Monitorare e risolvere i problemi

StorageGRID

NetApp
September 04, 2024

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-116/monitor/index.html on September 04, 2024. Always check docs.netapp.com for the latest.

Sommario

Monitorare e risolvere i problemi . . . 1
Monitoraggio e risoluzione dei problemi: Panoramica . . . 1
Visualizza la dashboard . . . 1
Visualizzare la pagina nodi . . . 5
Informazioni da monitorare regolarmente . . . 40
Gestire avvisi e allarmi . . . 75
Configurare i messaggi di audit e le destinazioni dei log . . . 121
Utilizzare un server syslog esterno . . . 126
Utilizzare il monitoraggio SNMP . . . 141
Raccogliere dati StorageGRID aggiuntivi . . . 156
Risolvere i problemi di un sistema StorageGRID . . . 191
Riferimenti agli avvisi . . . 260
Metriche Prometheus comunemente utilizzate . . . 297
Riferimento allarmi (sistema legacy) . . . 302
Riferimenti ai file di log . . . 332

Monitorare e risolvere i problemi

Monitoraggio e risoluzione dei problemi: Panoramica

Utilizzare queste istruzioni per monitorare un sistema StorageGRID e per valutare e risolvere i problemi che potrebbero verificarsi.

A proposito di queste istruzioni

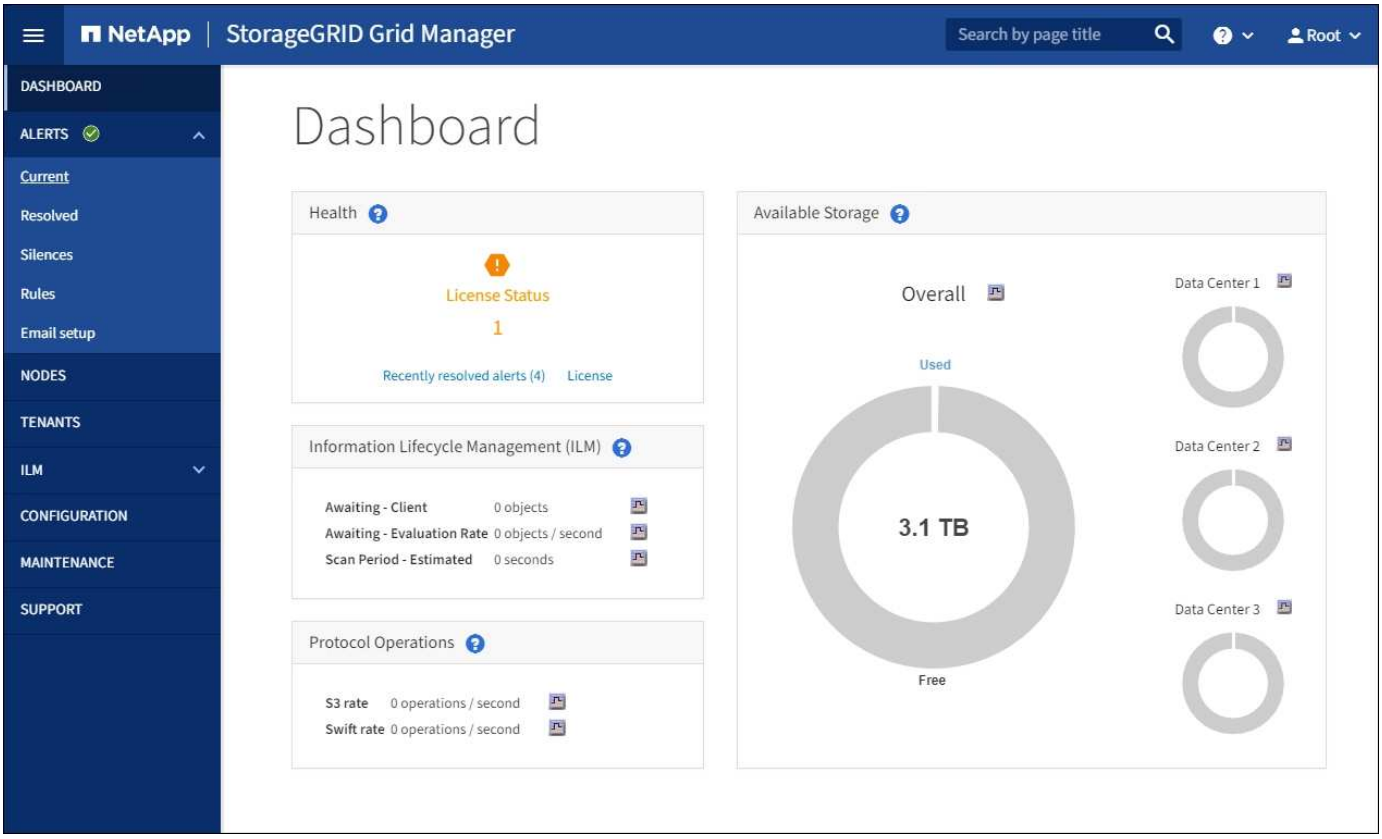
Queste istruzioni descrivono come utilizzare Grid Manager per monitorare un sistema StorageGRID. Verranno fornite informazioni su quali informazioni monitorare regolarmente, su come gestire gli avvisi e gli allarmi legacy, su come utilizzare SNMP per il monitoraggio e su come ottenere dati StorageGRID aggiuntivi, tra cui metriche e diagnostica.

Queste istruzioni descrivono anche come risolvere i problemi di un sistema StorageGRID e descrivere tutti gli avvisi di sistema, gli allarmi legacy e i file di registro.

Seguire queste istruzioni se si intende monitorare e supportare un sistema StorageGRID dopo averlo installato.

Visualizza la dashboard

Quando accedi per la prima volta a Grid Manager, puoi utilizzare la dashboard per monitorare le attività del sistema in un colpo d'occhio. La dashboard include informazioni sullo stato di salute del sistema, sulle metriche di utilizzo, sui trend e sui grafici operativi.



Campo di ricerca

Il campo **Search** nella barra di intestazione consente di accedere rapidamente a una pagina specifica o a una voce della barra laterale all'interno di Grid Manager. Ad esempio, è possibile immettere **key** per accedere alla pagina Key Management Server.

Pannello di salute

Descrizione	Visualizza ulteriori dettagli	Scopri di più
Riepiloga lo stato di salute del sistema. Un segno di spunta verde indica che non sono presenti avvisi correnti e che tutti i nodi della griglia sono connessi. Qualsiasi altra icona indica che è presente almeno un nodo di avviso o di disconnessione corrente.	Potrebbero essere visualizzati uno o più dei seguenti collegamenti: • **Dettagli griglia**: Viene visualizzato se alcuni nodi sono disconnessi (stato connessione sconosciuto o amministrativamente inattivo). Fare clic sul collegamento o sull'icona blu o grigia per determinare quale nodo o nodi sono interessati. • **Current alerts** (Avvisi correnti): Viene visualizzato se sono attivi degli avvisi. Fare clic sul collegamento oppure fare clic su **critico**, **maggiore** o **minore** per visualizzare i dettagli nella pagina **AVVISI corrente**. • **Recently Resolved alerts** (Avvisi risolti di recente): Viene visualizzato se gli avvisi attivati nell'ultima settimana sono stati risolti. Fare clic sul collegamento per visualizzare i dettagli nella pagina **ALERTS resolved**. • **Legacy alarms** (Allarmi legacy): Viene visualizzato se sono attivi allarmi (sistema legacy). Fare clic sul collegamento per visualizzare i dettagli nella pagina **SUPPORTO Allarmi (legacy) Allarmi correnti**. • **Licenza**: Viene visualizzato se si verifica un problema con la licenza software per questo sistema StorageGRID. Fare clic sul collegamento per visualizzare i dettagli nella pagina **MANUTENZIONE sistema licenza**.	• Monitorare gli stati di connessione del nodo • Visualizzare gli avvisi correnti • Visualizzare gli avvisi risolti • Visualizzare gli allarmi legacy • Amministrare StorageGRID

Pannello Available Storage (archiviazione disponibile)

Descrizione	Visualizza ulteriori dettagli	Scopri di più
Visualizza la capacità di storage disponibile e utilizzata nell'intera griglia, senza i supporti di archiviazione. Il grafico generale presenta i totali a livello di griglia. Se si tratta di una griglia multi-sito, vengono visualizzati grafici aggiuntivi per ciascun sito del data center. È possibile utilizzare queste informazioni per confrontare lo storage utilizzato con lo storage disponibile. Se si dispone di un grid multi-sito, è possibile determinare quale sito consuma più storage.	• Per visualizzare la capacità, posizionare il cursore sulle sezioni della capacità disponibile e utilizzata del grafico. • Per visualizzare le tendenze della capacità in un intervallo di date, fare clic sull'icona del grafico per il grid complessivo o per un sito del data center. • Per visualizzare i dettagli, selezionare **NODI**. Quindi, visualizzare la scheda Storage per l'intera griglia, un intero sito o un singolo nodo di storage.	• Visualizzare la scheda Storage (archiviazione) • Monitorare la capacità dello storage

Pannello ILM (Information Lifecycle Management)

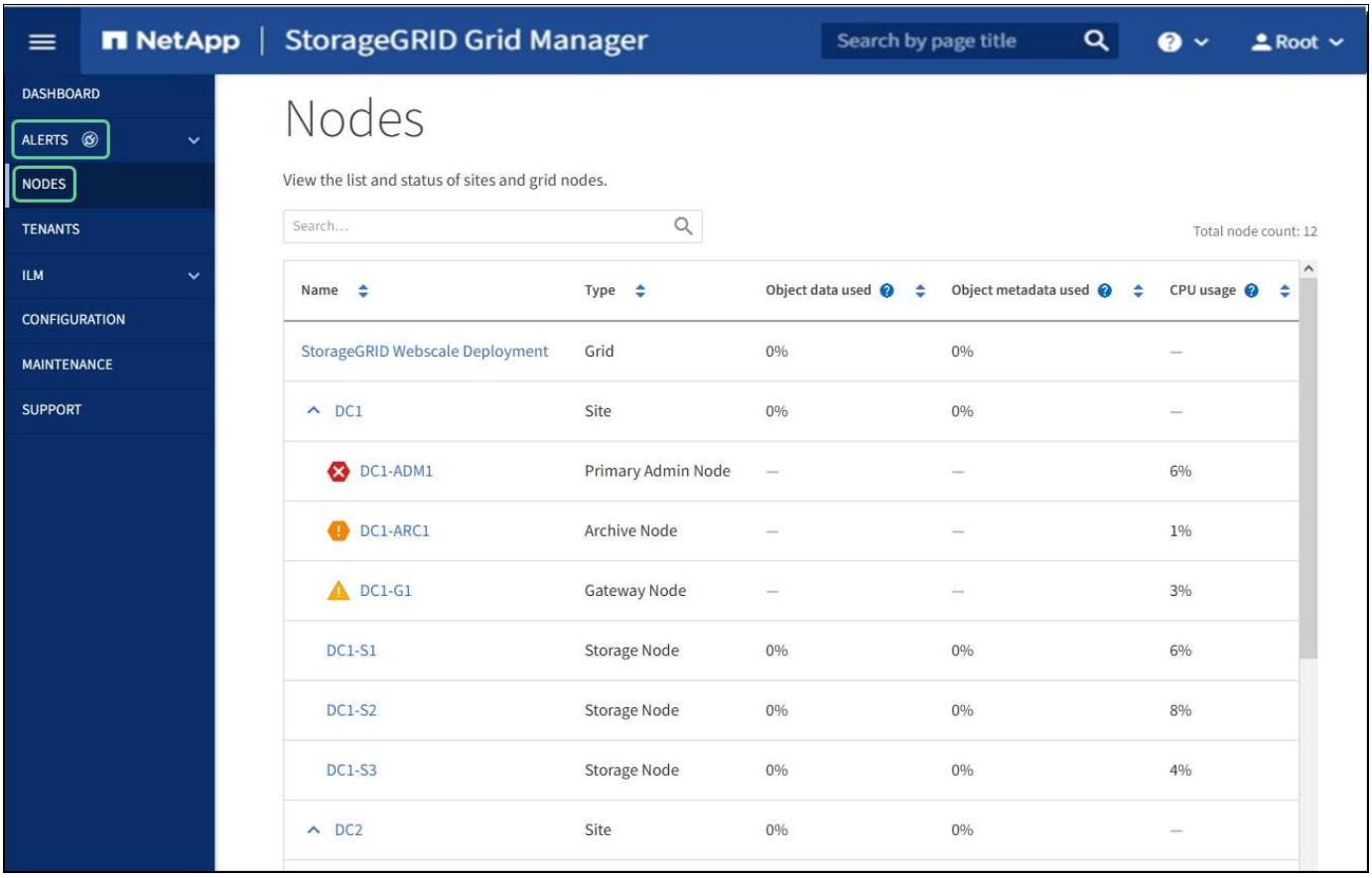
Descrizione	Visualizza ulteriori dettagli	Scopri di più
Visualizza le operazioni ILM correnti e le code ILM per il sistema. È possibile utilizzare queste informazioni per monitorare il carico di lavoro del sistema. • **In attesa - Client**: Il numero totale di oggetti in attesa di valutazione ILM dalle operazioni del client (ad esempio, acquisizione). • **In attesa - tasso di valutazione**: La velocità corrente alla quale gli oggetti vengono valutati in base alla policy ILM nella griglia. • **Scan Period (periodo di scansione) - Estimated (stimato)**: Tempo stimato per completare una scansione ILM completa di tutti gli oggetti. **Nota:** Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti.	• Per visualizzare i dettagli, selezionare **NODI**. Quindi, visualizzare la scheda ILM per l'intera griglia, un intero sito o un singolo nodo di storage. • Per visualizzare le regole ILM esistenti, selezionare **ILM Rules**. • Per visualizzare i criteri ILM esistenti, selezionare **ILM Policy**.	• Visualizzare la scheda ILM • Amministrare StorageGRID.

Pannello Protocol Operations (operazioni protocollo)

Descrizione	Visualizza ulteriori dettagli	Scopri di più
Visualizza il numero di operazioni specifiche del protocollo (S3 e Swift) eseguite dal sistema. Puoi utilizzare queste informazioni per monitorare i carichi di lavoro e le efficienze del tuo sistema. Le velocità dei protocolli vengono calcolate in media negli ultimi due minuti.	• Per visualizzare i dettagli, selezionare **NODI**. Quindi, visualizzare la scheda oggetti per l'intera griglia, un intero sito o un singolo nodo di storage. • Per visualizzare i trend in un intervallo di date, fare clic sull'icona del grafico A destra della velocità del protocollo S3 o Swift.	• Visualizzare la scheda oggetti • Utilizzare S3 • USA Swift

Visualizzare la pagina nodi

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



La tabella Nodes (nodi) elenca tutti i siti e i nodi nel sistema StorageGRID. Vengono visualizzate informazioni di riepilogo per ciascun nodo. Se un nodo ha 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.

Icone di stato della connessione

- **Non connesso - Sconosciuto** : Il nodo non è connesso alla rete per un motivo sconosciuto. Ad esempio, la connessione di rete tra i nodi è stata persa o l'alimentazione è inattiva. 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).

- **Non connesso - amministrazione non attiva** : 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.

Se un nodo viene disconnesso dalla griglia, potrebbe essere visualizzato 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

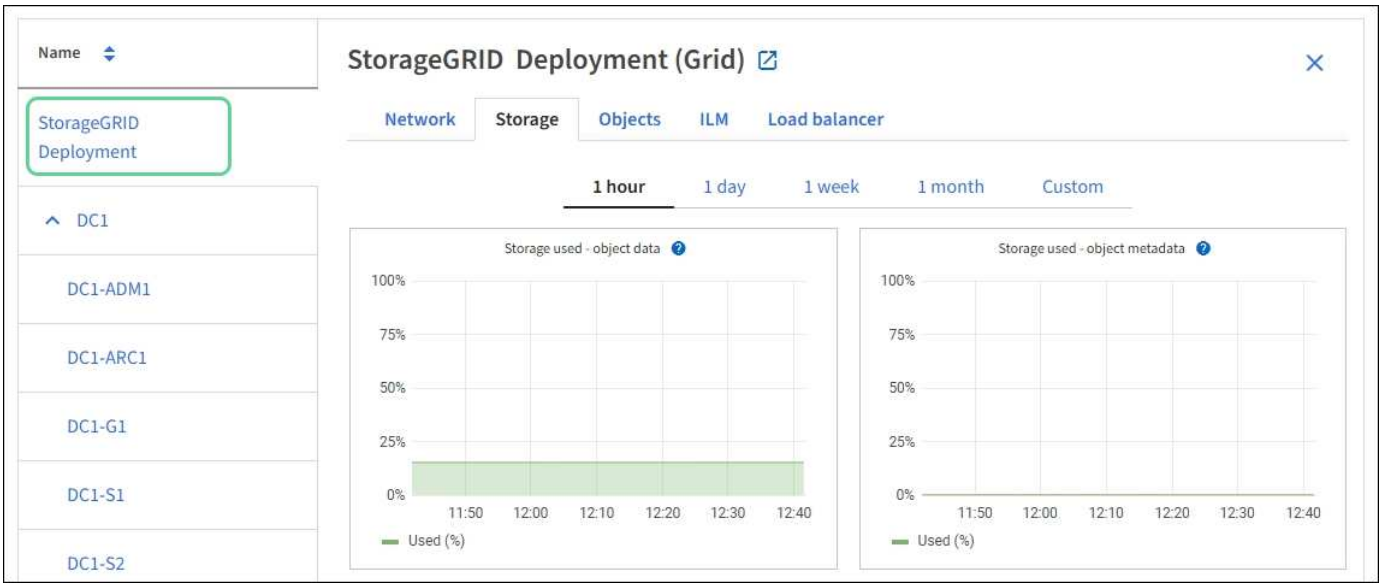
Se è presente un avviso attivo per un nodo, accanto al nome del nodo viene visualizzata una delle seguenti icone:

- **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.
- **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 assicurarsi che non causino problemi più gravi.

Visualizzazione dei dettagli di un sistema, sito o nodo

Per visualizzare le informazioni disponibili, selezionare il nome della griglia, del sito o del nodo nel modo seguente:

- 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.



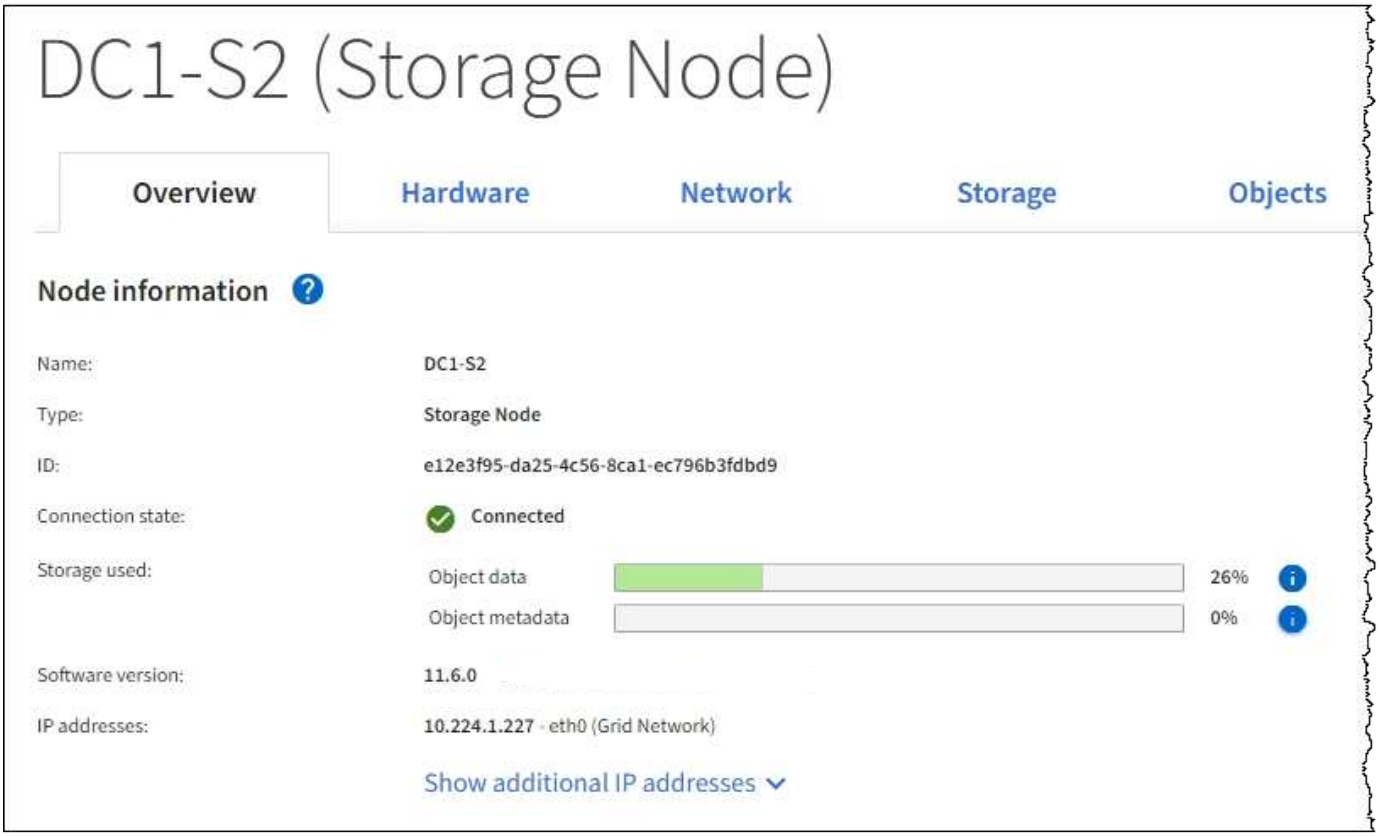
Visualizzare la scheda Panoramica

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 Grid (griglia).



Le informazioni generali per un nodo includono quanto segue:

- **Name**: Nome host assegnato al nodo e visualizzato in Grid Manager.
- **Type**: Il tipo di nodo — Admin Node, Primary Admin Node, Storage Node, Gateway Node o Archive Node.
- **ID**: Identificatore univoco del nodo, chiamato anche UUID.
- **Stato connessione**: Uno dei tre stati. Viene visualizzata l'icona dello stato più grave.
  - **Sconosciuto** : Il nodo non è connesso alla rete per un motivo sconosciuto. Ad esempio, la connessione di rete tra i nodi è stata persa o l'alimentazione è inattiva. 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 gli avvisi che attualmente interessano questo nodo e che non sono stati tacitati. Fare clic sul nome dell'avviso per visualizzare ulteriori dettagli e azioni consigliate.

Informazioni correlate

Monitorare gli stati di connessione del nodo

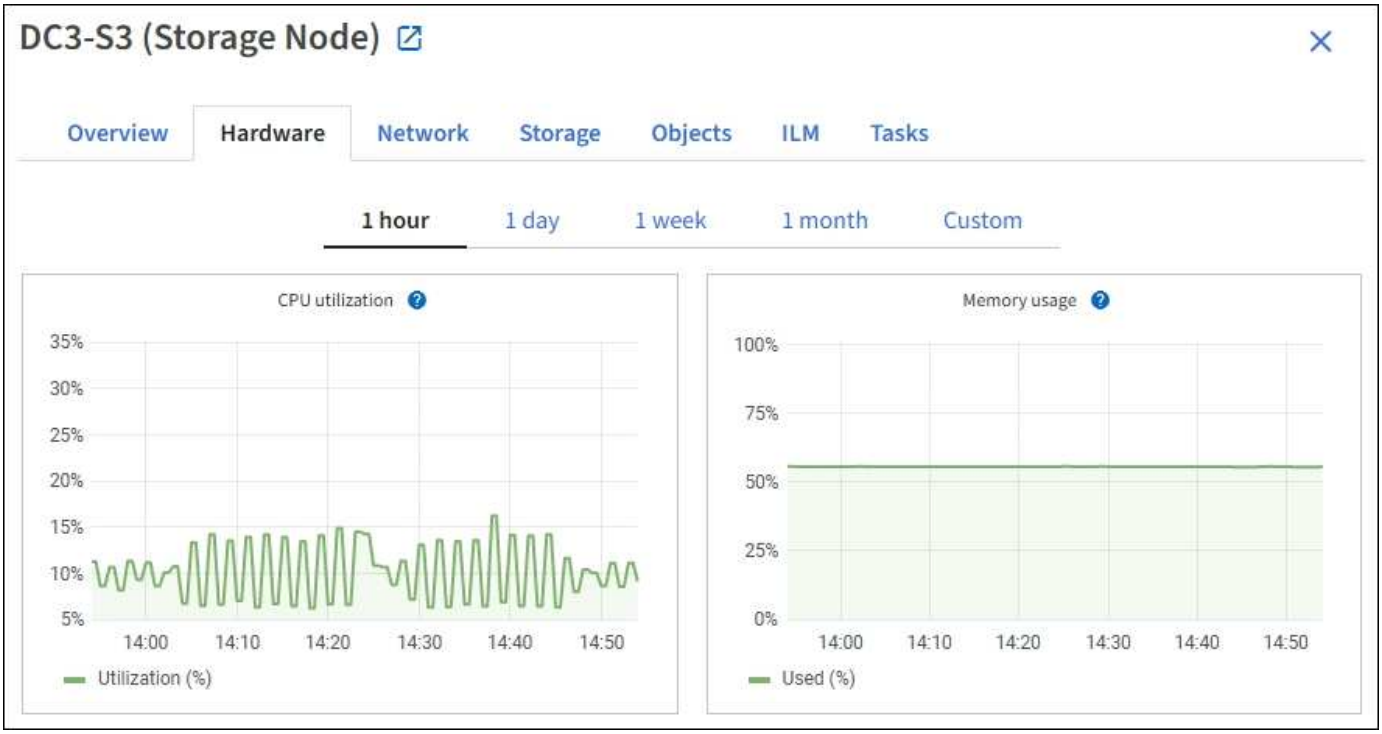
Visualizzare gli avvisi correnti

Visualizzare un avviso specifico

Visualizzare la scheda hardware

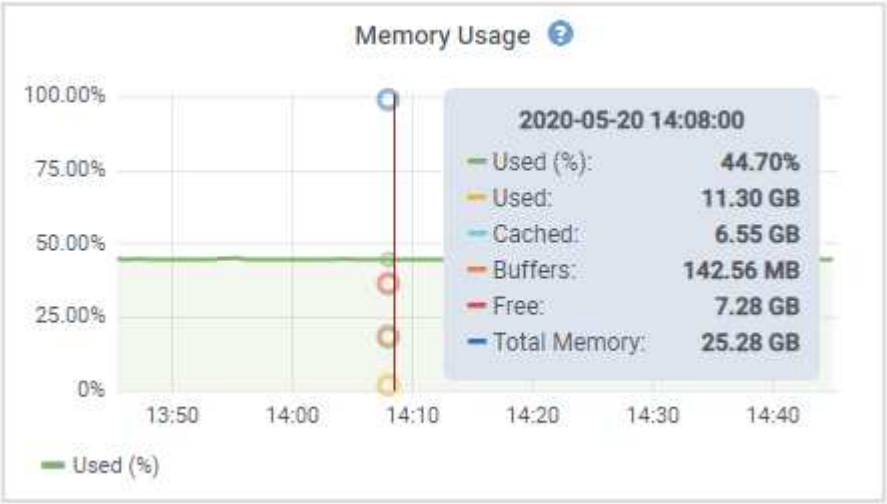
La scheda hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo, oltre a informazioni aggiuntive sull'hardware delle appliance.

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, spostare 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

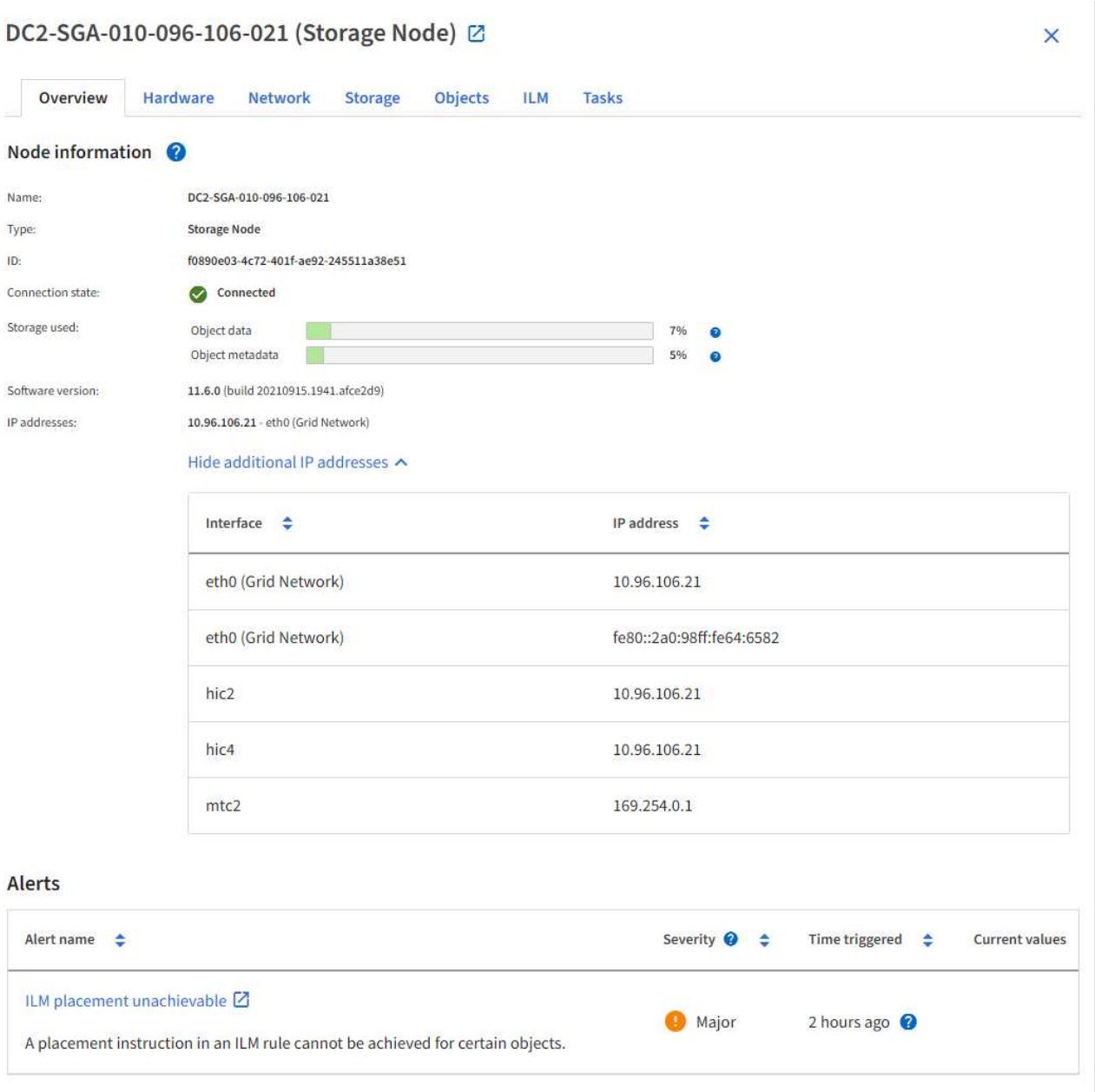
La pagina Nodes (nodi) elenca le informazioni sullo stato di salute del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ciascun nodo di storage dell'appliance. È inoltre possibile visualizzare memoria, hardware di storage, versione del firmware del controller, risorse di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

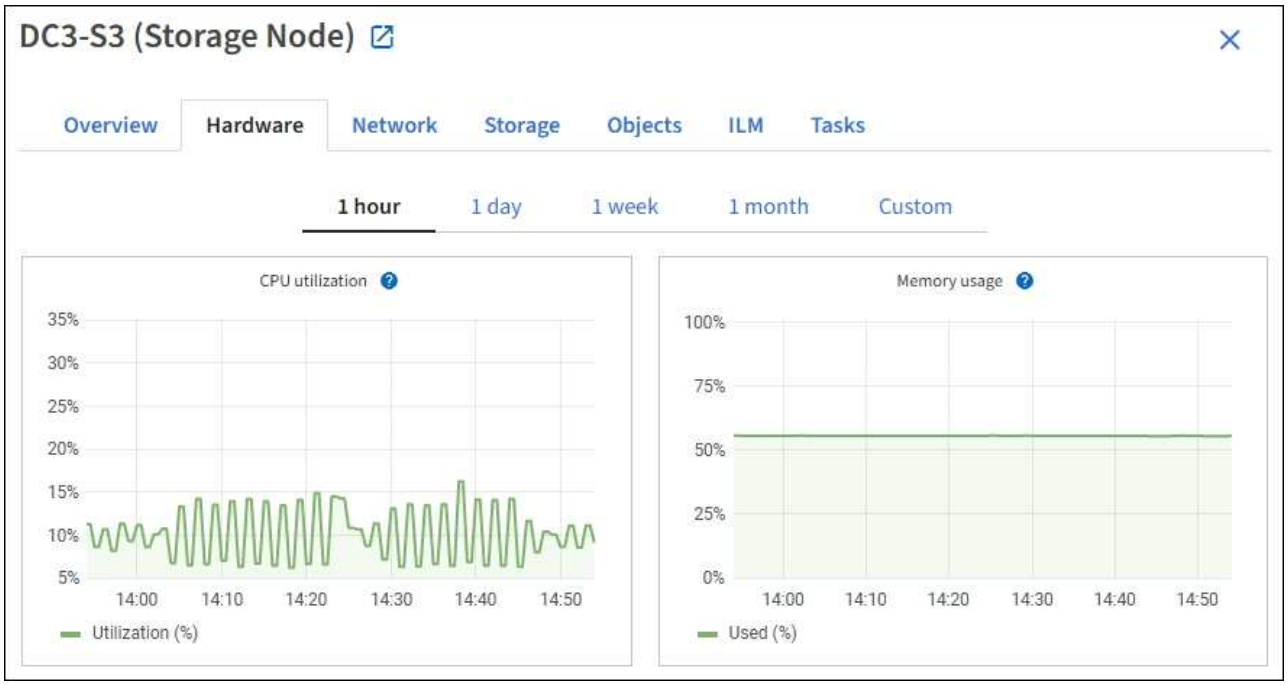
   - **eth**: Rete griglia, rete amministrativa o rete client.
   - **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
   - **mtc**: Una delle porte 1 GbE fisiche dell'appliance. 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.

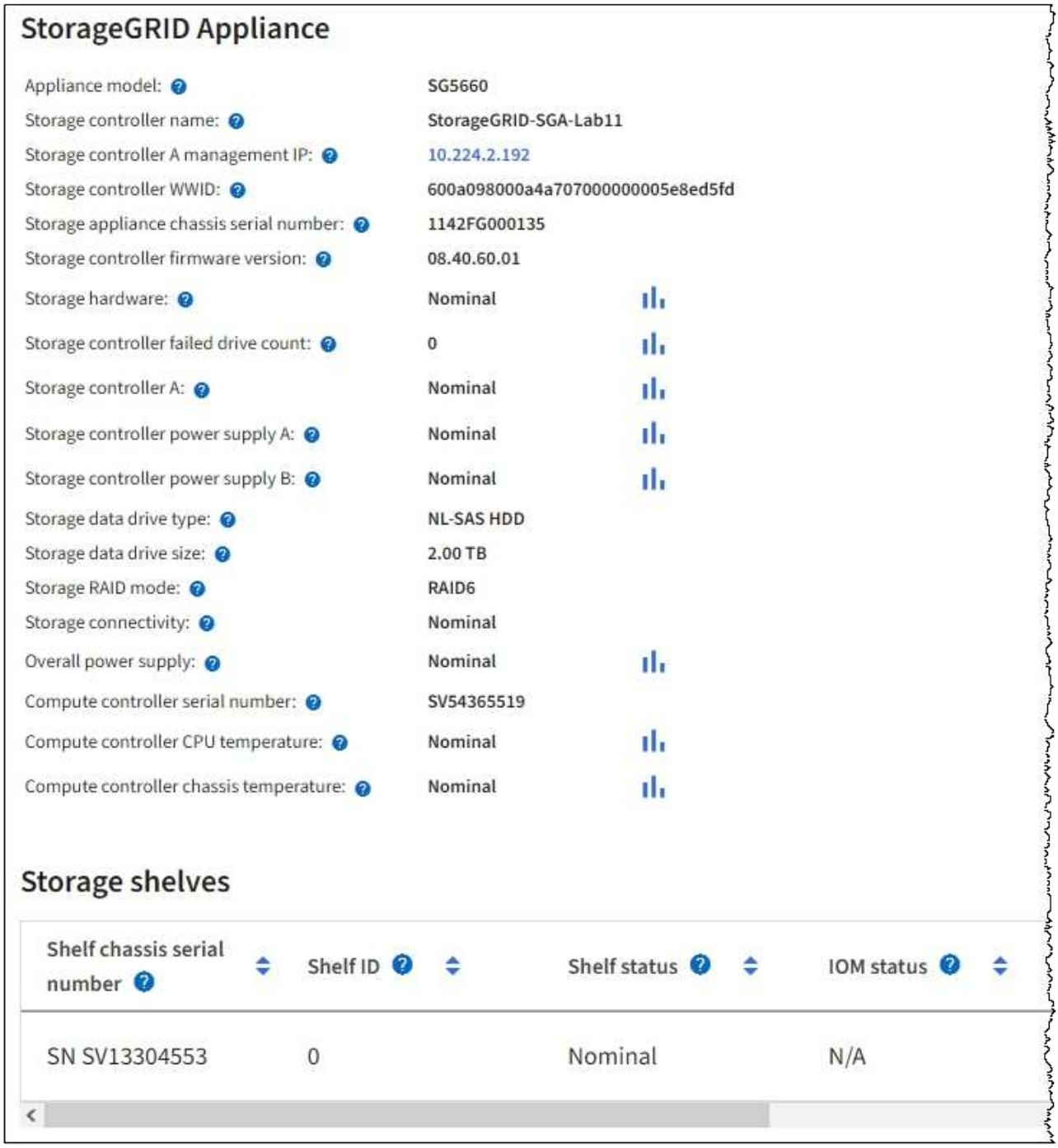
   a. Visualizzare i grafici relativi all'utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni 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 nel software SANtricity.
Nome dello storage controller	Il nome dell'appliance StorageGRID indicato nel software SANtricity.
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 software 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 software 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 del controller di storage mostrato nel software SANtricity.
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 "needs Attention" (richiede attenzione), controllare innanzitutto il controller dello storage utilizzando il software 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 shelf di espansione sono validi solo per SG6060 e SG6060X.
Stato dello shelf	Lo stato generale dello shelf di storage.

