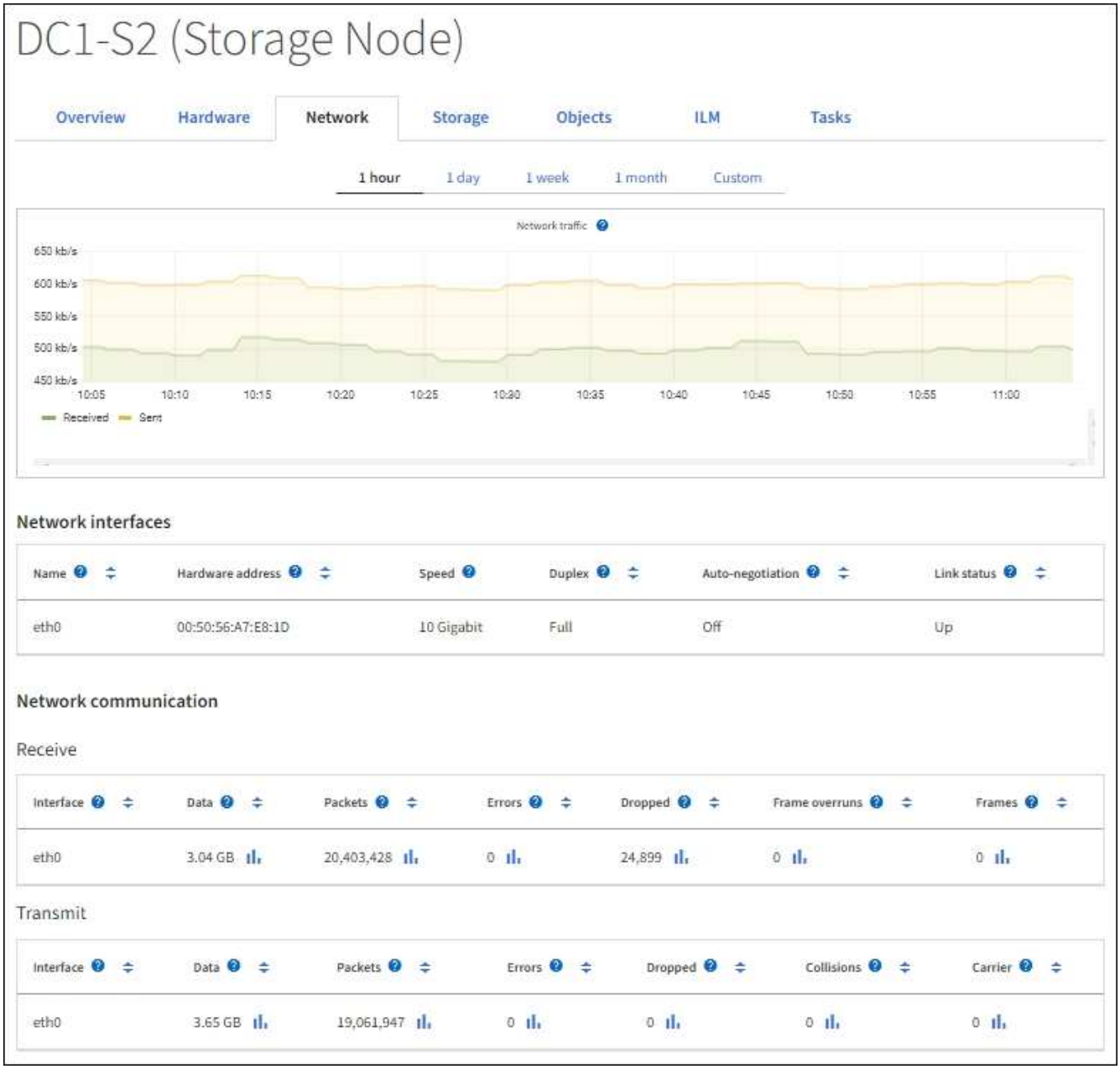
- Un elenco dei bucket più grandi (S3) o container (Swift) per il tenant
- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi
- La quantità totale di spazio utilizzato e, se viene impostata una quota, la quantità e la percentuale di spazio rimanente



Inoltre, i grafici che mostrano come le metriche e gli attributi StorageGRID cambiano nel tempo sono disponibili dalla pagina nodi e dalla pagina **SUPPORTO** > **Strumenti** > **topologia griglia**.

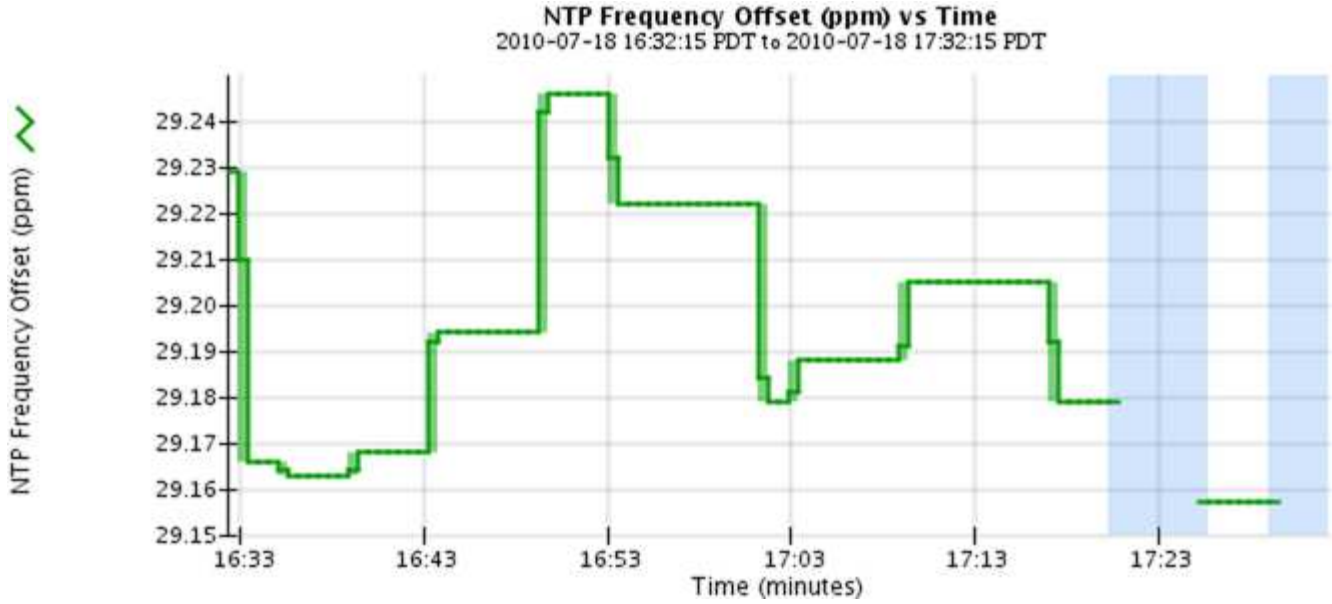
Esistono quattro tipi di grafici:

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

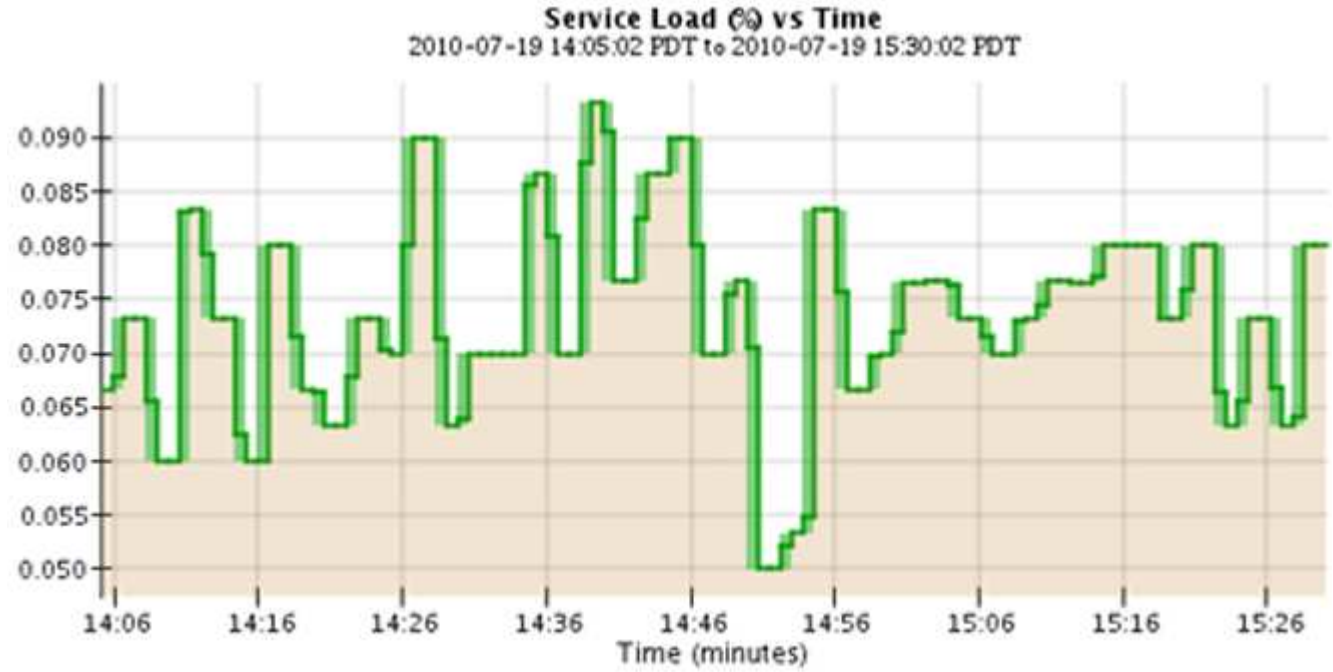


I grafici Grafana sono inclusi anche nelle dashboard predefinite disponibili nella pagina **SUPPORT** > **Tools** > **Metrics**.

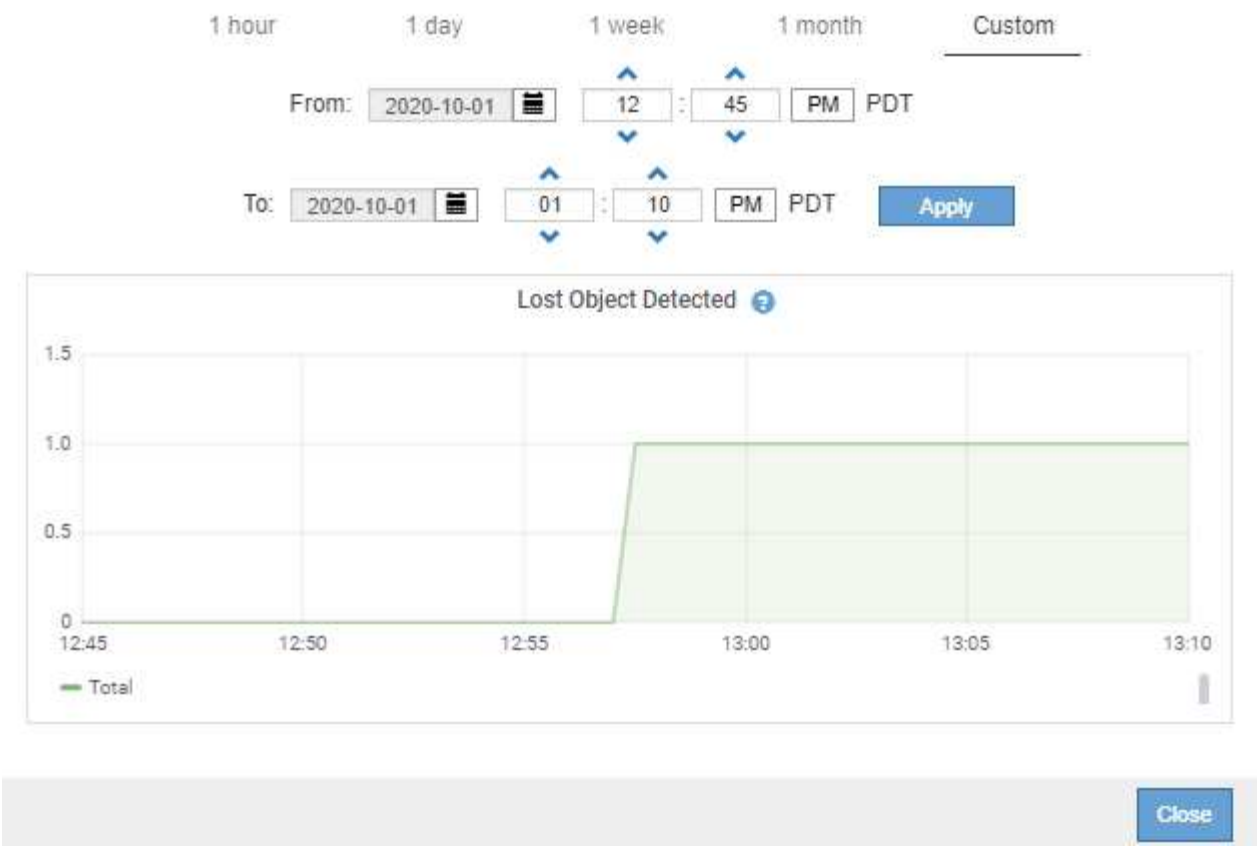
- **Grafici di linea**: Disponibili dalla pagina nodi e dalla pagina **SUPPORTO** > **Strumenti** > **topologia griglia** (selezionare l'icona del grafico) Dopo un valore di dati), i grafici a linee vengono utilizzati per rappresentare graficamente i valori degli attributi StorageGRID che hanno un valore unitario (ad esempio, offset di frequenza NTP, in ppm). Le modifiche al valore vengono tracciate a intervalli di dati regolari (bin) nel tempo.



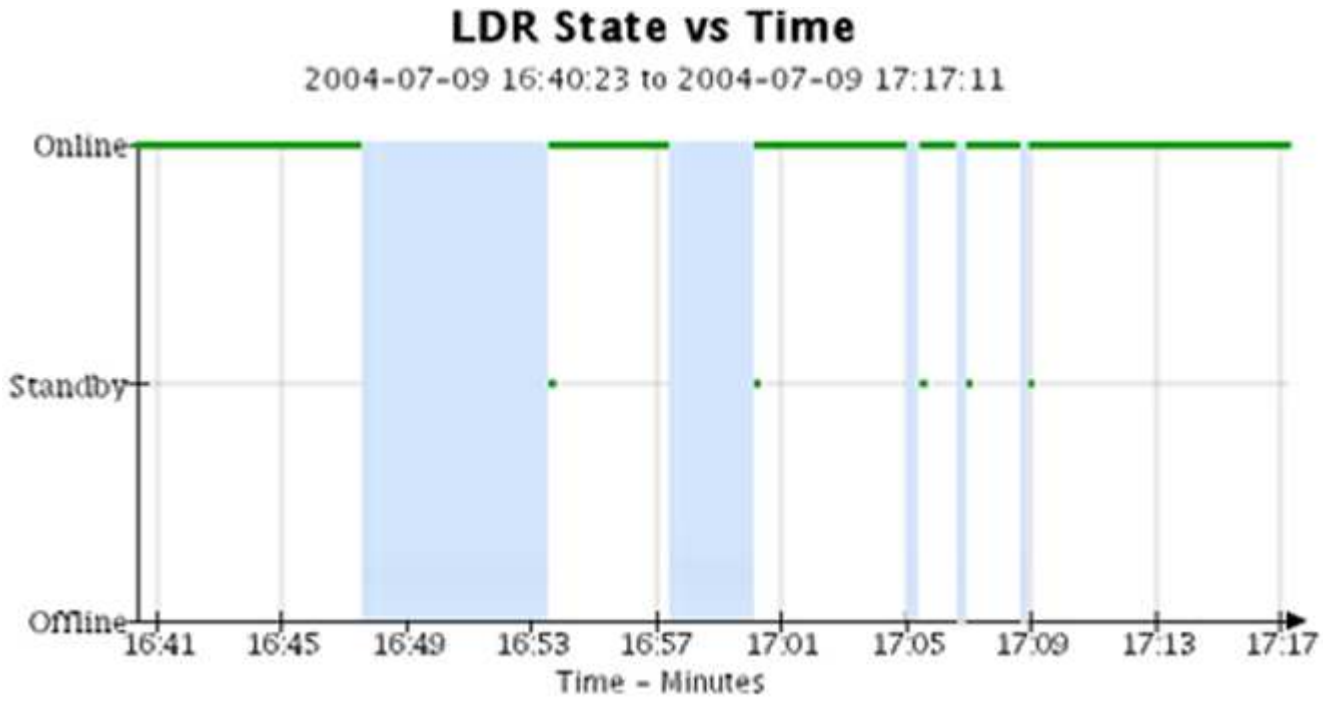
- **Area Graphs**: Disponibile dalla pagina Nodes e dalla pagina **SUPPORT** > **Tools** > **Grid topology** (Seleziona l'icona del grafico) dopo un valore di dati), i grafici di area vengono utilizzati per rappresentare graficamente le quantità di attributi volumetrici, come i conteggi di oggetti o i valori di carico del servizio. I grafici dell'area sono simili ai grafici a linee, ma includono un'ombreggiatura marrone chiaro sotto la linea. Le modifiche al valore vengono tracciate a intervalli di dati regolari (bin) nel tempo.



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



- **State graph**: Disponibile nella pagina **SUPPORT** > **Tools** > **Grid topology** (selezionare l'icona del grafico) dopo un valore di dati), i grafici di stato vengono utilizzati per rappresentare i valori degli attributi che rappresentano stati distinti, ad esempio uno stato del servizio che può essere in linea, in standby o offline. I grafici di stato sono simili ai grafici a linee, ma la transizione è discontinua, ovvero il valore passa da un valore di stato all'altro.



Informazioni correlate

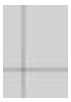
"Visualizzare la pagina nodi"

"Visualizzare l'albero topologia griglia"

"Rivedere le metriche di supporto"

Legenda del grafico

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

Esempio	Significato
	I valori degli attributi riportati vengono tracciati utilizzando linee di colore verde scuro.
	L'ombreggiatura verde chiaro intorno a linee verdi scure indica che i valori effettivi in quell'intervallo di tempo variano e sono stati "binned" (binning) per una tracciatura più rapida. La linea scura rappresenta la media ponderata. L'intervallo in verde chiaro indica i valori massimi e minimi all'interno del contenitore. L'ombreggiatura marrone chiaro viene utilizzata per i grafici dell'area per indicare i dati volumetrici.
	Le aree vuote (nessun dato plottato) indicano che i valori degli attributi non erano disponibili. Lo sfondo può essere blu, grigio o una combinazione di grigio e blu, a seconda dello stato del servizio che segnala l'attributo.
	L'ombreggiatura blu chiaro indica che alcuni o tutti i valori degli attributi in quel momento erano indeterminati; l'attributo non stava riportando i valori perché il servizio era in uno stato sconosciuto.
	L'ombreggiatura dei grigi indica che alcuni o tutti i valori degli attributi in quel momento non erano noti perché il servizio che riporta gli attributi era amministrativamente inattivo.
	Una combinazione di ombreggiature grigie e blu indica che alcuni dei valori degli attributi all'epoca erano indeterminati (perché il servizio era in uno stato sconosciuto), mentre altri non erano noti perché il servizio che riportava gli attributi era amministrativamente inattivo.

Visualizza grafici e grafici

La pagina Nodes (nodi) contiene i grafici a cui si dovrebbe accedere regolarmente per monitorare attributi come la capacità dello storage e il throughput. In alcuni casi, in particolare quando si lavora con il supporto tecnico, è possibile utilizzare la pagina **SUPPORT** > **Tools** > **Grid topology** per accedere a grafici aggiuntivi.

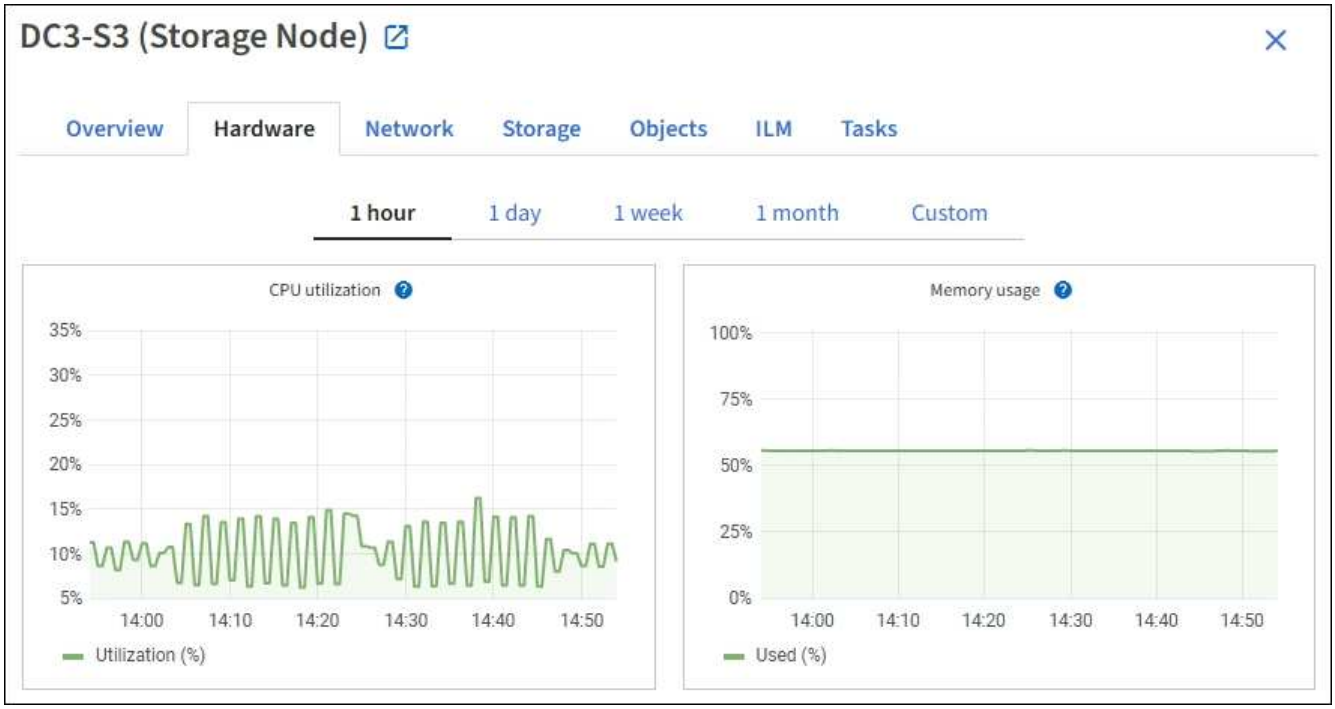
Prima di iniziare

È necessario accedere a Grid Manager utilizzando un "browser web supportato".

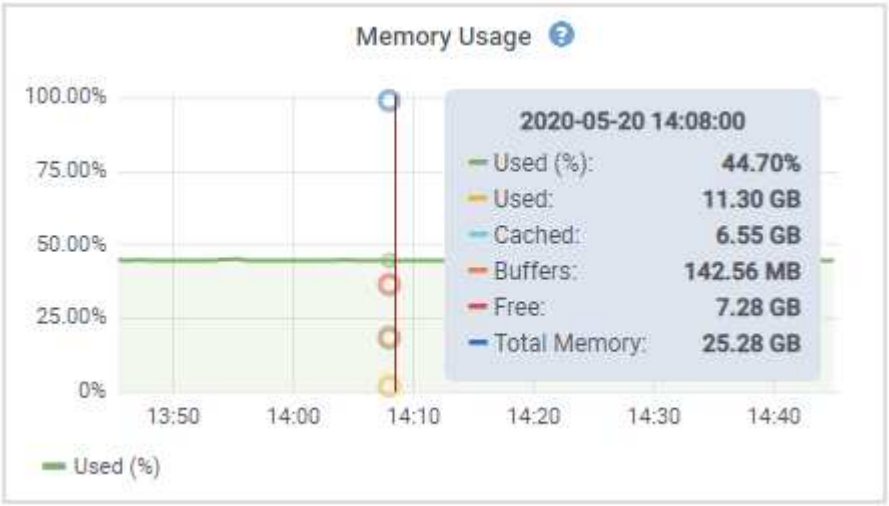
Fasi

1. Selezionare **NODI**. Quindi, selezionare un nodo, un sito o l'intera griglia.
2. Selezionare la scheda per la quale si desidera visualizzare le informazioni.

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



3. Se lo si desidera, posizionare il cursore sul grafico per visualizzare valori più dettagliati per un determinato punto nel tempo.

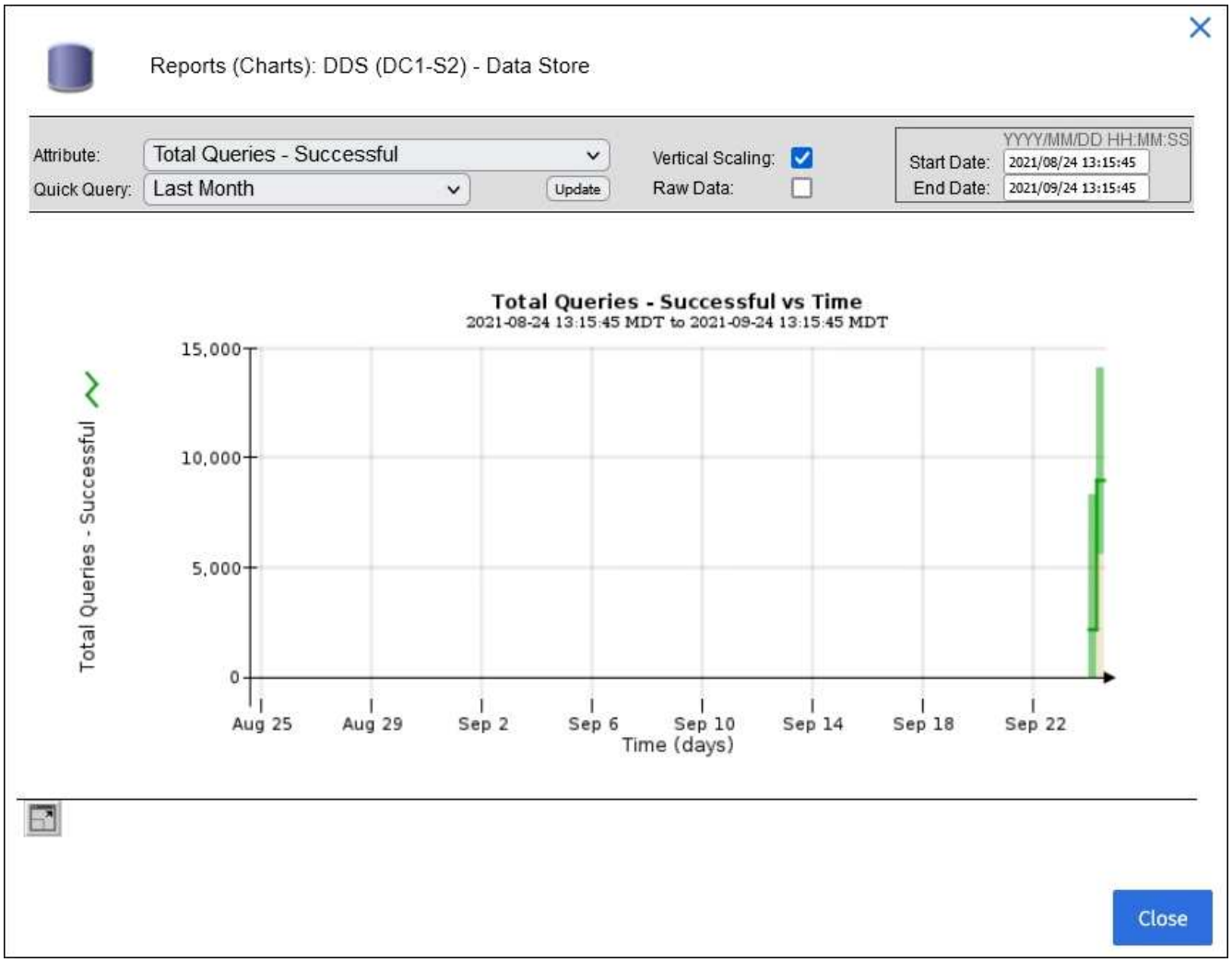


4. In base alle esigenze, spesso è possibile visualizzare un grafico per un attributo o una metrica specifici. Nella tabella della pagina nodi, selezionare l'icona del grafico a destra del nome dell'attributo.