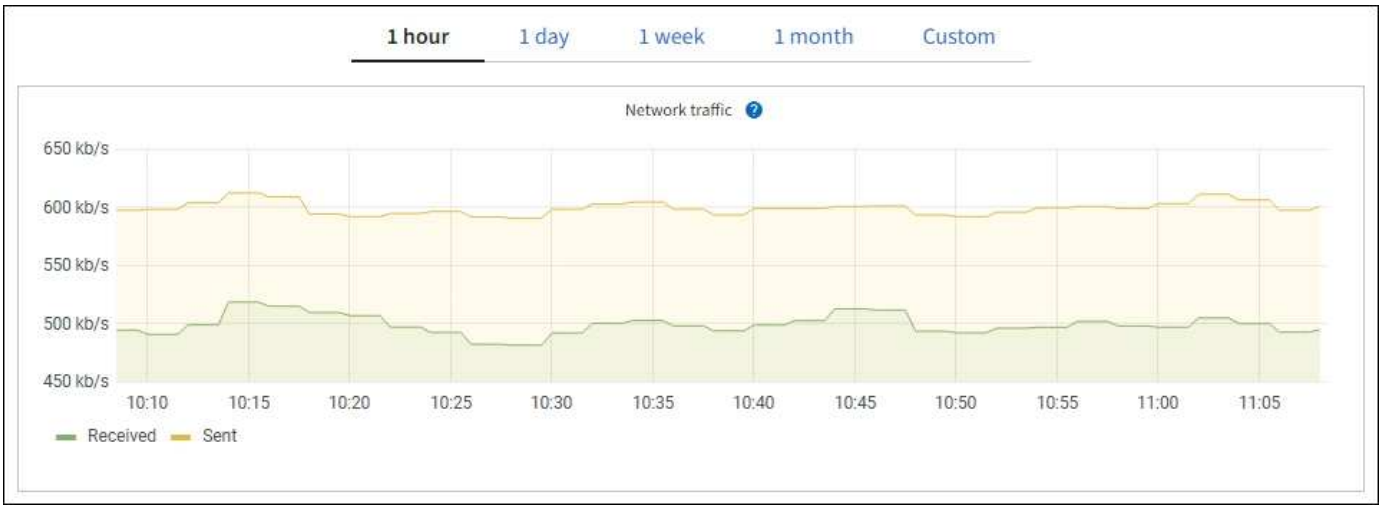
Nella tabella Storage shelf	Descrizione
Stato IOM	Lo stato dei moduli di input/output (IOM) in qualsiasi shelf di espansione. N/D se non si tratta di uno shelf di espansione.
Stato dell'alimentatore	Lo stato generale degli alimentatori per lo shelf di storage.
Stato del cassetto	Lo stato dei cassetti 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.

4. Verificare che tutti gli stati siano "nominali".

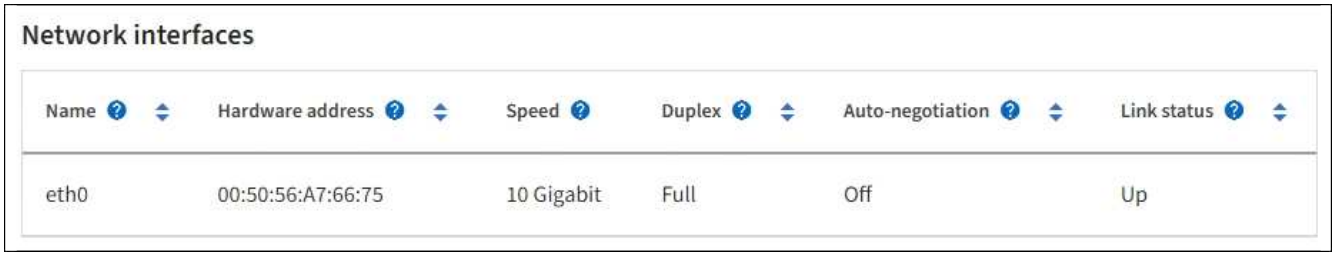
   Se uno stato non è "nominale", rivedere gli avvisi correnti. Puoi anche utilizzare Gestione di sistema di SANtricity per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

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

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



1. 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

Per ulteriori informazioni sulla configurazione delle porte 10/25-GbE, consultare le istruzioni di installazione e manutenzione dell'appliance.

2. 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

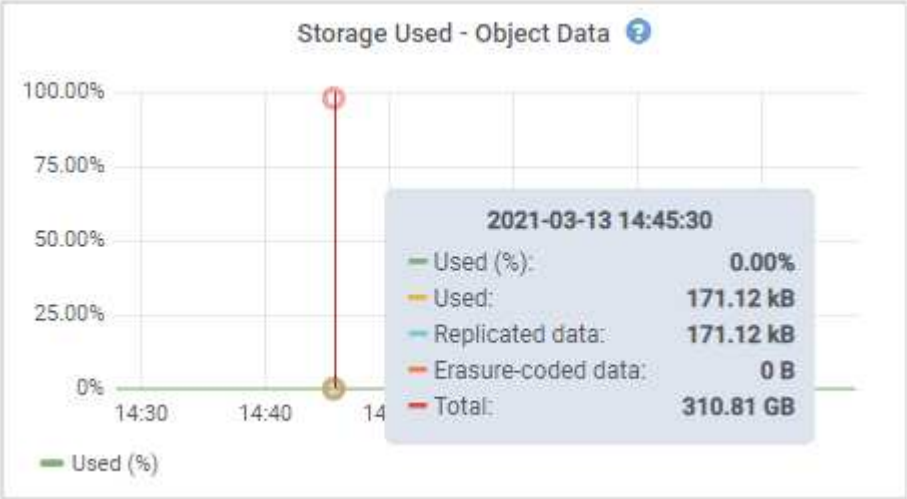
Receive

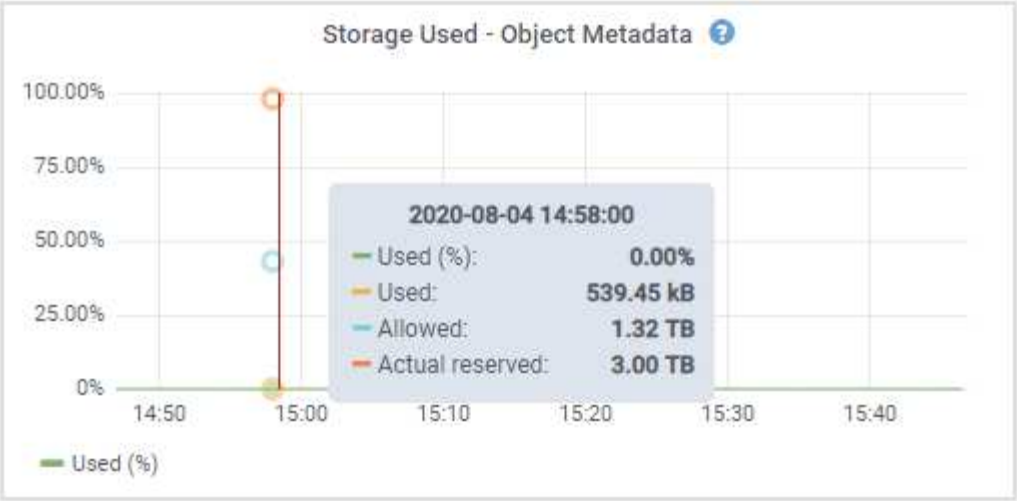
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

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

3. 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 nel software SANtricity (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

Informazioni correlate

Appliance di storage SG6000

Appliance di storage SG5700

Appliance di storage SG5600

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

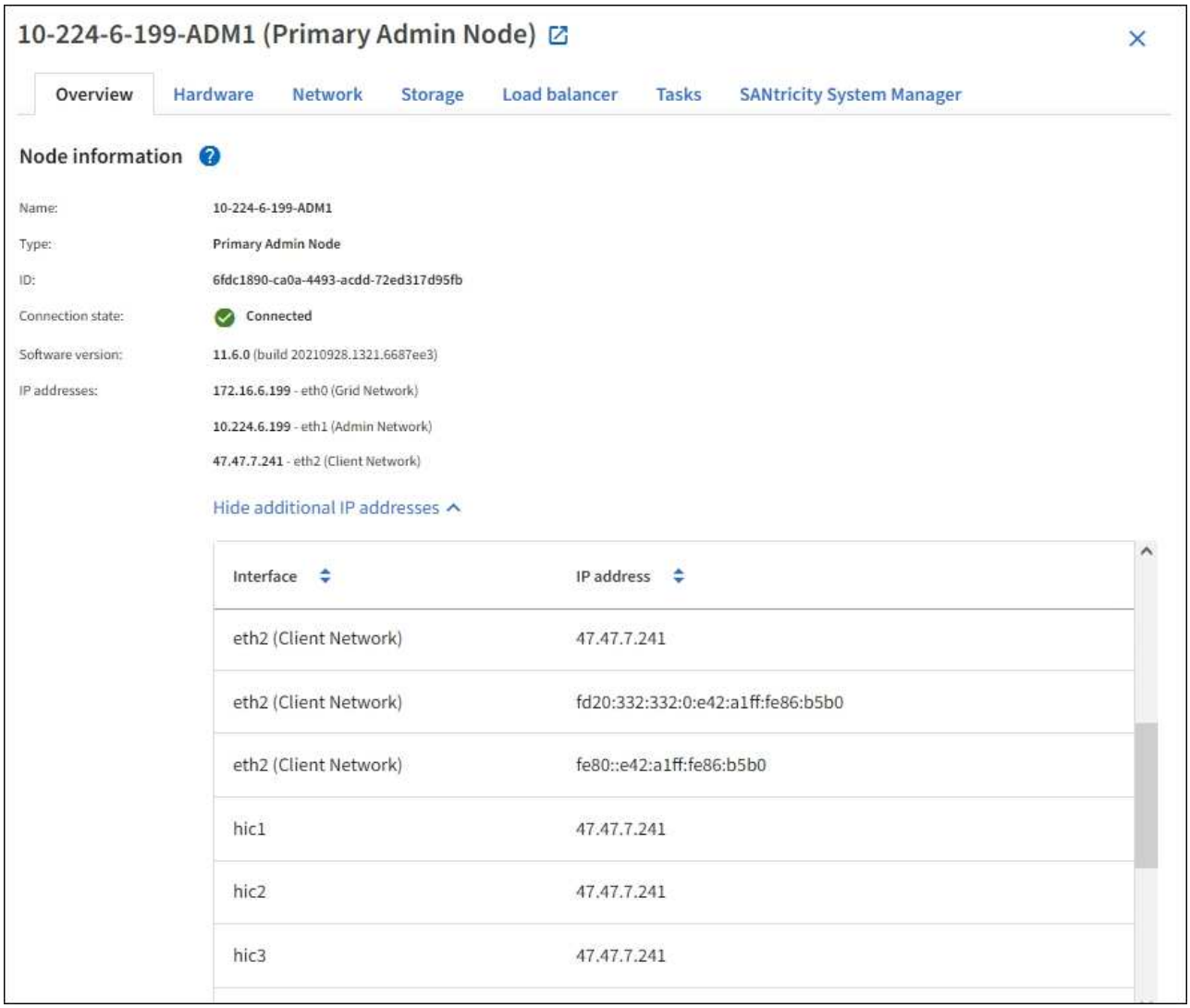
La pagina Nodes (nodi) elenca le informazioni sullo stato del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ogni appliance di servizi utilizzata come nodo di amministrazione o nodo gateway. È inoltre possibile visualizzare memoria, hardware di storage, risorse di rete,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

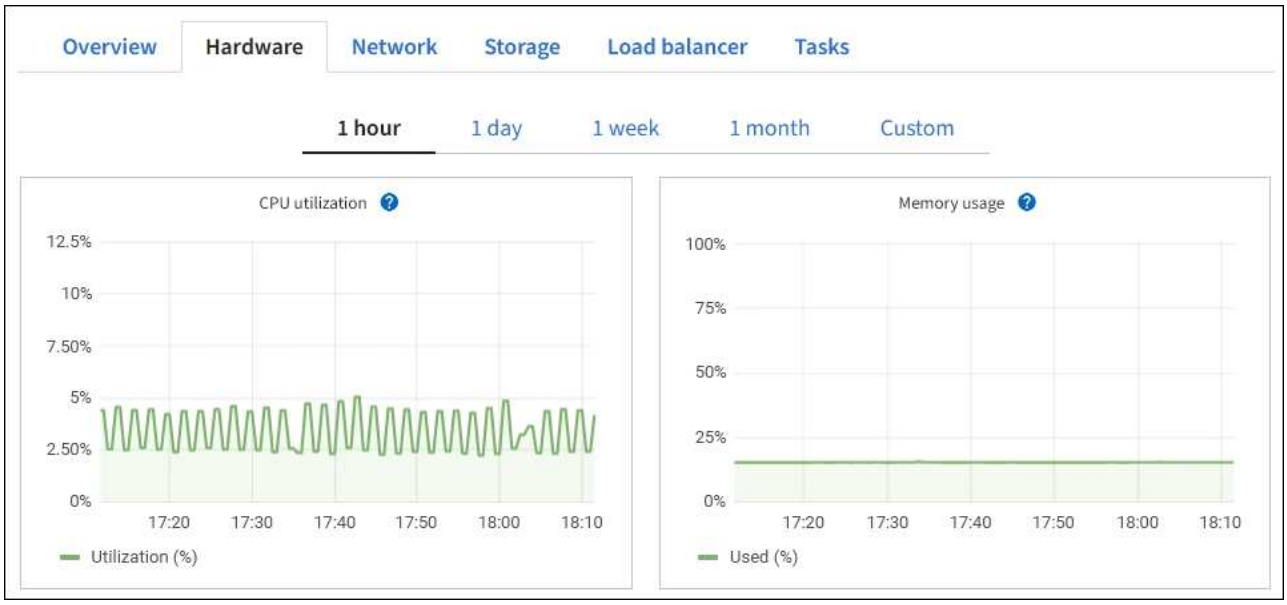
   - **Adllb** e **adlli**: Visualizzato se si utilizza il bonding Active/backup per l'interfaccia di Admin Network
   - **eth**: Rete griglia, rete amministrativa o rete client.
   - **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate 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.



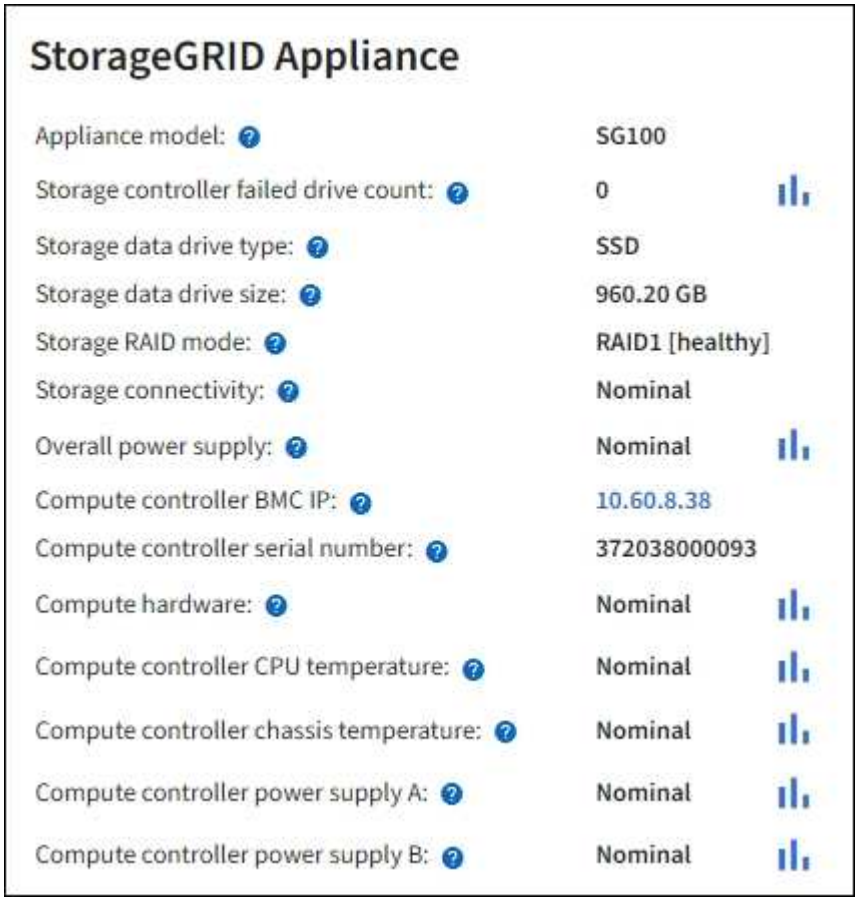
   La sezione Avvisi della scheda Panoramica visualizza gli avvisi attivi per il nodo.

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.



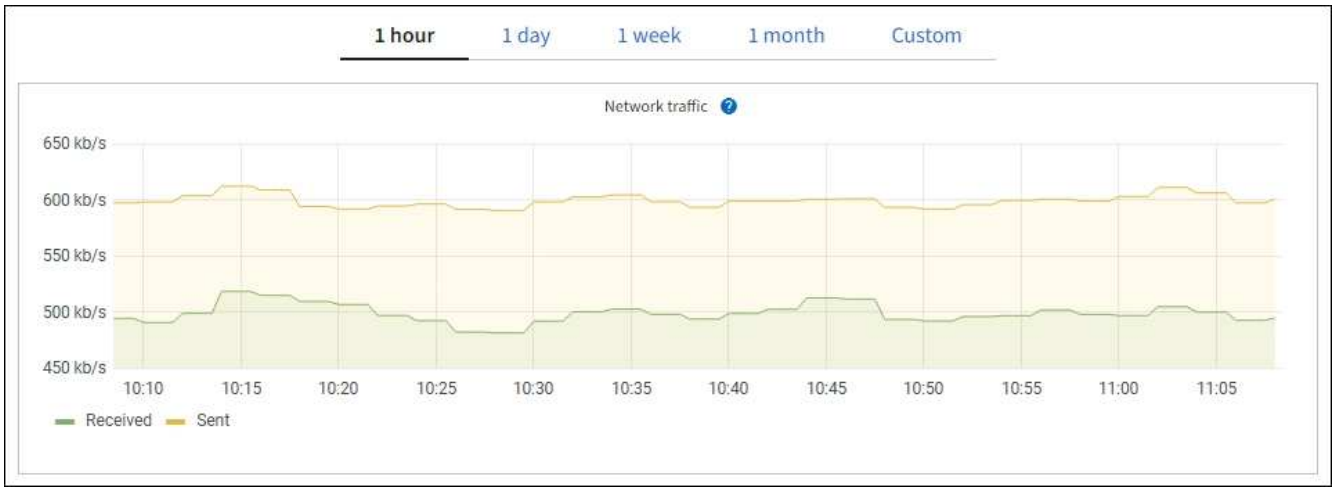
Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello dell'appliance StorageGRID.
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato 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 "nominali".

   Se uno stato non è "nominale", rivedere gli 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

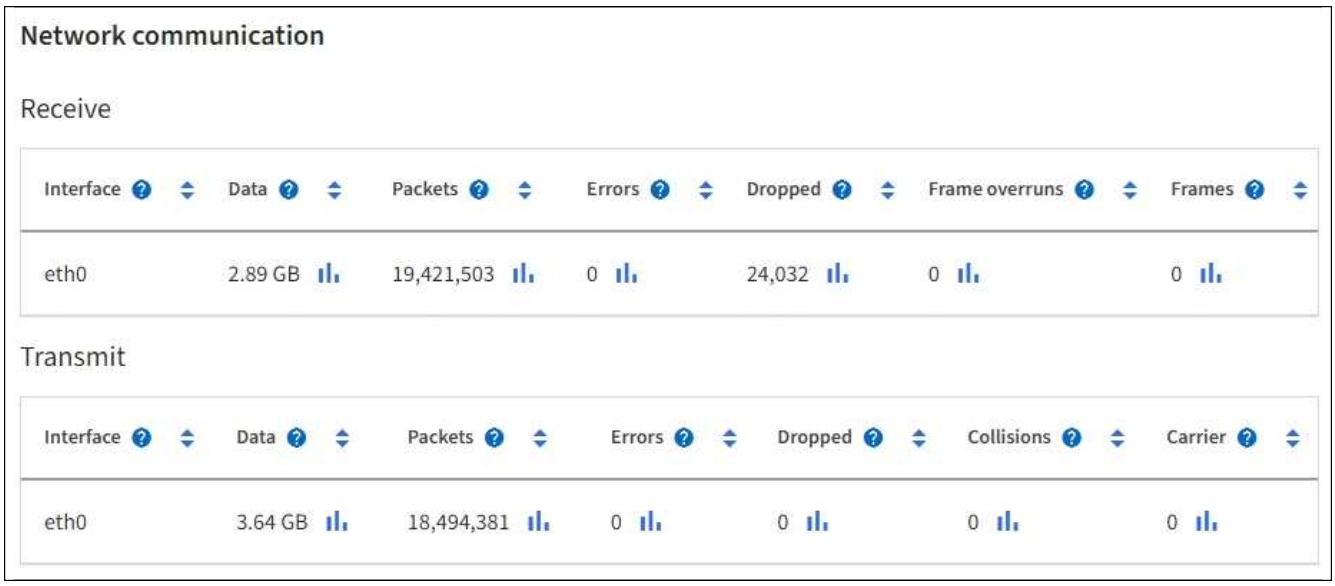
Utilizzare la seguente tabella con i valori nella colonna **Speed** della tabella Network Interfaces (interfacce di rete) per determinare se le quattro porte di rete 40/100-GbE dell'appliance sono state configurate per l'utilizzo della modalità Active/backup o LACP.

> 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

Informazioni correlate

Appliance di servizi SG100 e SG1000

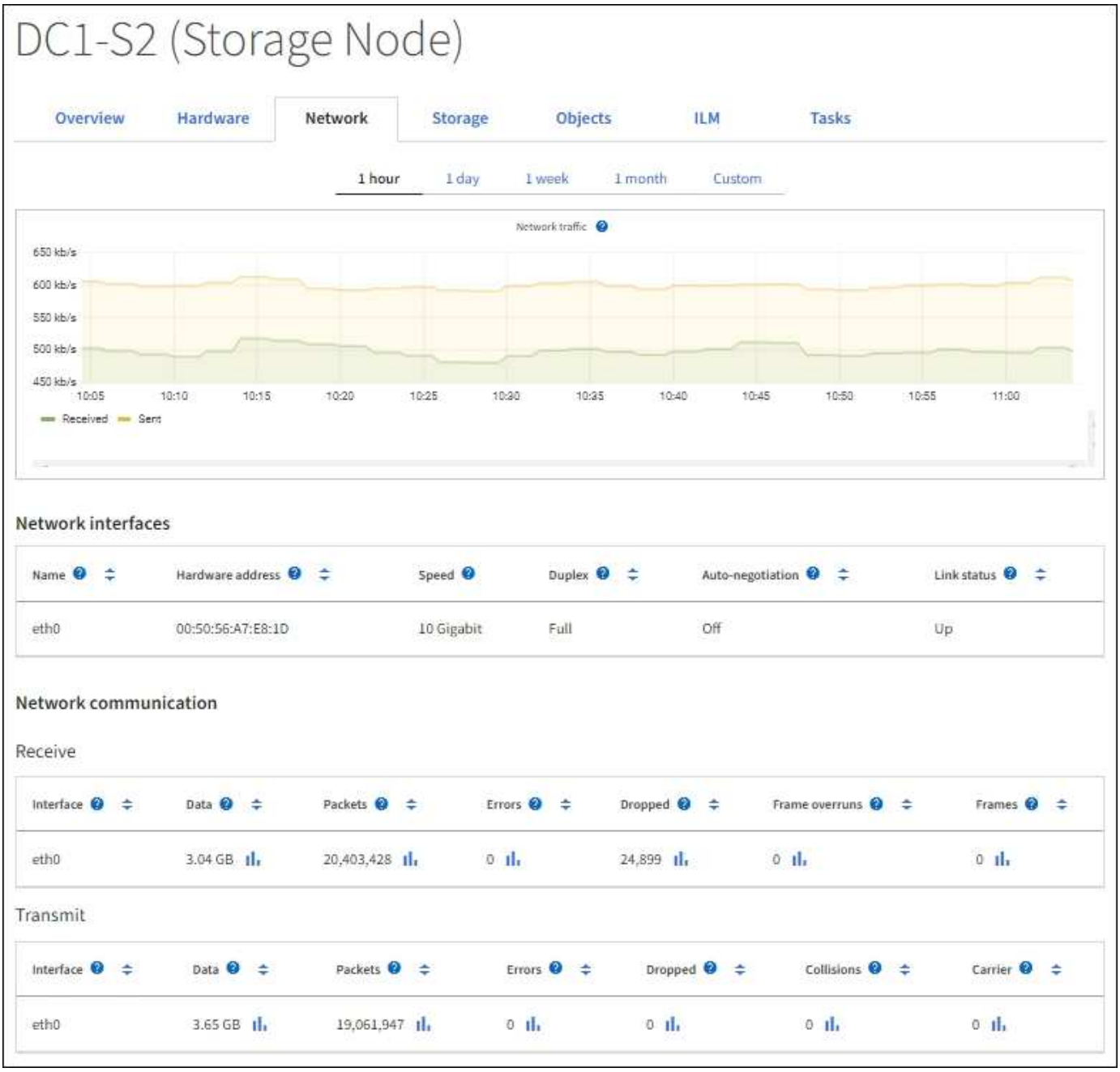
Visualizzare la scheda rete

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)

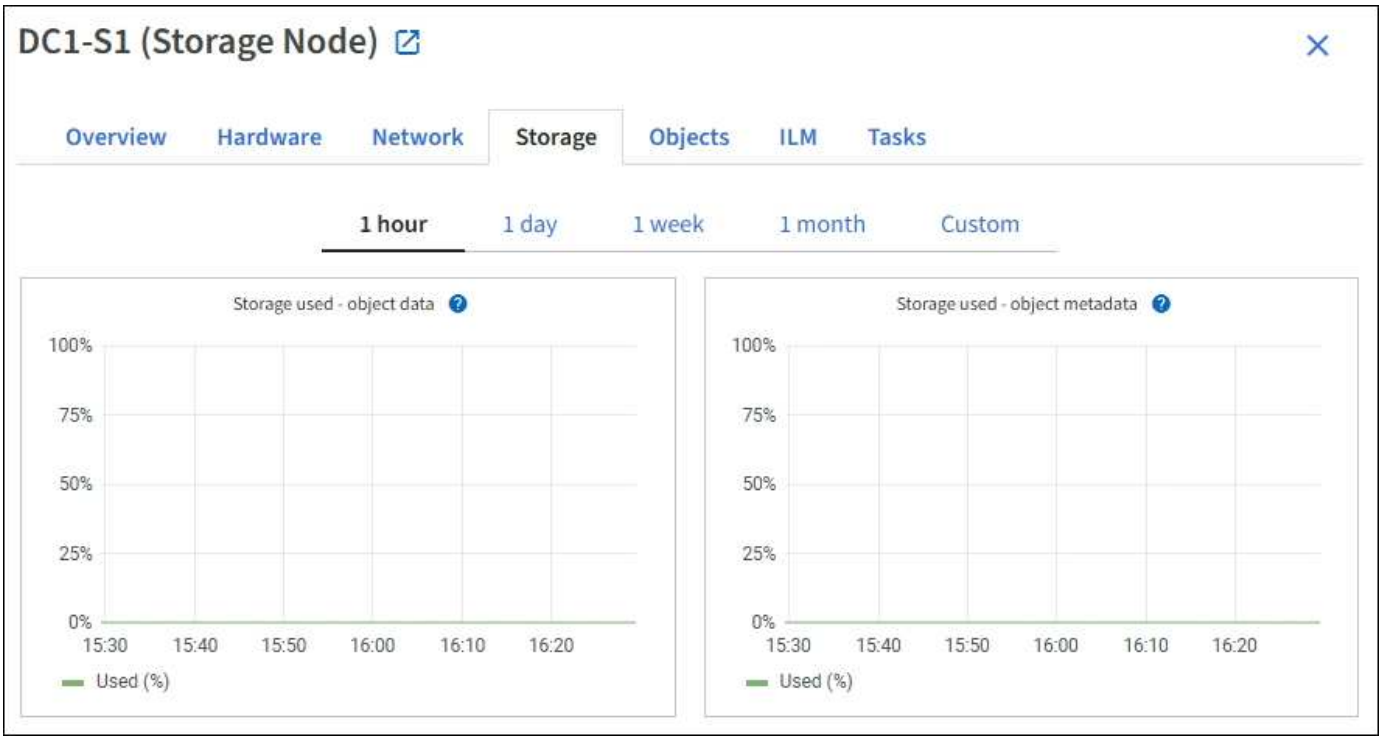
La scheda Storage riepiloga la disponibilità dello storage e altre metriche di storage.

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.

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



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

Utilizzare la scheda Task (attività) per riavviare un nodo Grid

La scheda Task (attività) consente di riavviare il nodo selezionato. Viene visualizzata la scheda Task (attività) per tutti i nodi.

Di cosa hai bisogno

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

- Si dispone dell'autorizzazione di accesso Maintenance o Root.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

È possibile utilizzare la scheda Task (attività) per riavviare un nodo. Per i nodi appliance, è possibile utilizzare la scheda Task (attività) per impostare la modalità di manutenzione dell'appliance.

- Il riavvio di un nodo Grid dalla scheda Task (attività) genera il comando reboot sul nodo di destinazione. Quando si riavvia un nodo, questo si spegne e si riavvia. Tutti i servizi vengono riavviati automaticamente.

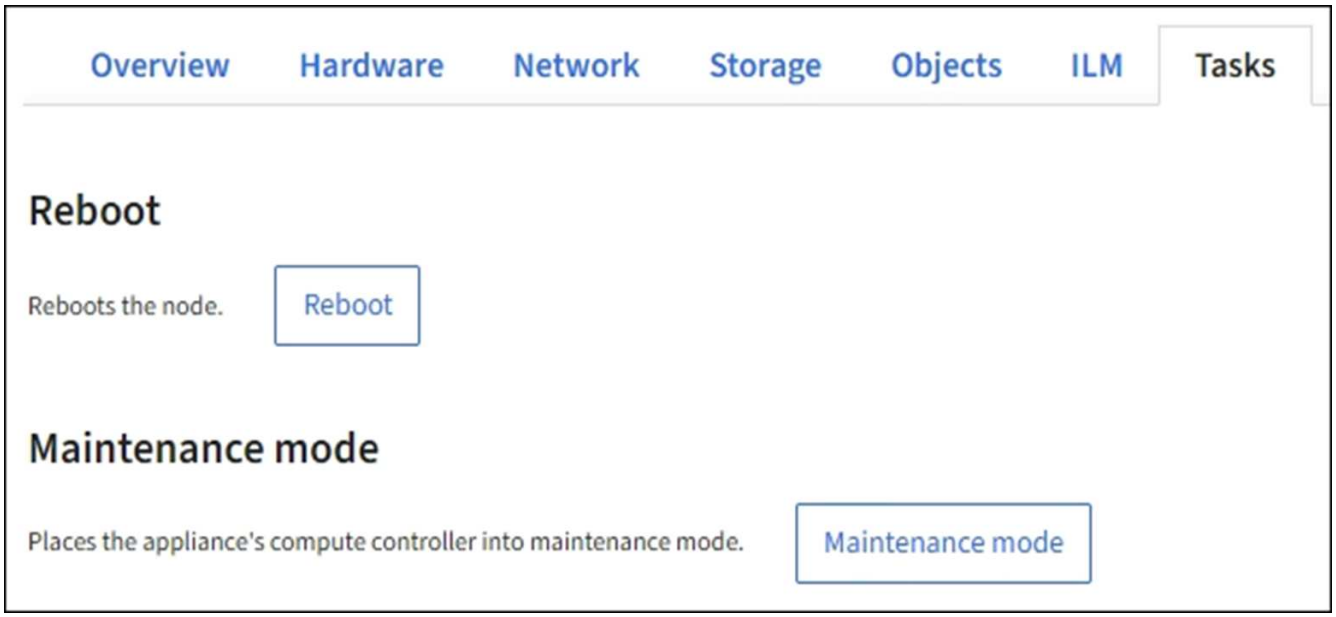
  Se si intende riavviare un nodo di storage, tenere presente quanto segue:

  - Se una regola ILM specifica un comportamento di acquisizione di doppio commit o la regola specifica Balanced (bilanciato) e non è possibile creare immediatamente tutte le copie richieste, StorageGRID commuta immediatamente tutti gli oggetti acquisiti di recente su due nodi di storage sullo stesso sito e valuta ILM in un secondo momento. Se si desidera riavviare due o più nodi di storage su un determinato sito, potrebbe non essere possibile accedere a questi oggetti per la durata del riavvio.
  - Per garantire l'accesso a tutti gli oggetti durante il riavvio di un nodo di storage, interrompere l'acquisizione di oggetti in un sito per circa un'ora prima di riavviare il nodo.
- Potrebbe essere necessario attivare la modalità di manutenzione di un'appliance StorageGRID per eseguire determinate procedure, ad esempio la modifica della configurazione del collegamento o la sostituzione di un controller di storage. Per istruzioni, consultare le istruzioni di installazione e manutenzione dell'hardware dell'apparecchio.

  In rari casi, l'attivazione della modalità di manutenzione di un'appliance StorageGRID potrebbe rendere l'appliance non disponibile per l'accesso remoto.

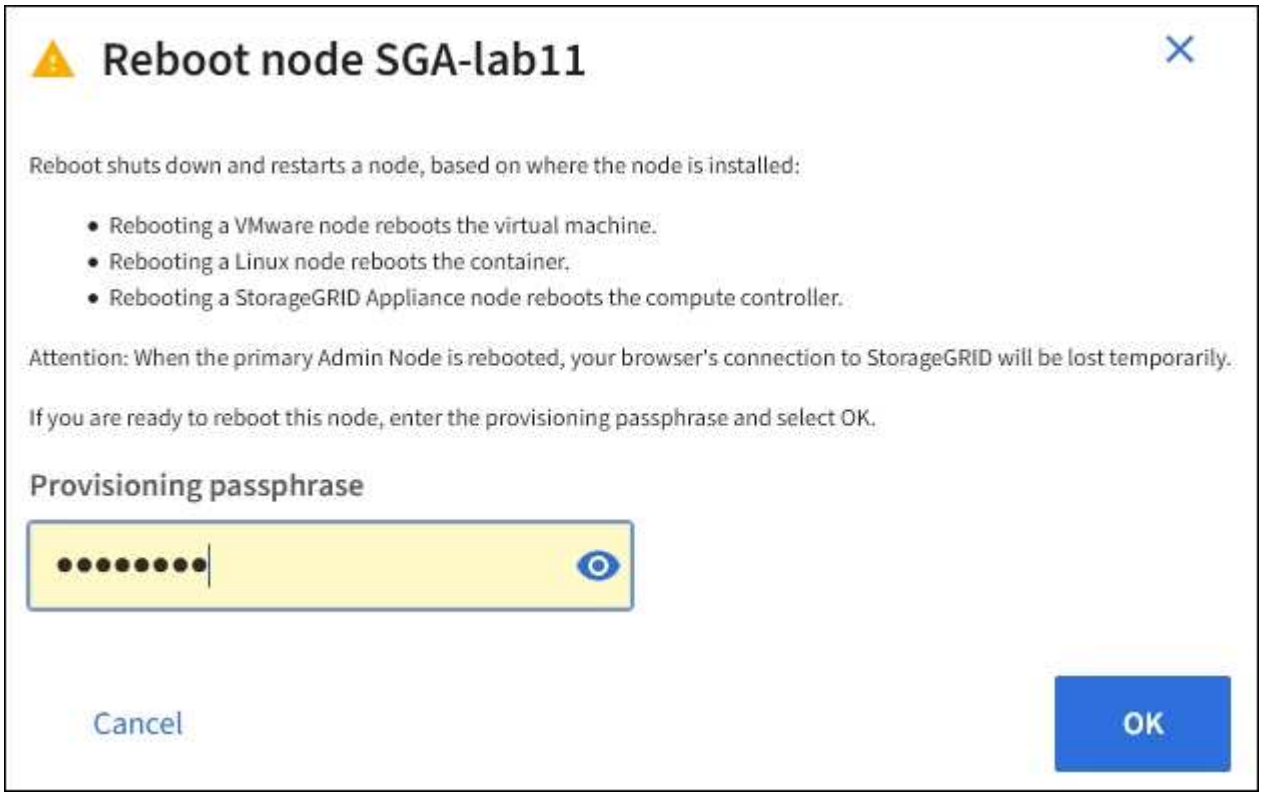
Fasi

1. Selezionare **NODI**.
2. Selezionare il nodo della griglia che si desidera riavviare.
3. Selezionare la scheda **Tasks**.



4. Selezionare **Reboot** (Riavvia).

   Viene visualizzata una finestra di dialogo di conferma.



> Se si sta riavviando il nodo di amministrazione primario, la finestra di dialogo di conferma ricorda che la connessione del browser a Grid Manager viene temporaneamente persa quando i servizi vengono arrestati.

5. Inserire la passphrase di provisioning e fare clic su **OK**.
6. Attendere il riavvio del nodo.

   L'arresto dei servizi potrebbe richiedere del tempo.

   Quando il nodo viene riavviato, l'icona grigia (amministrativamente in basso) viene visualizzata sul lato sinistro della pagina **Nodes**. Quando tutti i servizi sono stati riavviati e il nodo è connesso correttamente alla griglia, la pagina **Nodes** dovrebbe visualizzare uno stato normale (nessuna icona a sinistra del nome del nodo), a indicare che nessun avviso è attivo e che il nodo è connesso alla griglia.