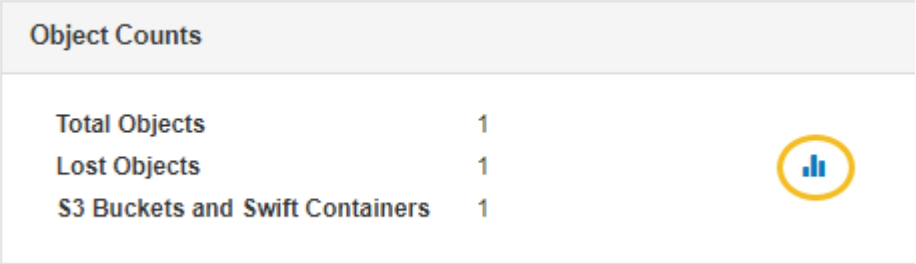
> I grafici non sono disponibili per tutte le metriche e gli attributi.

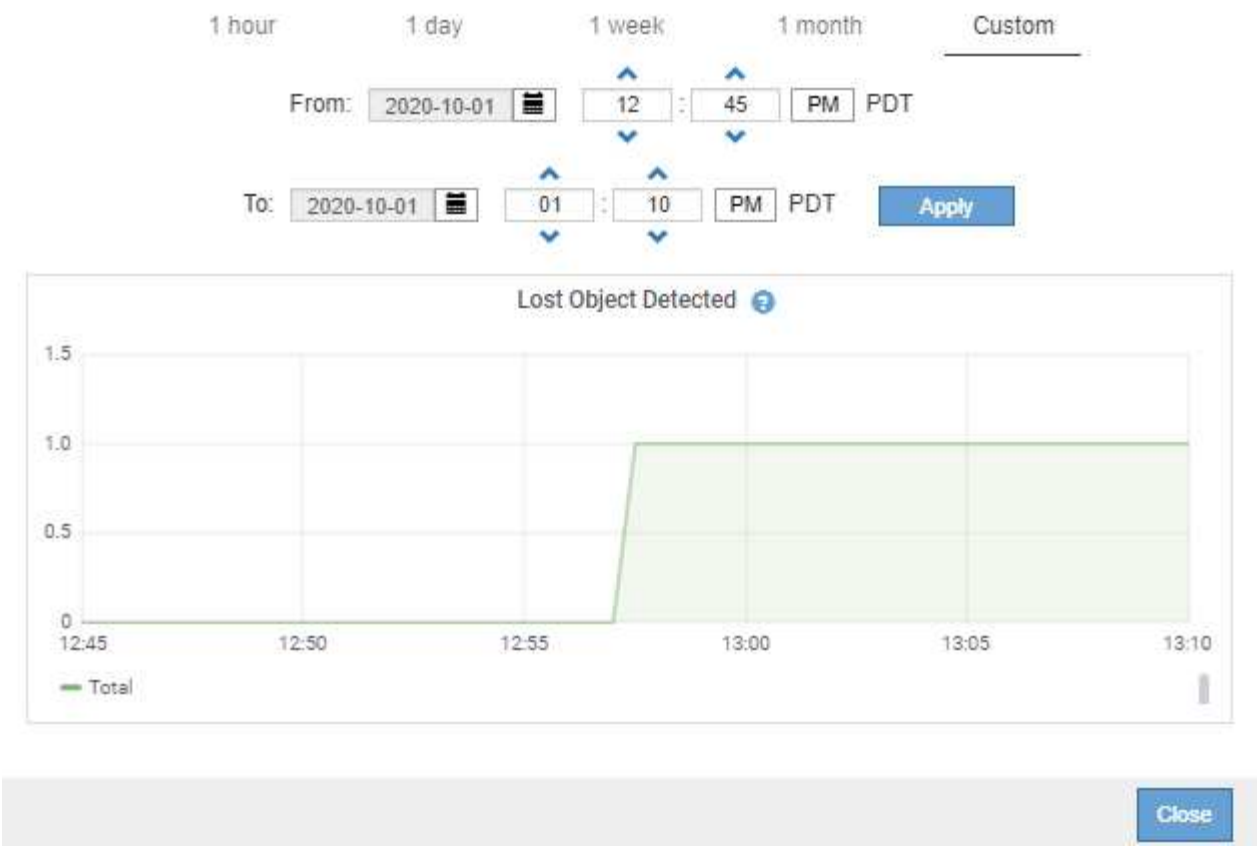
Esempio 1: Dalla scheda oggetti di un nodo di storage, è possibile selezionare l'icona del grafico Per visualizzare il numero totale di query di archiviazione dei metadati riuscite per il nodo di storage.

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

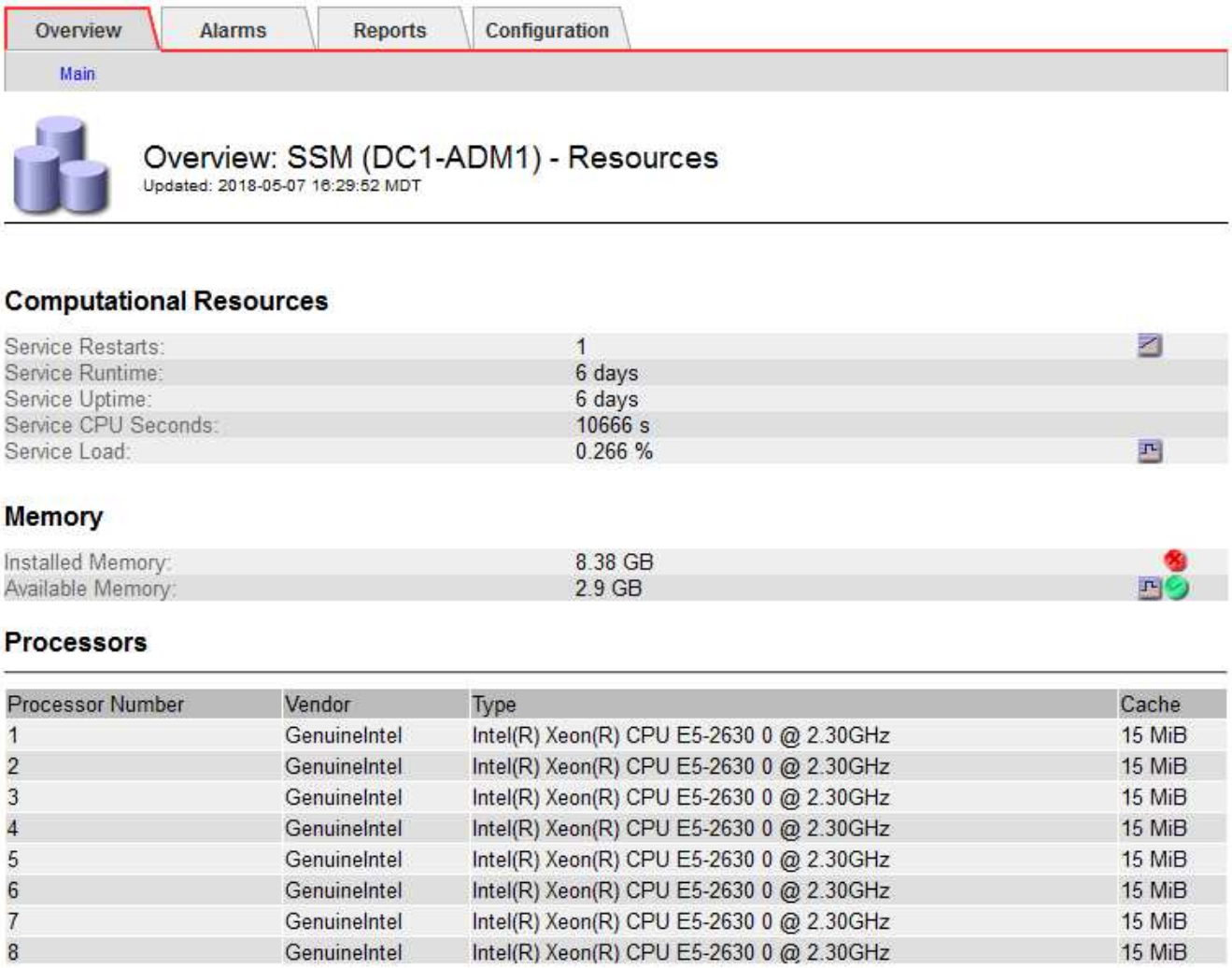


Esempio 2: Dalla scheda oggetti di un nodo di archiviazione, è possibile selezionare l'icona del grafico Per visualizzare il grafico Grafana del numero di oggetti persi rilevati nel tempo.





5. Per visualizzare i grafici degli attributi non visualizzati nella pagina nodo, selezionare **SUPPORT** > **Tools** > **Grid topology**.
6. Selezionare ***grid node*** > ***component or service*** > **Overview** > **Main**.



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

   Il display passa automaticamente alla pagina **Report** > **grafici**. Il grafico visualizza i dati dell'attributo nel giorno passato.

Generare grafici

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

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node*** > ***component or service*** > **Report** > **grafici**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **attributo**.
4. Per forzare l'inizio dell'asse Y a zero, deselezionare la casella di controllo **Vertical Scaling** (Scala verticale).

5. Per visualizzare i valori con la massima precisione, selezionare la casella di controllo **dati non elaborati** oppure per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselezionare la casella di controllo **dati non elaborati**.
6. Selezionare il periodo di tempo per il quale si desidera creare un report dall'elenco a discesa **Query rapida**.

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

   Il grafico viene visualizzato dopo alcuni istanti. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi.

7. Se si seleziona Custom Query (Query personalizzata), personalizzare il periodo di tempo per il grafico inserendo **Data di inizio** e **Data di fine**.

   Utilizzare il formato *YYYY/MM/DDHH:MM:SS* in ora locale. Gli zeri iniziali devono corrispondere al formato. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

8. Selezionare **Aggiorna**.

   Dopo alcuni secondi viene generato un grafico. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi. A seconda del periodo di tempo impostato per la query, viene visualizzato un report di testo raw o aggregato.

Utilizzare report di testo

I report di testo visualizzano una rappresentazione testuale dei valori dei dati degli attributi elaborati dal servizio NMS. Esistono due tipi di report generati in base al periodo di tempo in cui si esegue il reporting: Report di testo raw per periodi inferiori a una settimana e report di testo aggregati per periodi superiori a una settimana.

Report di testo raw

Un report di testo raw visualizza i dettagli relativi all'attributo selezionato:

- Time Received (ora ricezione): Data e ora locali in cui un valore di esempio dei dati di un attributo è stato elaborato dal servizio NMS.
- Sample Time (ora campione): Data e ora locali in cui un valore di attributo è stato campionato o modificato all'origine.
- Value (valore): Valore dell'attributo al momento del campionamento.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Aggregare report di testo

Un report di testo aggregato visualizza i dati in un periodo di tempo più lungo (di solito una settimana) rispetto a un report di testo raw. Ciascuna voce è il risultato di un riepilogo di più valori di attributo (un aggregato di valori di attributo) da parte del servizio NMS nel tempo in una singola voce con valori medi, massimi e minimi derivati dall'aggregazione.

Ciascuna voce visualizza le seguenti informazioni:

- Aggregate time (ora aggregata): L'ultima data e ora locale in cui il servizio NMS ha aggregato (raccolto) un insieme di valori di attributo modificati.
- Average value (valore medio): La media del valore dell'attributo nel periodo di tempo aggregato.
- Minimum Value (valore minimo): Il valore minimo nel periodo di tempo aggregato.
- Maximum Value (valore massimo): Il valore massimo nel periodo di tempo aggregato.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Generare report di testo

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

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Per i dati degli attributi che si prevede siano in continuo cambiamento, questi dati degli attributi vengono campionati dal servizio NMS (all'origine) a intervalli regolari. Per i dati degli attributi che cambiano di rado (ad esempio, dati basati su eventi come cambiamenti di stato o stato), un valore di attributo viene inviato al servizio NMS quando il valore cambia.

Il tipo di report visualizzato dipende dal periodo di tempo configurato. Per impostazione predefinita, i report di testo aggregati vengono generati per periodi di tempo superiori a una settimana.

Il testo grigio indica che il servizio è stato amministrativamente inattivo durante il campionamento. Il testo blu indica che il servizio si trova in uno stato sconosciuto.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node*** > ***component o service*** > **Report** > **testo**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **attributo**.
4. Selezionare il numero di risultati per pagina dall'elenco a discesa **risultati per pagina**.
5. Per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselezionare la casella di controllo **dati non elaborati**.
6. Selezionare il periodo di tempo per il quale si desidera creare un report dall'elenco a discesa **Query rapida**.

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

Il report viene visualizzato dopo alcuni istanti. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi.

7. Se si seleziona Custom Query (Query personalizzata), è necessario personalizzare il periodo di tempo per il quale si desidera creare un report inserendo **Data di inizio** e **Data di fine**.

   Utilizzare il formato `YYYY/MM/DDHH:MM:SS` in ora locale. Gli zeri iniziali devono corrispondere al formato. Ad esempio, 2017/4/6 7:30:00 non supera la convalida. Il formato corretto è: 2017/04/06 07:30:00.

8. Fare clic su **Aggiorna**.

   Dopo alcuni istanti viene generato un report di testo. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi. A seconda del periodo di tempo impostato per la query, viene visualizzato un report di testo raw o aggregato.

Esportare report di testo

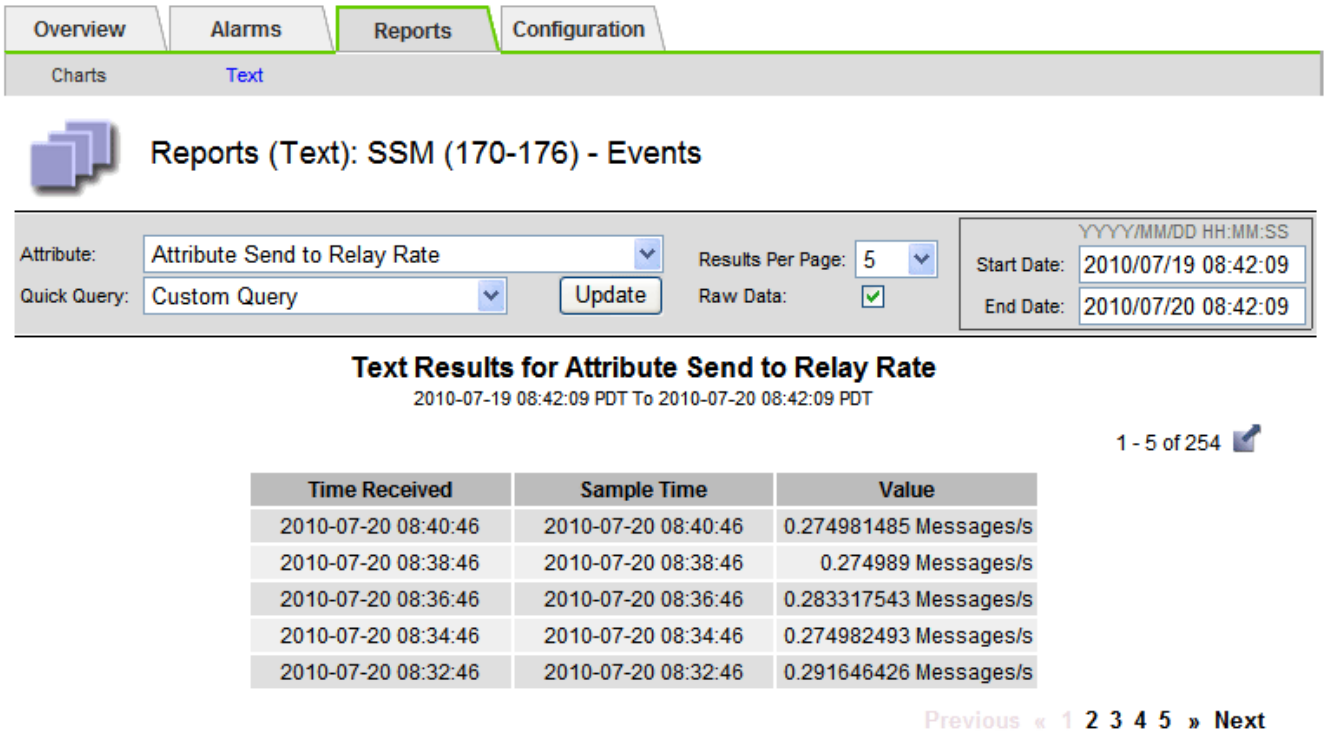
I report di testo esportati aprono una nuova scheda del browser che consente di selezionare e copiare i dati.

A proposito di questa attività

I dati copiati possono quindi essere salvati in un nuovo documento (ad esempio, un foglio di calcolo) e utilizzati per analizzare le prestazioni del sistema StorageGRID.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Creare un report di testo.
3. Fare clic su *Esporta*.



Viene visualizzata la finestra Export Text Report (Esporta report di testo) che visualizza il report.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. Selezionare e copiare il contenuto della finestra Esporta report di testo.

   Questi dati possono ora essere incollati in un documento di terze parti, ad esempio un foglio di calcolo.

Monitorare L'EFFICIENZA e OTTENERE le performance

È possibile monitorare le performance di alcune operazioni, come ad esempio l'archiviazione e il recupero di oggetti, per identificare le modifiche che potrebbero richiedere ulteriori analisi.

A proposito di questa attività

Per monitorare LE performance, puoi eseguire i comandi S3 e Swift direttamente da una workstation o utilizzando l'applicazione open-source S3tester. L'utilizzo di questi metodi consente di valutare le performance indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o problemi con una rete esterna.

Quando si eseguono i test delle operazioni PUT e GET, attenersi alle seguenti linee guida:

- Utilizzare dimensioni degli oggetti paragonabili agli oggetti che di solito si acquisiscono nella griglia.
- Eseguire operazioni su siti locali e remoti.

Messaggi in "log di audit" indicare il tempo totale necessario per eseguire determinate operazioni. Ad esempio, per determinare il tempo di elaborazione totale per una richiesta S3 GET, è possibile esaminare il valore dell'attributo TIME nel messaggio di audit SGET. È inoltre possibile trovare l'attributo TIME nei messaggi di audit per le seguenti operazioni:

- **S3**: DELETE, GET, HEAD, Metadata Updated, POST, IN PRIMO PIANO
- **SWIFT**: ELIMINA, OTTIENI, TESTA, METTI

Durante l'analisi dei risultati, esaminare il tempo medio richiesto per soddisfare una richiesta e il throughput complessivo che è possibile ottenere. Ripetere regolarmente gli stessi test e registrare i risultati, in modo da

poter identificare i trend che potrebbero richiedere un'indagine.

- È possibile "Scarica S3tester da github".

Monitorare le operazioni di verifica degli oggetti

Il sistema StorageGRID è in grado di verificare l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti danneggiati e mancanti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".

A proposito di questa attività

Due "processi di verifica" lavorare insieme per garantire l'integrità dei dati:

- **La verifica in background** viene eseguita automaticamente, controllando continuamente la correttezza dei dati dell'oggetto.

  La verifica in background verifica automaticamente e continuamente tutti i nodi di storage per determinare se sono presenti copie corrotte dei dati degli oggetti replicati e codificati in cancellazione. In caso di problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati dell'oggetto corrotto da copie memorizzate in un'altra parte del sistema. La verifica in background non viene eseguita sui nodi di archiviazione o sugli oggetti in un pool di storage cloud.

  > L'avviso **rilevato oggetto corrotto non identificato** viene attivato se il sistema rileva un oggetto corrotto che non può essere corretto automaticamente.

- **Il controllo dell'esistenza di oggetti** può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) dei dati dell'oggetto.

  Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti consente di verificare l'integrità dei dispositivi di storage, in particolare se un recente problema hardware potrebbe aver influenzato l'integrità dei dati.

È necessario esaminare regolarmente i risultati delle verifiche in background e dei controlli sull'esistenza degli oggetti. Esaminare immediatamente eventuali istanze di dati degli oggetti corrotti o mancanti per determinare la causa principale.

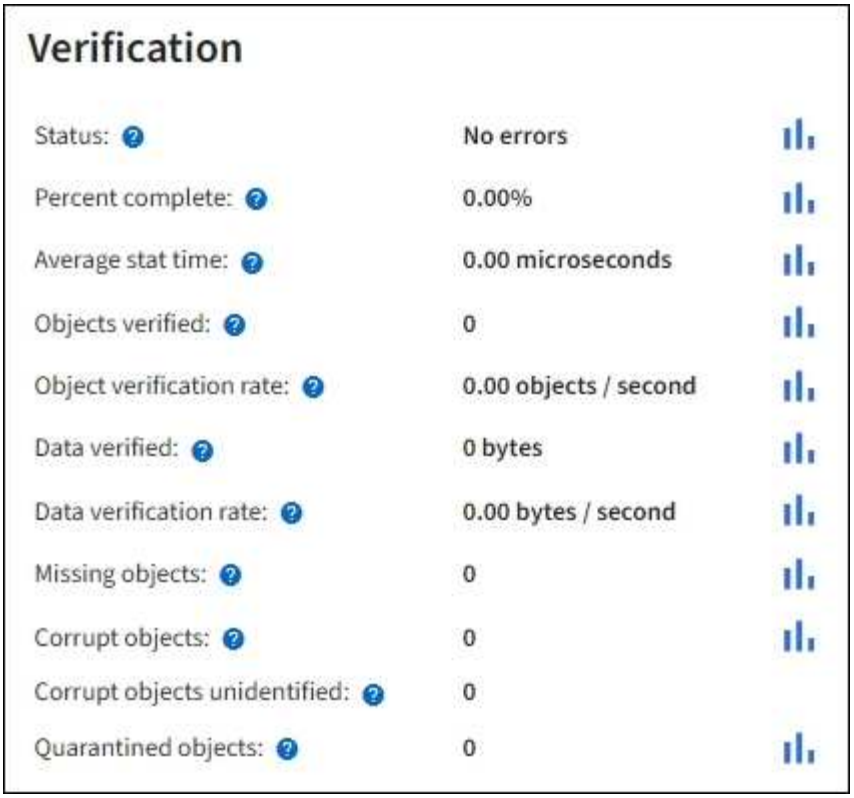
Fasi

1. Esaminare i risultati delle verifiche in background:

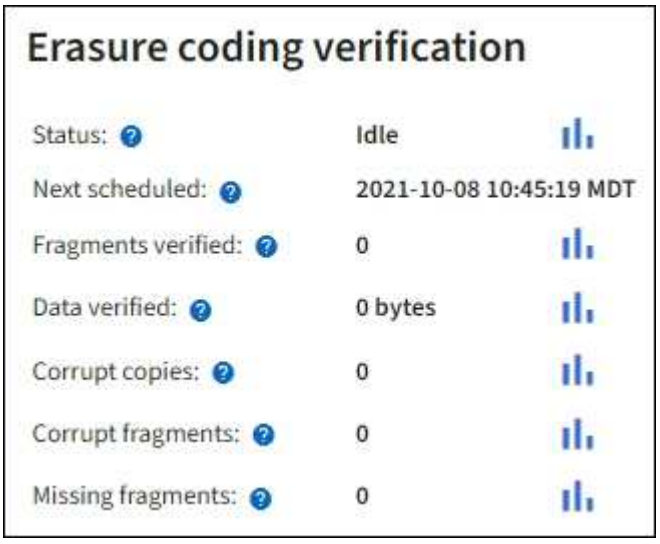
   a. Selezionare **NODI** > ***nodo di storage*** > **oggetti**.

   b. Verificare i risultati della verifica:

      - Per controllare la verifica dei dati degli oggetti replicati, esaminare gli attributi nella sezione verifica.