Informazioni correlate

Appliance di storage SG6000

Appliance di storage SG5700

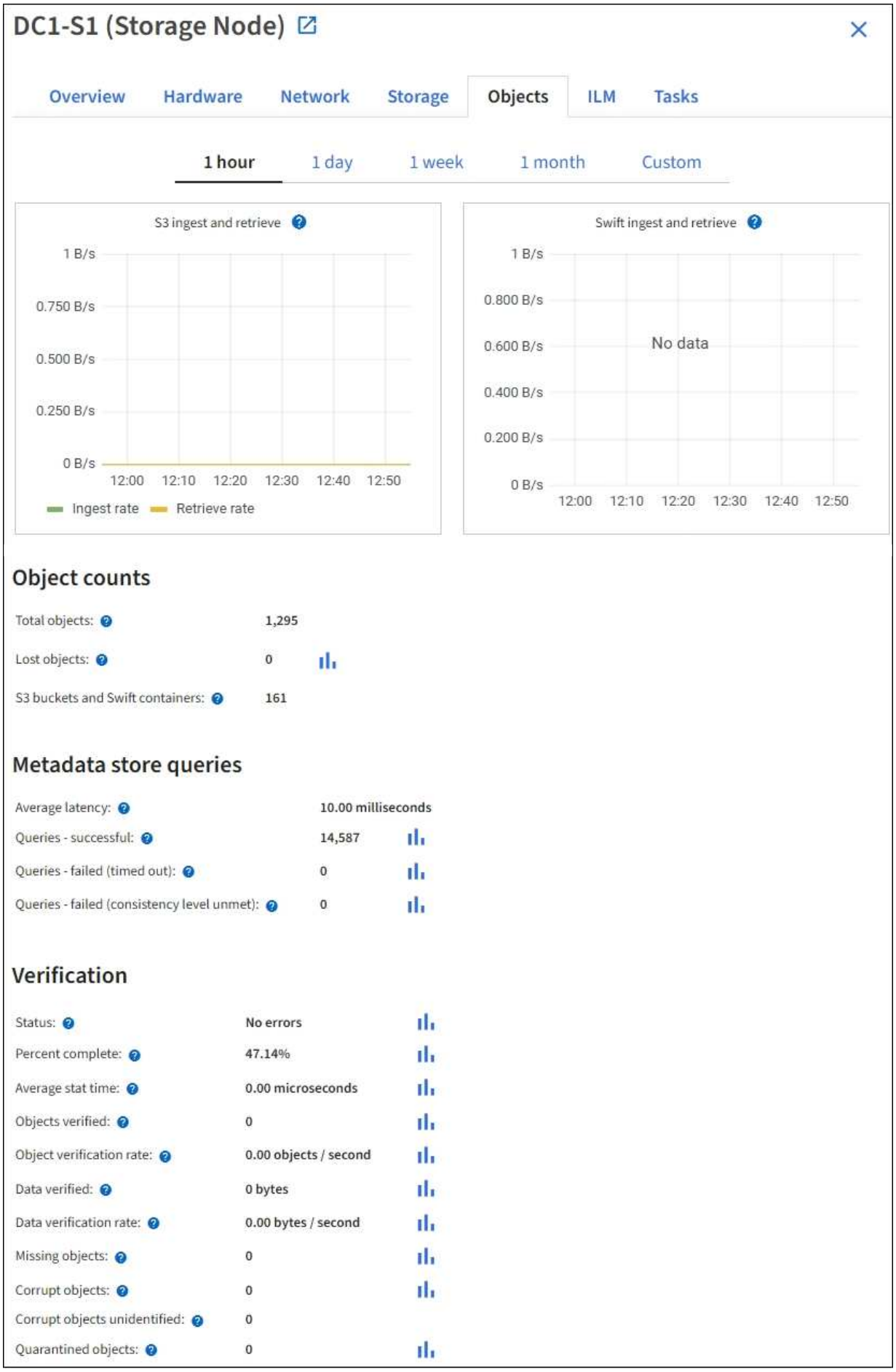
Appliance di storage SG5600

Appliance di servizi SG100 e SG1000

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.

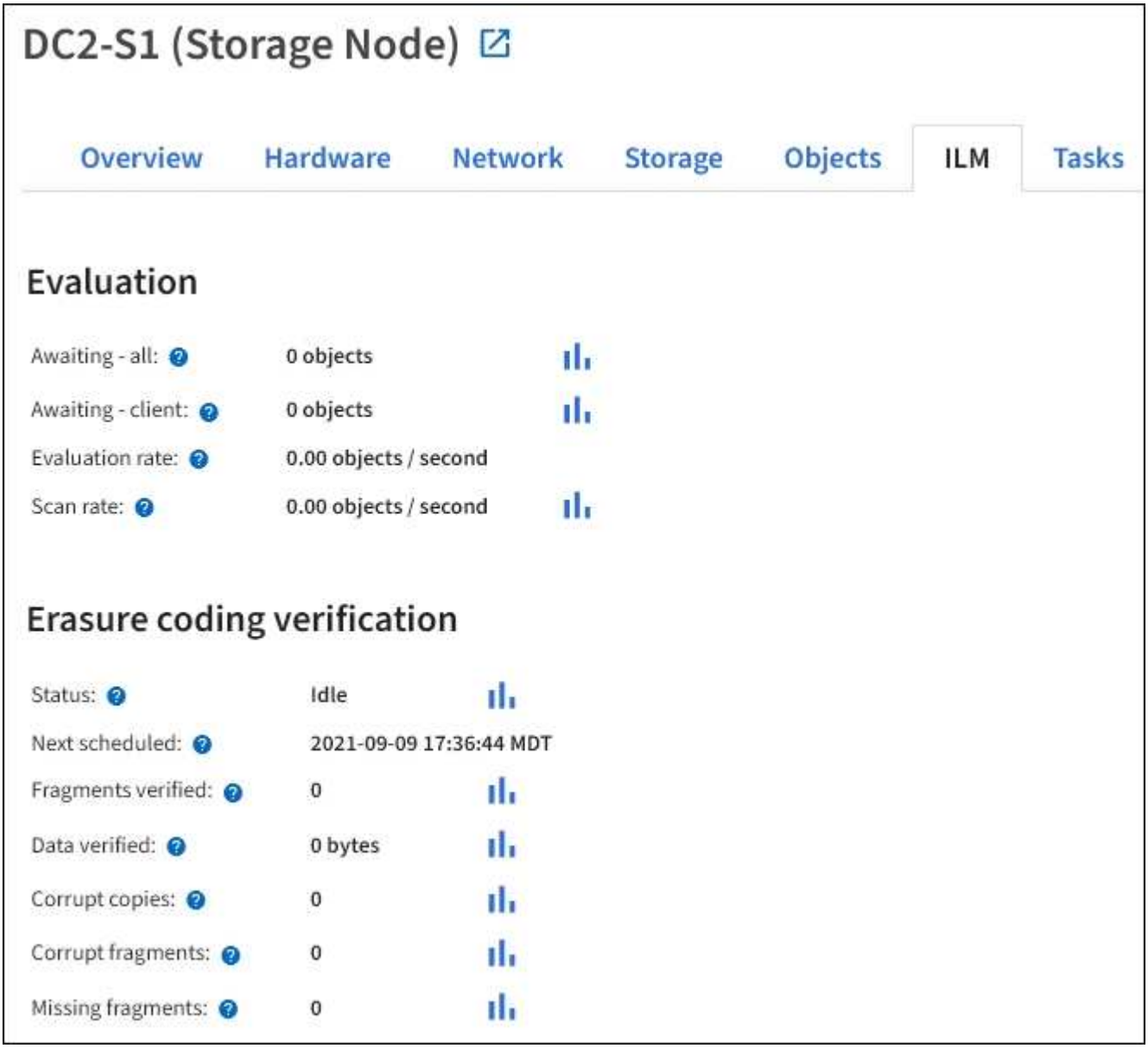

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

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 di storage, la scheda ILM fornisce dettagli sulla valutazione ILM e sulla verifica in background per l'eliminazione degli oggetti codificati.



Informazioni correlate

Monitorare la gestione del ciclo di vita delle informazioni

Amministrare StorageGRID

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 Load Balancer 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

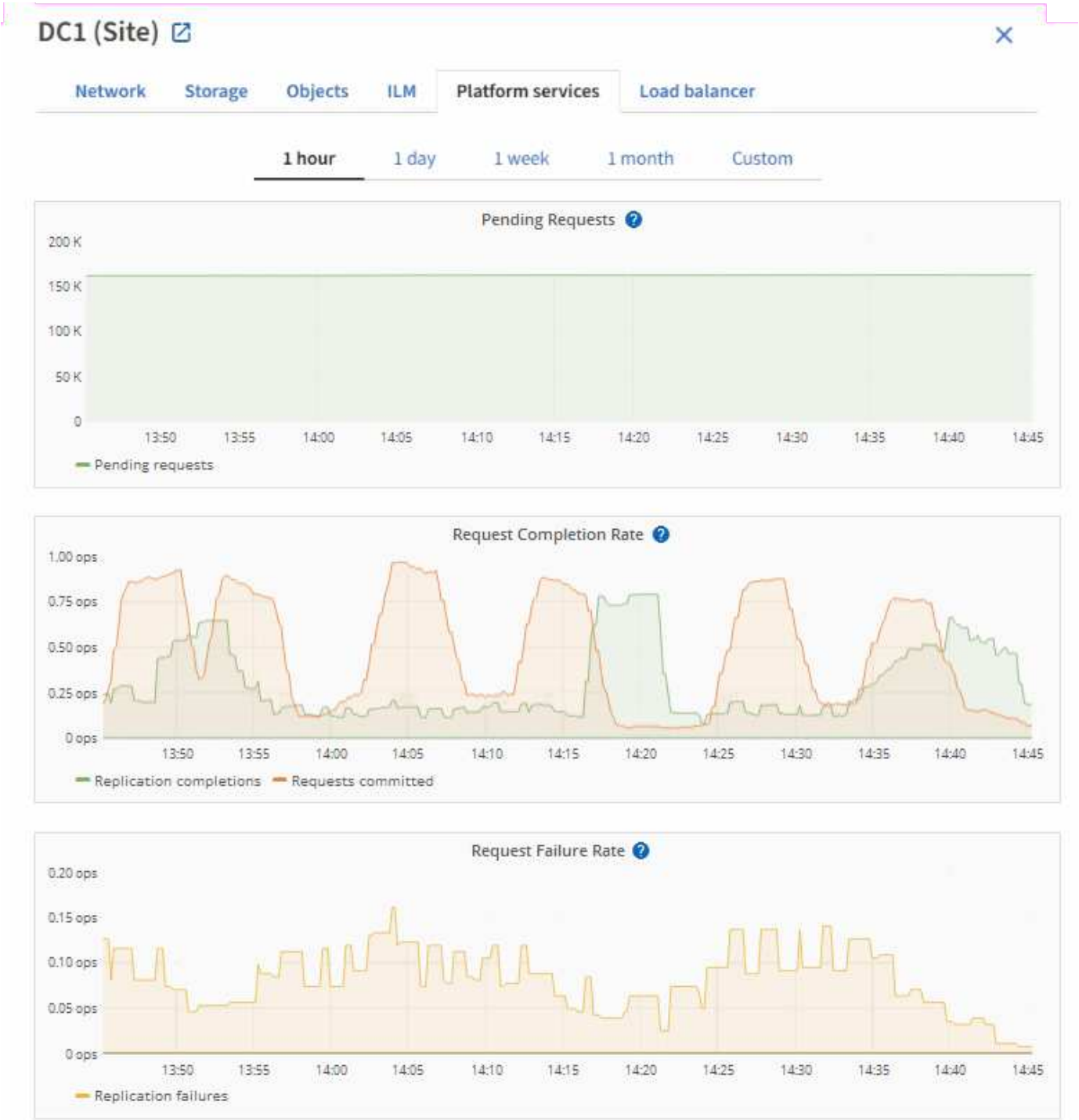
Monitorare le operazioni di bilanciamento del carico

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.

Visualizzare la scheda Gestore di sistema di SANtricity

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.

Viene visualizzata la scheda Gestore di sistema di SANtricity per i nodi dell'appliance di storage.

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, consultare le istruzioni in administeringStorageGRID.

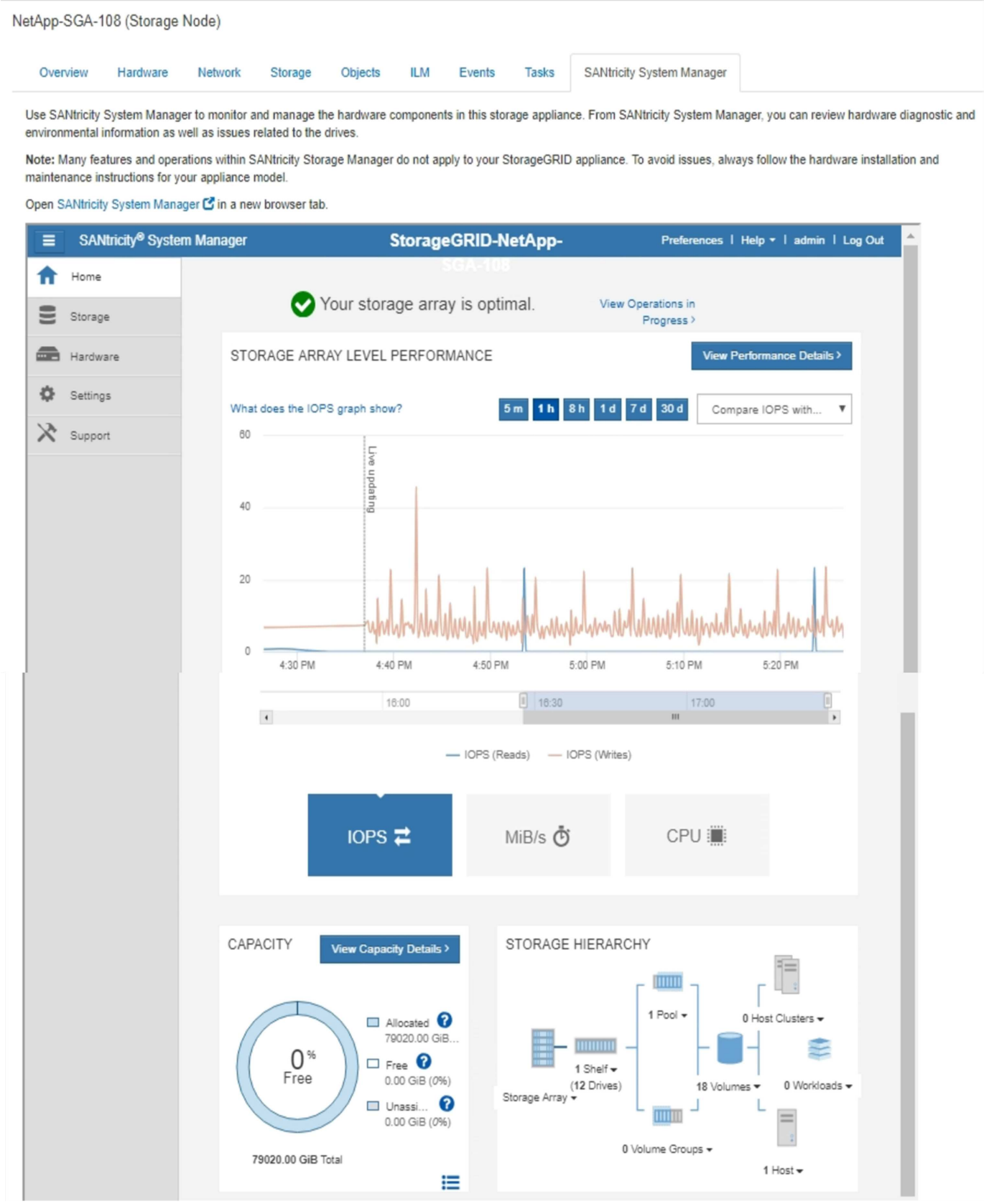
Amministrare StorageGRID

Per accedere a Gestione di sistema SANtricity tramite Gestione griglia, è necessario disporre dell'autorizzazione Amministratore appliance di storage o dell'autorizzazione di accesso root.

> È necessario disporre del firmware SANtricity 8.70 (11.70) o superiore per accedere a Gestore di sistema 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 di installazione e manutenzione dell'hardware dell'appliance.

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 alle prestazioni a livello di array storage e all'utilizzo della capacità,

posizionare il puntatore del mouse 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

StorageGRID è un sistema di storage distribuito e a tolleranza di errore progettato per continuare a funzionare anche quando si verificano errori o quando nodi o siti non sono disponibili. È necessario monitorare in modo proattivo lo stato di salute del sistema, i carichi di lavoro e le statistiche di utilizzo in modo da poter intervenire per risolvere potenziali problemi prima che influiscano sull'efficienza o sulla disponibilità del grid.

Un sistema occupato genera grandi quantità di informazioni. Questa sezione fornisce indicazioni sulle informazioni più importanti da monitorare costantemente.

Cosa monitorare	Frequenza
Il dati sullo stato di salute del sistema Mostrato nella dashboard di Grid Manager. Nota se qualcosa è cambiato rispetto al giorno precedente.	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
Connessioni di rete e performance	Settimanale
Risorse a livello di nodo	Settimanale
Attività del tenant	Settimanale
Capacità del sistema storage di archiviazione esterno	Settimanale
Operazioni di bilanciamento del carico	Dopo la configurazione iniziale e dopo eventuali modifiche alla configurazione
Disponibilità di hotfix software e aggiornamenti software	Mensile

Monitorare lo stato del sistema

È necessario monitorare quotidianamente lo stato di salute generale del sistema StorageGRID.

A proposito di questa attività

Il sistema StorageGRID è a tolleranza di errore e può continuare a funzionare anche quando parti della griglia non sono disponibili. Il primo segno di un potenziale problema con il sistema StorageGRID è probabilmente un

avviso o un allarme (sistema legacy) e non necessariamente un problema con le operazioni del sistema. Prestare attenzione allo stato di salute del sistema può aiutare a rilevare problemi minori prima che influiscano sulle operazioni o sull'efficienza della rete.

Il pannello Health (Salute) del pannello Grid Manager (Gestione griglia) fornisce un riepilogo dei problemi che potrebbero interessare il sistema. È necessario esaminare tutti i problemi visualizzati nella dashboard.

> Per ricevere una notifica degli avvisi non appena vengono attivati, è possibile impostare le notifiche e-mail per gli avvisi o configurare i trap SNMP.

Fasi

1. Accedi a Grid Manager per visualizzare la dashboard.
2. Esaminare le informazioni nel pannello Health (Salute).

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

Collegamento	Indica
Dettagli della griglia	Viene visualizzato se i nodi sono disconnessi (stato connessione sconosciuto o amministrativamente inattivo). Fare clic sul collegamento o sull'icona blu o grigia per determinare quale nodo o nodi sono interessati.
Avvisi correnti	Viene visualizzato se sono attivi avvisi. Fare clic sul collegamento oppure fare clic su **critico**, **maggiore** o **minore** per visualizzare i dettagli nella pagina **AVVISI corrente**.
Avvisi risolti di recente	Viene visualizzato se gli avvisi attivati nell'ultima settimana sono stati risolti. Fare clic sul collegamento per visualizzare i dettagli nella pagina **ALERTS resolved**.
Licenza	Viene visualizzato se si verifica un problema con la licenza software per questo sistema StorageGRID. Fare clic sul collegamento per visualizzare i dettagli nella pagina **MANUTENZIONE sistema licenza**.

Informazioni correlate

- Amministrare StorageGRID
- Imposta le notifiche via email per gli avvisi
- Utilizzare il monitoraggio SNMP

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. È necessario monitorare gli stati di connessione dei nodi e risolvere tempestivamente eventuali problemi.

Di cosa hai bisogno

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

A proposito di questa attività

I nodi possono avere uno dei tre stati di connessione:

- **Non connesso - Sconosciuto** : Il nodo non è connesso alla rete per un motivo sconosciuto. Ad esempio, la connessione di rete tra i nodi è stata persa o l'alimentazione è inattiva. 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).

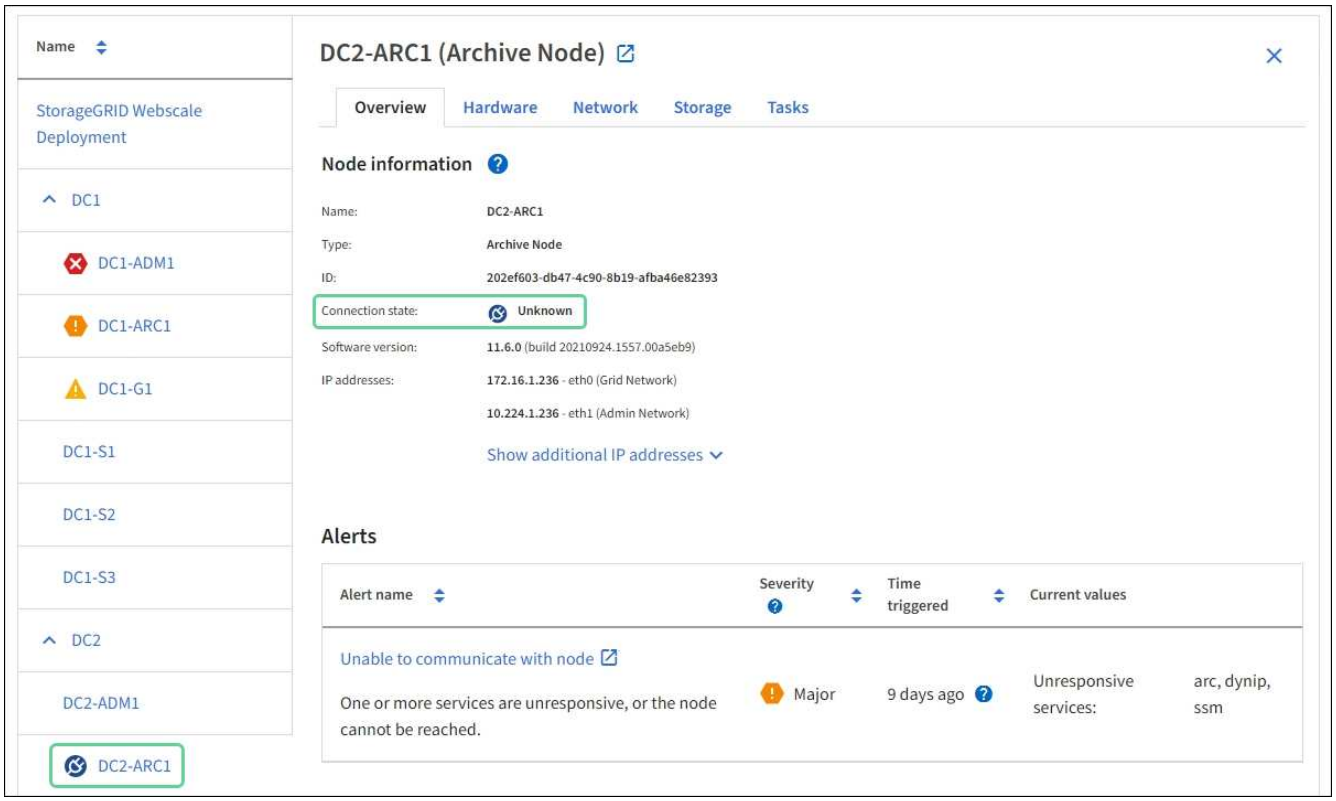
- **Non connesso - amministrazione non attiva** : Il nodo non è connesso alla rete per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.
- **Connesso** : Il nodo è collegato alla rete.

Fasi

1. Se viene visualizzata un'icona blu o grigia nel pannello Health (Salute) della dashboard, fare clic sull'icona o fare clic su **Grid details** (Dettagli griglia). (Le icone blu o grigie e il collegamento **Dettagli griglia** vengono visualizzati solo se almeno un nodo è scollegato dalla griglia).

   Viene visualizzata la pagina Overview (Panoramica) per il primo nodo blu nella struttura dei nodi. Se non sono presenti nodi blu, viene visualizzata la pagina Panoramica relativa al primo nodo grigio della struttura.

   Nell'esempio, il nodo di storage denominato DC1-S3 presenta un'icona blu. L'opzione **Connection state** (Stato connessione) nel pannello Node Information (informazioni nodo) è **Unknown** (Sconosciuto) e l'avviso **Unable to communicate with Node** (Impossibile comunicare con il nodo) è attivo. L'avviso indica che uno o più servizi non rispondono o che il nodo non può essere raggiunto.



2. Se un nodo presenta un'icona blu, attenersi alla seguente procedura:
   a. Selezionare ciascun avviso nella tabella e seguire le azioni consigliate.

      Ad esempio, potrebbe essere necessario riavviare un servizio che ha arrestato o riavviato l'host per il nodo.

   b. Se non riesci a riportare il nodo online, contatta il supporto tecnico.
3. Se un nodo presenta un'icona grigia, attenersi alla seguente procedura:

   I nodi grigi sono previsti durante le procedure di manutenzione e potrebbero essere associati a uno o più avvisi. In base al problema sottostante, questi nodi "amministrativamente giù" spesso tornano online senza alcun intervento.

   a. Consultare la sezione Avvisi e determinare se sono presenti avvisi che influiscono su questo nodo.
   b. Se uno o più avvisi sono attivi, selezionare ciascun avviso nella tabella e seguire le azioni consigliate.
   c. Se non riesci a riportare il nodo online, contatta il supporto tecnico.

Informazioni correlate

Riferimenti agli avvisi

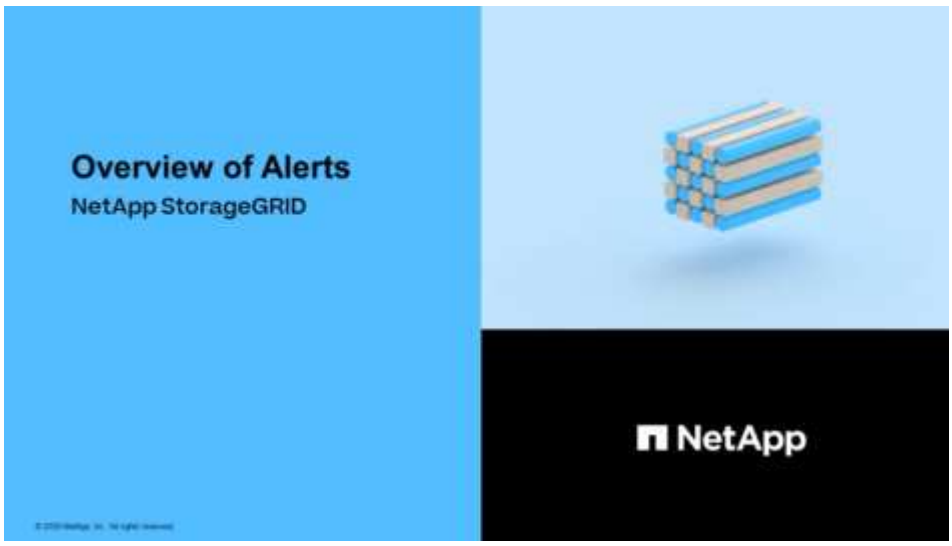
Ripristino e manutenzione

Visualizzare gli avvisi correnti

Quando viene attivato un avviso, viene visualizzata un'icona di avviso nella dashboard. Nella pagina nodi viene visualizzata anche un'icona di avviso per il nodo. Potrebbe essere inviata anche una notifica via email, a meno che l'avviso non sia stato tacitato.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- Facoltativamente, hai guardato il video: "Video: Panoramica degli avvisi".

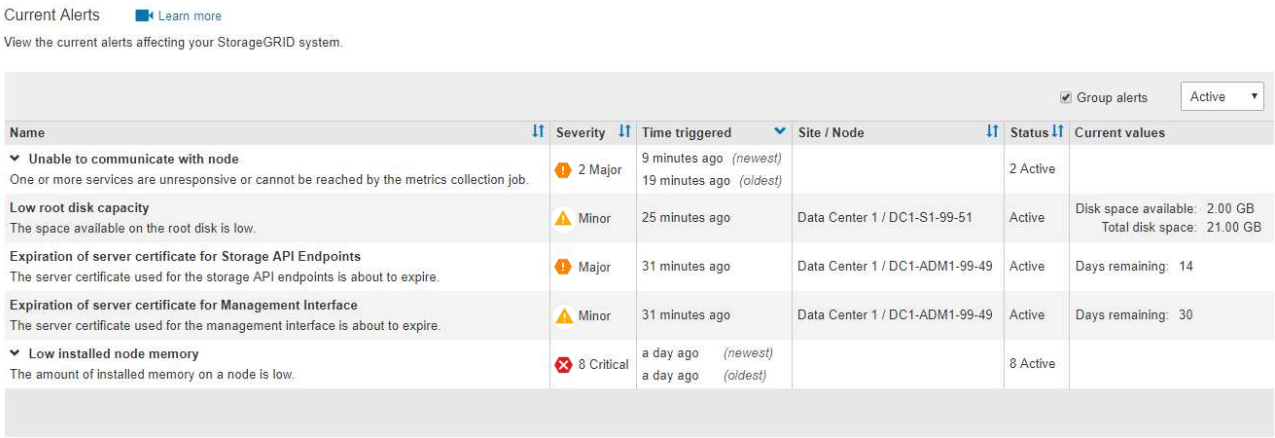


Fasi

1. Se sono attivi uno o più avvisi, effettuare una delle seguenti operazioni:

   - Dal pannello Health (Salute) della dashboard, fare clic sull'icona di avviso o fare clic su **Current alerts** (Avvisi correnti). (Un'icona di avviso e il collegamento **Current alerts** (Avvisi correnti) vengono visualizzati solo se almeno un avviso è attivo).
   - Selezionare **ALERTS current**.

     Viene visualizzata la pagina Avvisi correnti. Elenca tutti gli avvisi che attualmente interessano il sistema StorageGRID.



     Per impostazione predefinita, gli avvisi 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.

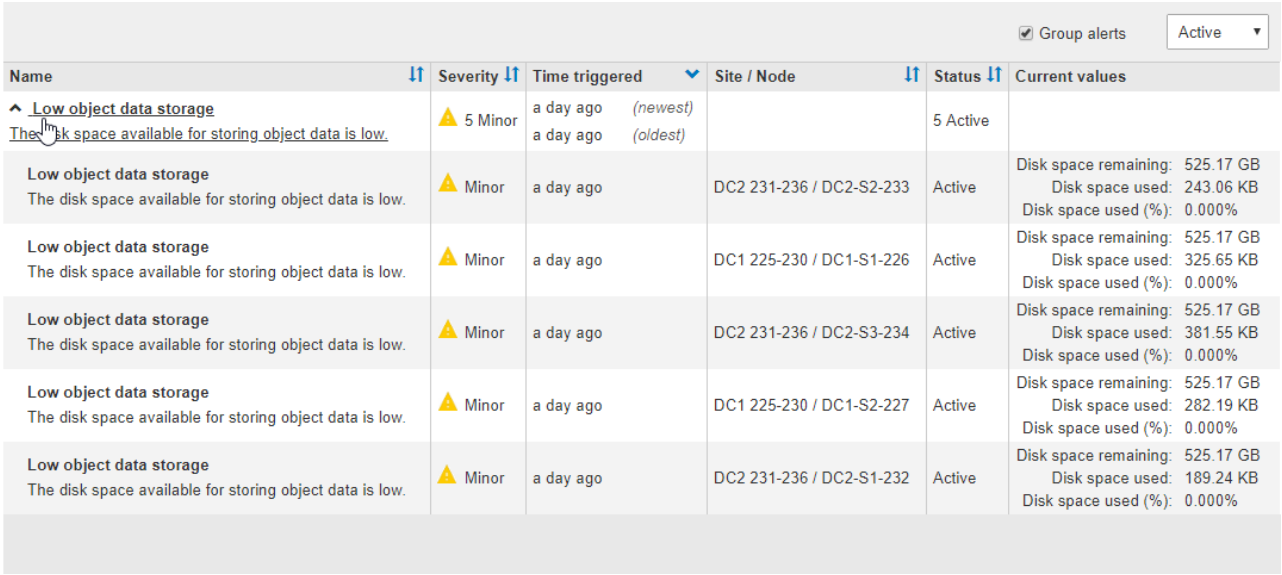
La pagina Current Alerts (Avvisi correnti) viene aggiornata ogni due minuti.

2. Esaminare le informazioni contenute nella tabella.

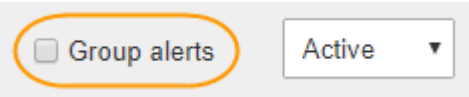
Intestazione di colonna	Descrizione
Nome	Il nome dell'avviso e la relativa descrizione.
Severità	La severità dell'avviso. Se vengono raggruppati più avvisi, la riga del titolo mostra il numero di istanze di tale avviso che si verificano a ogni livello di gravità. • **Critico** : Si verifica una condizione 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. • **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 assicurarsi che non causino problemi più gravi.
Tempo di attivazione	Quanto tempo fa è stato attivato l'avviso. 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*).
Sito/nodo	Il nome del sito e del nodo in cui si verifica l'avviso. Se vengono raggruppati più avvisi, i nomi del sito e del nodo non vengono visualizzati nella riga del titolo.
Stato	Se l'avviso è attivo o è stato tacitato. 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.

Intestazione di colonna	Descrizione
Valori correnti	Il valore corrente 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, i valori correnti non vengono visualizzati nella riga del titolo.

3. Per espandere e comprimere gruppi di avvisi:
   - Per visualizzare i singoli avvisi in un gruppo, fare clic sul pulsante freccia giù ⌄ nell'intestazione o fare clic sul nome del gruppo.
   - Per nascondere i singoli avvisi in un gruppo, fare clic sull'icona a forma di accento circonflesso ⌃ nell'intestazione o fare clic sul nome del gruppo.



4. Per visualizzare singoli avvisi invece di gruppi di avvisi, deselezionare la casella di controllo **Group alerts** (Avvisi di gruppo) nella parte superiore della tabella.



5. Per ordinare gli avvisi o i gruppi di avvisi, fare clic sulle 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.
   - Se l'opzione **Group alerts** (Avvisi di gruppo) non è selezionata, 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.
6. Per filtrare gli avvisi in base allo stato, utilizzare il menu a discesa nella parte superiore della tabella.

- Selezionare **All alerts** (tutti gli avvisi) per visualizzare tutti gli avvisi correnti (sia attivi che tacitati).
- Selezionare **Active** per visualizzare solo gli avvisi correnti attivi.
- Selezionare **silenziato** per visualizzare solo gli avvisi attualmente tacitati. Vedere Tacitare le notifiche di avviso.

7. Per visualizzare i dettagli di un avviso specifico, selezionarlo dalla tabella.

   Viene visualizzata una finestra di dialogo per l'avviso. Vedere Visualizzare un avviso specifico.

Visualizzare gli avvisi risolti

È possibile cercare e visualizzare una cronologia degli avvisi risolti.

Di cosa hai bisogno

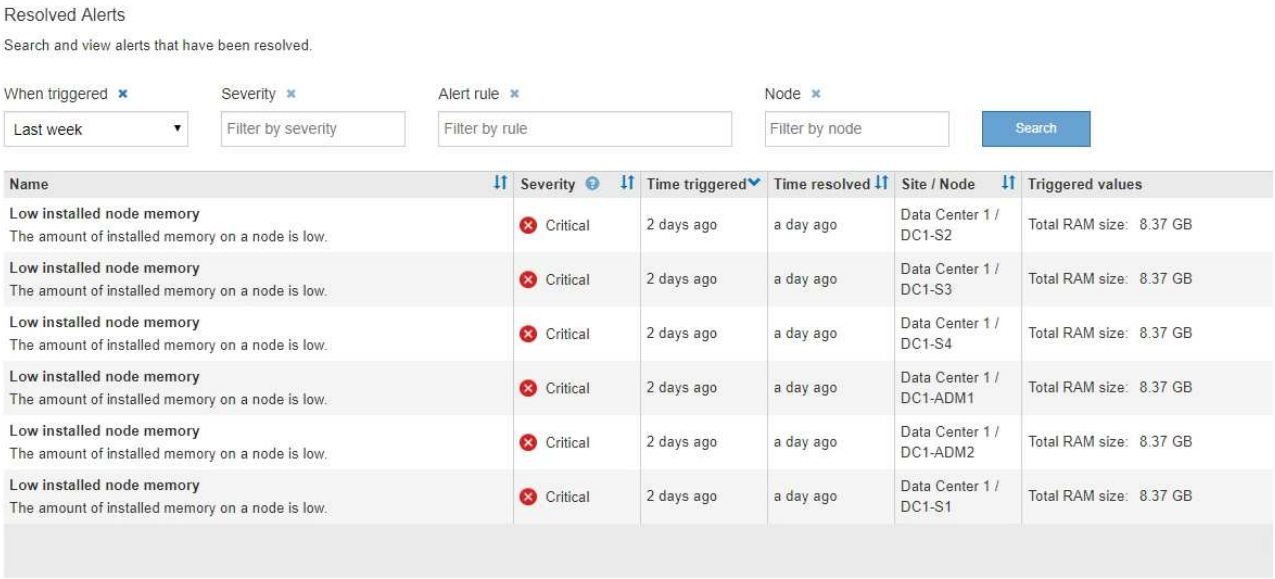
- È necessario accedere a Grid Manager utilizzando un browser web supportato.

Fasi

1. Per visualizzare gli avvisi risolti, effettuare una delle seguenti operazioni:
   - Dal pannello Health (Stato) della dashboard, fare clic su **Recently Resolved alerts** (Avvisi risolti di recente)

     Il collegamento **Recently Resolved alerts** (Avvisi risolti di recente) viene visualizzato solo se uno o più avvisi sono stati attivati nell'ultima settimana e sono stati risolti.

   - Selezionare **ALERTS resolved**. Viene visualizzata la pagina Avvisi risolti. Per impostazione predefinita, vengono visualizzati gli avvisi risolti che sono stati attivati nell'ultima settimana, con gli avvisi attivati più di recente. Gli avvisi presenti in questa pagina sono stati precedentemente visualizzati nella pagina Avvisi correnti o in una notifica via email.



2. Esaminare le informazioni contenute nella tabella.

Intestazione di colonna	Descrizione
Nome	Il nome dell'avviso e la relativa descrizione.
Severità	La severità dell'avviso. • **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 assicurarsi che non causino problemi più gravi.
Tempo di attivazione	Quanto tempo fa è stato attivato l'avviso.
Tempo risolto	Quanto tempo fa l'avviso è stato risolto.
Sito/nodo	Il nome del sito e del nodo in cui si è verificato l'avviso.
Valori attivati	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.

3. Per ordinare l'intero elenco degli avvisi risolti, fare clic sulle frecce su/giù in ogni intestazione di colonna.

Ad esempio, è possibile ordinare gli avvisi risolti in base a **Sito/nodo** per visualizzare gli avvisi che hanno interessato un nodo specifico.

4. In alternativa, filtrare l'elenco degli avvisi risolti utilizzando i menu a discesa nella parte superiore della tabella.
   a. Selezionare un periodo di tempo dal menu a discesa **quando attivato** per visualizzare gli avvisi risolti in base al tempo trascorso dall'attivazione.

      È possibile cercare gli avvisi attivati nei seguenti periodi di tempo:

      - Ultima ora
      - Ultimo giorno
      - Ultima settimana (vista predefinita)
      - Il mese scorso
      - In qualsiasi periodo di tempo
      - Custom (personalizzata): Consente di specificare la data di inizio e la data di fine del periodo di tempo.

   b. Selezionare una o più severità dal menu a discesa **severità** per filtrare gli avvisi risolti con una severità specifica.
   c. 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.
   d. Selezionare uno o più nodi dal menu a discesa **nodo** per filtrare gli avvisi risolti relativi a un nodo specifico.
   e. Fare clic su **Cerca**.
5. Per visualizzare i dettagli di uno specifico avviso risolto, selezionarlo dalla tabella.

   Viene visualizzata una finestra di dialogo per l'avviso. Vedere Visualizzare un avviso specifico.

Visualizzare un avviso specifico

È possibile visualizzare informazioni dettagliate su un avviso che sta interessando il sistema StorageGRID o un avviso che è stato risolto. I dettagli includono le azioni correttive consigliate, l'ora di attivazione dell'avviso e il valore corrente delle metriche correlate all'avviso.

Se lo si desidera, è possibile tacitare un avviso corrente oppure aggiornare la regola di avviso.

Di cosa hai bisogno

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

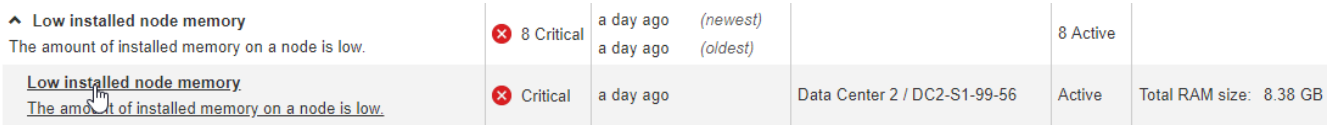
Fasi

1. Eseguire una delle seguenti operazioni, a seconda che si desideri visualizzare un avviso corrente o risolto:

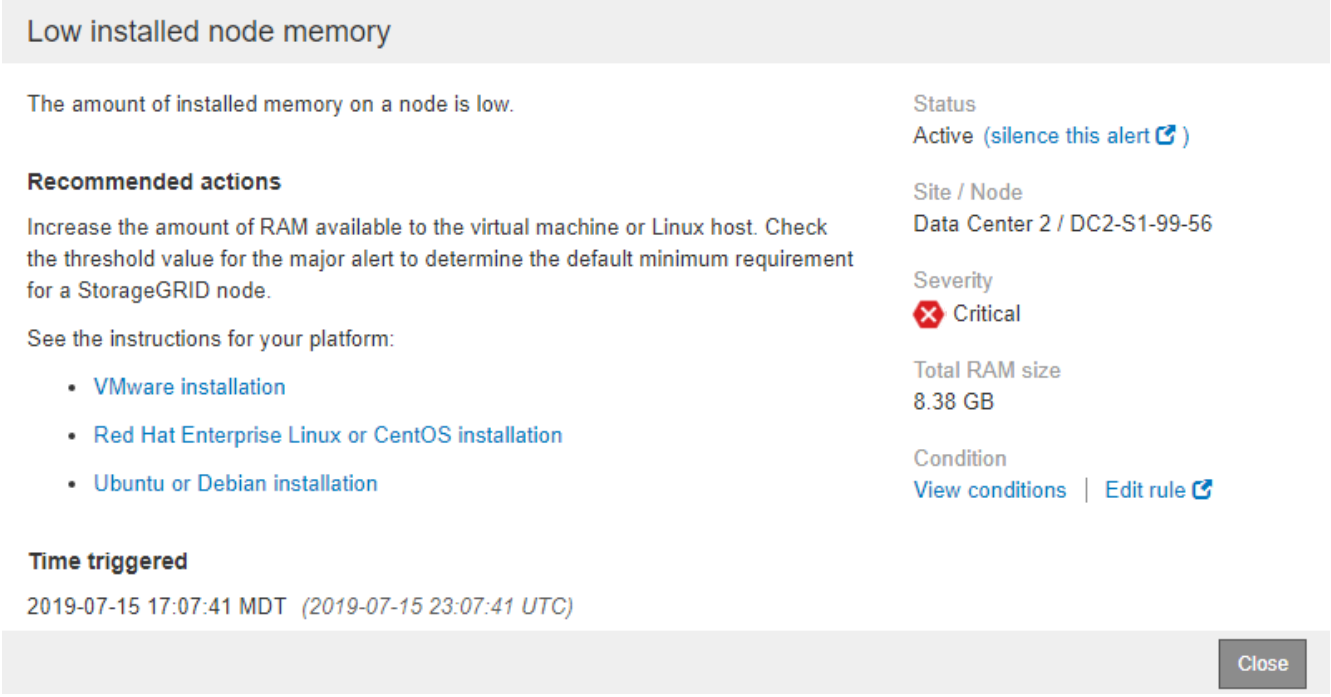
Intestazione di colonna	Descrizione
Avviso corrente	• Dal pannello Health (Salute) della dashboard, fare clic sul collegamento **Current alerts** (Avvisi correnti). Questo collegamento viene visualizzato solo se è attivo almeno un avviso. Questo collegamento è nascosto se non sono presenti avvisi correnti o se tutti gli avvisi correnti sono stati tacitati. • Selezionare **ALERTS current**. • Dalla pagina **NODI**, selezionare la scheda **Panoramica** per un nodo con un'icona di avviso. Quindi, nella sezione Avvisi, fare clic sul nome dell'avviso.
Avviso risolto	• Dal pannello Health (Stato) della dashboard, fare clic sul collegamento **Recently Resolved alerts** (Avvisi risolti di recente). (Questo collegamento viene visualizzato solo se uno o più avvisi sono stati attivati nella settimana precedente e sono stati risolti. Questo collegamento è nascosto se non sono stati attivati e risolti avvisi nell'ultima settimana). • Selezionare **ALERTS resolved**.

2. Se necessario, espandere un gruppo di avvisi e selezionare l'avviso da visualizzare.

Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.



Viene visualizzata una finestra di dialogo con i dettagli dell'avviso selezionato.



3. Esaminare i dettagli dell'avviso.

Informazioni	Descrizione
titolo	Il nome dell'avviso.
primo paragrafo	La descrizione dell'avviso.
Azioni consigliate	Le azioni consigliate per questo avviso.
Tempo di attivazione	La data e l'ora in cui l'avviso è stato attivato nell'ora locale e in UTC.
Tempo risolto	Solo per gli avvisi risolti, la data e l'ora in cui l'avviso è stato risolto nell'ora locale e in UTC.
Stato	Lo stato dell'avviso: Attivo, tacitato o risolto.
Sito/nodo	Il nome del sito e del nodo interessati dall'avviso.
Severità	La severità dell'avviso. • **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 assicurarsi che non causino problemi più gravi.
valori dei dati	Il valore corrente della metrica per questo 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 metadata storage** includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.

4. Facoltativamente, fare clic su **Silence this alert** (tacita questo avviso) per disattivare la regola di avviso che ha causato l'attivazione dell'avviso.

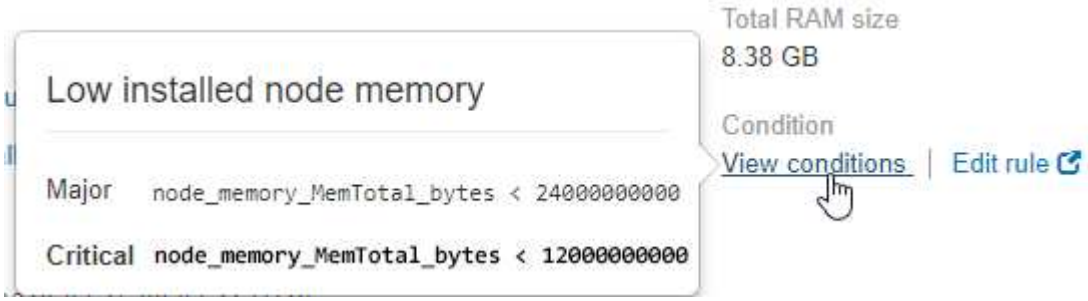
Per tacitare una regola di avviso, è necessario disporre dell'autorizzazione di accesso Gestisci avvisi o root.

> 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.

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

   a. Dai dettagli dell'avviso, fare clic su **View conditions** (Visualizza condizioni).

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



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

6. Facoltativamente, fare clic su **Edit rule** (Modifica regola) per modificare la regola di avviso che ha causato l'attivazione dell'avviso:

   Per modificare una regola di avviso, è necessario disporre dell'autorizzazione di accesso Gestisci avvisi o root.

   > 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.

7. Per chiudere i dettagli dell'avviso, fare clic su **Chiudi**.

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.

Di cosa hai bisogno

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

Fasi

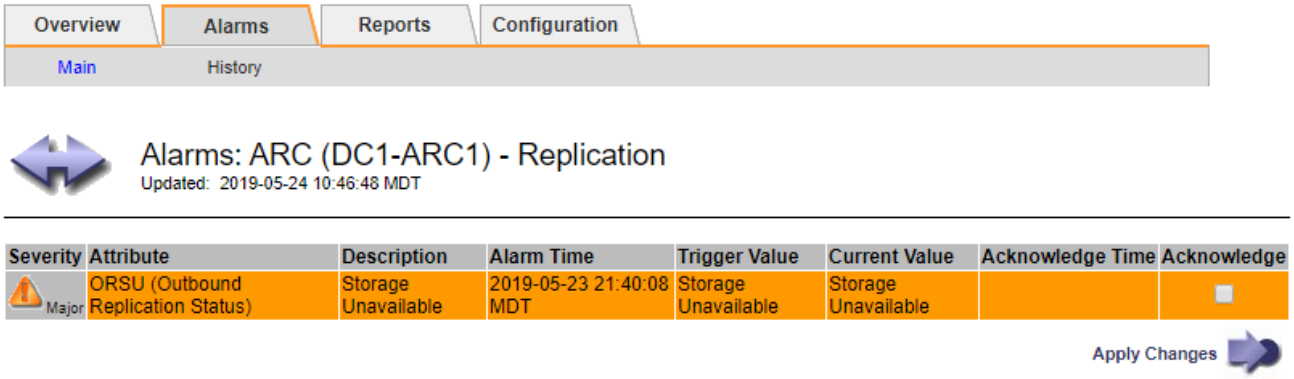
1. Selezionare **SUPPORTO Allarmi (legacy) Allarmi correnti**.

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)

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

È necessario monitorare la capacità di storage globale 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.

Di cosa hai bisogno

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

A proposito di questa attività

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.

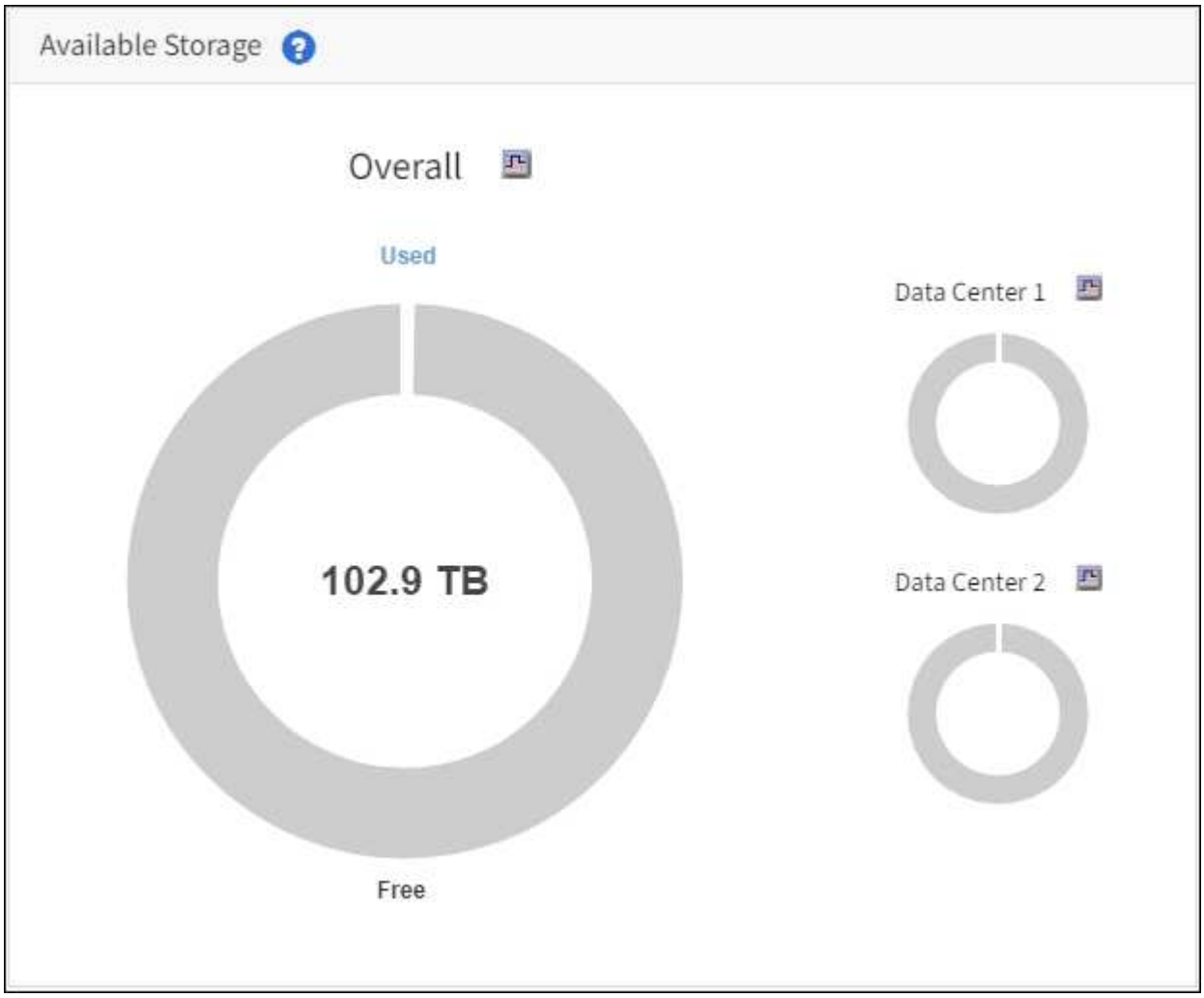
Fasi

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

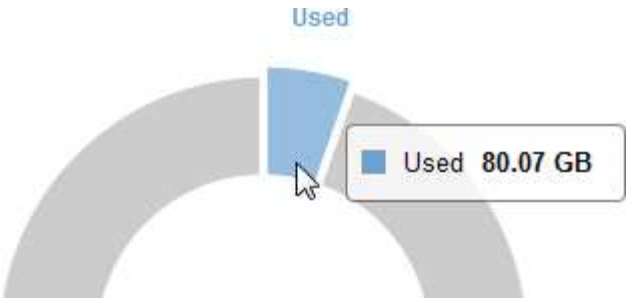
   a. Selezionare **Dashboard**.

   b. Nel pannello Available Storage (Storage disponibile), annotare il riepilogo generale della capacità di storage libera e utilizzata.

   Il riepilogo non include i supporti di archiviazione.



   a. Posiziona il cursore sulle sezioni Free o USed Capacity del grafico per vedere esattamente quanto spazio è libero o utilizzato.



b. Per le griglie multi-sito, esaminare il grafico di ciascun data center.

c. Fare clic sull'icona del grafico per visualizzare il grafico generale o per un singolo data center un grafico che mostra l'utilizzo della capacità nel tempo.

   Un grafico che mostra la percentuale di capacità di storage utilizzata (%) rispetto a. Viene visualizzata l'ora.

2. Determinare la quantità di storage utilizzata e la quantità di storage disponibile per i dati a oggetti e i metadati a oggetti.

   a. Selezionare **NODI**.

   b. Selezionare ***grid* Storage**.

   c. Spostare il cursore sopra i grafici **Storage used - Object data** e **Storage used - Object metadata** per visualizzare 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 una griglia non includono i 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

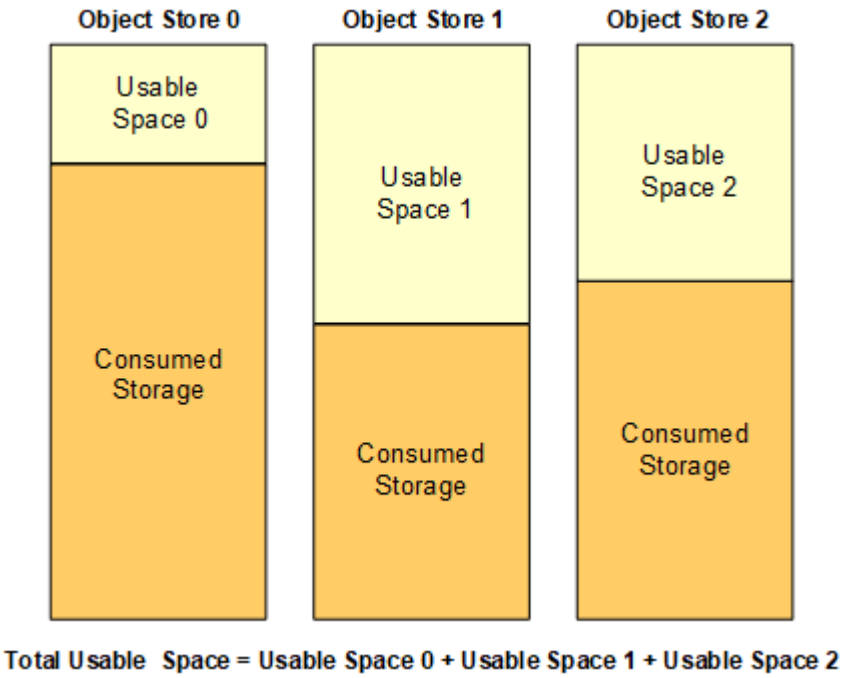
Monitorare lo spazio totale utilizzabile per ciascun nodo di storage per garantire che il nodo disponga di spazio sufficiente per i nuovi dati dell'oggetto.

Di cosa hai bisogno

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

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**.

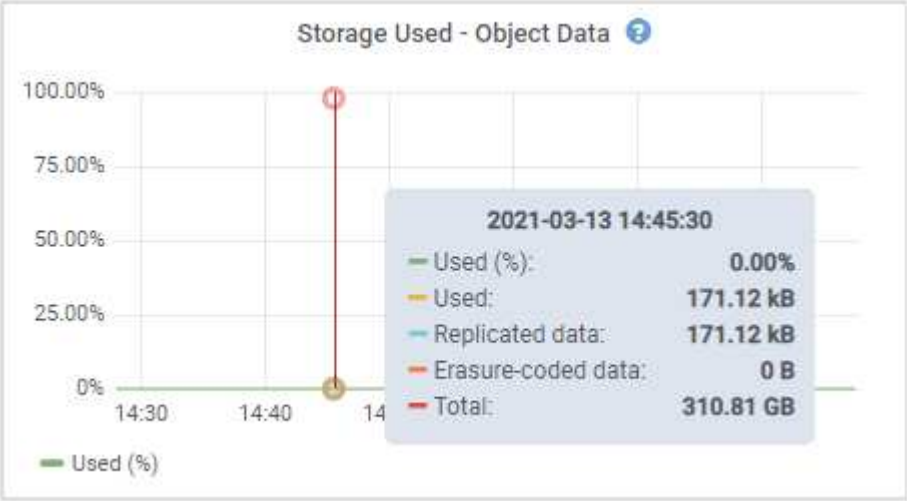
   Vengono visualizzati i grafici e le tabelle del nodo.

2. Spostare 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 **Basso storage dei dati a oggetti** 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.

Di cosa hai bisogno

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

A proposito di questa attività

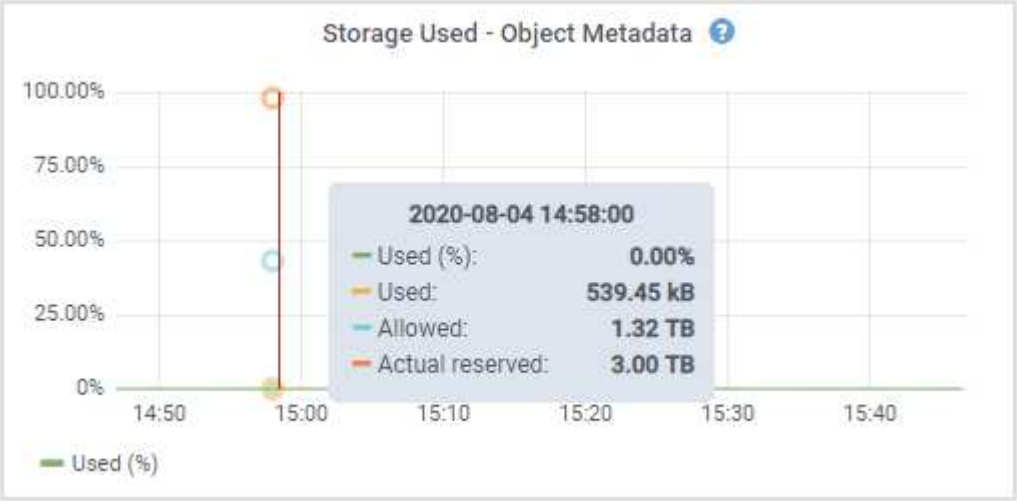
StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di storage di ogni sito utilizzando lo spazio riservato ai metadati sul volume di storage 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. Spostare il cursore sul grafico Storage used - Object metadata (Storage utilizzato - metadati oggetto) per visualizzare i valori relativi a un orario specifico.



Valore	Descrizione	Metrica Prometheus
Utilizzato (%)	La percentuale dello spazio consentito per i metadati che è stato utilizzato su questo nodo di storage.	`storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes`
Utilizzato	I byte dello spazio di metadati consentito che sono stati utilizzati su questo nodo di storage.	`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 Istruzioni per l'amministrazione di StorageGRID.	`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 Istruzioni per l'amministrazione di StorageGRID.	*Metric verrà aggiunto in una release futura.*

> I valori totali di un sito o di una griglia non includono i 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 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 ulteriori risorse.

Di cosa hai bisogno

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

A proposito di questa attività

Il sistema StorageGRID gestisce gli oggetti applicando il criterio ILM attivo. Il criterio ILM e le regole ILM associate determinano il numero di copie eseguite, il tipo di copie create, la posizione delle copie e il periodo di

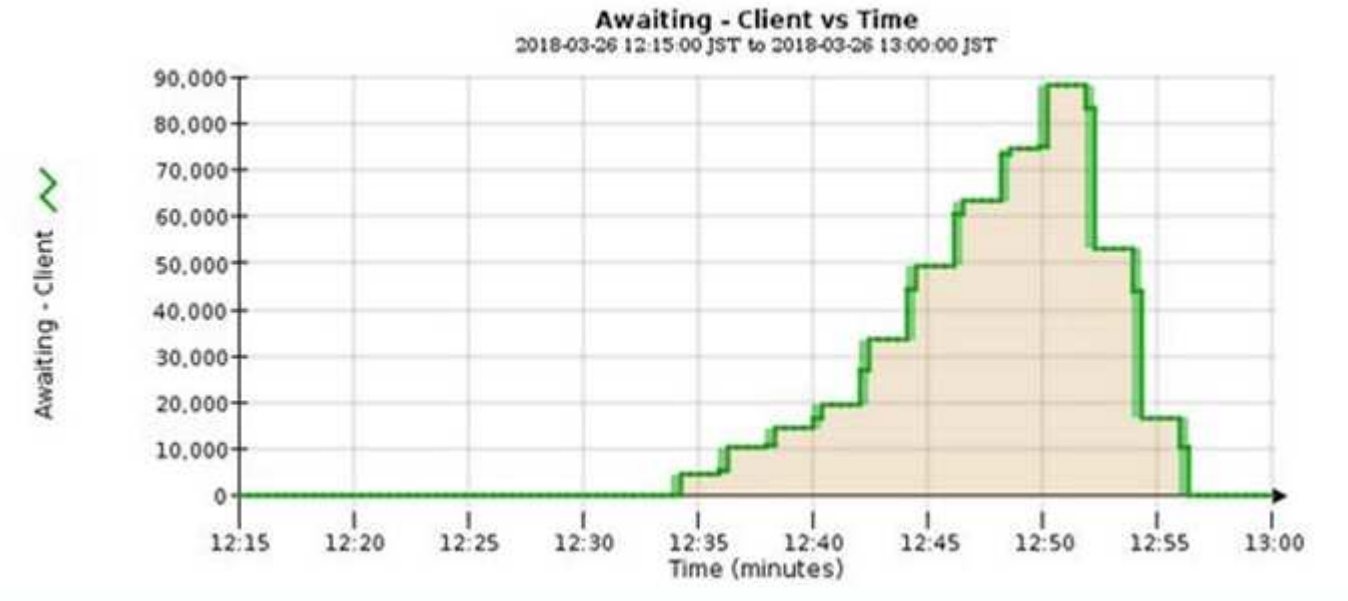
conservazione di ciascuna copia.

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 possibile controllare se StorageGRID sta mantenendo il passo con le azioni del client inserendo l'attributo in attesa - client.

Per inserire questo attributo:

1. Accedi a Grid Manager.
2. Dalla dashboard, individuare la voce **in attesa - Client** nel pannello ILM (Information Lifecycle Management).
3. Fare clic sull'icona del grafico .

Il grafico di esempio mostra una situazione in cui il numero di oggetti in attesa di valutazione ILM è aumentato temporaneamente in modo insostenibile, per poi diminuire. Tale tendenza indica che ILM non è stato temporaneamente soddisfatto quasi in tempo reale.



Sono previsti picchi temporanei nel grafico di in attesa - Client. Tuttavia, se il valore mostrato nel grafico continua ad aumentare e non diminuisce mai, la griglia richiede più risorse per funzionare in modo efficiente: Più nodi di storage o, se la policy ILM colloca gli oggetti in posizioni remote, maggiore larghezza di banda della rete.

È possibile analizzare ulteriormente le code ILM utilizzando la pagina **NODES**.

Fasi

1. Selezionare **NODI**.
2. Selezionare ***Grid name* ILM**.
3. Posizionare il cursore del mouse sul grafico ILM Queue per visualizzare il valore dei seguenti attributi in un dato 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 ILM Queue (coda ILM) è inclusa solo per la griglia. Queste informazioni non vengono visualizzate nella scheda ILM per un sito o un nodo di storage.

- **Scan Period (periodo di scansione) - Estimated (stimato)**: Tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

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

- **Riparazioni tentate**: Il numero totale di operazioni di riparazione di 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 connessioni di rete e le performance

I nodi della rete devono essere in grado di comunicare tra loro per consentire il funzionamento della rete. L'integrità della rete tra nodi e siti e la larghezza di banda della rete tra i siti sono fondamentali per operazioni efficienti.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

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 semplicemente a scarse performance di acquisizione e backlog ILM.

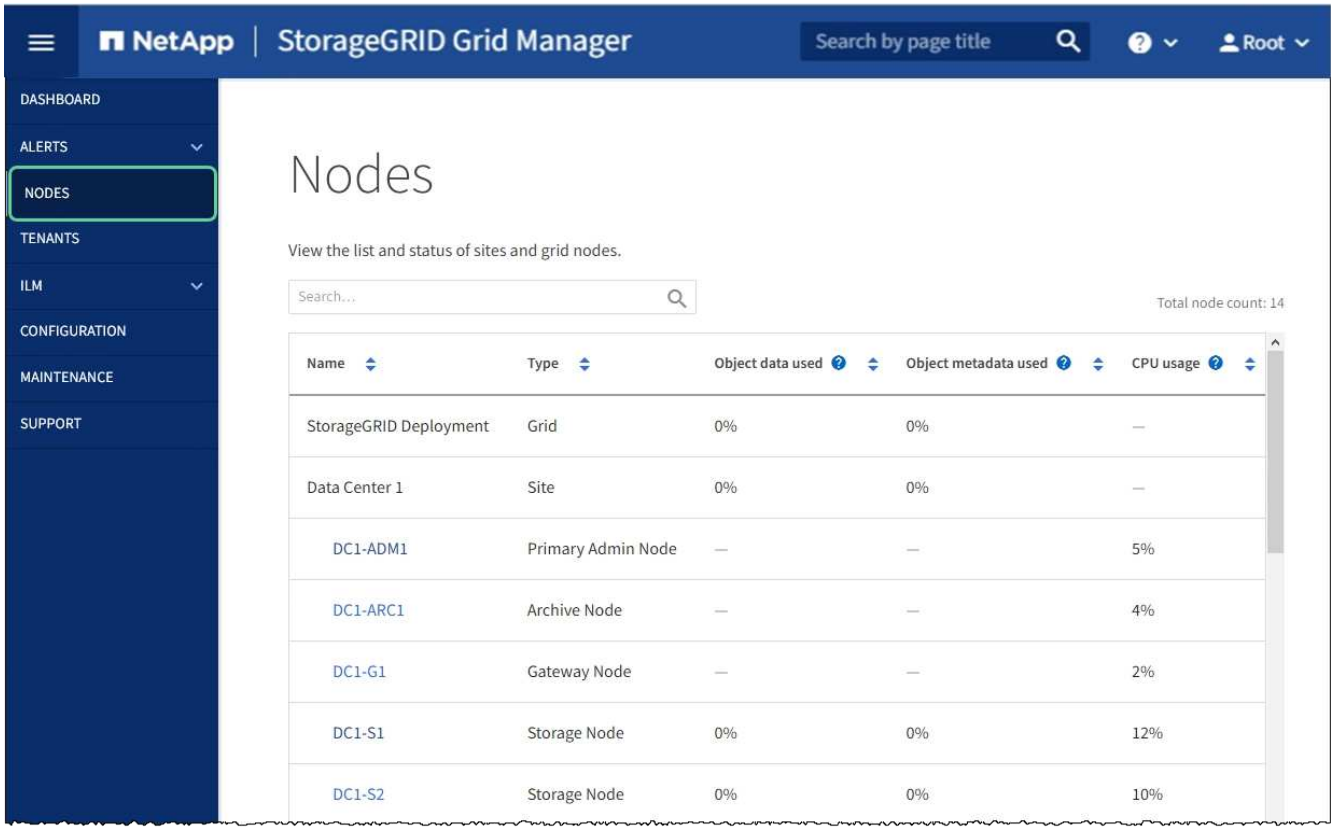
È possibile utilizzare Grid Manager per monitorare la connettività e le performance di rete, in modo da poter risolvere tempestivamente qualsiasi problema.

Inoltre, è consigliabile creare policy di classificazione del traffico di rete per fornire il monitoraggio e la limitazione del traffico relativo a tenant, bucket, subnet o endpoint specifici del bilanciamento del carico. Vedere Istruzioni per l'amministrazione di StorageGRID.

Fasi

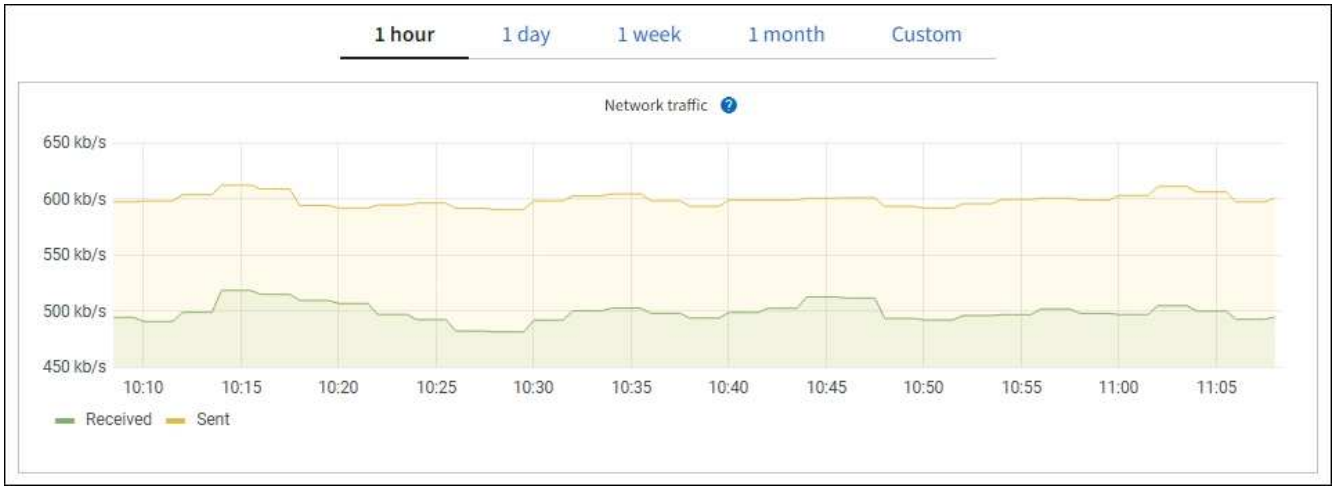
1. Selezionare **NODI**.

   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.

   b. 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**.

   c. 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.

Per creare, modificare o eliminare i criteri di classificazione del traffico, vedere Istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

Visualizzare la scheda rete

Monitorare gli stati di connessione del nodo

Monitorare le risorse a livello di nodo

È necessario monitorare i singoli nodi della griglia per verificarne i livelli di utilizzo delle risorse.

Di cosa hai bisogno

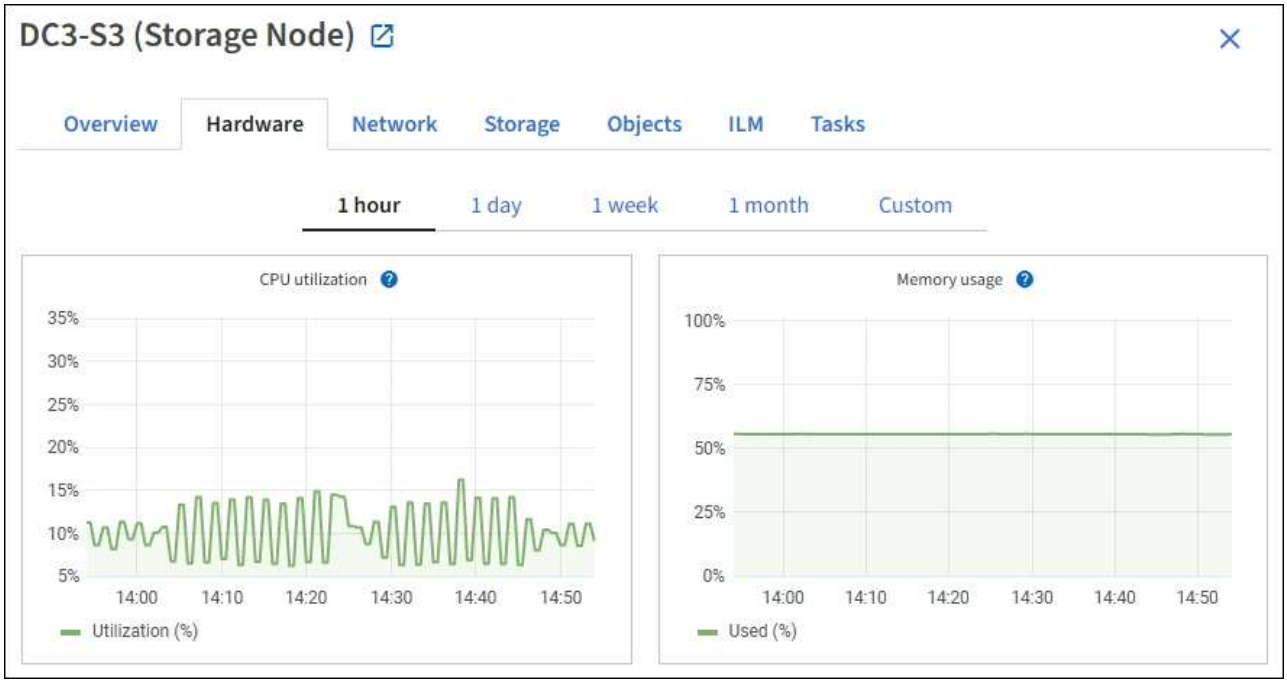
- È necessario accedere a Grid Manager utilizzando un browser web supportato.

A proposito di questa attività

Se i nodi sono costantemente sovraccarichi, potrebbero essere necessari più nodi per operazioni efficienti.

Fasi

1. Per visualizzare informazioni sull'utilizzo dell'hardware di un nodo grid:
   a. Dalla pagina **NODES**, selezionare il nodo.
   b. Selezionare la scheda **hardware** per visualizzare i grafici relativi all'utilizzo della CPU e della memoria.



   c. 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.

d. 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 con 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 del client sono associate a un account tenant. È possibile utilizzare Grid Manager per monitorare l'utilizzo dello storage o il traffico di rete di un tenant, oppure utilizzare il registro di controllo o le dashboard Grafana per ottenere informazioni più dettagliate sull'utilizzo di StorageGRID da parte dei tenant.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root o di amministratore.

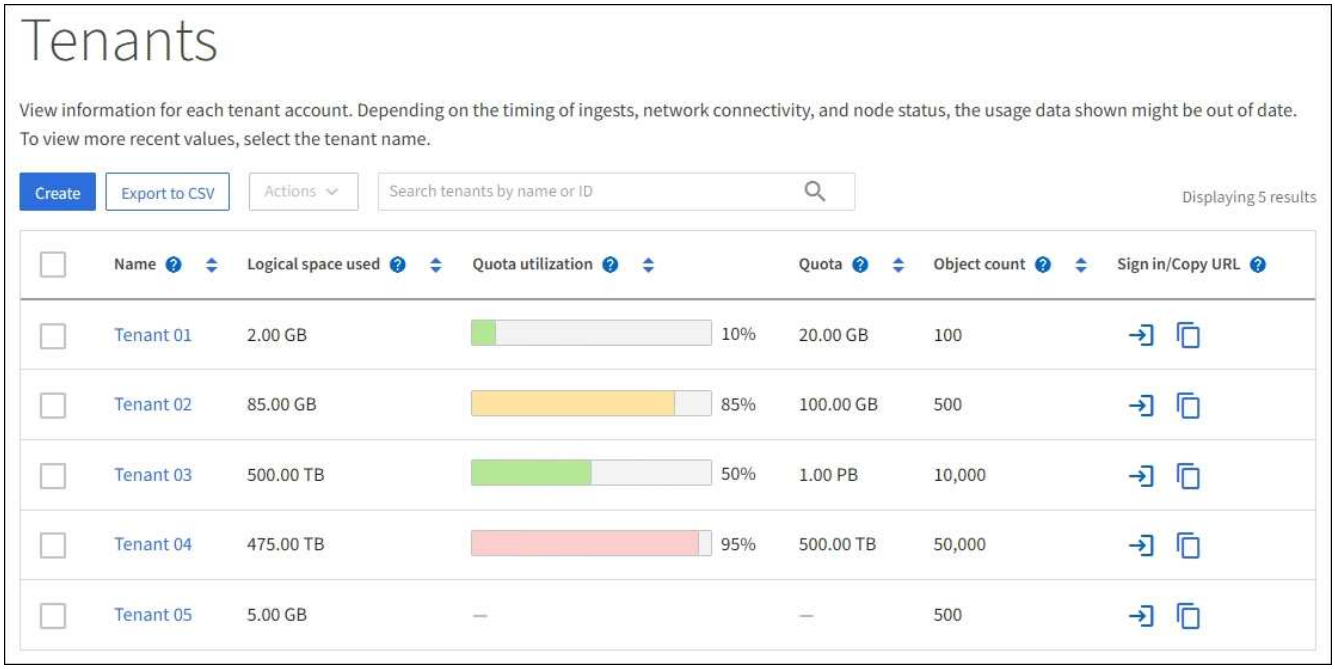
A proposito di questa attività

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

Fasi

1. Selezionare **TENANT** per esaminare la quantità di storage utilizzata da tutti i 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 quota e utilizzo della quota contengono un trattino (n. 8212;).



Puoi accedere a un account tenant selezionando il link di accesso Nella colonna **URL di accesso/copia** della tabella.

È possibile copiare l'URL della pagina di accesso di un tenant selezionando il collegamento URL copia Nella colonna **URL di accesso/copia** della tabella.