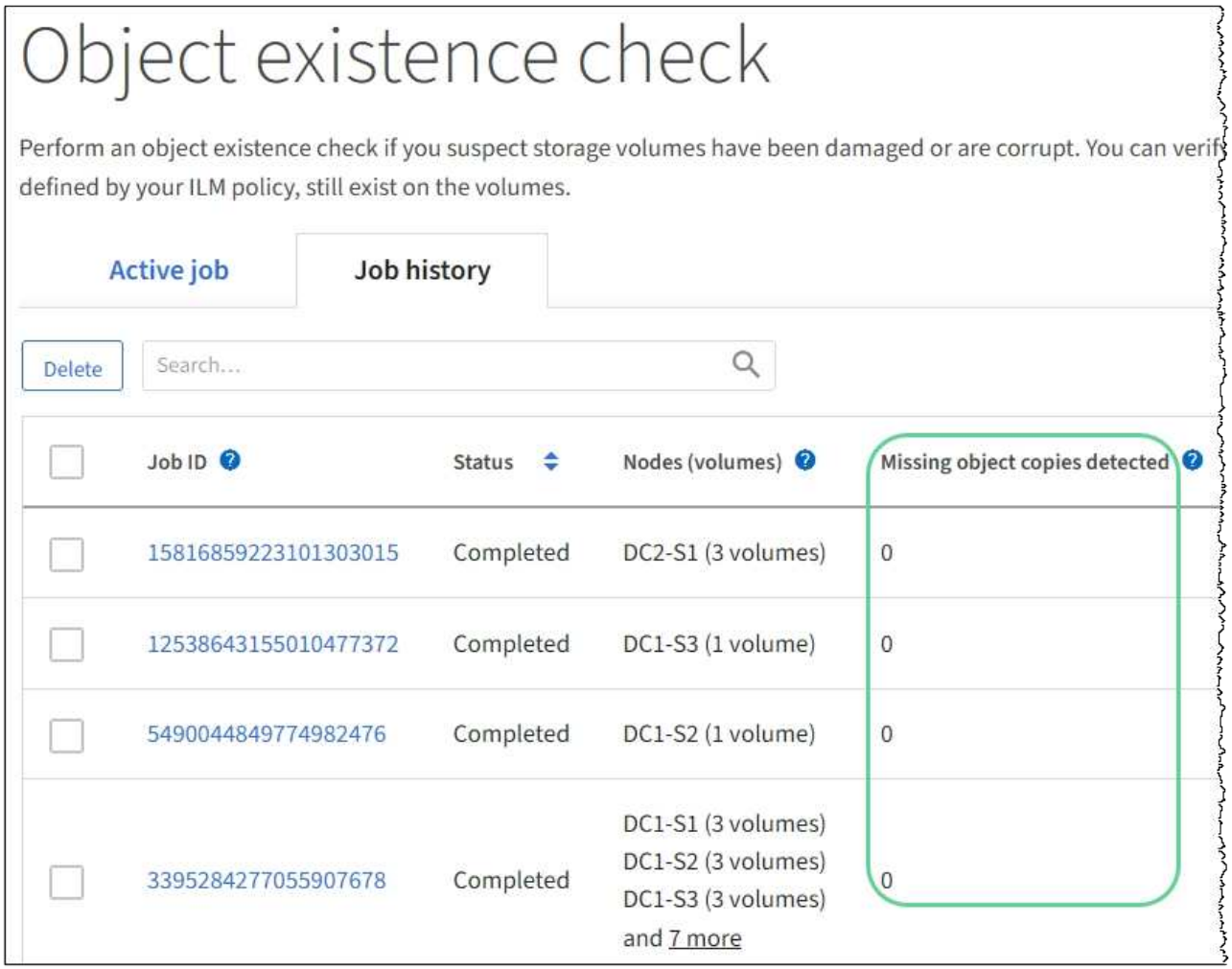


- Per controllare la verifica dei frammenti con codifica di cancellazione, selezionare ***Storage Node*** > **ILM** e controllare gli attributi nella sezione Erasure coding verifcation.



Selezionare il punto interrogativo ? accanto al nome di un attributo per visualizzare il testo della guida.

2. Esaminare i risultati dei job di controllo dell'esistenza di oggetti:
   a. Selezionare **MANUTENZIONE** > **verifica dell'esistenza dell'oggetto** > **Cronologia lavori**.
   b. Eseguire la scansione della colonna copie oggetto mancanti rilevate. Se un lavoro ha causato 100 o più copie di oggetti mancanti e l'avviso **oggetti persi** è stato attivato, contattare il supporto tecnico.



Monitorare gli eventi

È possibile monitorare gli eventi rilevati da un nodo grid, inclusi gli eventi personalizzati creati per tenere traccia degli eventi registrati nel server syslog. Il messaggio Last Event (ultimo evento) visualizzato in Grid Manager fornisce ulteriori informazioni sull'evento più recente.

I messaggi degli eventi sono elencati anche in `/var/local/log/bycast-err.log` file di log. Vedere "Riferimenti ai file di log".

L'allarme SMTT (Total events) può essere ripetutamente attivato da problemi come problemi di rete, interruzioni di corrente o aggiornamenti. Questa sezione contiene informazioni sull'analisi degli eventi, in modo da comprendere meglio il motivo per cui si sono verificati questi allarmi. Se un evento si è verificato a causa di un problema noto, è possibile ripristinare i contatori degli eventi in tutta sicurezza.

Fasi

1. Esaminare gli eventi di sistema per ciascun nodo della griglia:
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***site*** > ***grid node*** > **SSM** > **Eventi** > **Panoramica** > **principale**.
2. Genera un elenco di messaggi di eventi precedenti per isolare i problemi verificatisi in passato:

a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.

b. Selezionare ***site*** > ***grid node*** > **SSM** > **Eventi** > **Report**.

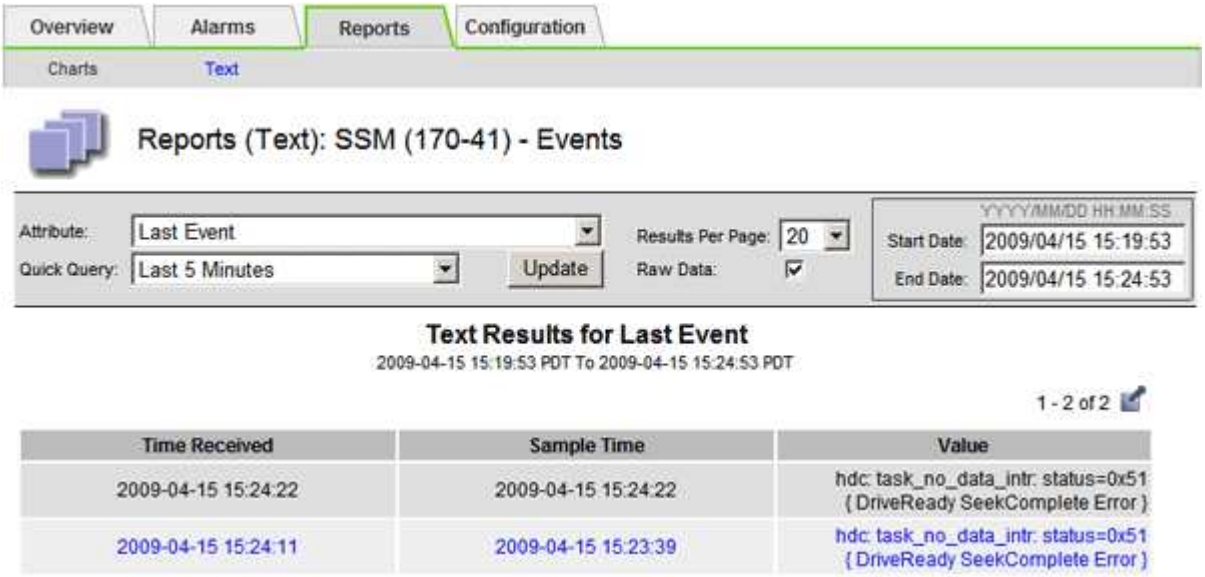
c. Selezionare **testo**.

L'attributo **Last Event** non viene visualizzato in "vista dei grafici". Per visualizzarlo:

d. Modificare **attributo** in **ultimo evento**.

e. Facoltativamente, selezionare un periodo di tempo per **Query rapida**.

f. Selezionare **Aggiorna**.



Creare eventi syslog personalizzati

Gli eventi personalizzati consentono di tenere traccia di tutti gli eventi utente di kernel, daemon, errori e livello critico registrati sul server syslog. Un evento personalizzato può essere utile per monitorare l'occorrenza dei messaggi del registro di sistema (e quindi gli eventi di sicurezza della rete e gli errori hardware).

A proposito di questa attività

Prendere in considerazione la creazione di eventi personalizzati per monitorare i problemi ricorrenti. Le seguenti considerazioni si applicano agli eventi personalizzati.

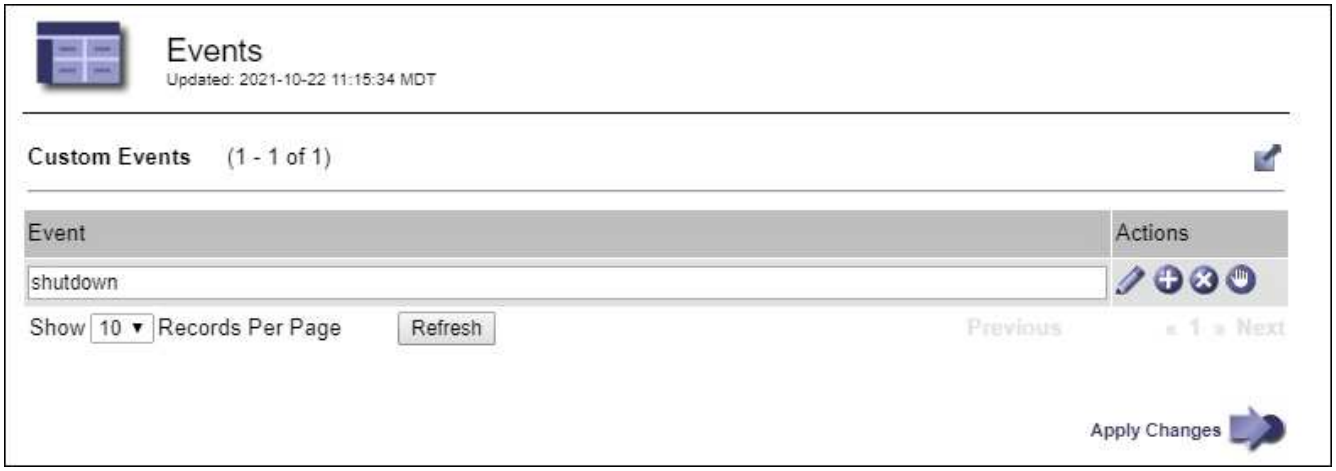
- Dopo la creazione di un evento personalizzato, viene monitorata ogni occorrenza.
- Per creare un evento personalizzato in base alle parole chiave in `/var/local/log/messages` i log in questi file devono essere:
  - Generato dal kernel
  - Generato da daemon o programma utente a livello di errore o critico

Nota: non tutte le voci in `/var/local/log/messages` i file verranno abbinati a meno che non soddisfino i requisiti indicati in precedenza.

Fasi

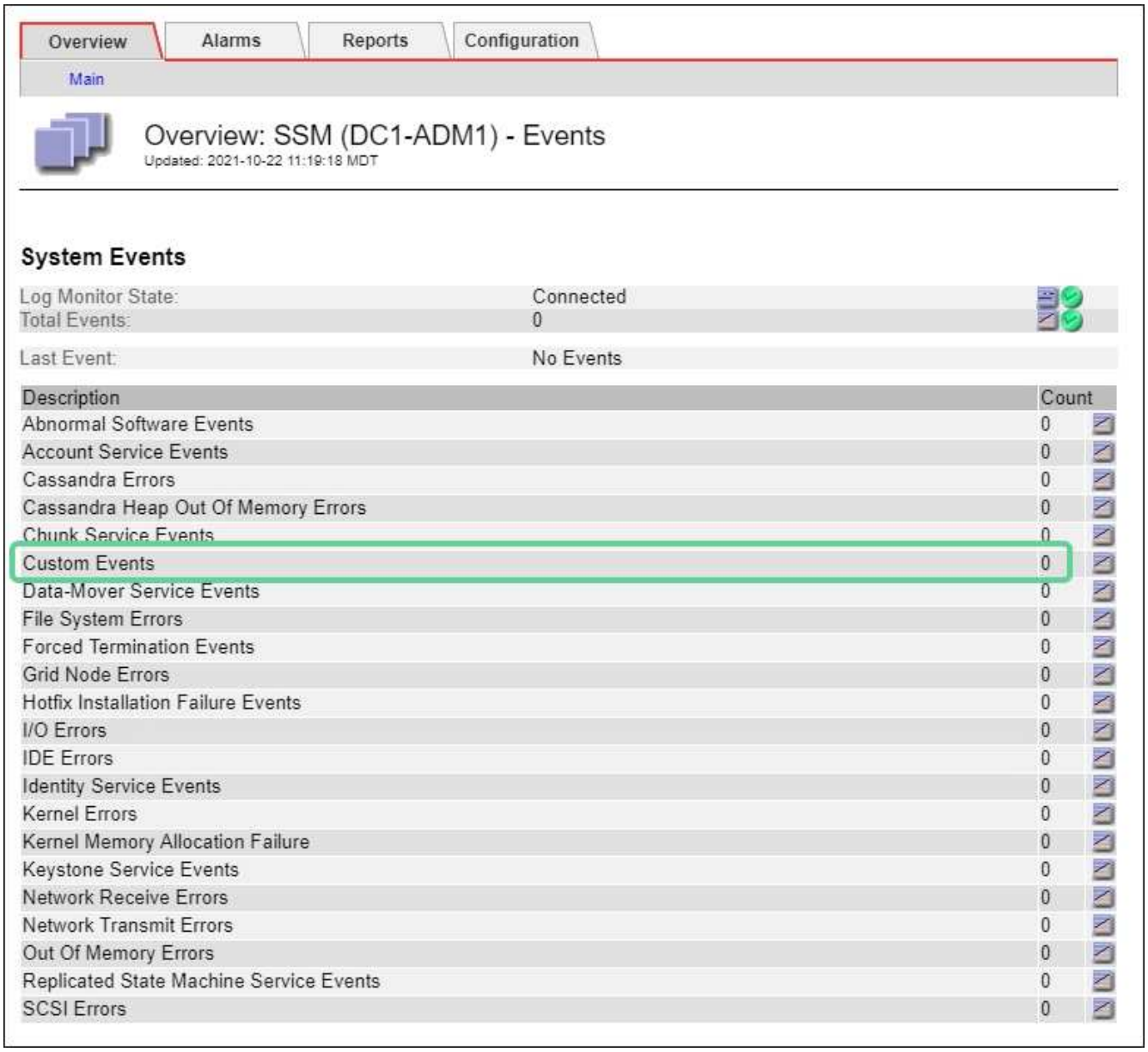
1. Selezionare **SUPPORTO** > **Allarmi (legacy)** > **Eventi personalizzati**.
2. Fare clic su **Edit** (Modifica) (O **Inserisci** se questo non è il primo evento).