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

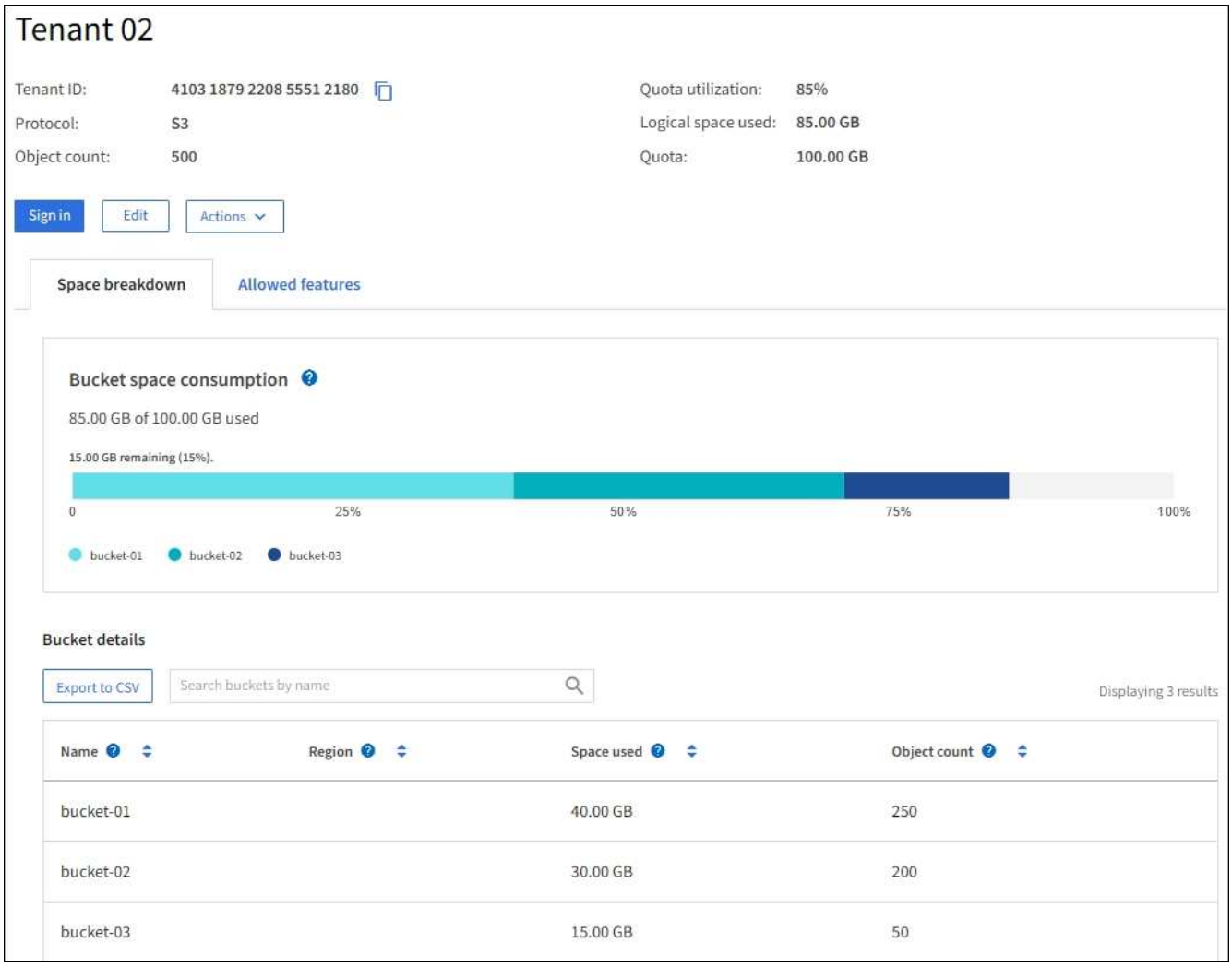
   Viene richiesto di aprire o salvare `.csv` file.

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

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

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

3. Per visualizzare i dettagli di un tenant specifico, inclusi i grafici di utilizzo, selezionare il nome dell'account tenant dalla pagina tenant.



- **Panoramica del tenant**

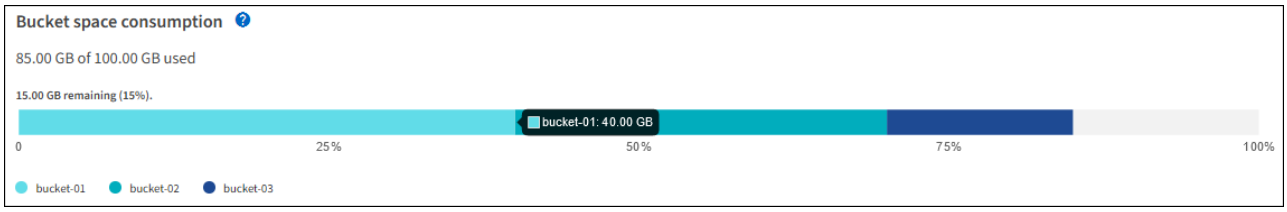
  L'area panoramica del tenant contiene i valori per il conteggio degli oggetti, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

- **Suddivisione dello spazio — consumo di spazio**

  La scheda Space breakdown (suddivisione spazio) include i valori per il consumo di spazio totale del bucket (S3) o del container (Swift), nonché lo spazio utilizzato e il numero di oggetti per ciascun bucket o container.

  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 l'avviso **quota elevata del 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 ulteriori informazioni, vedere il riferimento agli avvisi.

- **Suddivisione dello spazio — Dettagli del bucket o del container**

  La tabella **Dettagli bucket** (S3) o **Dettagli container** (Swift) elenca i bucket o i container 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.

4. 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 del file .csv di un singolo tenant S3 è simile al seguente esempio:

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

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

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

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

      Per creare, modificare o eliminare i criteri di classificazione del traffico, consultare le istruzioni per l'amministrazione di StorageGRID.

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

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

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

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

Per ulteriori informazioni, consultare le istruzioni relative ai messaggi di audit.

7. 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.

Informazioni correlate

Riferimenti agli avvisi

Esaminare i registri di audit

Amministrare StorageGRID

Rivedere le metriche di supporto

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.

Di cosa hai bisogno

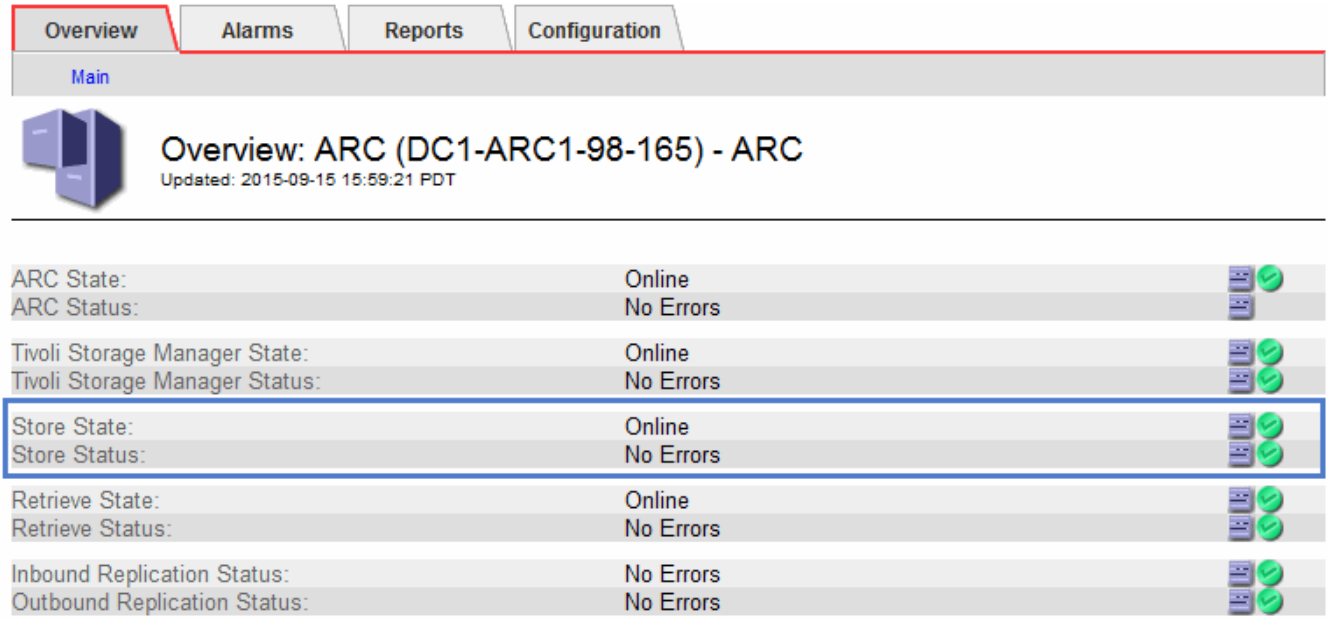
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

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.

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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

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

> Il servizio CLB è obsoleto.

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.

Consultare la sezione sulla configurazione delle connessioni client nelle istruzioni per l'amministrazione di StorageGRID.

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** (Panoramica), verificare se un'interfaccia di nodo si trova in un gruppo ha e se l'interfaccia di nodo ha il ruolo di Master.

      I nodi con il ruolo di master 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 la scheda **Load Balancer**.
   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. Se si desidera, utilizzare le policy di classificazione del traffico per visualizzare una suddivisione più dettagliata del traffico fornito dal servizio Load Balancer.
2. Se i client S3 o Swift si connettono utilizzando il servizio CLB (obsoleto), eseguire i seguenti controlli:
   a. Selezionare **NODI**.
   b. Selezionare un nodo gateway.
   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 Master.

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

   d. Per ogni nodo gateway che deve distribuire attivamente le richieste client, selezionare **SUPPORT Tools Grid topology**.
   e. Selezionare ***Gateway Node* CLB HTTP Panoramica principale**.
   f. Esaminare il numero di **sessioni in entrata - stabilite** per verificare che il nodo gateway stia gestendo attivamente le richieste.
3. 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.

Informazioni correlate

Amministrare StorageGRID

Visualizzare la scheda bilanciamento del carico

Applicare hotfix o aggiornare il software, se necessario

Se è disponibile una correzione rapida o una nuova versione del software StorageGRID, è necessario verificare se l'aggiornamento è appropriato per il sistema e installarlo, se necessario.

A proposito di questa attività

Le hotfix StorageGRID contengono modifiche software rese disponibili al di fuori di una release di funzionalità o patch. Le stesse modifiche sono incluse in una release futura.

Fasi

1. Vai alla pagina dei download NetApp per StorageGRID.

   "Download NetApp: StorageGRID"

2. Selezionare la freccia verso il basso del campo **tipo/Seleziona versione** per visualizzare un elenco degli aggiornamenti disponibili per il download:
   - **Versioni software StorageGRID**: 11.*x.y*
   - **Hotfix StorageGRID**: 11.*x.a. .z*
3. Esaminare le modifiche incluse nell'aggiornamento:
   a. Selezionare la versione dal menu a discesa e fare clic su **Go**.
   b. Accedi utilizzando il nome utente e la password del tuo account NetApp.
   c. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).

      Viene visualizzata la pagina dei download per la versione selezionata.

4. Informazioni sulle modifiche incluse nella versione software o nella correzione rapida.
   - Per una nuova versione del software, consultare l'argomento "Novità" nelle istruzioni per l'aggiornamento di StorageGRID.
   - Per una correzione rapida, scaricare il file README per un riepilogo delle modifiche incluse nella correzione rapida.
5. Se si decide di richiedere un aggiornamento software, individuare le istruzioni prima di procedere.
   - Per una nuova versione del software, seguire attentamente le istruzioni per l'aggiornamento di StorageGRID.
   - Per una correzione rapida, individuare la procedura di correzione rapida nelle istruzioni di ripristino e manutenzione

Informazioni correlate

Aggiornare il software

Ripristino e manutenzione

Gestire 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 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 delle autorizzazioni di configurazione della pagina topologia griglia e 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 **CONFIGURAZIONE monitoraggio agente SNMP**. Utilizzare il monitoraggio SNMP	Selezionare **CONFIGURAZIONE monitoraggio agente SNMP**. Utilizzare il monitoraggio SNMP **Nota**: Le notifiche SNMP non vengono inviate per ogni allarme o gravità dell'allarme. Allarmi che generano notifiche SNMP (sistema legacy)

	Avvisi	Allarmi (sistema precedente)
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)
Quali nodi di amministrazione inviano notifiche?	Un singolo nodo Admin (il "Preferred sender"). Amministrare StorageGRID	Un singolo nodo Admin (il "Preferred sender"). Amministrare StorageGRID
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	1. Selezionare **CONFIGURAZIONE** > **sistema** > **Opzioni di visualizzazione**. 2. Selezionare la casella di controllo **notifica Sospendi tutto**. **Nota**: La soppressione delle notifiche e-mail a livello di sistema elimina anche le e-mail AutoSupport attivate dagli eventi. Gestire gli allarmi (sistema legacy)

	Avvisi	Allarmi (sistema precedente)
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)
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

Gli avvisi consentono di monitorare diversi eventi e condizioni all'interno del sistema StorageGRID. È possibile gestire gli avvisi creando avvisi personalizzati, modificando o disattivando gli avvisi predefiniti, impostando le notifiche e-mail per gli avvisi e tacitando le notifiche.

Informazioni sugli avvisi StorageGRID

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.

- Il sistema di allerta si concentra su problemi pratici nel sistema. Gli avvisi vengono attivati per gli eventi che richiedono l'attenzione immediata dell'utente, non per gli eventi che possono essere ignorati in modo sicuro.
- La pagina Current Alerts (Avvisi correnti) fornisce un'interfaccia intuitiva per la visualizzazione dei problemi correnti. È possibile ordinare l'elenco in base a singoli avvisi e gruppi di avvisi. Ad esempio, è possibile ordinare tutti gli avvisi per nodo/sito per visualizzare gli avvisi che interessano un nodo specifico. In alternativa, è possibile ordinare gli avvisi in un gruppo in base all'ora attivata per trovare l'istanza più recente di un avviso specifico.
- La pagina Resolved Alerts (Avvisi risolti) fornisce informazioni simili a quelle della pagina Current Alerts (Avvisi correnti), ma consente di cercare e visualizzare una cronologia degli avvisi risolti, anche quando l'avviso è stato attivato e quando è stato risolto.

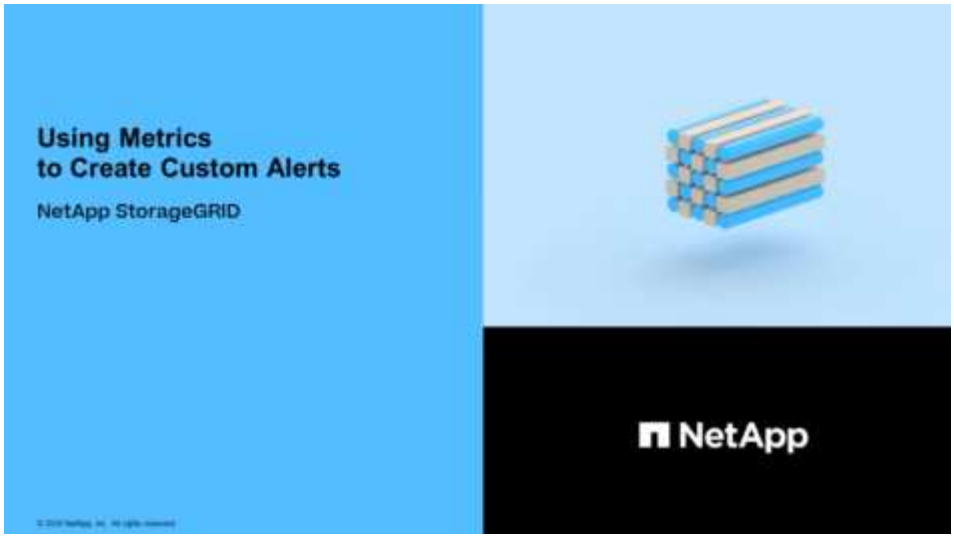
- Più avvisi dello stesso tipo sono raggruppati in un'e-mail per ridurre il numero di notifiche. Inoltre, nella pagina Avvisi vengono visualizzati più avvisi dello stesso tipo come gruppo. È possibile espandere e comprimere i gruppi di avvisi per mostrare o nascondere i singoli avvisi. Ad esempio, se diversi nodi segnalano l'avviso **Impossibile comunicare con il nodo** circa contemporaneamente, viene inviato un solo messaggio e-mail e l'avviso viene visualizzato come gruppo nella pagina Avvisi.
- Gli avvisi utilizzano nomi e descrizioni intuitivi per comprendere rapidamente il problema. Le notifiche di avviso includono dettagli sul nodo e sul sito interessati, la severità dell'avviso, l'ora in cui è stata attivata la regola di avviso e il valore corrente delle metriche correlate all'avviso.
- Le notifiche e-mail di avviso e gli elenchi degli avvisi presenti nelle pagine Avvisi correnti e Avvisi risolti forniscono le azioni consigliate per la risoluzione di un avviso. Queste azioni consigliate spesso includono collegamenti diretti al centro di documentazione di StorageGRID per semplificare la ricerca e l'accesso a procedure di risoluzione dei problemi più dettagliate.
- Se è necessario sospendere temporaneamente le notifiche per un avviso a uno o più livelli di severità, è possibile disattivare facilmente una regola di avviso specifica per una durata specificata e per l'intera griglia, un singolo sito o un singolo nodo. È inoltre possibile disattivare tutte le regole di avviso, ad esempio durante una procedura di manutenzione pianificata, ad esempio un aggiornamento del software.
- È possibile modificare le regole di avviso predefinite in base alle esigenze. È possibile disattivare completamente una regola di avviso o modificarne le condizioni di attivazione e la durata.
- È possibile creare regole di avviso personalizzate per definire le condizioni specifiche pertinenti alla situazione e per fornire le azioni consigliate. Per definire le condizioni per un avviso personalizzato, creare espressioni utilizzando le metriche Prometheus disponibili nella sezione metriche dell'API Grid Management.

Scopri di più

Per ulteriori informazioni, consulta questi video:

- "Video: Panoramica degli avvisi"

- "Video: Utilizzo delle metriche per creare avvisi personalizzati"



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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root.
- Facoltativamente, hai guardato il video: "Video: Panoramica degli avvisi"

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.
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 assicurarsi che non causino problemi più gravi.

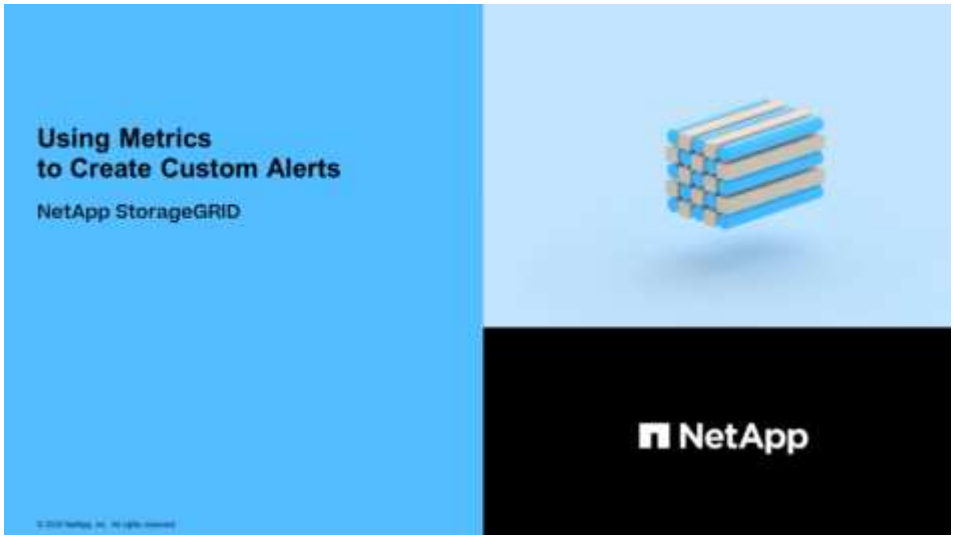
Intestazione di colonna	Descrizione
Tipo	Il tipo di regola di avviso: • **Default**: Una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificare le condizioni e la durata di una regola di avviso predefinita. Non è possibile rimuovere una regola di 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root
- 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"



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 "scompleta" potrebbe essere semplicemente 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.

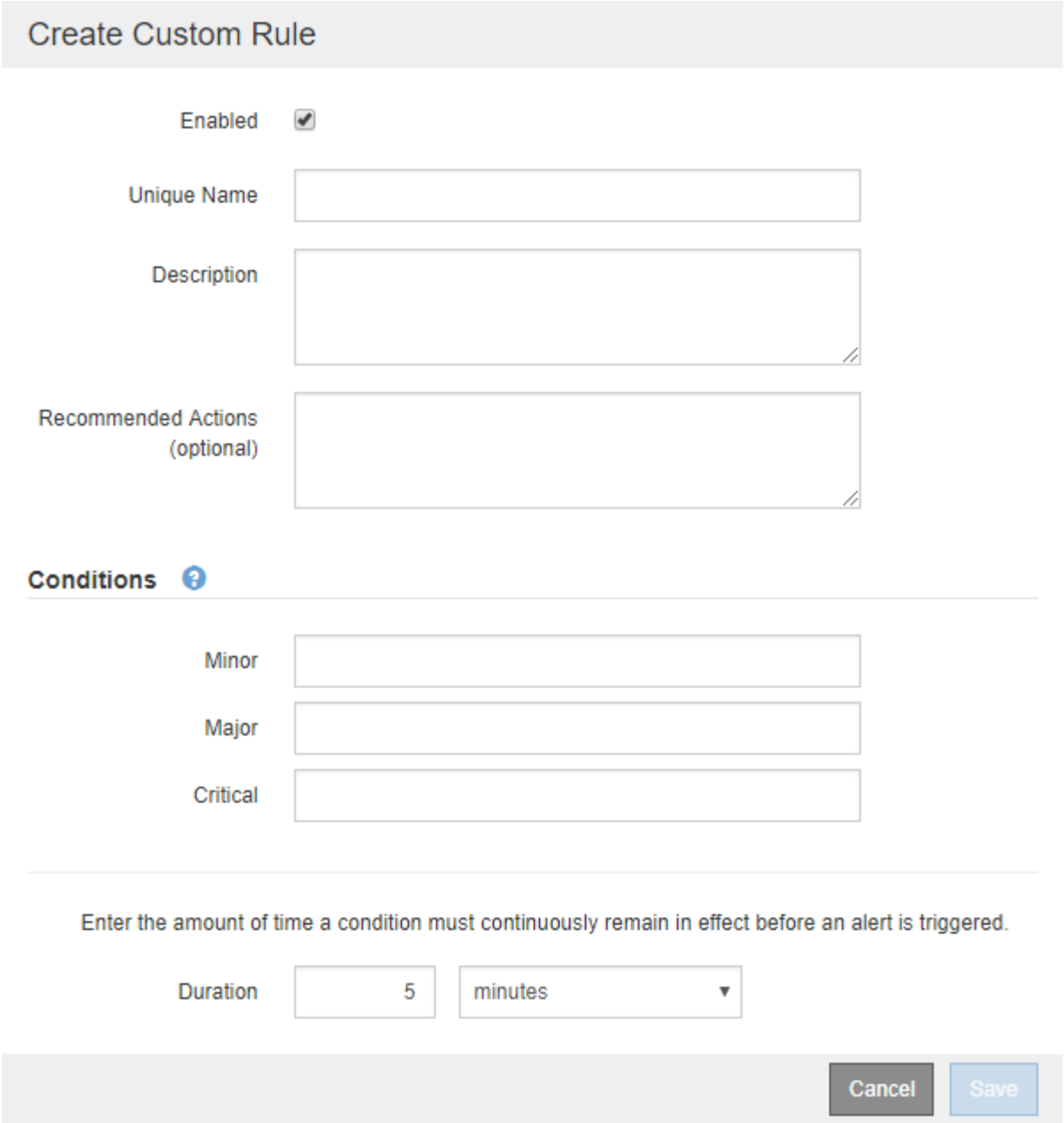
Fasi

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 relative 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root.

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.

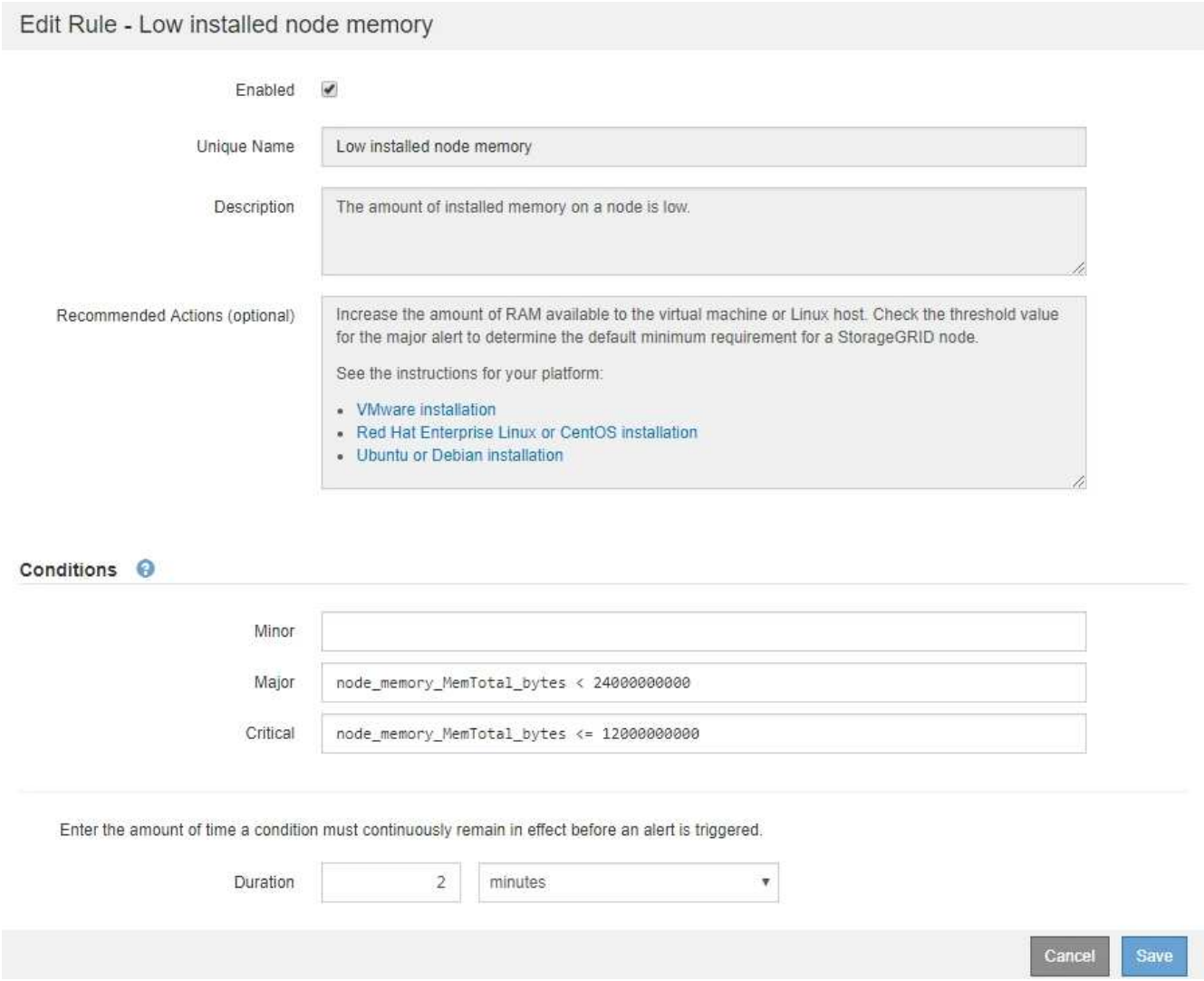
Fasi

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 relative 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.

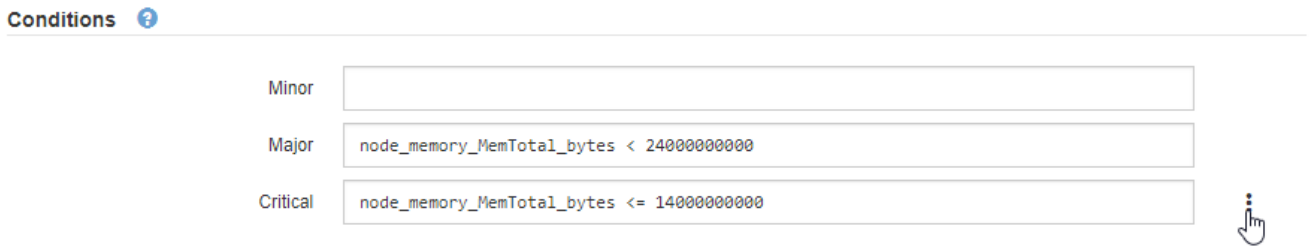
5. Per le regole di avviso personalizzate, aggiornare le seguenti informazioni secondo necessità.

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

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root.

A proposito di questa attività

Quando una regola di avviso viene disattivata, le relative 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 relative 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root.

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 di 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.

Le notifiche di avviso vengono inviate da qualsiasi nodo amministrativo configurato come mittente preferito. Per impostazione predefinita, viene selezionato il nodo di amministrazione principale. Vedere Istruzioni per l'amministrazione di StorageGRID.

> Le notifiche di trap e notifica vengono inviate anche quando determinati allarmi (sistema legacy) vengono attivati a livelli di gravità specificati o superiori; tuttavia, le notifiche SNMP non vengono inviate per ogni allarme o per ogni gravità. Vedere Allarmi che generano notifiche SNMP (sistema legacy).

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root.

A proposito di questa attività

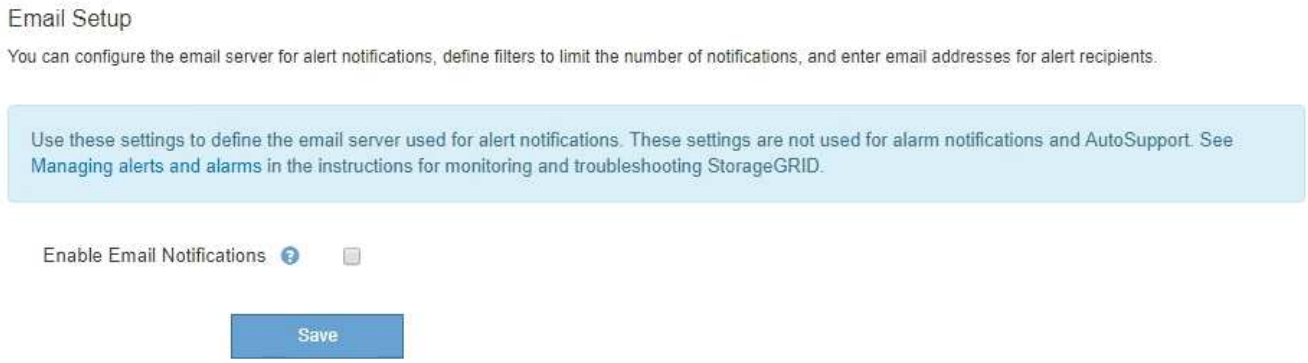
Poiché gli allarmi e gli avvisi sono sistemi indipendenti, la configurazione dell'e-mail utilizzata per le notifiche di avviso non viene utilizzata per le notifiche di allarme e i messaggi AutoSupport. Tuttavia, è possibile utilizzare lo stesso server di posta elettronica per tutte le notifiche.

Se l'implementazione di StorageGRID include più nodi di amministrazione, è possibile selezionare quale nodo di amministrazione deve essere il mittente preferito delle notifiche di avviso. Lo stesso "Preferred sender" viene utilizzato anche per le notifiche di allarme e i messaggi AutoSupport. Per impostazione predefinita, viene selezionato il nodo di amministrazione principale. Per ulteriori informazioni, vedere Istruzioni per l'amministrazione di StorageGRID.

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.

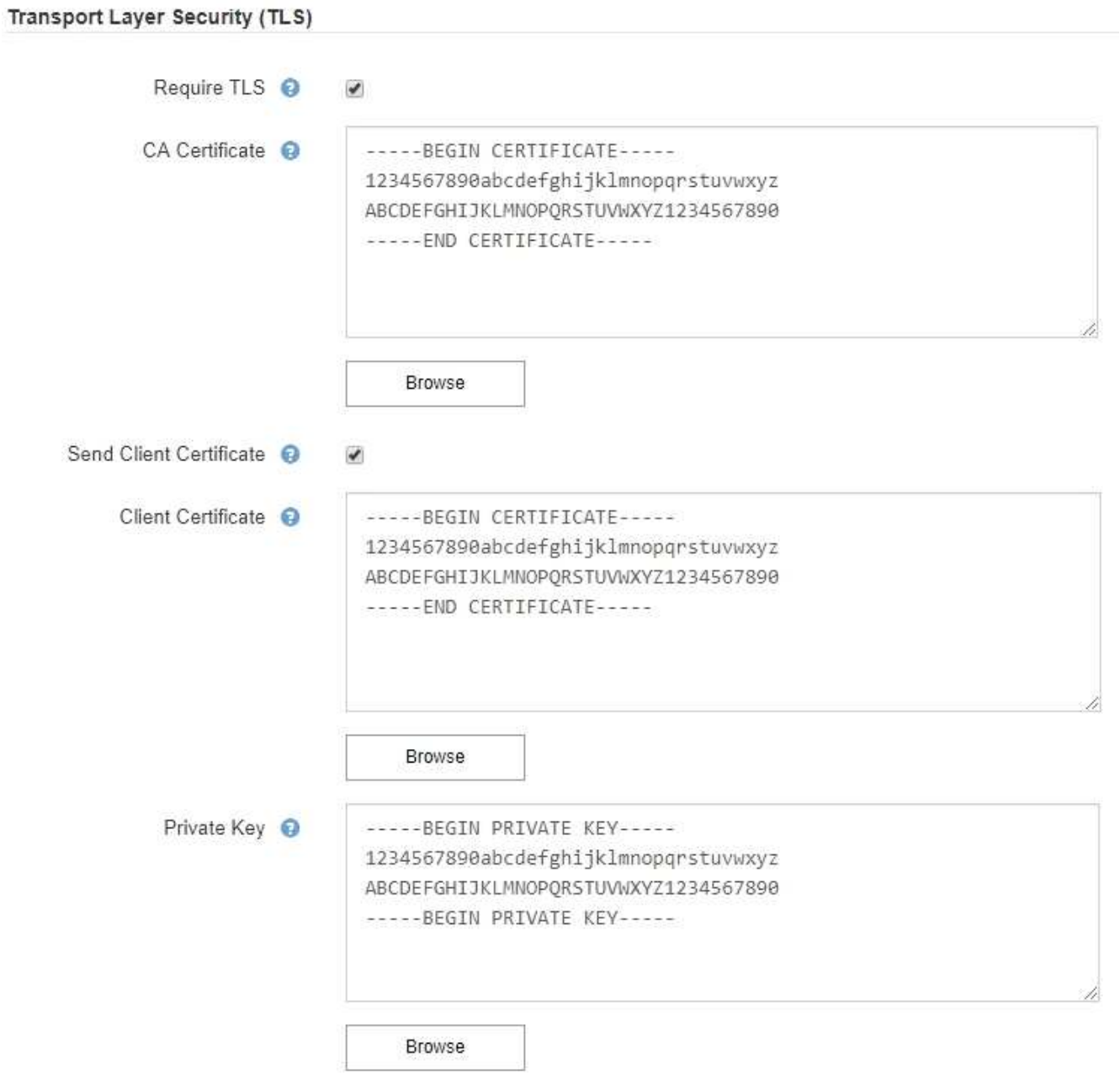
c. Nel campo **certificato client**, fornire il certificato client con codifica PEM da inviare al server SMTP.

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 delle notifiche di allarme e dei messaggi AutoSupport, in cui tutti i nodi amministrativi inviano l'email di test.

8. Selezionare **Salva**.

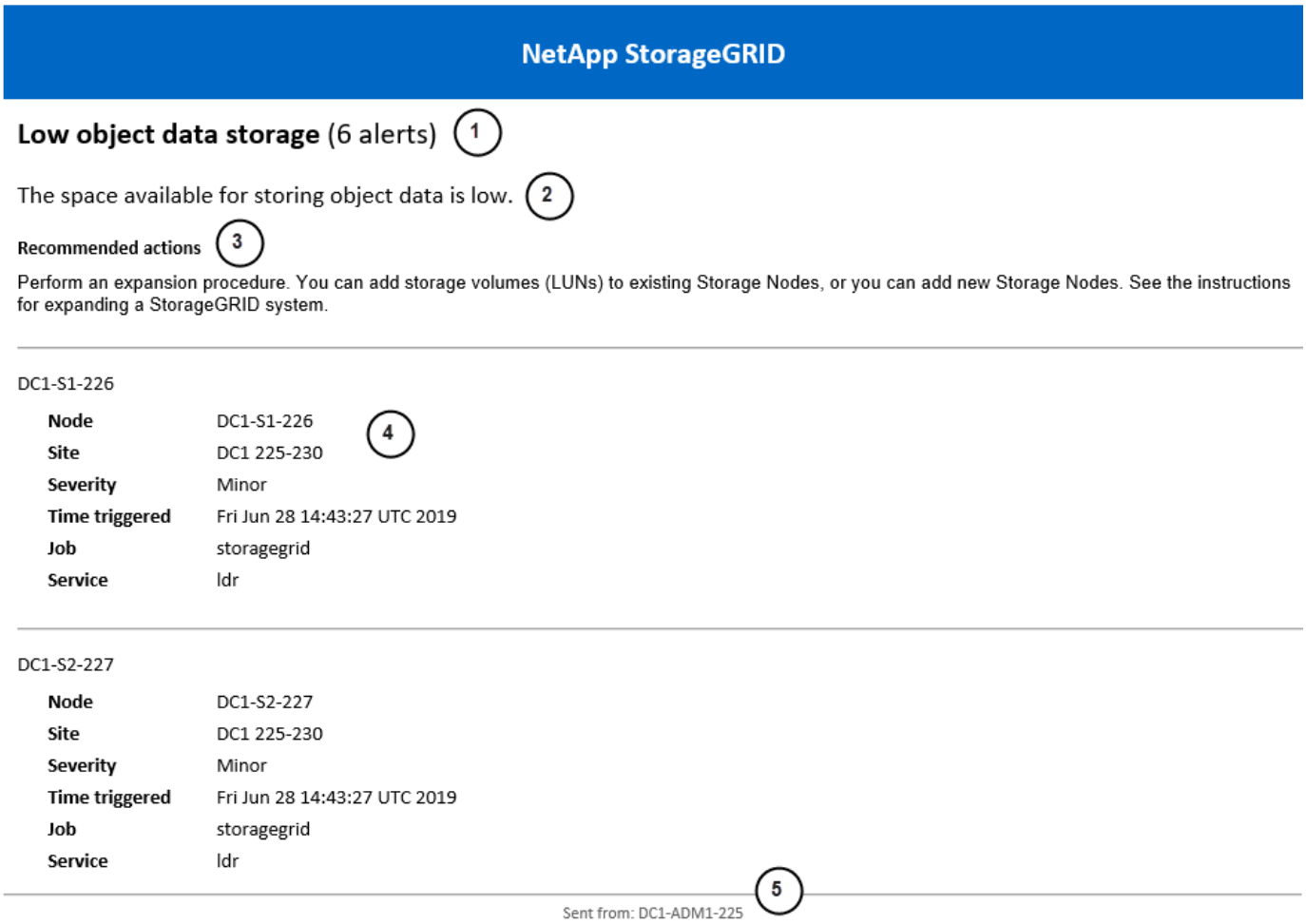
   L'invio di un'e-mail di prova non salva le impostazioni. Selezionare **Salva**.

   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. Viene attivato l'avviso A 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root.