3. Inserire una stringa di eventi personalizzata, ad esempio shutdown



4. Selezionare **Applica modifiche**.
5. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
6. Selezionare ***grid node*** > **SSM** > **Events**.
7. Individuare la voce per gli eventi personalizzati nella tabella Eventi e monitorare il valore per **Conteggio**.

   Se il numero aumenta, viene attivato un evento personalizzato monitorato su quel nodo della griglia.



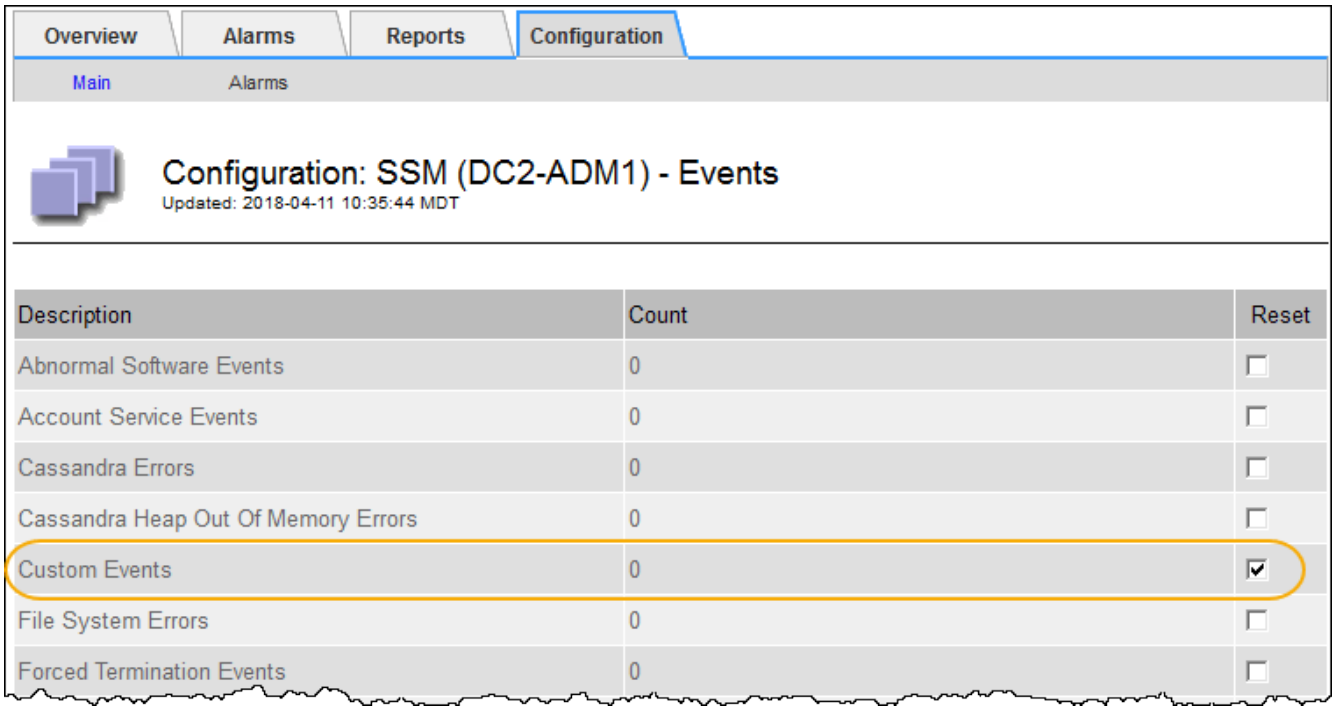
Azzerare il numero di eventi personalizzati

Se si desidera reimpostare il contatore solo per eventi personalizzati, è necessario utilizzare la pagina Grid Topology (topologia griglia) nel menu Support (supporto).

La reimpostazione di un contatore provoca l'attivazione dell'allarme all'evento successivo. Al contrario, quando si riconosce un allarme, questo viene riattivato solo se viene raggiunto il livello di soglia successivo.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node*** > **SSM** > **Eventi** > **Configurazione** > **principale**.
3. Selezionare la casella di controllo **Reset** (Ripristina) per Custom Events (Eventi personalizzati).



4. Selezionare **Applica modifiche**.

Esaminare i messaggi di audit

I messaggi di audit possono aiutarti a comprendere meglio le operazioni dettagliate del tuo sistema StorageGRID. È possibile utilizzare i registri di audit per risolvere i problemi e valutare le performance.

Durante il normale funzionamento del sistema, tutti i servizi StorageGRID generano messaggi di audit, come segue:

- I messaggi di audit del sistema sono correlati al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema e alle operazioni di backup del servizio.
- I messaggi di audit dello storage a oggetti sono correlati allo storage e alla gestione degli oggetti all'interno di StorageGRID, tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.
- I messaggi di controllo in lettura e scrittura del client vengono registrati quando un'applicazione client S3 o Swift richiede di creare, modificare o recuperare un oggetto.
- I messaggi di controllo della gestione registrano le richieste degli utenti all'API di gestione.

Ogni nodo amministrativo memorizza i messaggi di audit in file di testo. La condivisione dell'audit contiene il file attivo (audit.log) e i registri di audit compressi dei giorni precedenti. Ogni nodo della griglia memorizza anche una copia delle informazioni di audit generate sul nodo.

Per un facile accesso ai registri di controllo, è possibile "Configurare l'accesso client di audit per NFS". È inoltre possibile accedere ai file di log di audit direttamente dalla riga di comando del nodo di amministrazione.

StorageGRID può inviare informazioni di audit per impostazione predefinita, oppure è possibile modificare la destinazione:

- Il valore predefinito di StorageGRID per le destinazioni di audit dei nodi locali.

- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione.
- In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno.
- "Informazioni sulla configurazione dei messaggi di controllo e delle destinazioni dei log".

Per informazioni dettagliate sul file di log di audit, sul formato dei messaggi di audit, sui tipi di messaggi di audit e sugli strumenti disponibili per analizzare i messaggi di audit, vedere "Esaminare i registri di audit".

Raccogliere i file di log e i dati di sistema

È possibile utilizzare Grid Manager per recuperare i file di log e i dati di sistema (inclusi i dati di configurazione) per il sistema StorageGRID.

Prima di iniziare

- È necessario accedere a Grid Manager sul nodo di amministrazione primario utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- È necessario disporre della passphrase di provisioning.

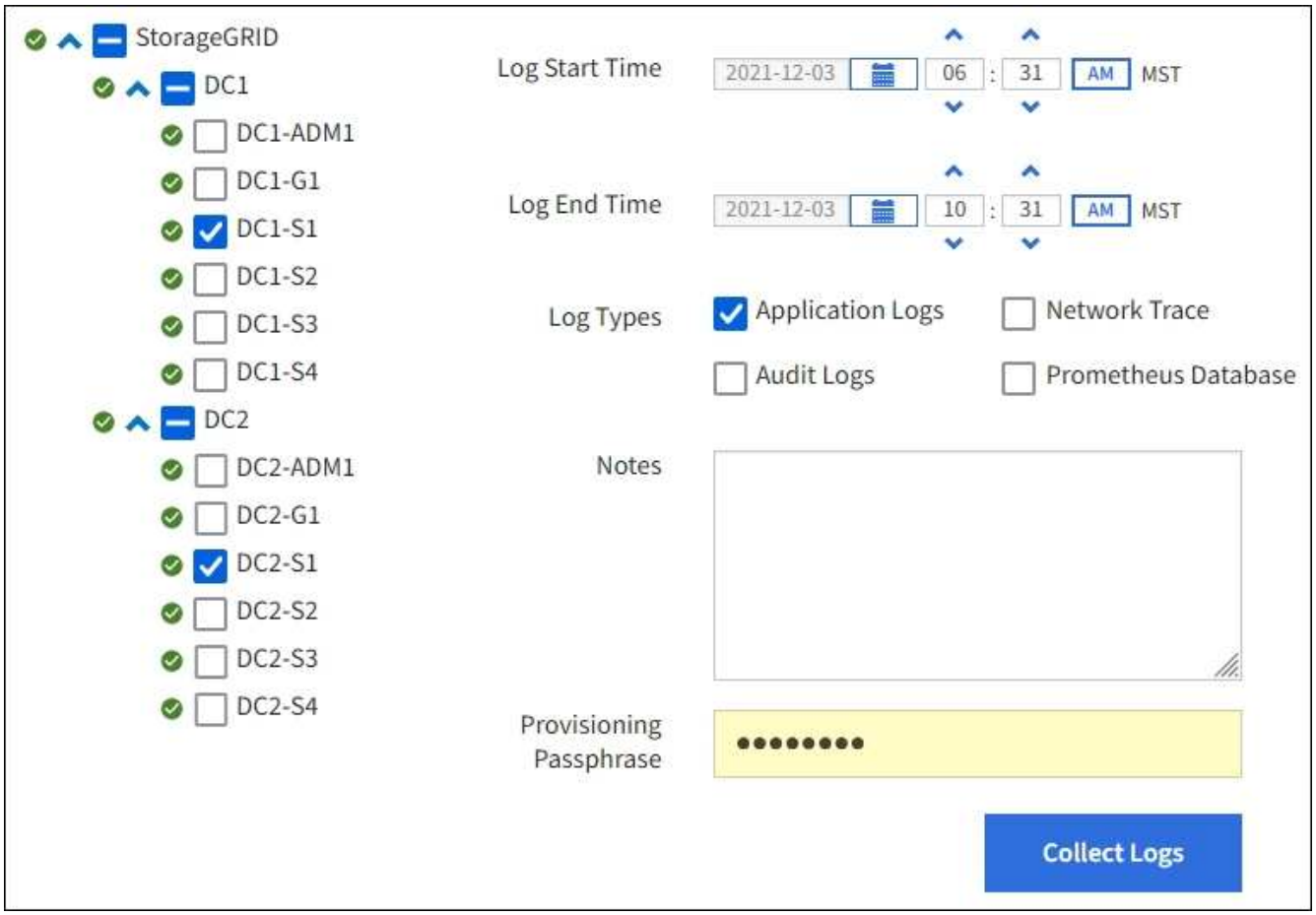
A proposito di questa attività

È possibile utilizzare Grid Manager per la raccolta "file di log", dati di sistema e dati di configurazione da qualsiasi nodo della griglia per il periodo di tempo selezionato. I dati vengono raccolti e archiviati in un file .tar.gz che è possibile scaricare sul computer locale.

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

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Logs**.



2. Selezionare i nodi della griglia per i quali si desidera raccogliere i file di log.

   Se necessario, è possibile raccogliere i file di log per l'intera griglia o per un intero sito del data center.

3. Selezionare **ora di inizio** e **ora di fine** per impostare l'intervallo di tempo dei dati da includere nei file di log.

   Se si seleziona un periodo di tempo molto lungo o si raccolgono i registri da tutti i nodi di una griglia di grandi dimensioni, l'archivio del registro potrebbe diventare troppo grande per essere memorizzato su un nodo o troppo grande per essere raccolto nel nodo di amministrazione primario per il download. In questo caso, è necessario riavviare la raccolta dei log con un set di dati più piccolo.

4. Selezionare i tipi di log che si desidera raccogliere.
   - **Registri delle applicazioni**: Registri specifici delle applicazioni che il supporto tecnico utilizza più frequentemente per la risoluzione dei problemi. I log raccolti sono un sottoinsieme dei log dell'applicazione disponibili.
   - **Audit Logs**: Registri contenenti i messaggi di audit generati durante il normale funzionamento del sistema.
   - **Network Trace**: Registri utilizzati per il debug della rete.
   - **Database Prometheus**: Metriche delle serie temporali dei servizi su tutti i nodi.
5. Se si desidera, inserire le note relative ai file di registro che si stanno raccogliendo nella casella di testo **Notes**.

   È possibile utilizzare queste note per fornire informazioni di supporto tecnico sul problema che ha richiesto di raccogliere i file di log. Le note vengono aggiunte a un file chiamato `info.txt`, insieme ad altre

informazioni sulla raccolta di file di log. Il `info.txt` il file viene salvato nel pacchetto di archiviazione del file di log.

6. Inserire la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.
7. Selezionare **Collect Logs** (raccolta registri).

   Quando si invia una nuova richiesta, la raccolta precedente di file di log viene eliminata.

   È possibile utilizzare la pagina Logs per monitorare l'avanzamento della raccolta dei file di log per ciascun nodo della griglia.

   Se viene visualizzato un messaggio di errore relativo alle dimensioni del registro, provare a raccogliere i registri per un periodo di tempo più breve o per un numero inferiore di nodi.

8. Selezionare **Download** al termine della raccolta dei file di log.

   Il file *.tar.gz* contiene tutti i file di log di tutti i nodi della griglia in cui la raccolta dei log ha avuto esito positivo. All'interno del file *.tar.gz* combinato, è presente un archivio di file di log per ciascun nodo della griglia.