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. Chiedere all'amministratore dell'e-mail 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci avvisi o accesso root.

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.

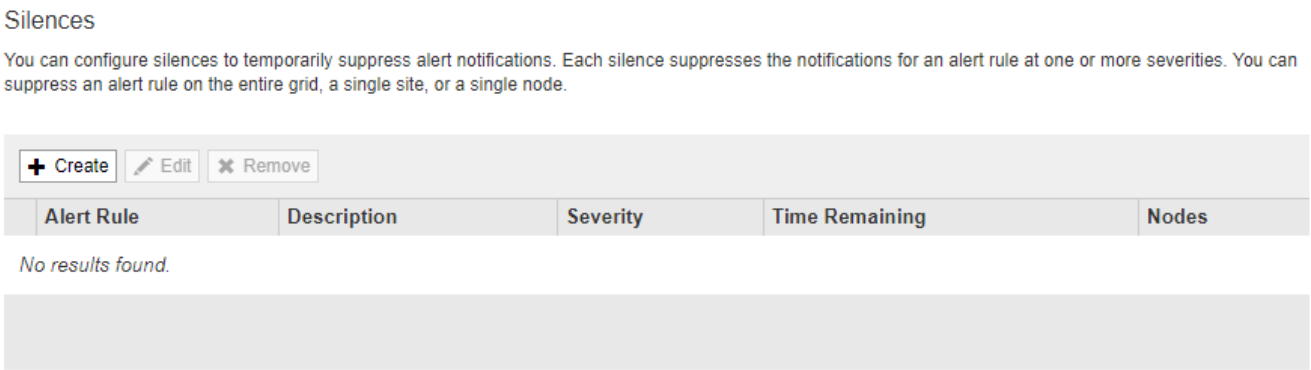
> Prestare attenzione quando si decide di tacitare una regola di avviso. Se si tacita un avviso, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

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

Fasi

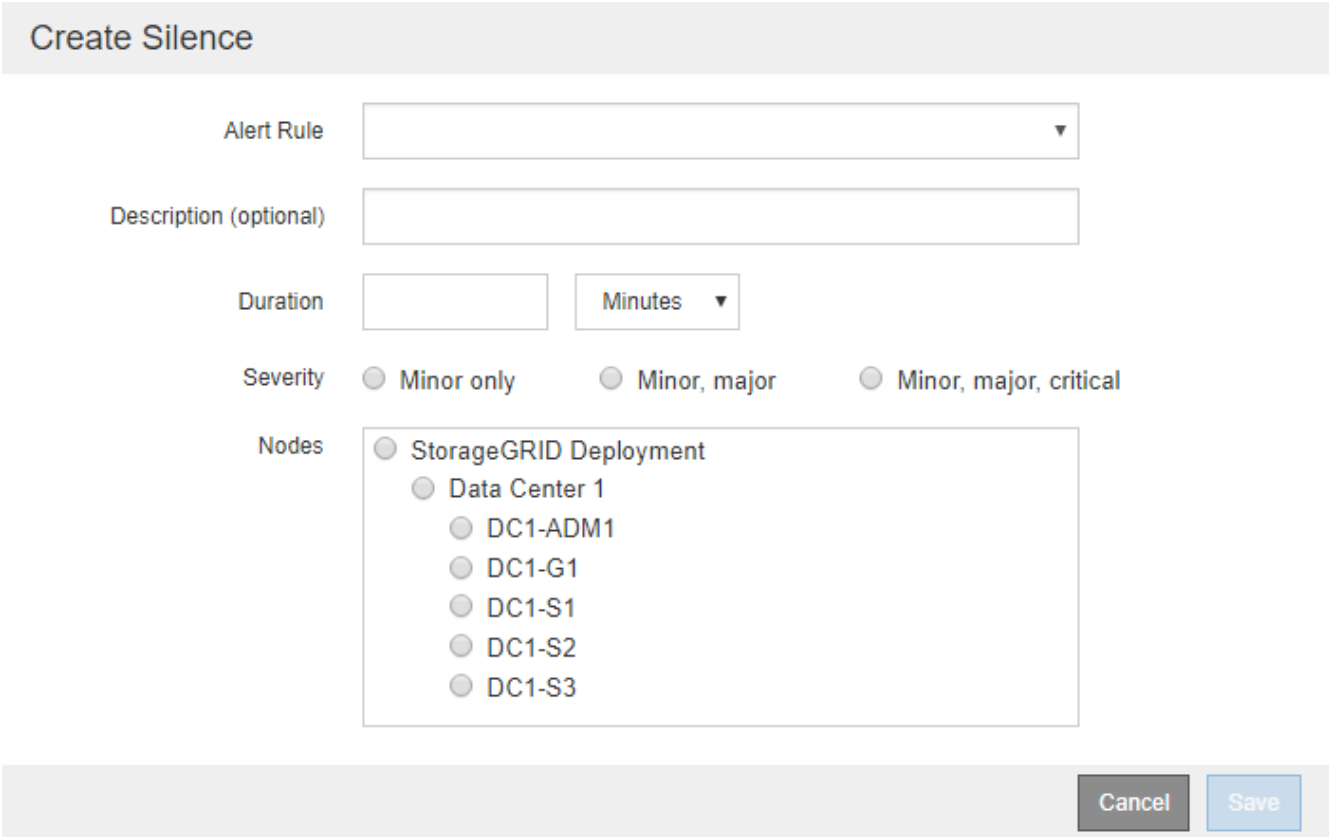
1. Selezionare **ALERTS silences**.

   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 ciascun 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

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 ciascun 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.

Icona	Colore	Severità degli allarmi	Significato
	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**

	Soglia di allarme Global Custom (abilitata)	Soglia di allarme predefinita (attivata)
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.

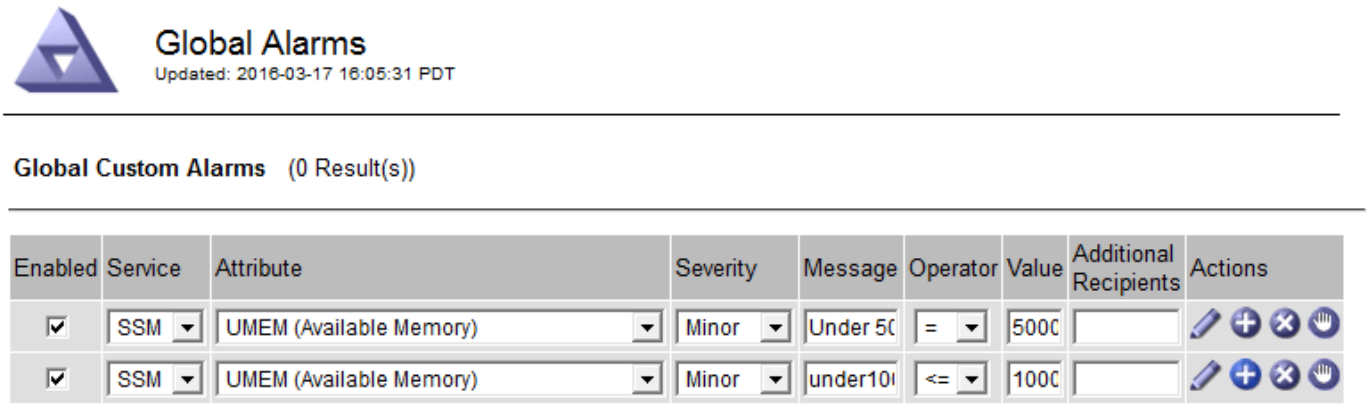
Dopo lo scenario precedente, se l'allarme Global Custom è disattivato, non cambia nulla. Il valore dell'attributo deve essere rivalutato prima che venga attivato un nuovo livello di allarme.

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.

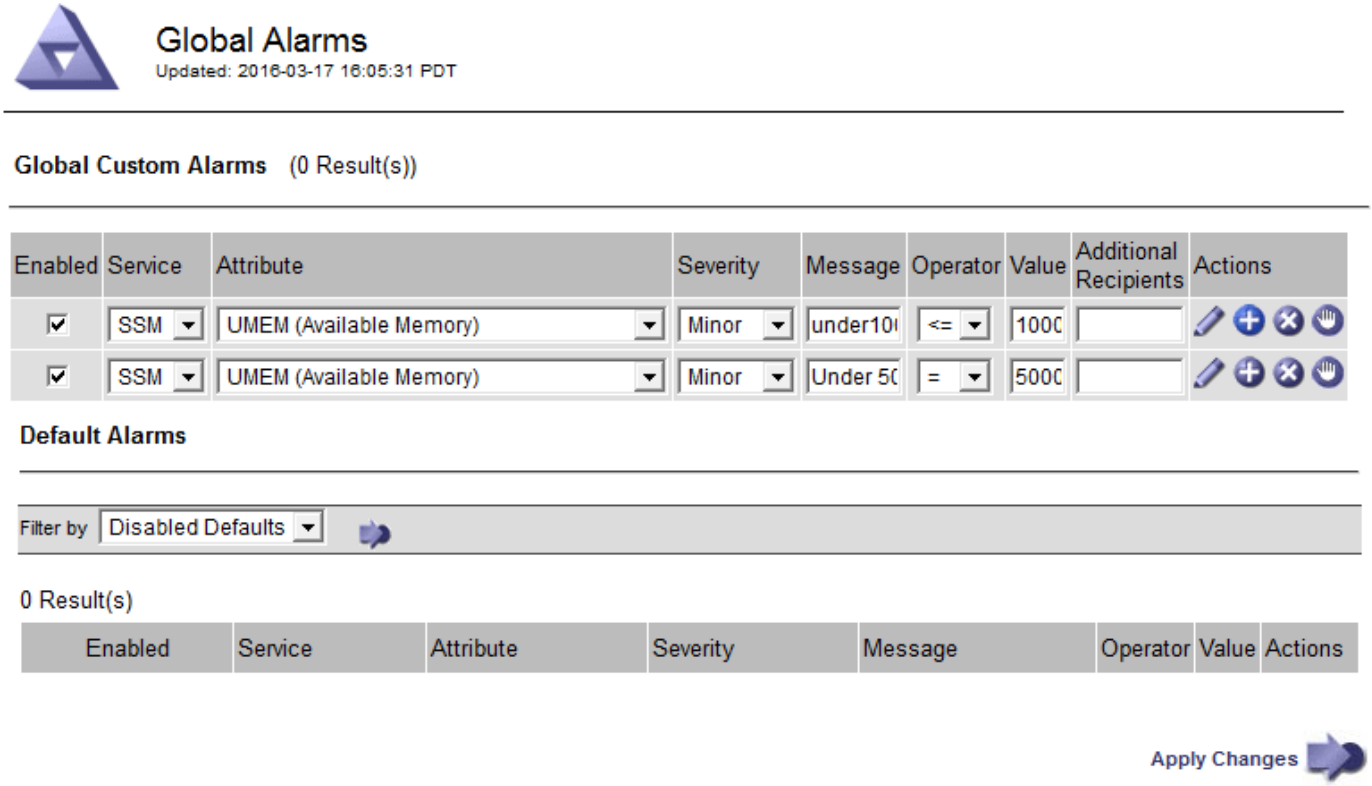
Allarmi della stessa severità

Se due allarmi Global Custom per lo stesso attributo hanno la stessa severità, gli allarmi vengono valutati con una priorità "top down".

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. Gli allarmi non possono essere disattivati per le 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.

Di cosa hai bisogno

- 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 (dal momento che 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

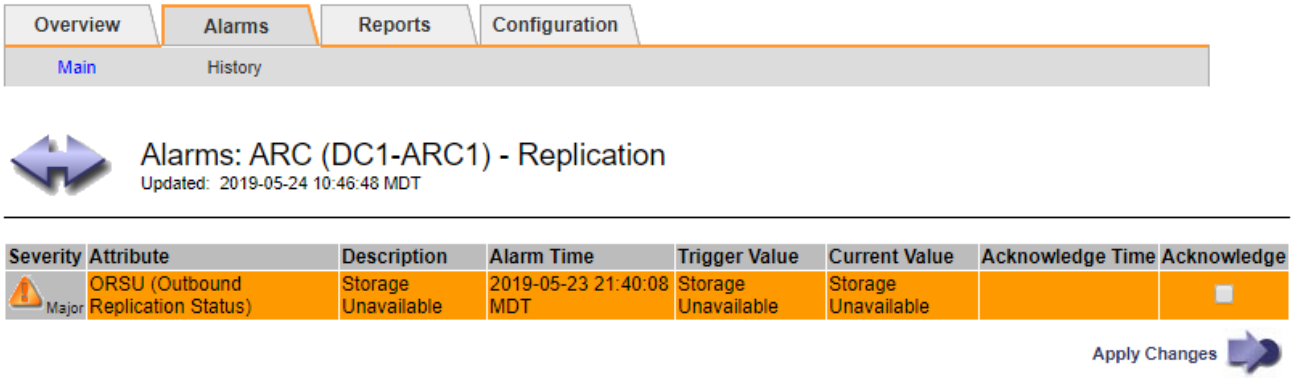
Show Acknowledged Alarms (1 - 1 of 1)

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 **Conferma** per l'allarme e fare clic su **Applica modifiche**.

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

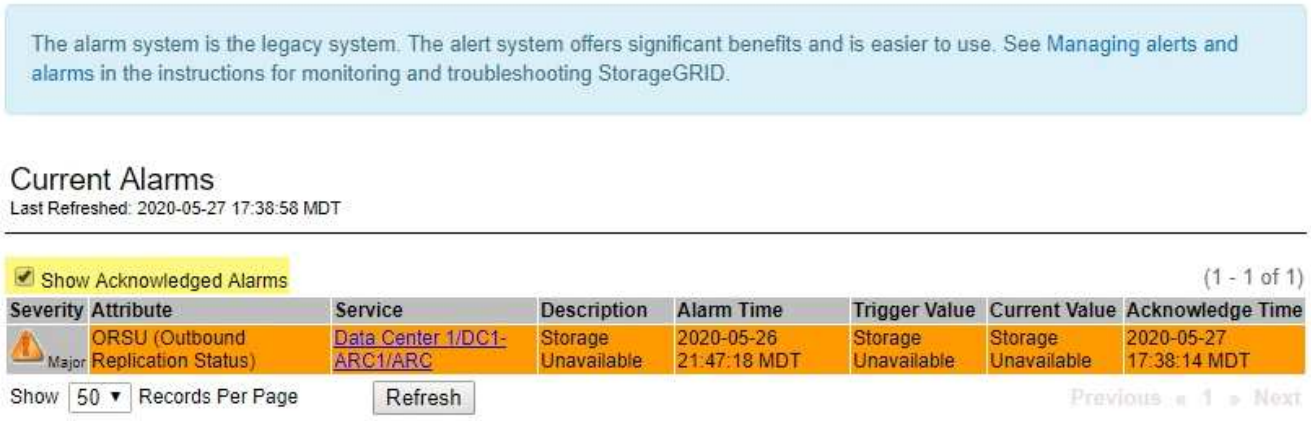
   > Quando si riconosce un allarme, la conferma non viene copiata in altri nodi di amministrazione. Per questo motivo, se si visualizza la dashboard da un altro nodo amministrativo, è possibile continuare a visualizzare l'allarme attivo.

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.

Di cosa hai bisogno

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

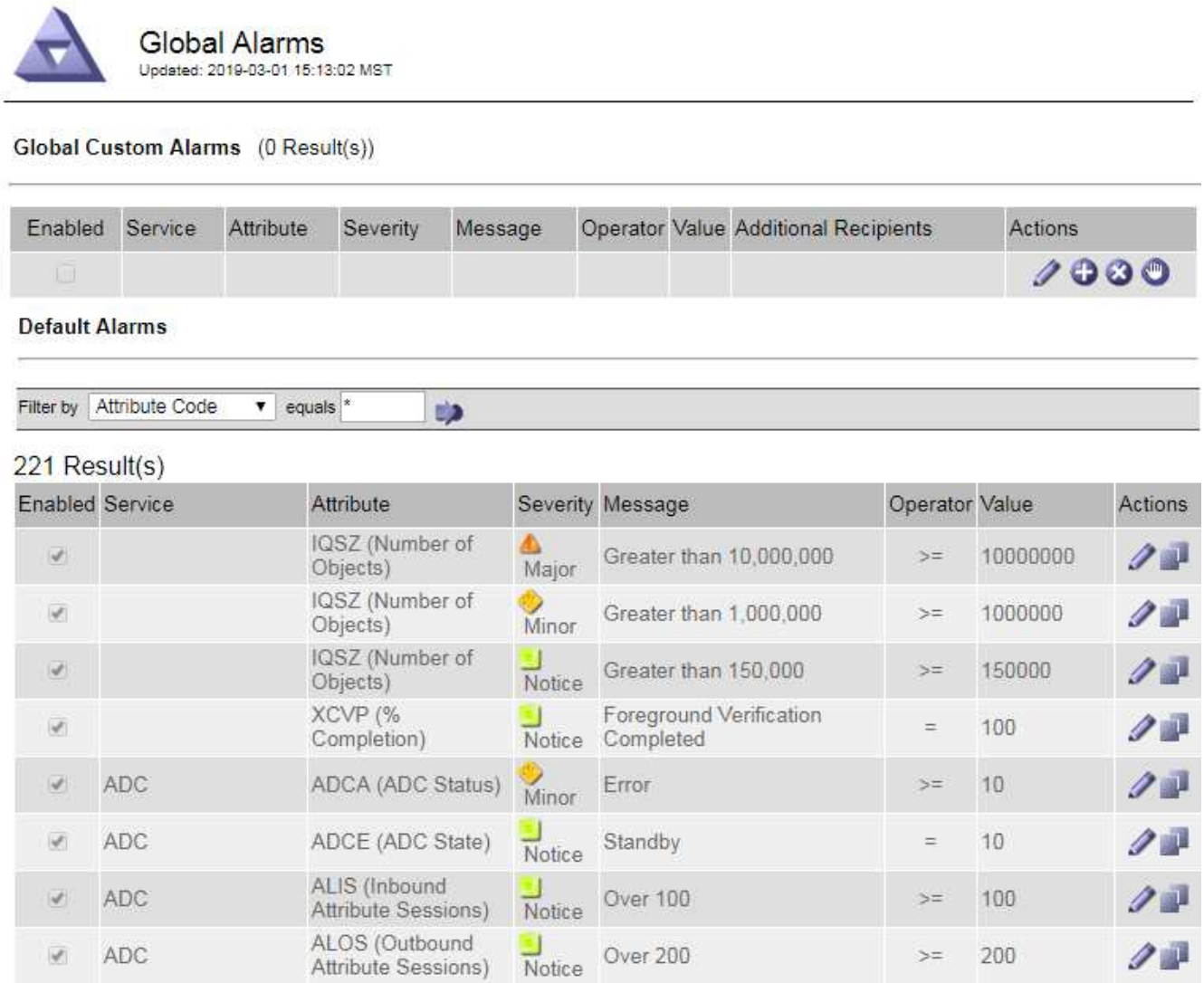
- È necessario disporre di autorizzazioni di accesso specifiche.

> 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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di 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 monitorare attributi che non hanno un allarme predefinito.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

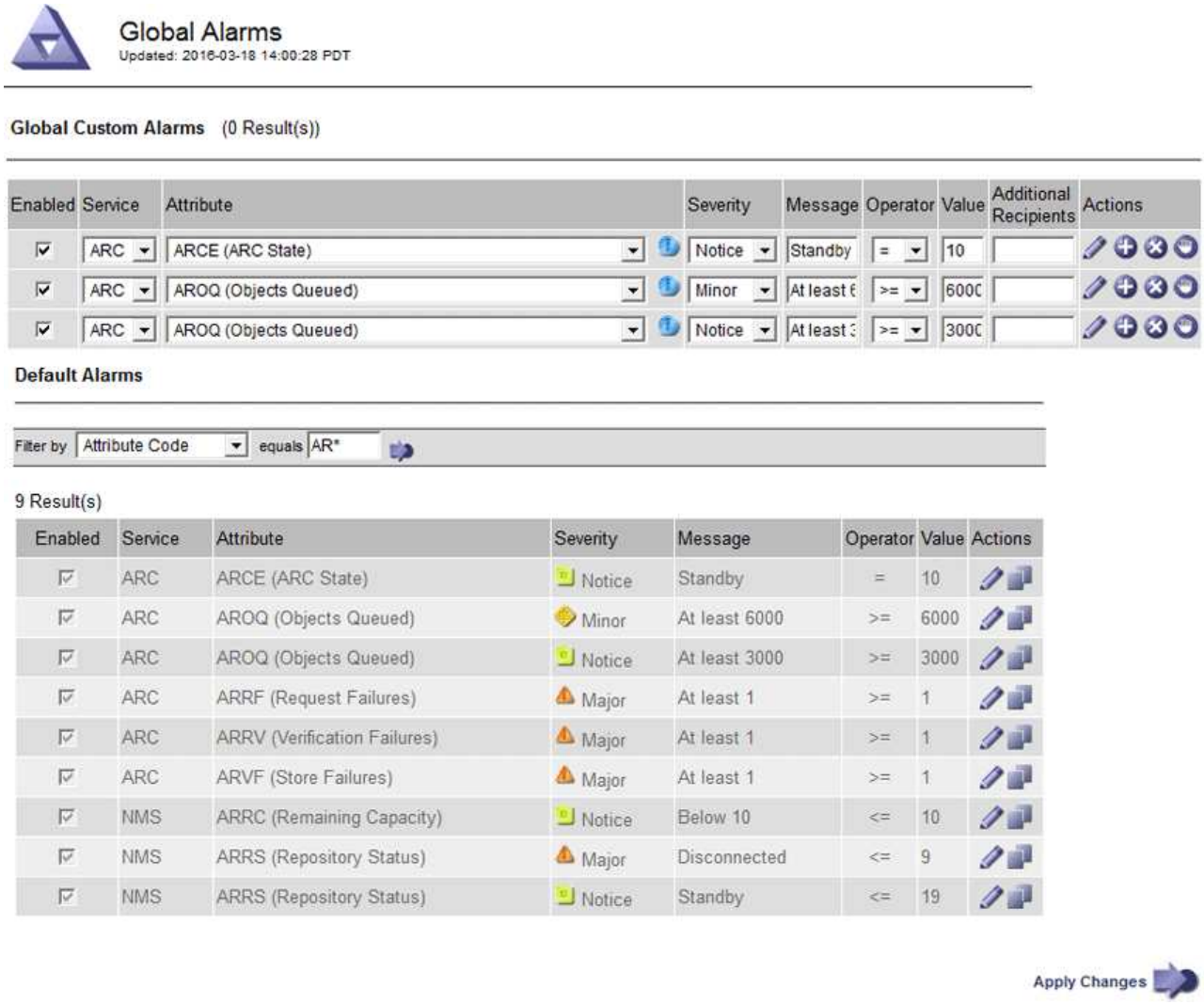
> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

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 molta 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 • inferiore a. • = 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 poter 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.

Intestazione	Descrizione
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. 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.

Di cosa hai bisogno

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

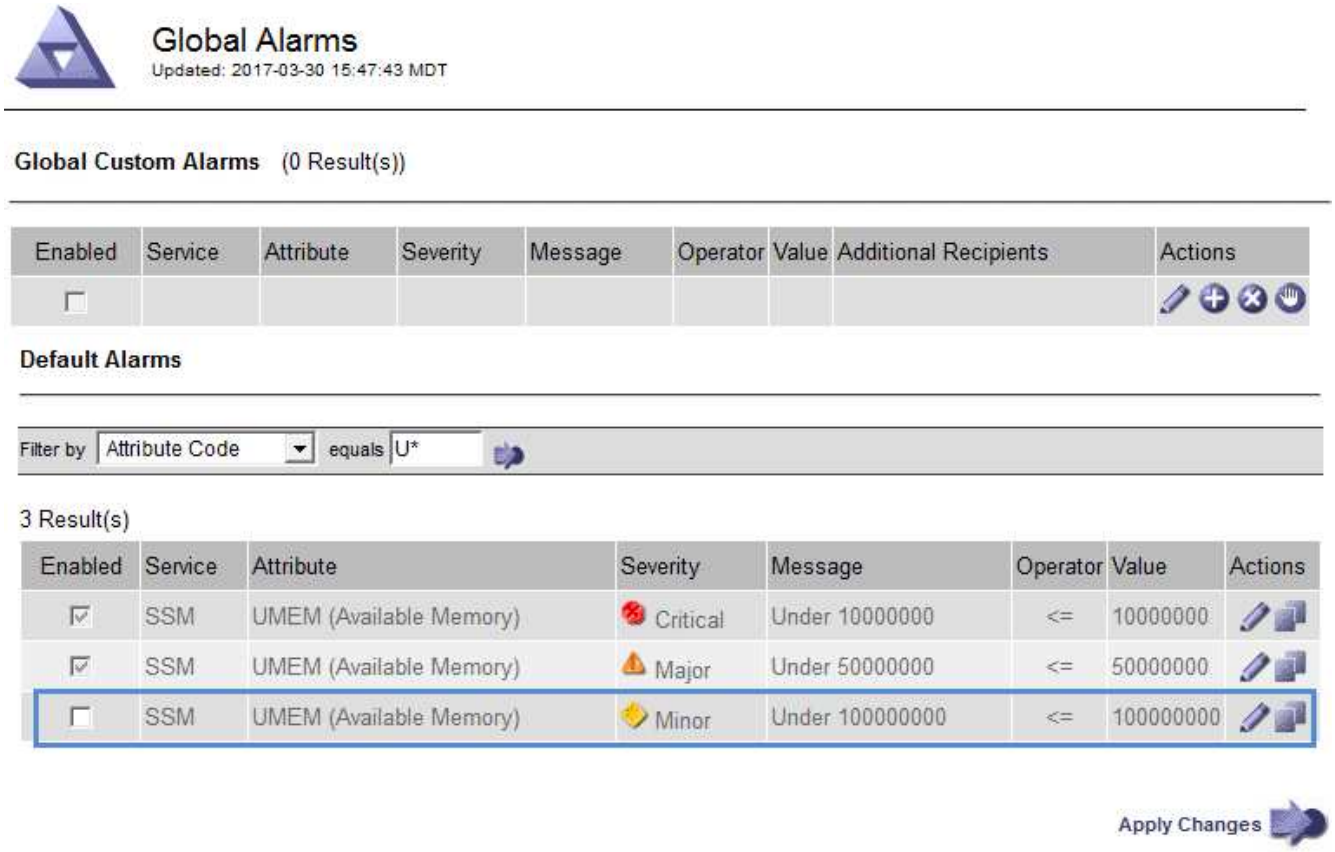
1. Selezionare **SUPPORTO Allarmi (legacy) Allarmi globali**.
2. Cercare l'allarme predefinito da disattivare.
   a. Nella sezione Allarmi predefiniti, selezionare **Filtra per Codice attributo** o **Nome attributo**.
   b. Digitare una stringa di ricerca.

      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.

Di cosa hai bisogno

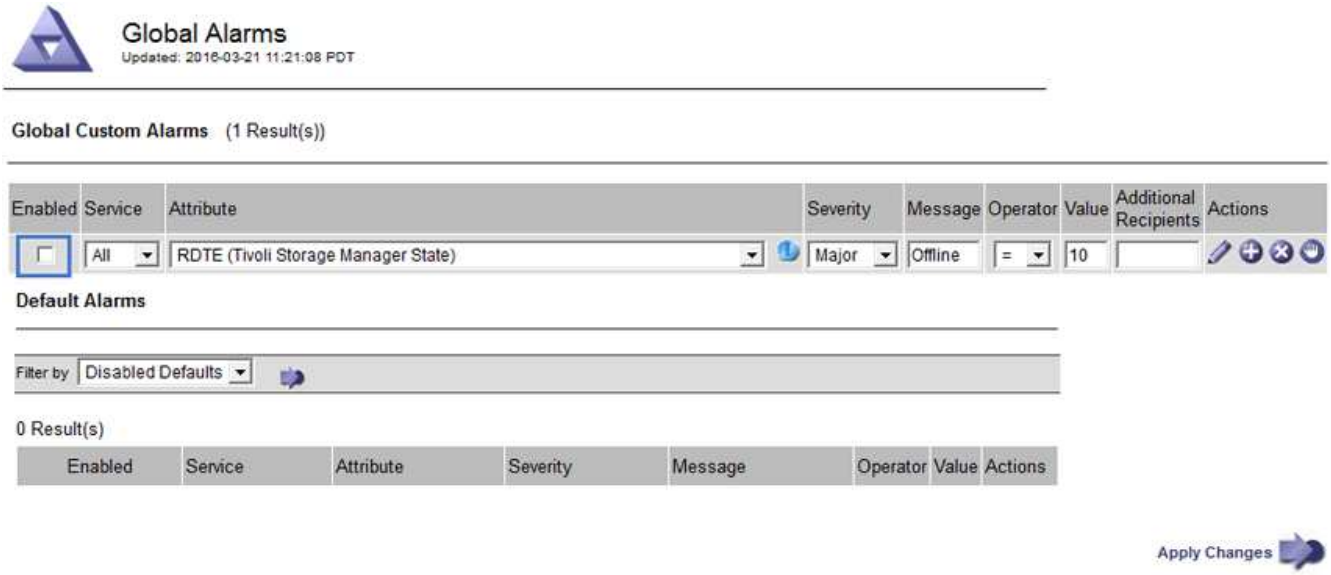
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

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.

Di cosa hai bisogno

- 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.

Di cosa hai bisogno

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

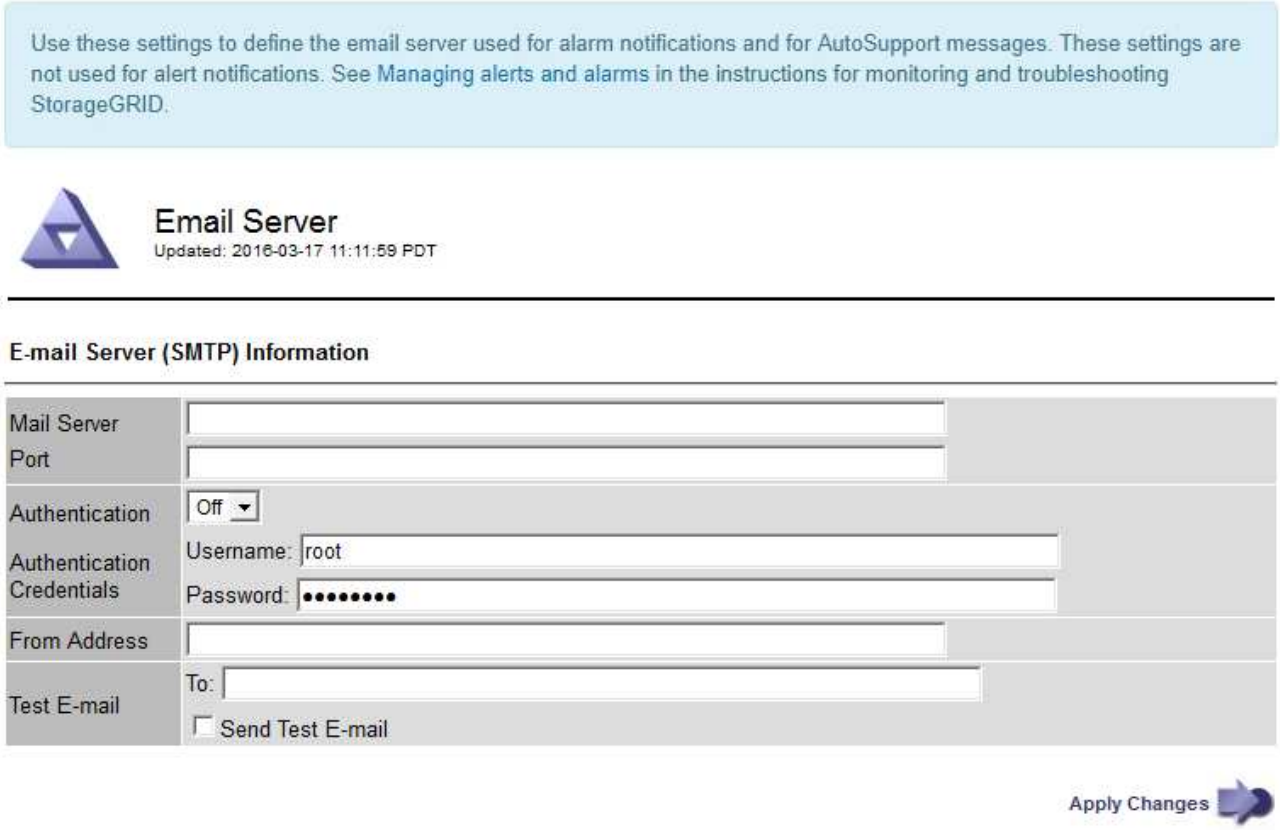
> Se si utilizza SMTP come protocollo per i messaggi AutoSupport, potrebbe essere già stato configurato un server di posta SMTP. Lo stesso server SMTP viene utilizzato per le notifiche e-mail di allarme, pertanto è possibile saltare questa procedura. Vedere Istruzioni per l'amministrazione di StorageGRID.

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 messaggi 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.

Elemento	Descrizione
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.
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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

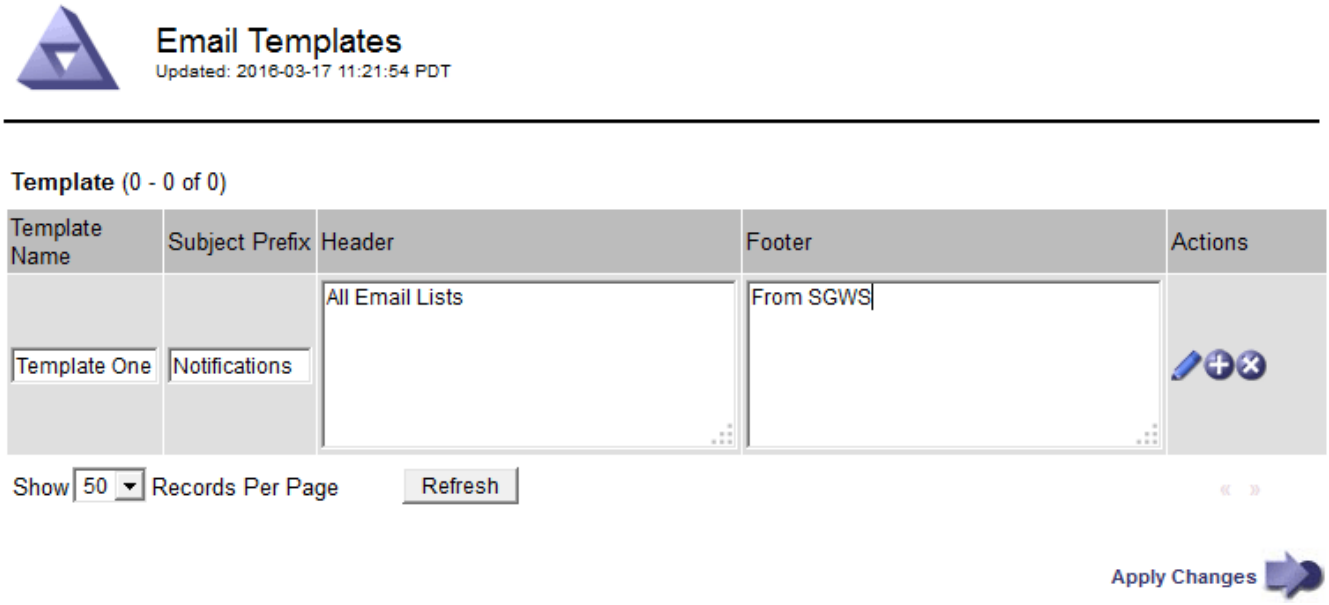
A proposito di questa attività

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 di posta elettronica.

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.

Di cosa hai bisogno

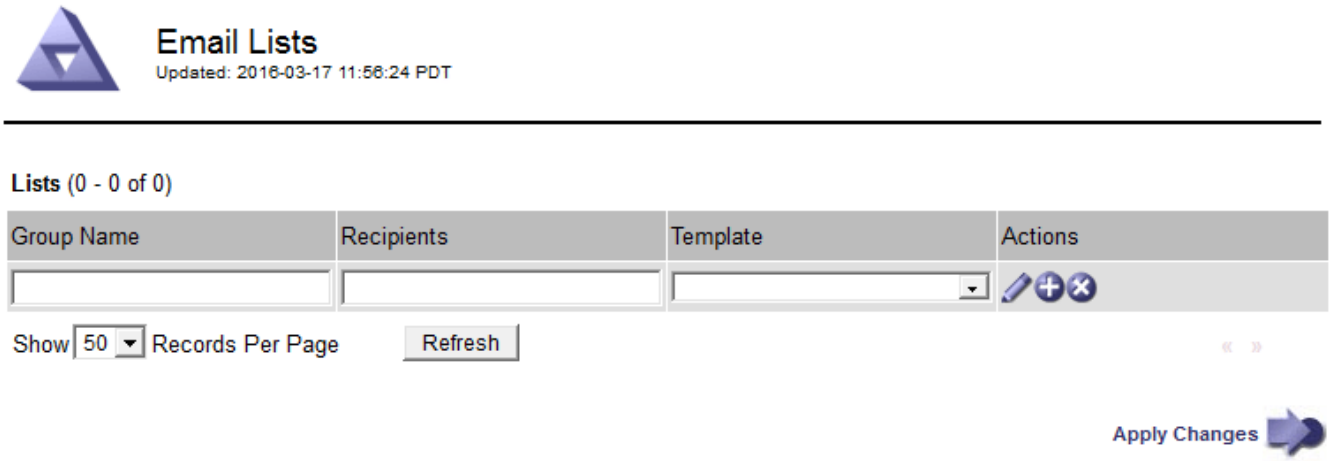
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si desidera specificare un modello e-mail per la mailing list (intestazione personalizzata, piè di pagina e oggetto), è necessario aver già creato il modello.

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.

Elemento	Descrizione
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.
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.

Di cosa hai bisogno

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

Di cosa hai bisogno

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

Elimina le notifiche e-mail a livello di sistema

È possibile bloccare la capacità del sistema StorageGRID di inviare notifiche e-mail per gli allarmi legacy e i messaggi AutoSupport attivati dagli eventi.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

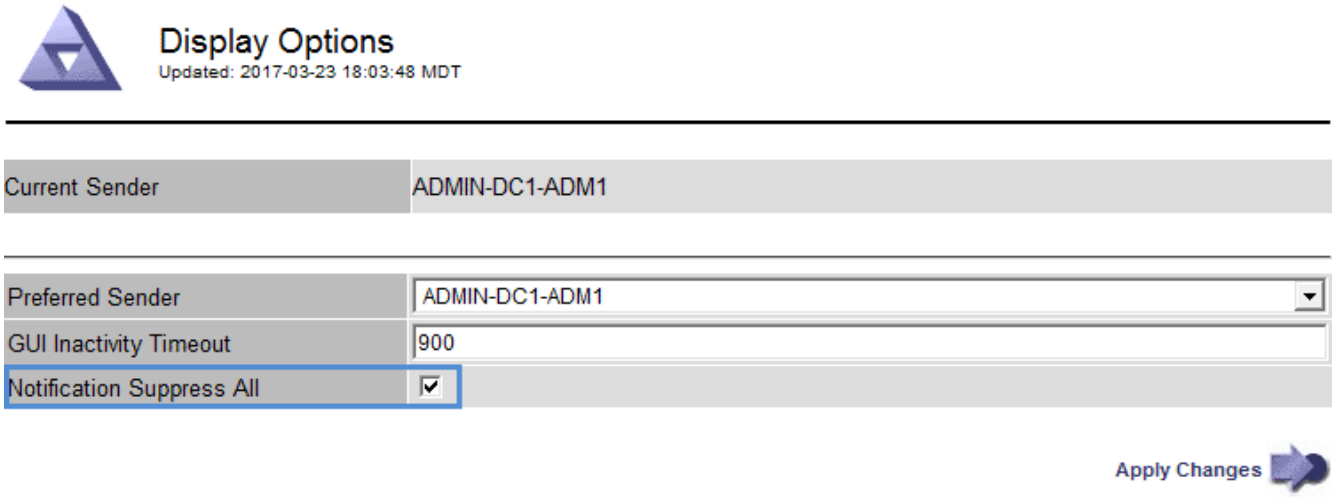
A proposito di questa attività

Utilizzare questa opzione per eliminare le notifiche e-mail per gli allarmi legacy e i messaggi AutoSupport attivati dagli eventi.

> Questa opzione non elimina le notifiche email di avviso. Inoltre, non elimina i messaggi AutoSupport settimanali o attivati dall'utente.

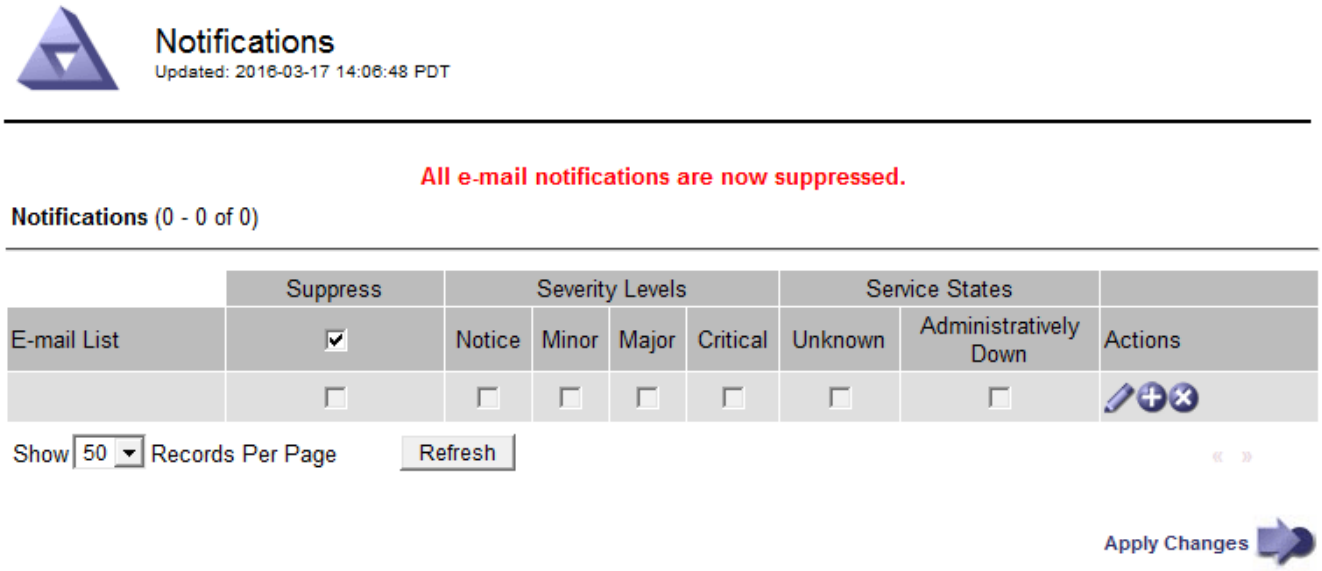
Fasi

1. Selezionare **CONFIGURAZIONE Impostazioni di sistema Opzioni di visualizzazione**.
2. Dal menu Display Options (Opzioni di visualizzazione), selezionare **Options** (Opzioni).
3. Selezionare **notifica Sospendi tutto**.



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

   Nella pagina Notifiche (**Configurazione Notifiche**) viene visualizzato il seguente messaggio:



Configurare i messaggi di audit e le destinazioni dei log

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. È possibile regolare i livelli di audit per aumentare o diminuire il tipo e il numero di messaggi di audit registrati. Facoltativamente, è possibile definire le intestazioni delle richieste HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client. È inoltre possibile configurare un server syslog esterno e modificare la destinazione delle informazioni di controllo.

Per ulteriori informazioni sui messaggi di audit, vedere Esaminare i registri di audit.

Di cosa hai bisogno

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

- Si dispone delle autorizzazioni di accesso Maintenance o Root.

A proposito di questa attività

Tutti i nodi StorageGRID generano messaggi di audit e registri per tenere traccia dell'attività e degli eventi del sistema. Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile regolare i livelli di audit per aumentare o diminuire il tipo e il numero di messaggi di audit registrati nel registro di audit. In alternativa, è possibile configurare le informazioni di controllo da inviare a un server syslog remoto o da memorizzare temporaneamente sui nodi di origine per la raccolta manuale.

Modificare i livelli dei messaggi di audit nel registro di audit

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

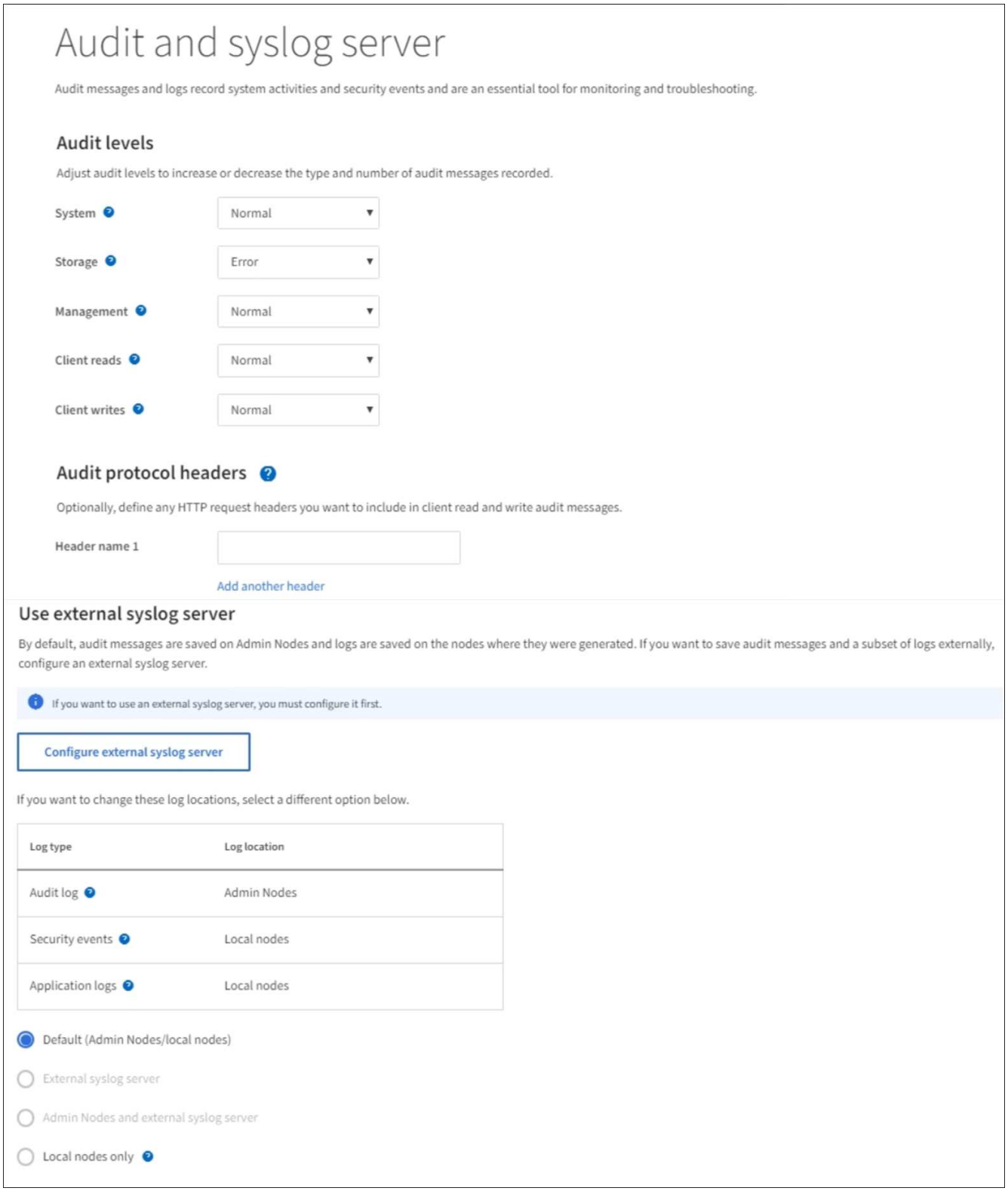
Categoria di audit	Descrizione
Sistema	Per impostazione predefinita, questo livello è impostato su normale. Vedere Messaggi di audit del sistema.
Storage	Per impostazione predefinita, questo livello è impostato su Error (errore). Vedere Messaggi di audit dello storage a oggetti.
Gestione	Per impostazione predefinita, questo livello è impostato su normale. Vedere Messaggio di audit della gestione.
Letture del client	Per impostazione predefinita, questo livello è impostato su normale. Vedere Messaggi di audit in lettura del client.
Il client scrive	Per impostazione predefinita, questo livello è impostato su normale. Vedere Messaggi di audit di scrittura del client.

Queste impostazioni predefinite si applicano se StorageGRID è stato installato inizialmente utilizzando la versione 10.3 o successiva. Se è stato eseguito l'aggiornamento da 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.

Livello di audit	Descrizione
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.

3. Facoltativamente, in **Audit Protocol headers**, definire le intestazioni delle richieste 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.

   Le intestazioni dei protocolli di audit si applicano solo alle richieste S3 e Swift.

4. 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**.

5. Selezionare **Salva**

   Viene visualizzato un banner verde per indicare che la configurazione è stata salvata correttamente.

Utilizzare un server syslog esterno

È possibile configurare un server syslog esterno se si desidera salvare le informazioni di audit in remoto.

- Se si desidera salvare le informazioni di controllo su un server syslog esterno, visitare il sito Web Configurare un server syslog esterno.
- Se non si utilizza un server syslog esterno, visitare il sito Web all'indirizzo Selezionare le destinazioni delle informazioni di audit.

Selezionare le destinazioni delle informazioni di audit

È possibile specificare dove inviare registri di audit, registri eventi di protezione e registri delle applicazioni.

Alcune destinazioni sono disponibili solo se si utilizza un server syslog esterno. Vedere Configurare un server syslog esterno per configurare un server syslog esterno.

Per ulteriori informazioni sui registri del software StorageGRID, vedere Log del software StorageGRID.

1. Nella pagina Audit and syslog server, selezionare la destinazione per le informazioni di audit dalle opzioni elencate:

Opzione	Descrizione
Predefinito (nodi amministrativi/nodi locali)	I messaggi di audit vengono inviati al registro di audit (`audit.log`) Nel nodo di amministrazione, i registri degli eventi di protezione e i registri delle applicazioni vengono memorizzati nei nodi in cui sono stati generati (anche denominati "nodo locale").
Server syslog esterno	Le informazioni di audit vengono inviate a un server syslog esterno e salvate sul nodo locale. 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 audit vengono inviati al registro di audit (`audit.log`) Sul nodo Admin e le informazioni di audit vengono inviate al server syslog esterno e salvate sul nodo locale. Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.
Solo nodi locali	Nessuna informazione di controllo viene inviata a un nodo di amministrazione o a un server syslog remoto. Le informazioni di audit vengono salvate solo sui nodi che le hanno generate. **Nota**: StorageGRID rimuove periodicamente questi 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.

Le informazioni di audit generate su ogni nodo locale sono memorizzate in `/var/local/log/localaudit.log`

1. Selezionare **Salva**.

Viene visualizzato un messaggio di avviso:

Modificare la destinazione del log?

1. Confermare che si desidera modificare la destinazione per le informazioni di controllo selezionando **OK**.

   Viene visualizzato un banner verde che informa che la configurazione dell'audit è stata salvata correttamente.

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

Informazioni correlate

Considerazioni sul server syslog esterno

Amministrare StorageGRID

Risolvere i problemi del server syslog esterno

Utilizzare un server syslog esterno

Considerazioni sul server syslog esterno

Utilizzare le seguenti linee guida per stimare le dimensioni del server syslog esterno necessario.

Che cos'è 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 configurare le destinazioni delle informazioni di audit in modo da ridurre il traffico di rete sui nodi di amministrazione e gestire le informazioni in modo più efficiente. 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

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	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

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

Utilizziamo K per rappresentare la dimensione media della somma dei nomi account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi 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	Velocità log di audit = 8 x S3 Operations Rate
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.
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	Chiave 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 nomi account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi 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 nomi account S3, del bucket S3 e della chiave S3. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi 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 tuo grid è dimensionato per 1,000 operazioni S3 al secondo, il tuo carico di lavoro è pari al 50% 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 2,250 log delle applicazioni al secondo e dovrebbe essere in grado di ricevere e ricevere (e in genere memorizzare) i dati delle applicazioni a una velocità di 0.6 MB al secondo.

Per ulteriori informazioni sulla configurazione dei livelli dei messaggi di controllo e di un server syslog esterno, vedere quanto segue:

- Configurare un server syslog esterno
- Configurare i messaggi di audit e le destinazioni dei log

Configurare un server syslog esterno

Se si desidera salvare registri di controllo, registri delle applicazioni e registri degli eventi di protezione in una posizione esterna alla griglia, utilizzare questa procedura per configurare un server syslog esterno.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone delle autorizzazioni di accesso Maintenance o Root.
- Si dispone di un server syslog in grado di ricevere e memorizzare i file di log. Per ulteriori informazioni, vedere Considerazioni sul server syslog esterno.
- Se si intende utilizzare TLS o RELP/TLS, si dispone delle certificazioni client e server corrette.

A proposito di questa attività

Se si desidera inviare le informazioni di controllo a un server syslog esterno, è necessario prima configurare il

server esterno.

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, log delle applicazioni ed eventi di sicurezza
- Riduci il traffico di rete sui nodi di amministrazione perché le informazioni di audit vengono trasferite direttamente dai vari nodi di storage al server syslog esterno, senza dover passare attraverso un nodo di amministrazione

> Quando i log vengono inviati a un server syslog esterno, i singoli log superiori a 8192 byte vengono troncati alla fine del messaggio per soddisfare le limitazioni comuni delle implementazioni esterne dei server syslog.

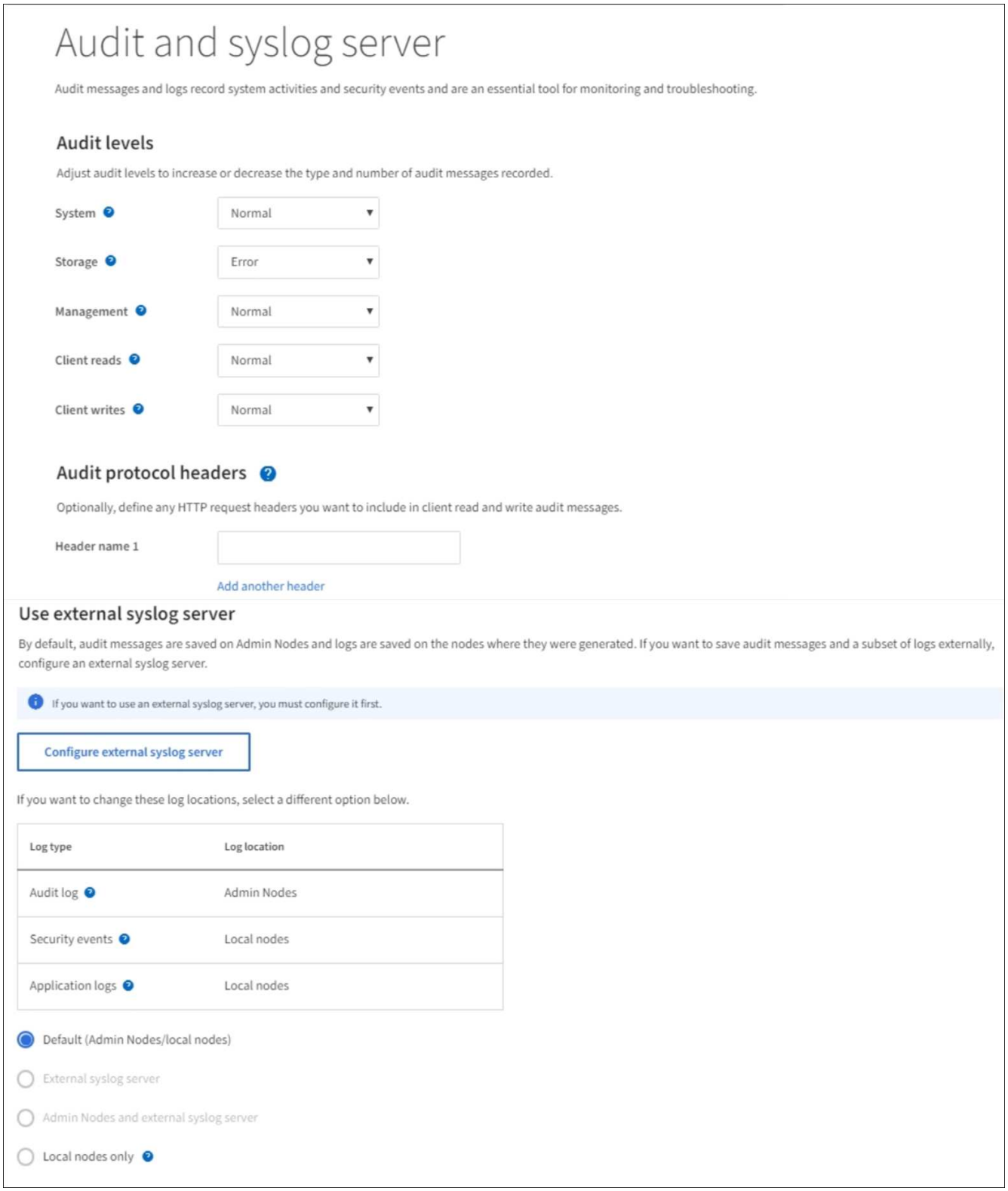
> Per massimizzare le opzioni per il ripristino completo dei dati in caso di guasto del server syslog esterno, su ciascun nodo vengono mantenuti fino a 20 GB di registri locali dei record di controllo (localaudit.log).

> Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili per soddisfare i requisiti, è possibile applicare ulteriori opzioni di configurazione utilizzando l'API privata `audit-destinations` endpoint. Ad esempio, è possibile utilizzare diversi server syslog per diversi gruppi di nodi.

Accedere alla configurazione guidata del server syslog

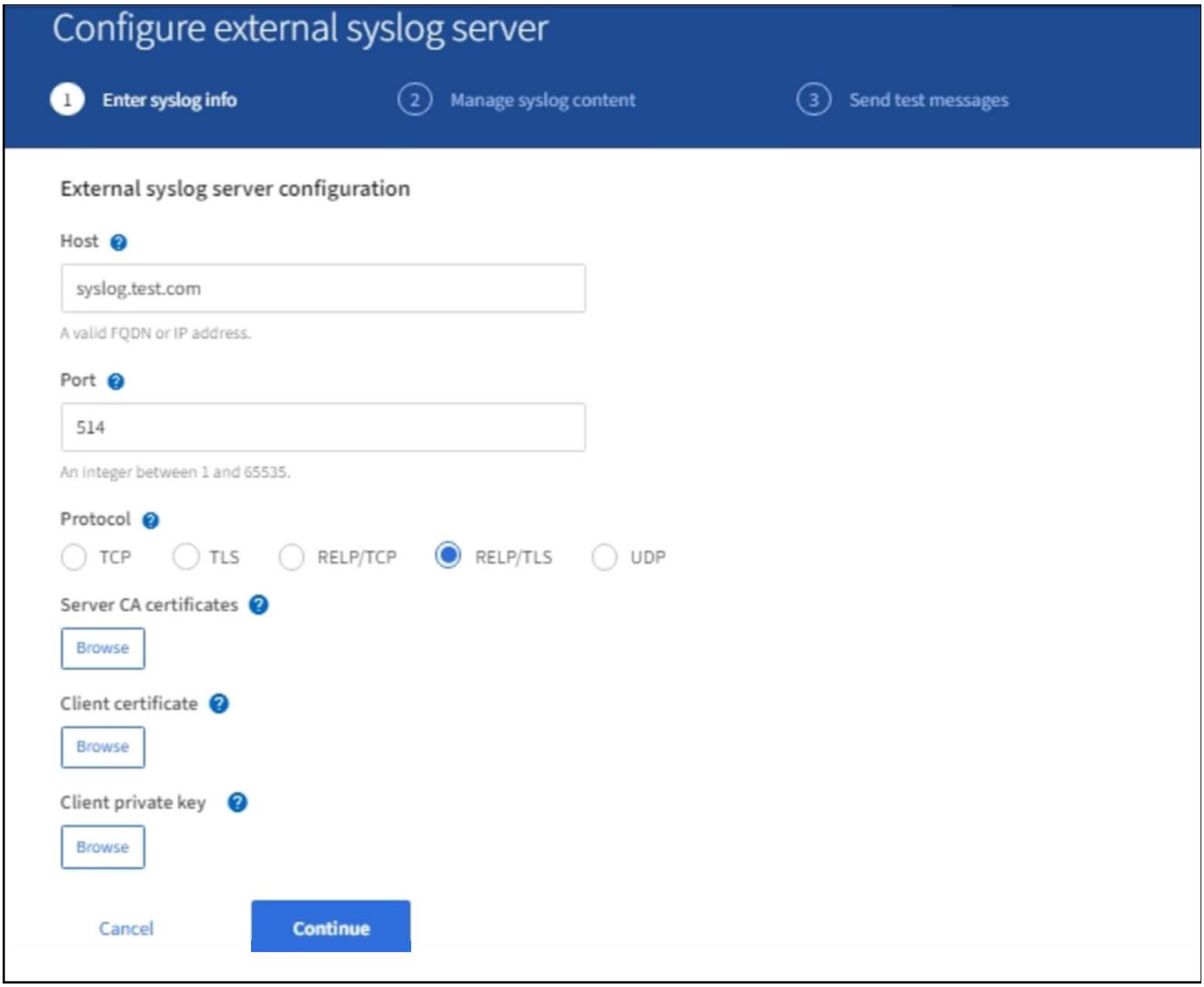
Fasi

1. Selezionare **CONFIGURATION Monitoring Audit and syslog server**.



2. Dalla pagina Audit and syslog server (controllo e server syslog), selezionare **Configure external syslog server** (Configura server syslog esterno Se in precedenza è stato configurato un server syslog esterno, selezionare **Edit external syslog server** (Modifica server syslog esterno).

Inserire le informazioni syslog



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

   Si consiglia 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 Utilizzare i certificati di sicurezza StorageGRID.

   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.

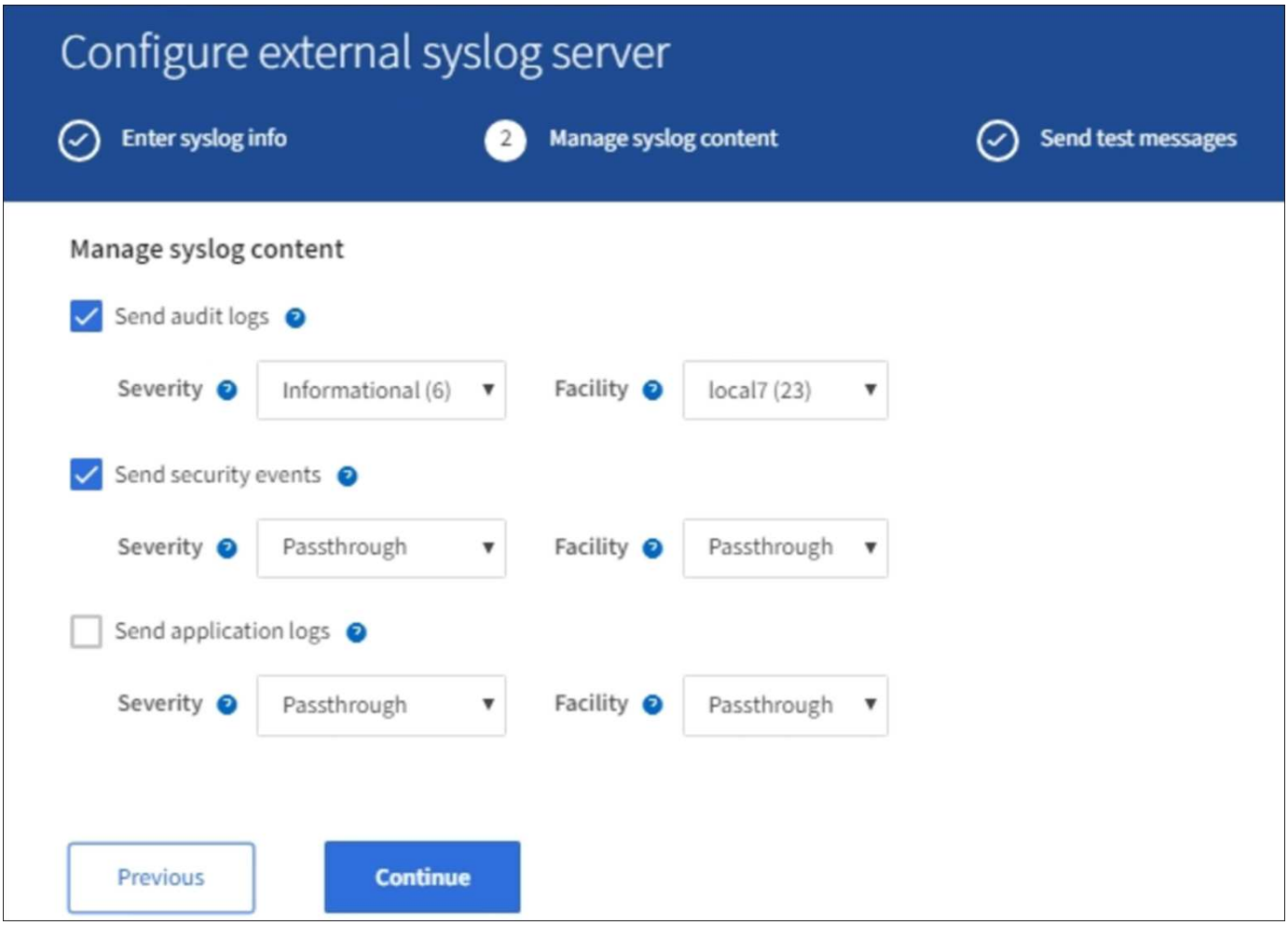
4. Selezionare **continua**.
5. se si seleziona **TLS** o **RELP/TLS**, caricare i seguenti certificati:
   - **Certificati CA del server**: Uno o più certificati CA attendibili per la verifica del server syslog esterno (con codifica PEM). Se omesso, verrà utilizzato il certificato Grid CA predefinito. Il file caricato qui potrebbe essere un bundle CA.
   - **Certificato client**: Certificato client per l'autenticazione al server syslog esterno (in codifica PEM).
   - **Chiave privata del client**: Chiave privata per il certificato del client (in 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.

     i. Selezionare **Sfoglia** per il certificato o la chiave che si desidera utilizzare.
     ii. Selezionare il file di certificato o il file delle chiavi.
     iii. 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.
6. Selezionare **continua**.

Gestire il contenuto syslog



1. Selezionare ciascun tipo di informazioni di controllo che si desidera inviare al server syslog esterno.
   - **Invia log di audit**: Eventi StorageGRID e attività di sistema
   - **Send Security events**: Eventi di sicurezza come quando un utente non autorizzato tenta di accedere o un utente accede come root
   - **Send application logs**: 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
2. Utilizzare i menu a discesa per selezionare la severità e la struttura (tipo di messaggio) per la categoria di informazioni di audit che si desidera inviare.

   Se si seleziona **Passthrough** per severità e struttura, le informazioni inviate al server syslog remoto riceveranno lo stesso livello di severità e struttura di cui hanno fatto l'accesso locale al nodo. L'impostazione della struttura e della severità consente di aggregare i registri in modi personalizzabili per semplificare l'analisi.

Per ulteriori informazioni sui registri del software StorageGRID, vedere Log del software StorageGRID.

a. Per **severità**, selezionare **Passthrough** se si desidera che ogni messaggio inviato al syslog esterno abbia lo stesso valore di severità del syslog locale.

   Per i registri di controllo, se si seleziona **Passthrough**, la severità è 'info'.

   Per gli eventi di sicurezza, se si seleziona **Passthrough**, i valori di severità vengono generati dalla distribuzione linux sui nodi.

   Per i registri delle applicazioni, se si seleziona **Passthrough**, le severità variano tra 'info' e 'notice', a seconda del problema. Ad esempio, l'aggiunta di un server NTP e la configurazione di un gruppo ha danno come valore "info", mentre l'interruzione intenzionale del servizio ssm o rsm dà come valore "notice".

b. Se non si desidera utilizzare il valore passthrough, selezionare un valore di severità compreso tra 0 e 7.

   Il valore selezionato verrà applicato a tutti i messaggi di questo tipo. Le informazioni relative ai diversi gradi di severità andranno perse quando si sceglie di eseguire l'override della severità con un valore fisso.

Severità	Descrizione
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
7	Debug: Messaggi a livello di debug

c. Per **Facility**, selezionare **Passthrough** se si desidera che ogni messaggio inviato al syslog esterno abbia lo stesso valore di Facility come nel syslog locale.

   Per i registri di controllo, se si seleziona **Passthrough**, la struttura inviata al server syslog esterno sarà 'local7'.

   Per gli eventi di sicurezza, se si seleziona **Passthrough**, i valori della struttura vengono generati dalla distribuzione linux sui nodi.

   Per i log delle applicazioni, se si seleziona **Passthrough**, i log delle applicazioni inviati al server syslog

esterno hanno i seguenti valori di struttura:

Log dell'applicazione	Valore passthrough
bycast.log	utente o daemon
bycast-err.log	user, daemon, local3 o local4
jaeger.log	locale2
nms.log	locale3
prometheus.log	locale4
raft.log	locale5
hagroups.log	locale6

d. Se non si desidera utilizzare il valore passthrough, selezionare il valore della struttura compreso tra 0 e 23.

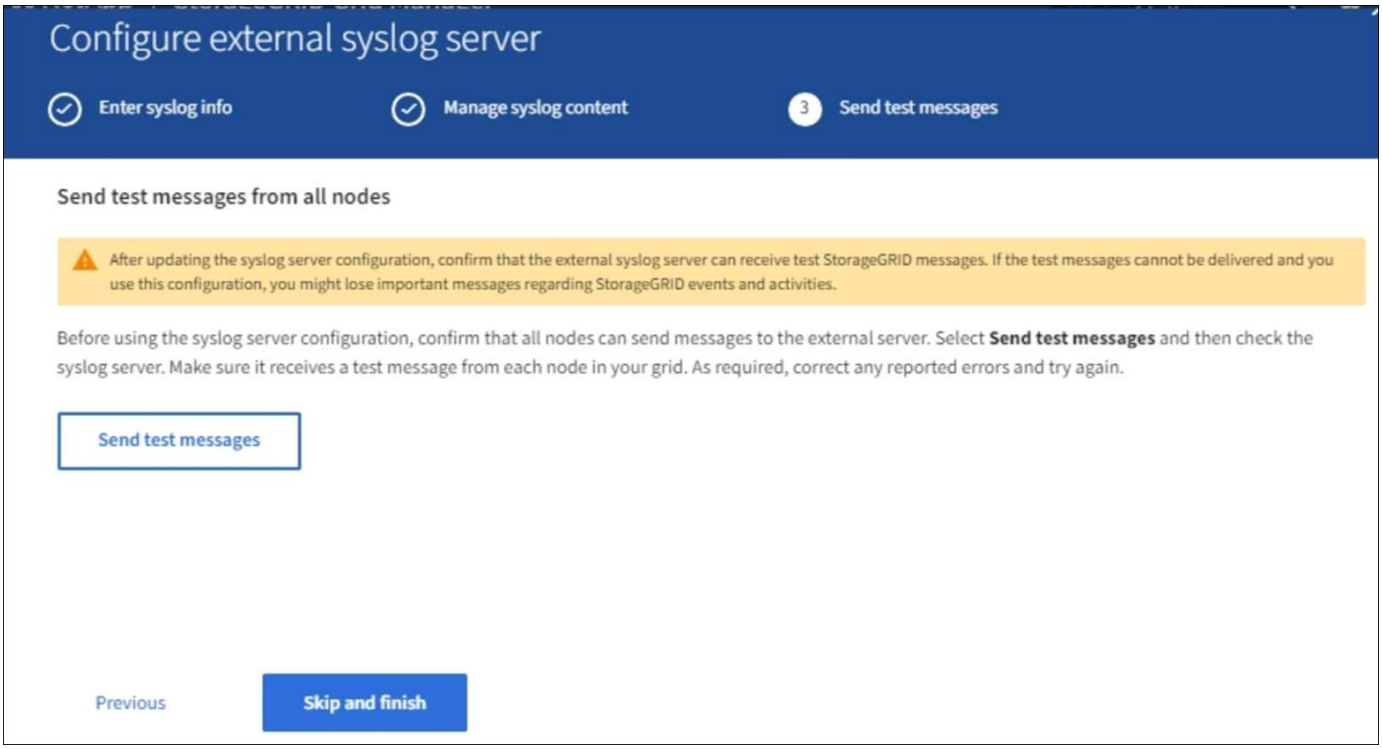
   Il valore selezionato verrà applicato a tutti i messaggi di questo tipo. Le informazioni relative alle diverse strutture andranno perse quando si sceglie di eseguire l'override della struttura con un valore fisso.

Struttura	Descrizione
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)
8	UUCP
9	cron (daemon di clock)

Struttura	Descrizione
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.

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

   Viene visualizzato un banner verde per indicare che la configurazione è stata salvata correttamente.

2. In caso contrario, selezionare **Invia messaggi di prova**.

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

3. Se si ricevono errori, correggerli e selezionare di nuovo **Invia messaggi di prova**. Vedere Risoluzione dei problemi relativi al 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 gli altri protocolli.

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

Viene nuovamente visualizzata la pagina **Audit and syslog server**. Viene visualizzato un banner verde che informa che la configurazione del server syslog è stata salvata correttamente.

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

Selezionare le destinazioni delle informazioni di audit

È possibile specificare dove inviare i registri degli eventi di protezione, i registri delle applicazioni e i registri dei messaggi di controllo.

> Per ulteriori informazioni sui registri del software StorageGRID, vedere Log del software StorageGRID.

1. Nella pagina Audit and syslog server, selezionare la destinazione per le informazioni di audit dalle opzioni elencate:

Opzione	Descrizione
Predefinito (nodi amministrativi/nodi locali)	I messaggi di audit vengono inviati al registro di audit (`audit.log`) Nel nodo di amministrazione, i registri degli eventi di protezione e i registri delle applicazioni vengono memorizzati nei nodi in cui sono stati generati (anche denominati "nodo locale").
Server syslog esterno	Le informazioni di audit vengono inviate a un server syslog esterno e salvate sul nodo locale. 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 audit vengono inviati al registro di audit (`audit.log`) Sul nodo Admin e le informazioni di audit vengono inviate al server syslog esterno e salvate sul nodo locale. Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.
Solo nodi locali	Nessuna informazione di controllo viene inviata a un nodo di amministrazione o a un server syslog remoto. Le informazioni di audit vengono salvate solo sui nodi che le hanno generate. **Nota**: StorageGRID rimuove periodicamente questi 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.

> Le informazioni di audit generate su ogni nodo locale sono memorizzate in `/var/local/log/localaudit.log`

1. Selezionare **Salva**. Quindi, selezionare OK per accettare la modifica alla destinazione del registro.
2. Se si seleziona **External syslog server** o **Admin Node and external syslog server** come destinazione per le informazioni di controllo, viene visualizzato un ulteriore avviso. Esaminare il testo dell'avviso.

> È necessario confermare che il server syslog esterno possa ricevere messaggi StorageGRID di prova.

1. Confermare che si desidera modificare la destinazione per le informazioni di controllo selezionando **OK**.

   Viene visualizzato un banner verde che informa che la configurazione dell'audit è stata salvata correttamente.

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

Informazioni correlate

Panoramica dei messaggi di audit

Configurare i messaggi di audit e le destinazioni dei log

Messaggi di audit del sistema

Messaggi di audit dello storage a oggetti

Messaggio di audit della gestione

Messaggi di audit in lettura del client

Amministrare StorageGRID

Utilizzare il monitoraggio SNMP

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

- Configurare l'agente SNMP
- Aggiornare l'agente SNMP

Funzionalità

Ogni nodo StorageGRID esegue un agente SNMP, o daemon, che fornisce una base di informazioni di gestione (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.

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:

- **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 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 qualsiasi nodo amministrativo configurato come 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 una descrizione degli avvisi che possono attivare questi trap, vedere Riferimenti agli avvisi.

- Alcuni allarmi (sistema legacy) vengono attivati a livelli di severità 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	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	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.

Accedere al MIB

È possibile accedere al file di definizione MIB nella seguente posizione su qualsiasi nodo StorageGRID:

```
/usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt
```

Informazioni correlate

- Riferimenti agli avvisi
- Riferimento allarmi (sistema legacy)
- Allarmi che generano notifiche SNMP (sistema legacy)
- Tacitare le notifiche di avviso

Configurare l'agente SNMP

È possibile configurare l'agente SNMP StorageGRID se si desidera utilizzare un sistema di gestione SNMP di terze parti per l'accesso MIB di sola lettura e le notifiche.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root.

A proposito di questa attività

L'agente SNMP StorageGRID supporta tutte e tre le versioni del protocollo SNMP. È possibile configurare l'agente per una o più versioni.