Al termine

Se necessario, è possibile scaricare nuovamente il pacchetto di archiviazione del file di log in un secondo momento.

In alternativa, è possibile selezionare **Delete** (Elimina) per rimuovere il pacchetto di archiviazione del file di log e liberare spazio su disco. Il pacchetto di archiviazione del file di log corrente viene automaticamente rimosso alla successiva raccolta dei file di log.

Attivare manualmente un pacchetto AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- È necessario disporre dell'autorizzazione di accesso root o di altra configurazione della griglia.

Fasi

1. Selezionare **SUPPORTO** > **Strumenti** > **AutoSupport**.
2. Nella scheda **azioni**, selezionare **Invia AutoSupport** attivato dall'utente.

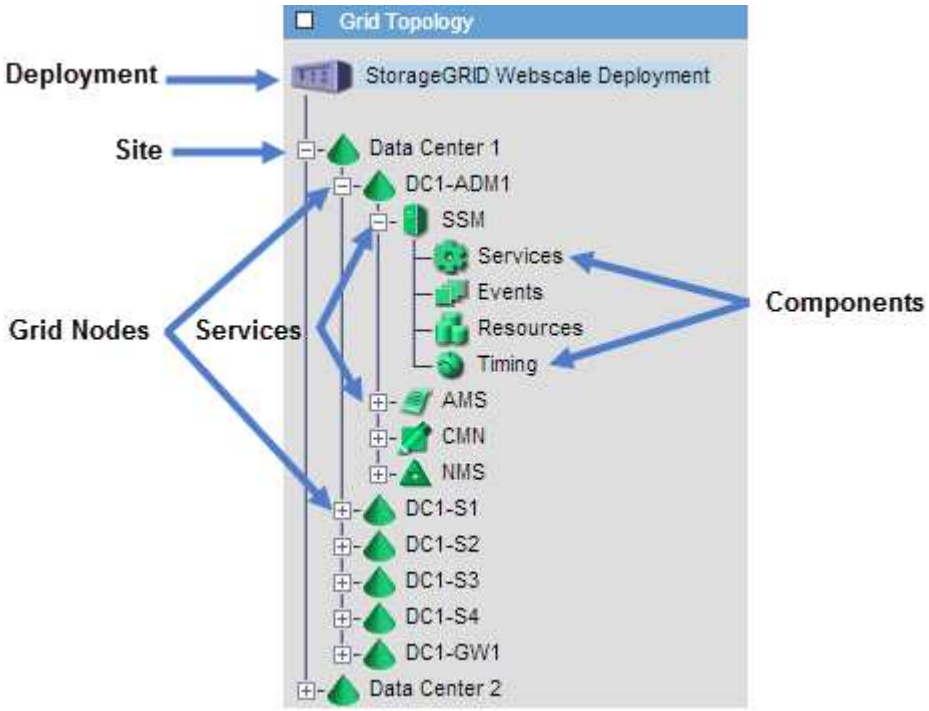
   StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp. Se il tentativo ha esito positivo, i valori **risultato più recente** e **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. Se si verifica un problema, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il pacchetto AutoSupport.

   > Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Visualizzare l’albero topologia griglia

L’albero topologia griglia consente di accedere a informazioni dettagliate sugli elementi del sistema StorageGRID, inclusi siti, nodi griglia, servizi e componenti. Nella maggior parte dei casi, è necessario accedere all’albero topologia griglia solo quando indicato nella documentazione o quando si lavora con il supporto tecnico.

Per accedere all’albero topologia griglia, selezionare **SUPPORTO** > **Strumenti** > **topologia griglia**.



Per espandere o comprimere l’albero topologia griglia, fare clic su ⊞ oppure ⊟ a livello di sito, nodo o servizio. Per espandere o comprimere tutti gli elementi dell’intero sito o di ciascun nodo, tenere premuto il tasto **<Ctrl>** e fare clic su.

Attributi StorageGRID

Gli attributi riportano valori e stati per molte delle funzioni del sistema StorageGRID. I valori degli attributi sono disponibili per ciascun nodo della griglia, per ciascun sito e per l’intera griglia.

Gli attributi StorageGRID vengono utilizzati in diversi punti del grid manager:

- Pagina **Nodes**: Molti dei valori mostrati nella pagina Nodes sono attributi StorageGRID. (Le metriche Prometheus sono visualizzate anche nelle pagine dei nodi).
- **Allarmi**: Quando gli attributi raggiungono valori di soglia definiti, gli allarmi StorageGRID (sistema legacy) vengono attivati a livelli di severità specifici.
- **Grid Topology tree**: I valori degli attributi vengono visualizzati nell’albero Grid Topology (**SUPPORT** > **Tools** > **Grid Topology**).
- **Eventi**: Gli eventi di sistema si verificano quando alcuni attributi registrano una condizione di errore o di errore per un nodo, inclusi errori come gli errori di rete.

Valori degli attributi

Gli attributi vengono riportati con il massimo sforzo e sono approssimativamente corretti. In alcuni casi, gli aggiornamenti degli attributi possono andare persi, ad esempio il crash di un servizio o il guasto e la ricostruzione di un nodo di rete.

Inoltre, i ritardi di propagazione potrebbero rallentare il reporting degli attributi. I valori aggiornati per la maggior parte degli attributi vengono inviati al sistema StorageGRID a intervalli fissi. Possono essere necessari alcuni minuti prima che un aggiornamento sia visibile nel sistema e due attributi che cambiano più o meno contemporaneamente possono essere riportati in momenti leggermente diversi.

Rivedere le metriche di supporto

Durante la risoluzione di un problema, puoi lavorare con il supporto tecnico per rivedere metriche e grafici dettagliati per il tuo sistema StorageGRID.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

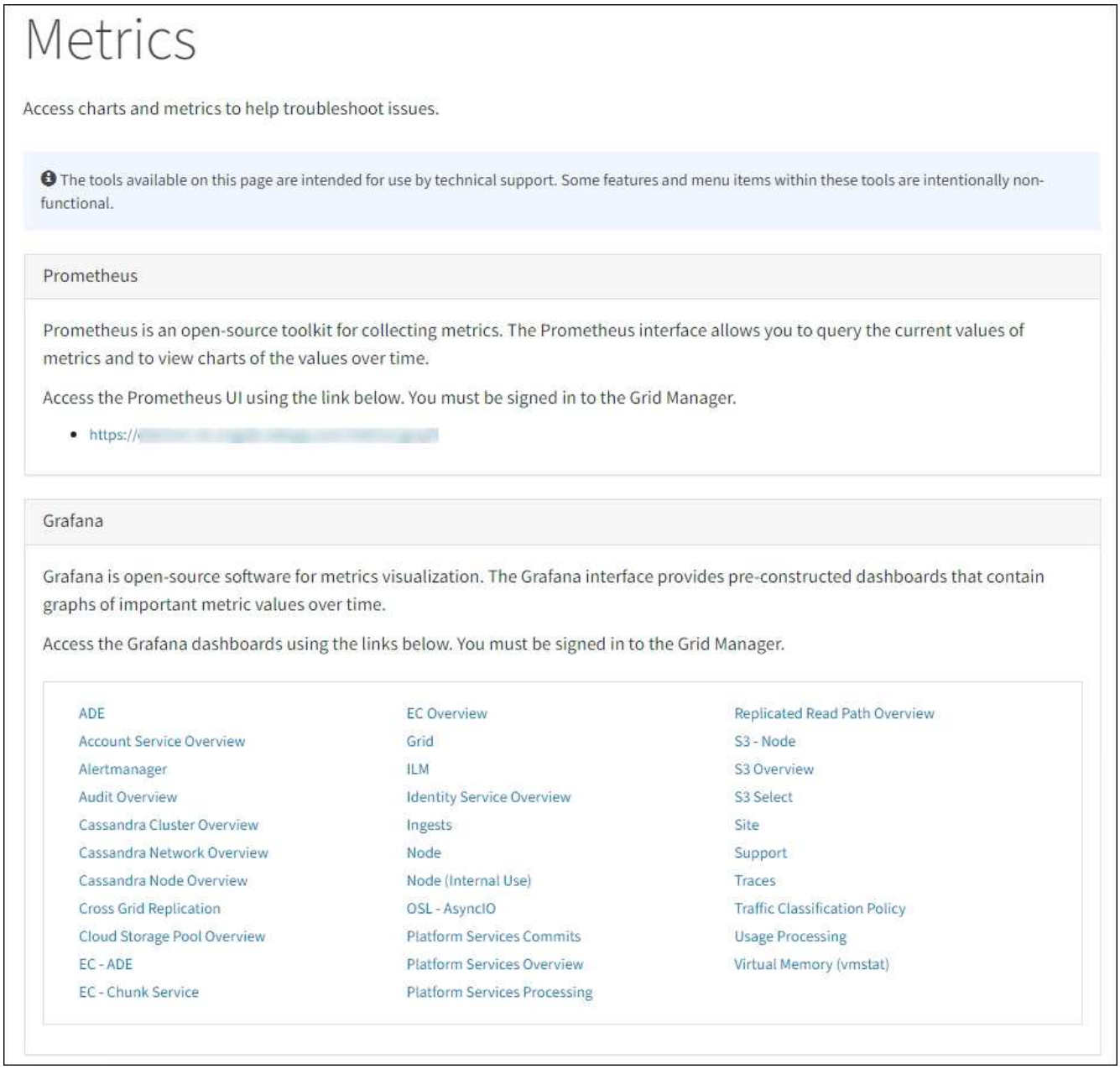
La pagina metriche consente di accedere alle interfacce utente Prometheus e Grafana. Prometheus è un software open-source per la raccolta di metriche. Grafana è un software open-source per la visualizzazione delle metriche.

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

Fasi

1. Come indicato dal supporto tecnico, selezionare **SUPPORTO** > **Strumenti** > **metriche**.

   Di seguito è riportato un esempio della pagina Metrics (metriche):



2. Per interrogare i valori correnti delle metriche StorageGRID e visualizzare i grafici dei valori nel tempo, fare clic sul collegamento nella sezione Prometheus.

   Viene visualizzata l'interfaccia Prometheus. È possibile utilizzare questa interfaccia per eseguire query sulle metriche StorageGRID disponibili e per rappresentare graficamente le metriche StorageGRID nel tempo.

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

3. Per accedere alle dashboard predefinite contenenti grafici delle metriche StorageGRID nel tempo, fare clic sui collegamenti nella sezione Grafana.

   Viene visualizzata l'interfaccia Grafana per il collegamento selezionato.

Eseguire la diagnostica

Durante la risoluzione di un problema, è possibile collaborare con il supporto tecnico per eseguire la diagnostica sul sistema StorageGRID e rivedere i risultati.

- "Rivedere le metriche di supporto"
- "Metriche Prometheus comunemente utilizzate"

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

La pagina Diagnostics (Diagnostica) esegue una serie di controlli diagnostici sullo stato corrente della griglia. Ogni controllo diagnostico può avere uno dei tre stati seguenti:

- **Normale**: Tutti i valori rientrano nell'intervallo normale.
- **Attenzione**: Uno o più valori non rientrano nell'intervallo normale.
- **Attenzione**: Uno o più valori sono significativamente al di fuori dell'intervallo normale.

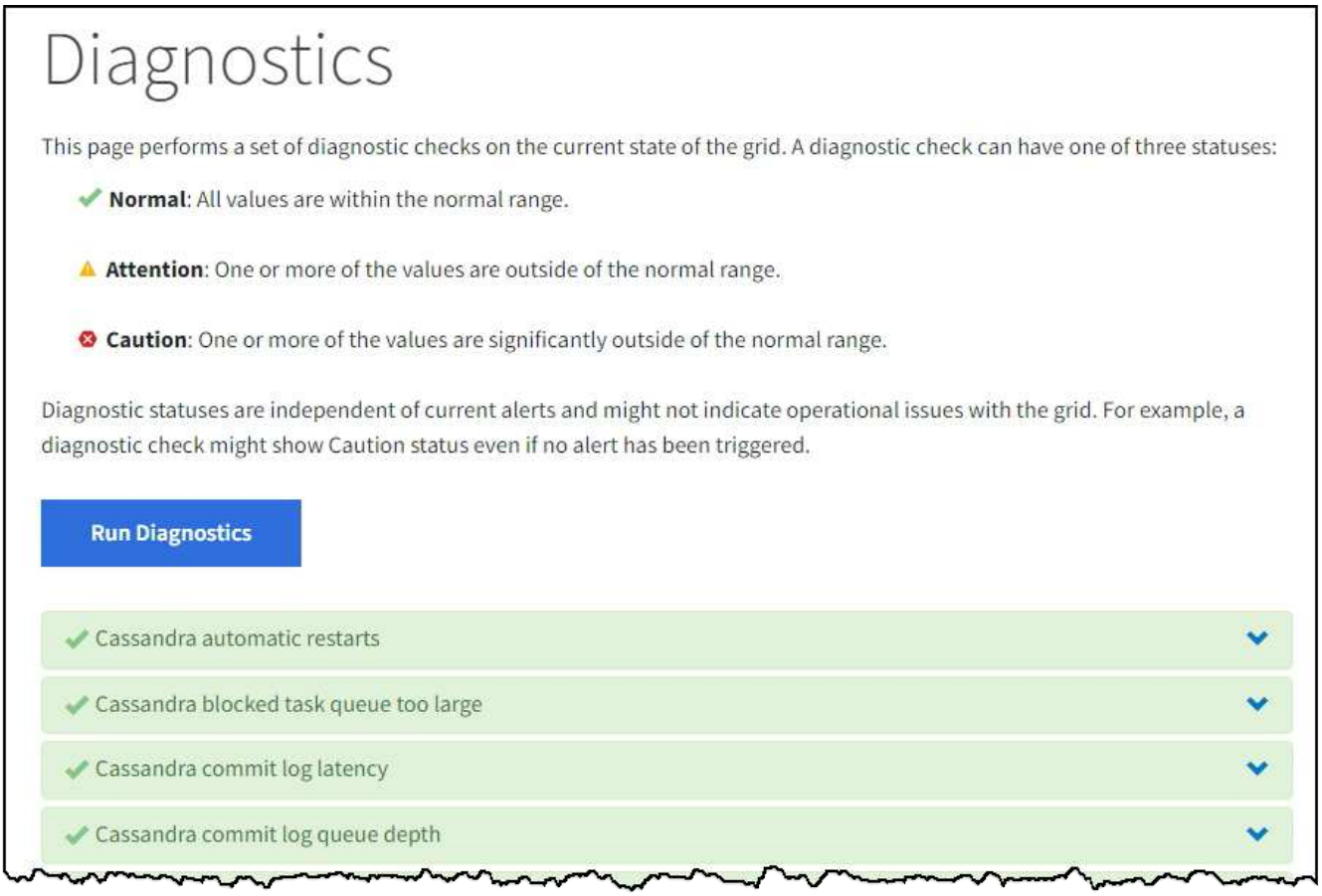
Gli stati di diagnostica sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la griglia. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato di attenzione anche se non è stato attivato alcun allarme.

Fasi

1. Selezionare **SUPPORTO** > **Strumenti** > **Diagnostica**.

   Viene visualizzata la pagina Diagnostics (Diagnostica) che elenca i risultati di ciascun controllo diagnostico. I risultati vengono ordinati in base alla gravità (attenzione, attenzione e quindi normale). All'interno di ciascuna severità, i risultati sono ordinati in ordine alfabetico.

   In questo esempio, tutte le diagnostiche hanno uno stato normale.



2. Per ulteriori informazioni su una diagnostica specifica, fare clic in un punto qualsiasi della riga.

   Vengono visualizzati i dettagli relativi alla diagnostica e ai risultati correnti. Sono elencati i seguenti dettagli:

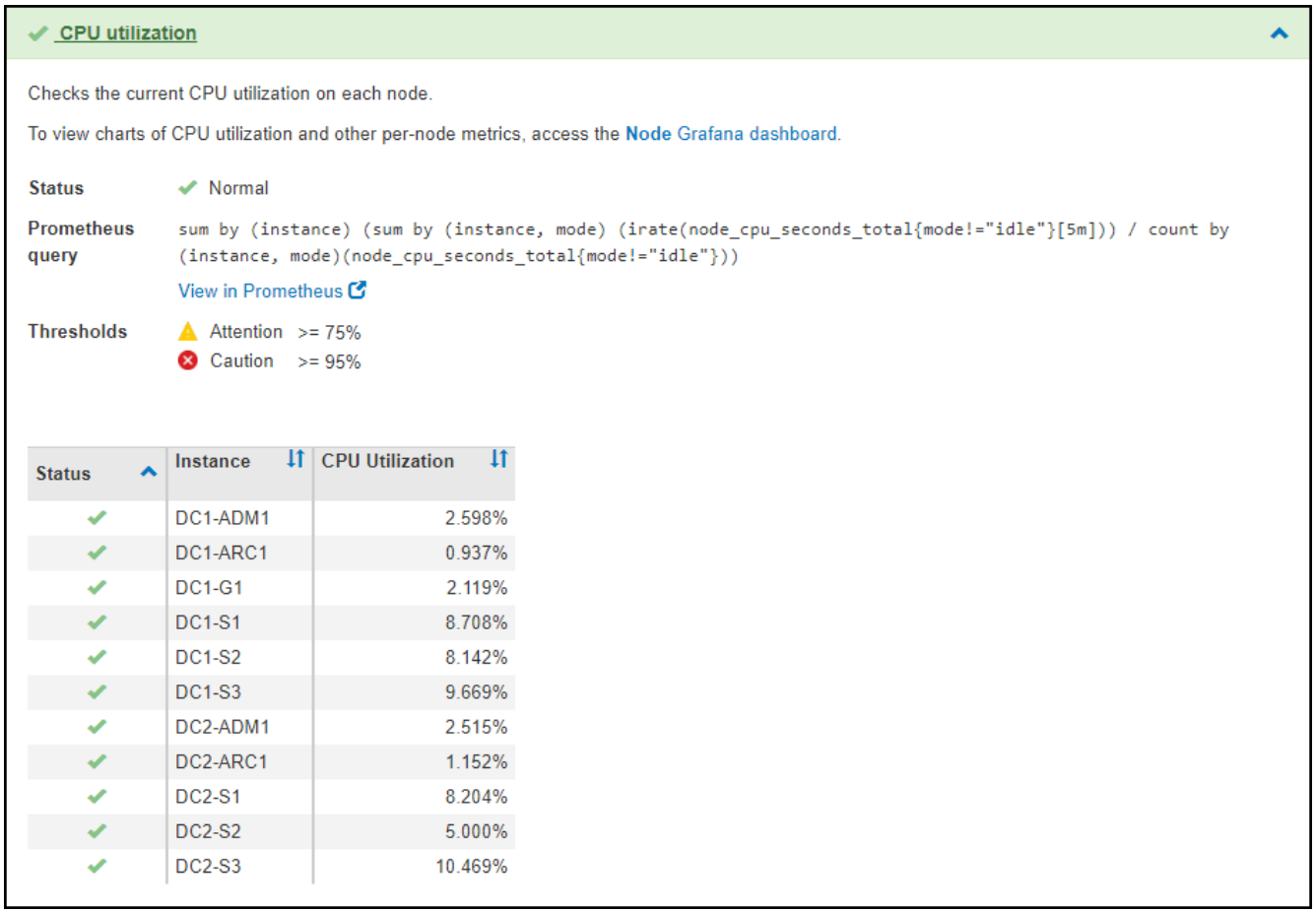
   - **Status** (Stato): Lo stato corrente di questa diagnostica: Normal (normale), Attention (attenzione) o Caution (attenzione).
   - **Query Prometheus**: Se utilizzata per la diagnostica, l'espressione Prometheus utilizzata per generare

i valori di stato. (Un'espressione Prometheus non viene utilizzata per tutte le diagnostiche).

- **Soglie**: Se disponibili per la diagnostica, le soglie definite dal sistema per ogni stato di diagnostica anomalo. (I valori di soglia non vengono utilizzati per tutte le diagnostiche).

  Non puoi modificare queste soglie.

- **Valori di stato**: Una tabella che mostra lo stato e il valore della diagnostica nel sistema StorageGRID. In questo esempio, viene mostrato l'utilizzo corrente della CPU per ogni nodo in un sistema StorageGRID. Tutti i valori dei nodi sono al di sotto delle soglie di attenzione e attenzione, quindi lo stato generale della diagnostica è normale.



Status	Instance	CPU Utilization
✔	DC1-ADM1	2.598%
✔	DC1-ARC1	0.937%
✔	DC1-G1	2.119%
✔	DC1-S1	8.708%
✔	DC1-S2	8.142%
✔	DC1-S3	9.669%
✔	DC2-ADM1	2.515%
✔	DC2-ARC1	1.152%
✔	DC2-S1	8.204%
✔	DC2-S2	5.000%
✔	DC2-S3	10.469%

3. **Opzionale**: Per visualizzare i grafici Grafana relativi a questa diagnostica, fare clic sul collegamento **dashboard Grafana**.

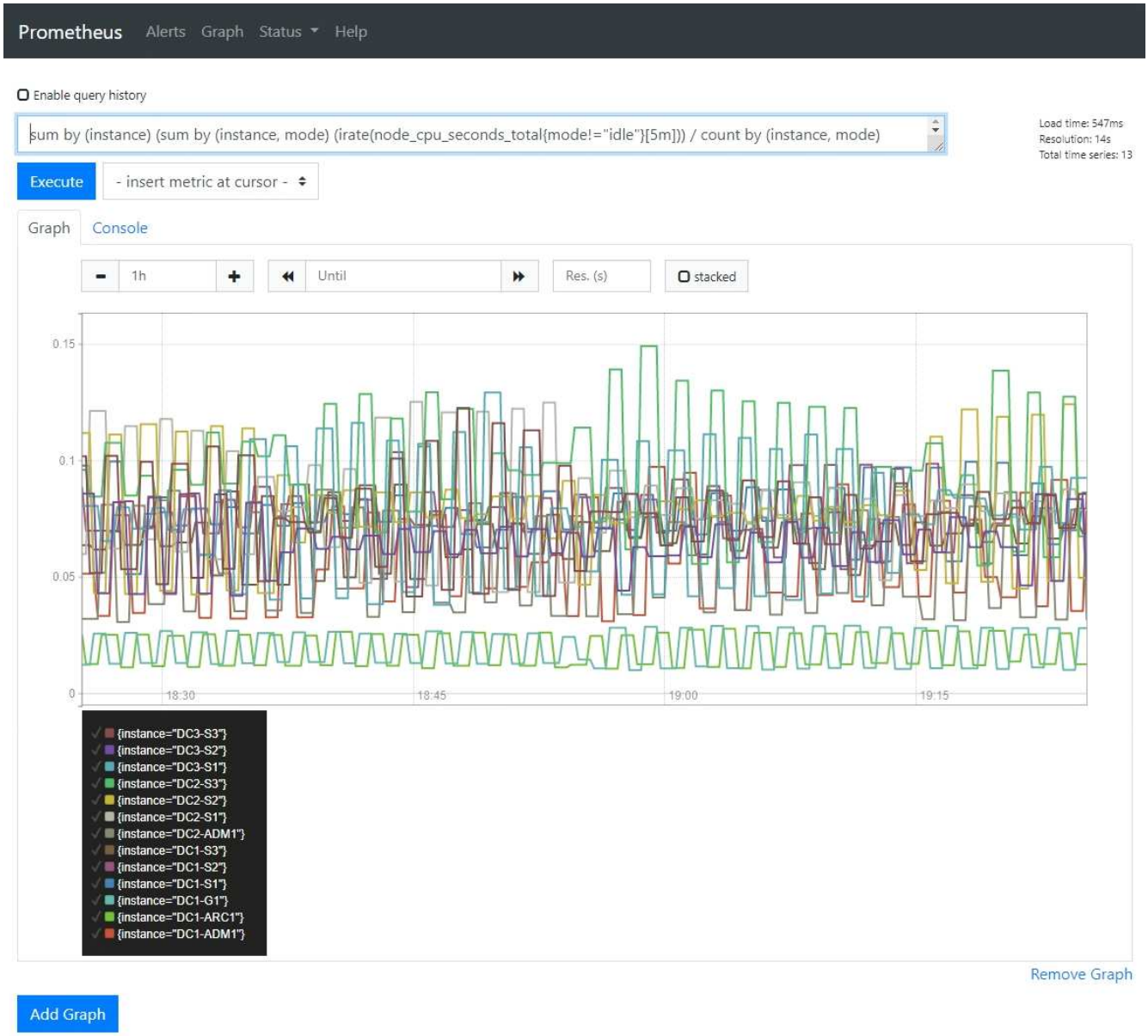
   Questo collegamento non viene visualizzato per tutte le diagnostiche.

   Viene visualizzata la dashboard Grafana correlata. In questo esempio, viene visualizzata la dashboard Node (nodo) che mostra l'utilizzo della CPU nel tempo per questo nodo e altri grafici Grafana per il nodo.

   Puoi anche accedere ai dashboard di Grafana già costruiti dalla sezione Grafana della pagina **SUPPORT** > **Tools** > **Metrics**.

4. **Opzionale**: Per visualizzare un grafico dell'espressione Prometheus nel tempo, fare clic su **Visualizza in Prometheus**.

   Viene visualizzato un grafico Prometheus dell'espressione utilizzata nella diagnostica.



Creare applicazioni di monitoraggio personalizzate

Puoi creare dashboard e applicazioni di monitoraggio personalizzate utilizzando le metriche StorageGRID disponibili nell'API di gestione del grid.

Se si desidera monitorare le metriche non visualizzate in una pagina esistente di Grid Manager o se si desidera creare dashboard personalizzati per StorageGRID, è possibile utilizzare l'API di gestione griglia per eseguire query sulle metriche StorageGRID.

Puoi anche accedere direttamente alle metriche Prometheus con uno strumento di monitoraggio esterno, come Grafana. L'utilizzo di uno strumento esterno richiede il caricamento o la generazione di un certificato client amministrativo per consentire a StorageGRID di autenticare lo strumento per la sicurezza. Vedere "Istruzioni per l'amministrazione di StorageGRID".

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, accedere a Grid Manager. Nella parte superiore della pagina, selezionare l'icona della guida e selezionare **documentazione API** > **metriche**.

metrics Operations on metrics

GET	`/grid/metric-labels/{label}/values`	Lists the values for a metric label
GET	`/grid/metric-names`	Lists all available metric names
GET	`/grid/metric-query`	Performs an instant metric query at a single point in time
GET	`/grid/metric-query-range`	Performs a metric query over a range of time

I dettagli su come implementare un'applicazione di monitoraggio personalizzata esulano dall'ambito di questa documentazione.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.