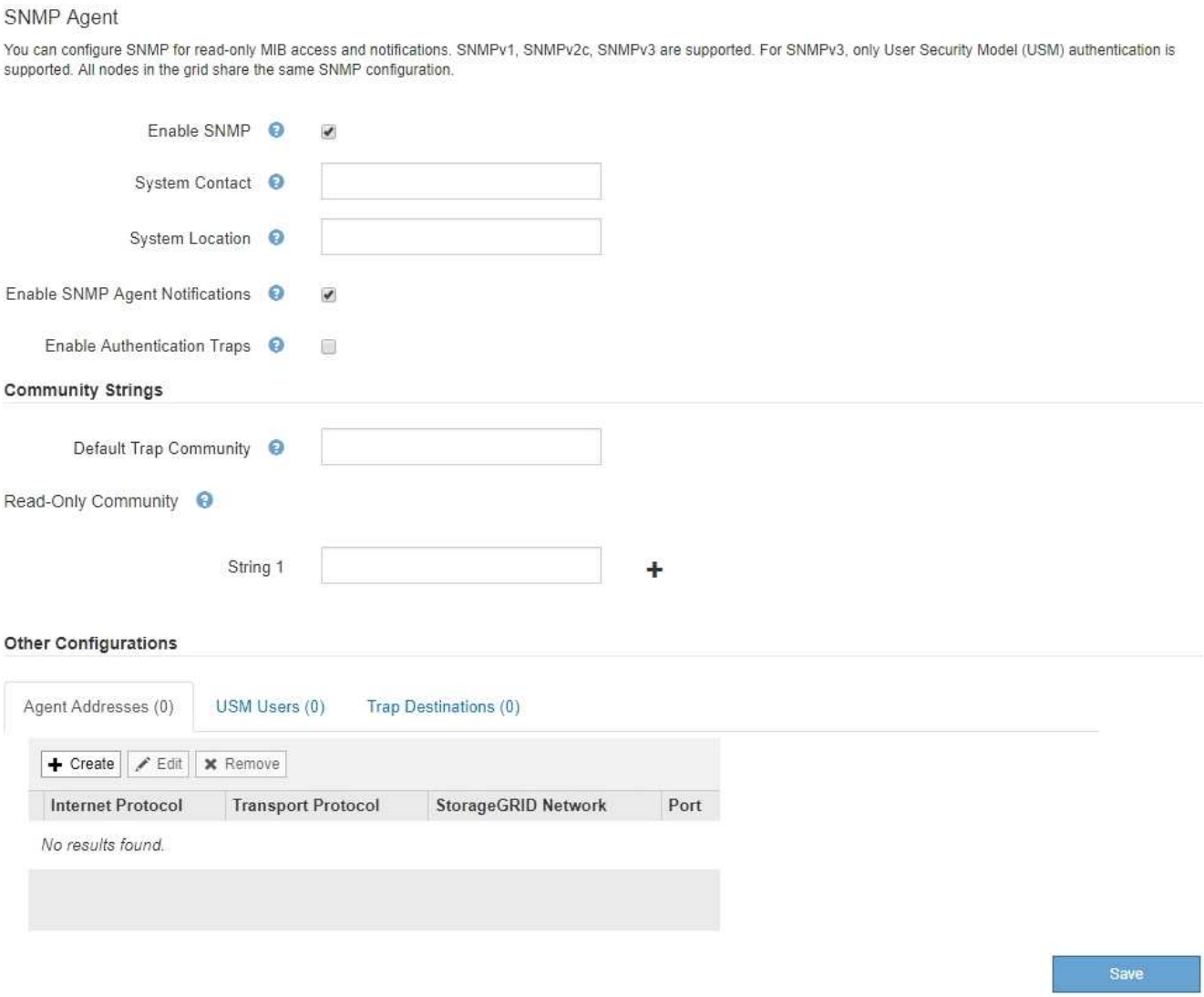
Fasi

1. Selezionare **CONFIGURAZIONE monitoraggio agente SNMP**.

   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).

   Vengono visualizzati i campi per la configurazione di un agente SNMP.



3. Nel campo **contatto di sistema**, immettere il valore che StorageGRID deve fornire nei messaggi SNMP per sysContact.

   Il contatto di sistema in genere è un indirizzo e-mail. Il valore fornito si applica a tutti i nodi nel sistema StorageGRID. **Il campo System Contact** può contenere al massimo 255 caratteri.

4. Nel campo **posizione sistema**, immettere il valore che si desidera che StorageGRID fornisca nei messaggi SNMP per sysLocation.

   La posizione del sistema può essere qualsiasi informazione utile per identificare la posizione del sistema StorageGRID. Ad esempio, è possibile utilizzare l'indirizzo di una struttura. Il valore fornito si applica a tutti i nodi nel sistema StorageGRID. **System Location** può contenere un massimo di 255 caratteri.

5. Mantenere selezionata la casella di controllo **attiva notifiche agente SNMP** se si desidera che l'agente SNMP StorageGRID invii messaggi trap e avvisi.

   Se questa casella di controllo non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.

6. Selezionare la casella di controllo **attiva trap di autenticazione** se si desidera che l'agente SNMP di StorageGRID invii una trap di autenticazione se riceve un messaggio di protocollo autenticato in modo errato.

7. Se si utilizza SNMPv1 o SNMPv2c, completare la sezione Community Strings.

   I campi di questa sezione vengono utilizzati per l'autenticazione basata sulla community in SNMPv1 o SNMPv2c. Questi campi non si applicano a SNMPv3.

   a. Nel campo **Default Trap Community** (Comunità trap predefinita), immettere facoltativamente la stringa di comunità predefinita che si desidera utilizzare per le destinazioni trap.

      Se necessario, è possibile fornire una stringa di community diversa ("custom") definire una destinazione trap specifica.

      Default Trap Community può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

   b. Per **Read-only Community**, immettere una o più stringhe di comunità per consentire l'accesso MIB di sola lettura sugli indirizzi degli agenti IPv4 e IPv6. Fare clic sul segno più ➕ per aggiungere più stringhe.

      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.

      Ogni stringa di comunità può contenere un massimo di 32 caratteri e non può contenere spazi vuoti. Sono consentite fino a cinque stringhe.

      > ⓘ Per garantire la sicurezza del sistema StorageGRID, non utilizzare "public" come stringa di community. Se non si immette una stringa di comunità, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa di comunità.

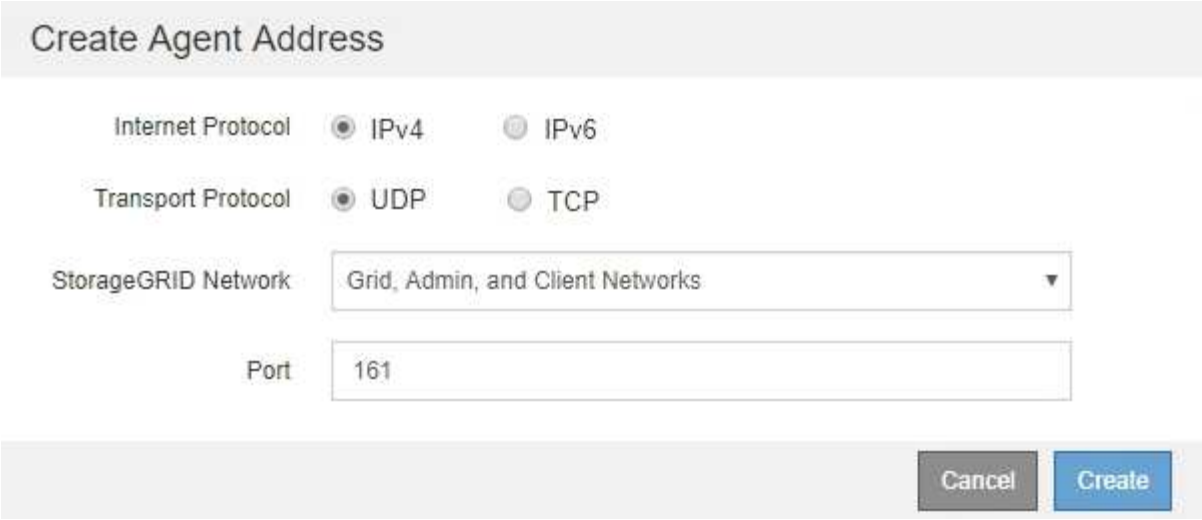
8. Facoltativamente, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

   Utilizzare questa scheda per specificare uno o più "indirizzi in attesa". Questi sono gli indirizzi StorageGRID sui quali l'agente SNMP può ricevere le query. Ogni indirizzo dell'agente include un protocollo Internet, un protocollo di trasporto, una rete StorageGRID e, facoltativamente, una porta.

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

   a. Fare clic su **Create** (Crea).

      Viene visualizzata la finestra di dialogo Create Agent Address (Crea indirizzo agente).



b. Per **Internet Protocol**, selezionare se questo indirizzo utilizzerà IPv4 o IPv6.

   Per impostazione predefinita, SNMP utilizza IPv4.

c. Per **Transport Protocol**, selezionare se questo indirizzo utilizzerà UDP o TCP.

   Per impostazione predefinita, SNMP utilizza UDP.

d. Nel campo **rete StorageGRID**, selezionare la rete StorageGRID su cui si desidera ricevere la query.

   - Reti griglia, amministratore e client: StorageGRID deve rimanere in attesa delle query SNMP su tutte e tre le reti.
   - Grid Network
   - Admin Network (rete amministrativa)
   - Rete client

   > Per garantire che le comunicazioni client con StorageGRID rimangano sicure, non creare un indirizzo agente per la rete client.

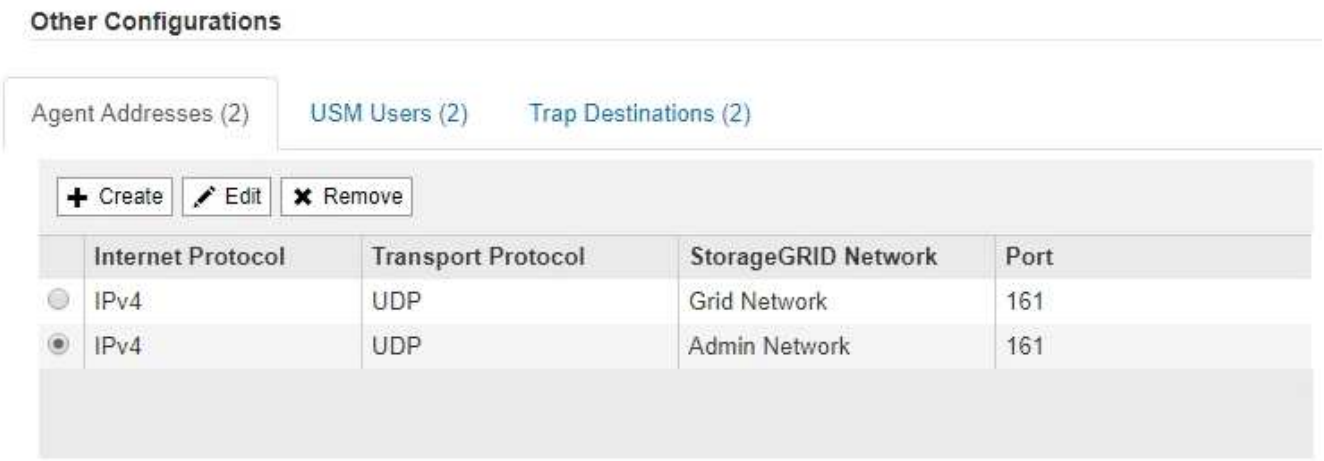
e. Nel campo **Port** (porta), immettere il numero di porta su cui l'agente SNMP deve rimanere in attesa.

   La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta inutilizzato.

   > 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.

f. Fare clic su **Create** (Crea).

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



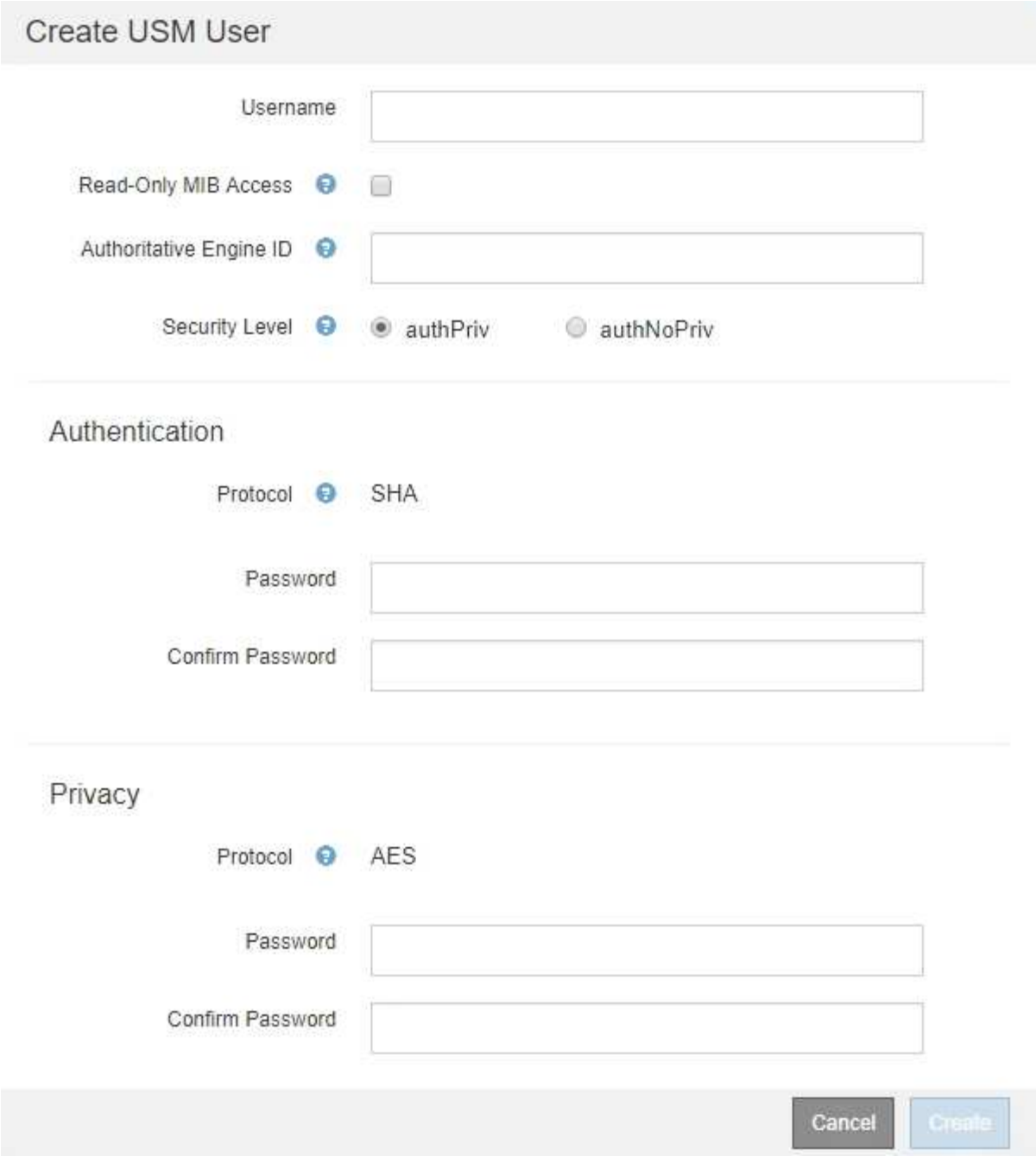
9. Se si utilizza SNMPv3, selezionare la scheda utenti USM nella sezione altre configurazioni.

   Utilizzare questa scheda per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

   > Questo passaggio non è valido se si utilizza solo SNMPv1 o SNMPv2c.

   a. Fare clic su **Create** (Crea).

      Viene visualizzata la finestra di dialogo Create USM User (Crea utente USM).



b. Immettere un **Username** univoco per questo utente USM.

   I nomi utente hanno un massimo di 32 caratteri e non possono contenere spazi vuoti. Il nome utente non può essere modificato dopo la creazione dell'utente.

c. Selezionare la casella di controllo **Read-only MIB Access** (accesso MIB di sola lettura) se l'utente deve disporre dell'accesso di sola lettura al MIB.

   Se si seleziona **Read-only MIB Access** (accesso MIB di sola lettura), il campo **Authoritative Engine ID** (ID motore autorevole) viene disattivato.

   > Gli utenti USM con accesso MIB di sola lettura non possono disporre di ID motore.

d. Se questo utente verrà utilizzato in una destinazione di tipo inform, immettere il **Authoritative Engine**

ID per questo utente.

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

L'ID del motore autorevole può essere compreso tra 5 e 32 byte in formato esadecimale.

e. Selezionare un 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.

f. Inserire e confermare la password che verrà utilizzata dall'utente per l'autenticazione.

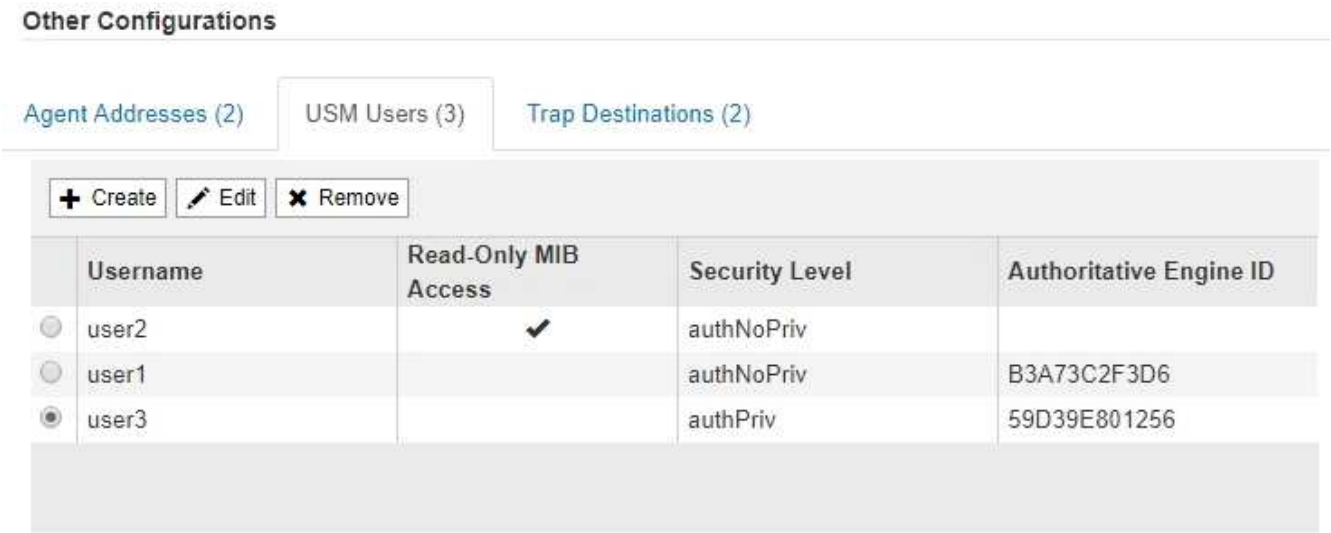
> L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).

g. Se si seleziona **authprim**, immettere e confermare la password che verrà utilizzata dall'utente per la privacy.

> L'unico protocollo per la privacy supportato è AES.

h. Fare clic su **Create** (Crea).

   L'utente USM viene creato e aggiunto alla tabella.

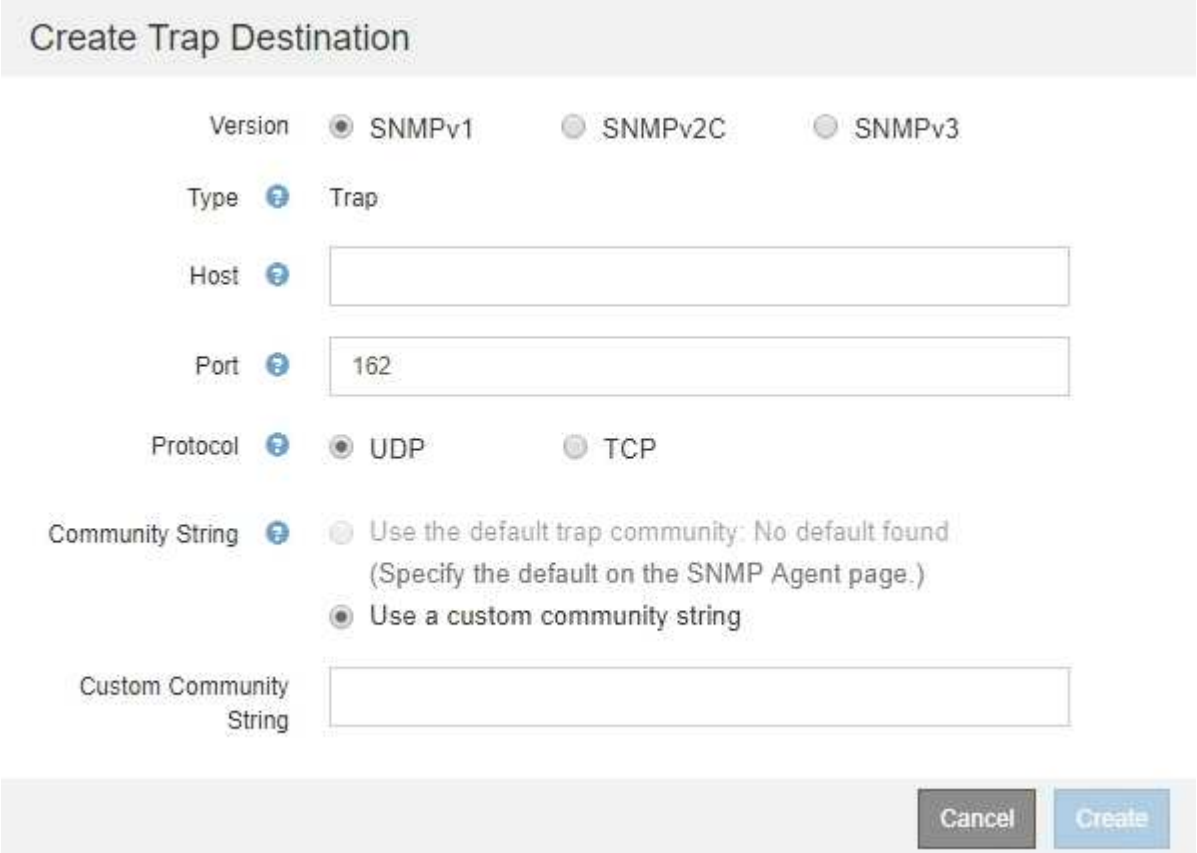


10. nella sezione Other Configurations (altre configurazioni), selezionare la scheda Trap Destinations (Destinazioni trap).

    La scheda Destinazioni trap consente di definire una o più destinazioni per le trap StorageGRID o le notifiche di notifica. Quando si attiva l'agente SNMP e si fa clic su **Salva**, StorageGRID inizia a inviare notifiche a ciascuna destinazione definita. Le notifiche vengono inviate quando vengono attivati avvisi e allarmi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

a. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Create Trap Destination (Crea destinazione trap).



b. Nel campo **Version**, selezionare la versione SNMP da utilizzare per questa notifica.

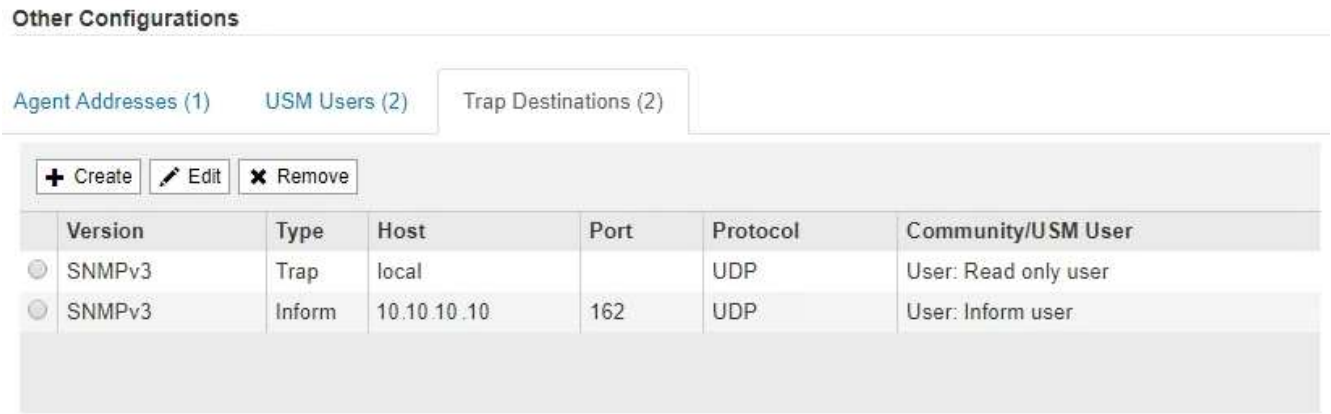
c. Completare il modulo in base alla versione selezionata

Versione	Specificare queste informazioni
SNMPv1	**Nota:** per SNMPv1, l'agente SNMP può inviare solo trap. Le informazioni non sono supportate. i. Nel campo **host**, immettere un indirizzo IPv4 o IPv6 (o FQDN) per ricevere la trap. ii. Per **Port**, utilizzare il valore predefinito (162), a meno che non sia necessario utilizzare un altro valore. (162 è la porta standard per i trap SNMP). iii. Per **Protocol** (protocollo), utilizzare il valore predefinito (UDP). È supportato anche il protocollo TCP. (UDP è il protocollo SNMP trap standard). iv. Utilizzare la community trap predefinita, se specificata nella pagina SNMP Agent, oppure immettere una stringa di community personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.
SNMPv2c	i. Selezionare se la destinazione deve essere utilizzata per trap o informazioni. ii. Nel campo **host**, immettere un indirizzo IPv4 o IPv6 (o FQDN) per ricevere la trap. iii. Per **Port**, utilizzare il valore predefinito (162), a meno che non sia necessario utilizzare un altro valore. (162 è la porta standard per i trap SNMP). iv. Per **Protocol** (protocollo), utilizzare il valore predefinito (UDP). È supportato anche il protocollo TCP. (UDP è il protocollo SNMP trap standard). v. Utilizzare la community trap predefinita, se specificata nella pagina SNMP Agent, oppure immettere una stringa di community personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

Versione	Specificare queste informazioni
SNMPv3	i. Selezionare se la destinazione deve essere utilizzata per trap o informazioni. ii. Nel campo **host**, immettere un indirizzo IPv4 o IPv6 (o FQDN) per ricevere la trap. iii. Per **Port**, utilizzare il valore predefinito (162), a meno che non sia necessario utilizzare un altro valore. (162 è la porta standard per i trap SNMP). iv. Per **Protocol** (protocollo), utilizzare il valore predefinito (UDP). È supportato anche il protocollo TCP. (UDP è il protocollo SNMP trap standard). v. Selezionare 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.

d. Fare clic su **Create** (Crea).

   La destinazione trap viene creata e aggiunta alla tabella.



11. Una volta completata la configurazione dell'agente SNMP, fare clic su **Save** (Salva)

    La nuova configurazione dell'agente SNMP diventa attiva.

Informazioni correlate

Tacitare le notifiche di avviso

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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

Ogni volta che si aggiorna Configurazione dell'agente SNMP, Tenere presente che è necessario fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent per confermare le modifiche apportate in ciascuna scheda.

Fasi

1. Selezionare **CONFIGURAZIONE monitoraggio agente SNMP**.

   Viene visualizzata la pagina SNMP Agent.

2. Se si desidera disattivare l'agente SNMP su tutti i nodi della griglia, deselezionare la casella di controllo **Enable SNMP** (attiva SNMP) e fare clic su **Save** (Salva).

   L'agente SNMP è disattivato per tutti i nodi della griglia. Se in seguito si riattiva l'agente, vengono mantenute le impostazioni di configurazione SNMP precedenti.

3. In alternativa, aggiornare i valori immessi per **contatto di sistema** e **posizione di sistema**.
4. Facoltativamente, deselezionare la casella di controllo **attiva notifiche agente SNMP** se non si desidera più che l'agente SNMP StorageGRID invii messaggi trap e avvisi.

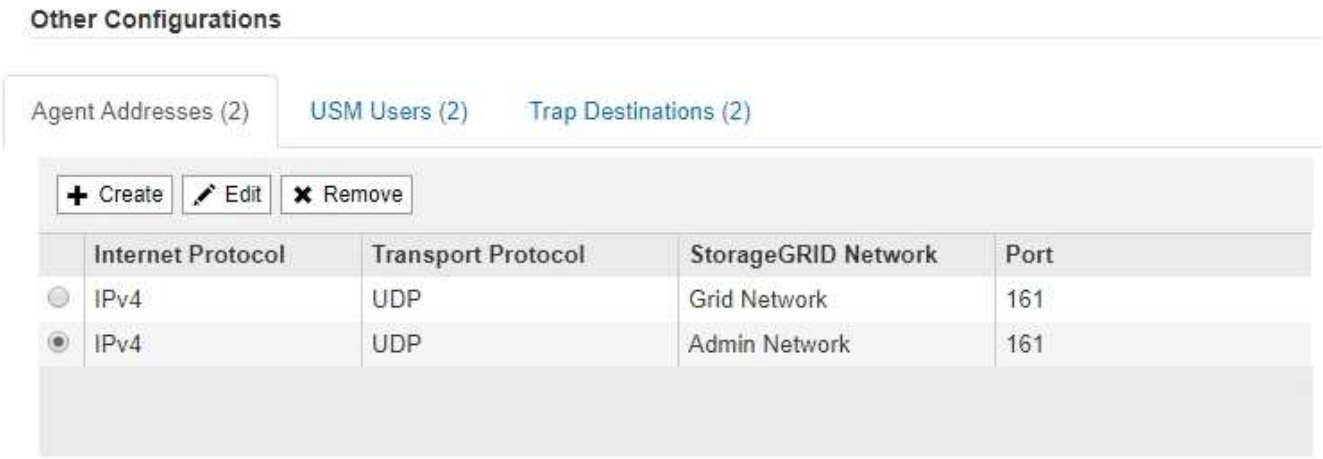
   Se questa casella di controllo non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.

5. Facoltativamente, deselezionare la casella di controllo **attiva trap di autenticazione** se non si desidera più che l'agente SNMP di StorageGRID invii una trap di autenticazione quando riceve un messaggio di protocollo autenticato in modo errato.
6. Se si utilizza SNMPv1 o SNMPv2c, aggiornare la sezione Community Strings (stringhe di comunità).

   I campi di questa sezione vengono utilizzati per l'autenticazione basata sulla community in SNMPv1 o SNMPv2c. Questi campi non si applicano a SNMPv3.

   > Se si desidera rimuovere la stringa di comunità predefinita, assicurarsi innanzitutto che tutte le destinazioni trap utilizzino una stringa di comunità personalizzata.

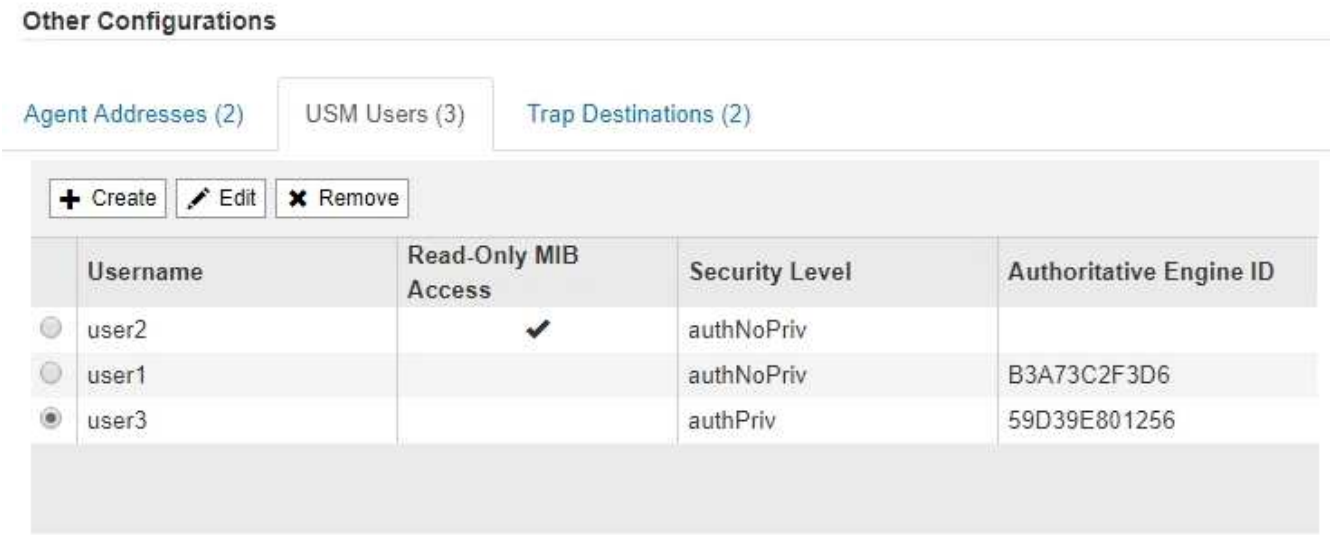
7. Se si desidera aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agenti nella sezione altre configurazioni.



Utilizzare questa scheda per specificare uno o più “indirizzi in attesa”. Questi sono gli indirizzi StorageGRID sui quali l’agente SNMP può ricevere le query. Ogni indirizzo dell’agente include un protocollo Internet, un protocollo di trasporto, una rete StorageGRID e una porta.

a. Per aggiungere un indirizzo agente, fare clic su **Crea**. Quindi, fare riferimento alla fase relativa agli indirizzi degli agenti nelle istruzioni per la configurazione dell’agente SNMP.
b. Per modificare l’indirizzo di un agente, selezionare il pulsante di opzione corrispondente all’indirizzo e fare clic su **Modifica**. Quindi, fare riferimento alla fase relativa agli indirizzi degli agenti nelle istruzioni per la configurazione dell’agente SNMP.
c. Per rimuovere un indirizzo dell’agente, selezionare il pulsante di opzione corrispondente all’indirizzo e fare clic su **Remove** (Rimuovi). Quindi, fare clic su **OK** per confermare che si desidera rimuovere questo indirizzo.
d. Per confermare le modifiche, fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent.

8. Se si desidera 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.

a. Per aggiungere un utente USM, fare clic su **Crea**. Quindi, fare riferimento alla fase per gli utenti USM nelle istruzioni per la configurazione dell’agente SNMP.

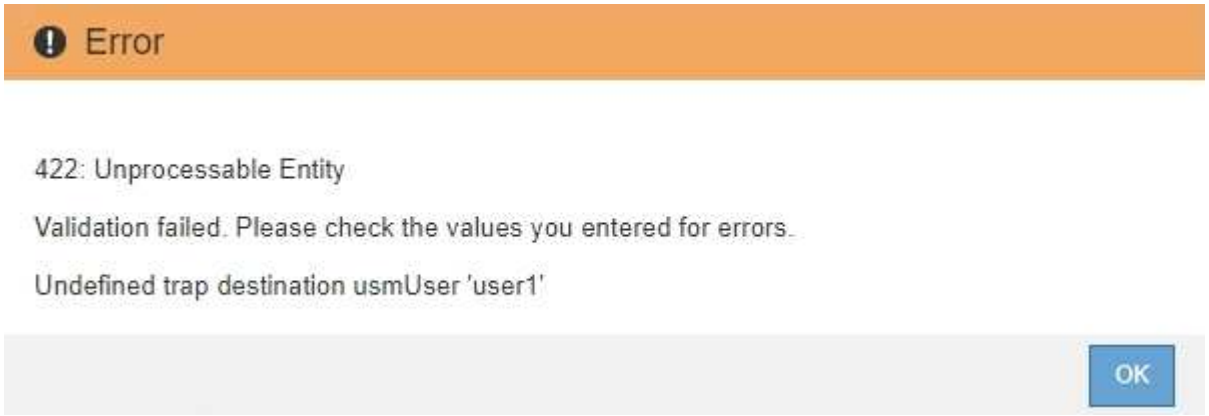
b. Per modificare un utente USM, selezionare il pulsante di opzione dell'utente e fare clic su **Edit** (Modifica). Quindi, fare riferimento alla fase per gli utenti USM nelle istruzioni per la configurazione dell'agente SNMP.

   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 rimuove l'ID motore autorevole di un utente e tale utente è attualmente selezionato per una destinazione, è necessario modificare o rimuovere la destinazione, come descritto al punto Destinazione trap SNMP. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

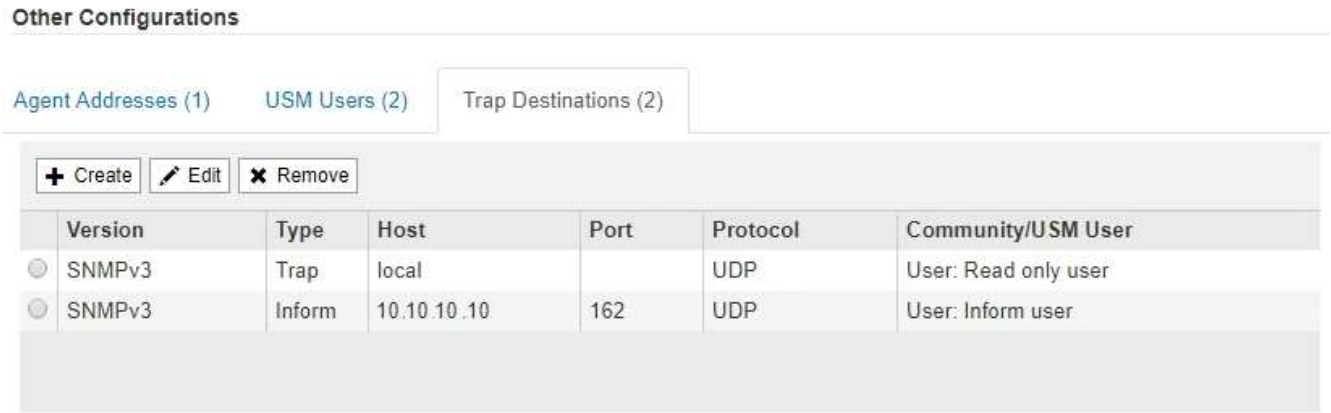
c. Per rimuovere un utente USM, selezionare il pulsante di opzione dell'utente e fare clic su **Remove** (Rimuovi). Quindi, fare clic su **OK** per confermare che si desidera rimuovere l'utente.

   > Se l'utente rimosso è attualmente selezionato per una destinazione trap, è necessario modificare o rimuovere la destinazione, come descritto al punto Destinazione trap SNMP. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.



a. Per confermare le modifiche, fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent.

9. se si desidera aggiornare le destinazioni trap, selezionare la scheda Destinations trap nella sezione Other Configurations (altre configurazioni).



La scheda Destinazioni trap consente di definire una o più destinazioni per le trap StorageGRID o le notifiche di notifica. Quando si attiva l'agente SNMP e si fa clic su **Salva**, StorageGRID inizia a inviare notifiche a ciascuna destinazione definita. Le notifiche vengono inviate quando vengono attivati avvisi e

allarmi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

a. Per aggiungere una destinazione trap, fare clic su **Create** (Crea). Quindi, fare riferimento alla fase relativa alle destinazioni trap nelle istruzioni per la configurazione dell'agente SNMP.
b. Per modificare una destinazione trap, selezionare il pulsante di opzione dell'utente e fare clic su **Edit** (Modifica). Quindi, fare riferimento alla fase relativa alle destinazioni trap nelle istruzioni per la configurazione dell'agente SNMP.
c. Per rimuovere una destinazione trap, selezionare il pulsante di opzione corrispondente alla destinazione e fare clic su **Remove** (Rimuovi). Quindi, fare clic su **OK** per confermare che si desidera rimuovere questa destinazione.
d. Per confermare le modifiche, fare clic su **Save** (Salva) nella parte inferiore della pagina SNMP Agent.

10. Una volta aggiornata la configurazione dell'agente SNMP, fare clic su **Save** (Salva).

Raccogliere dati StorageGRID aggiuntivi

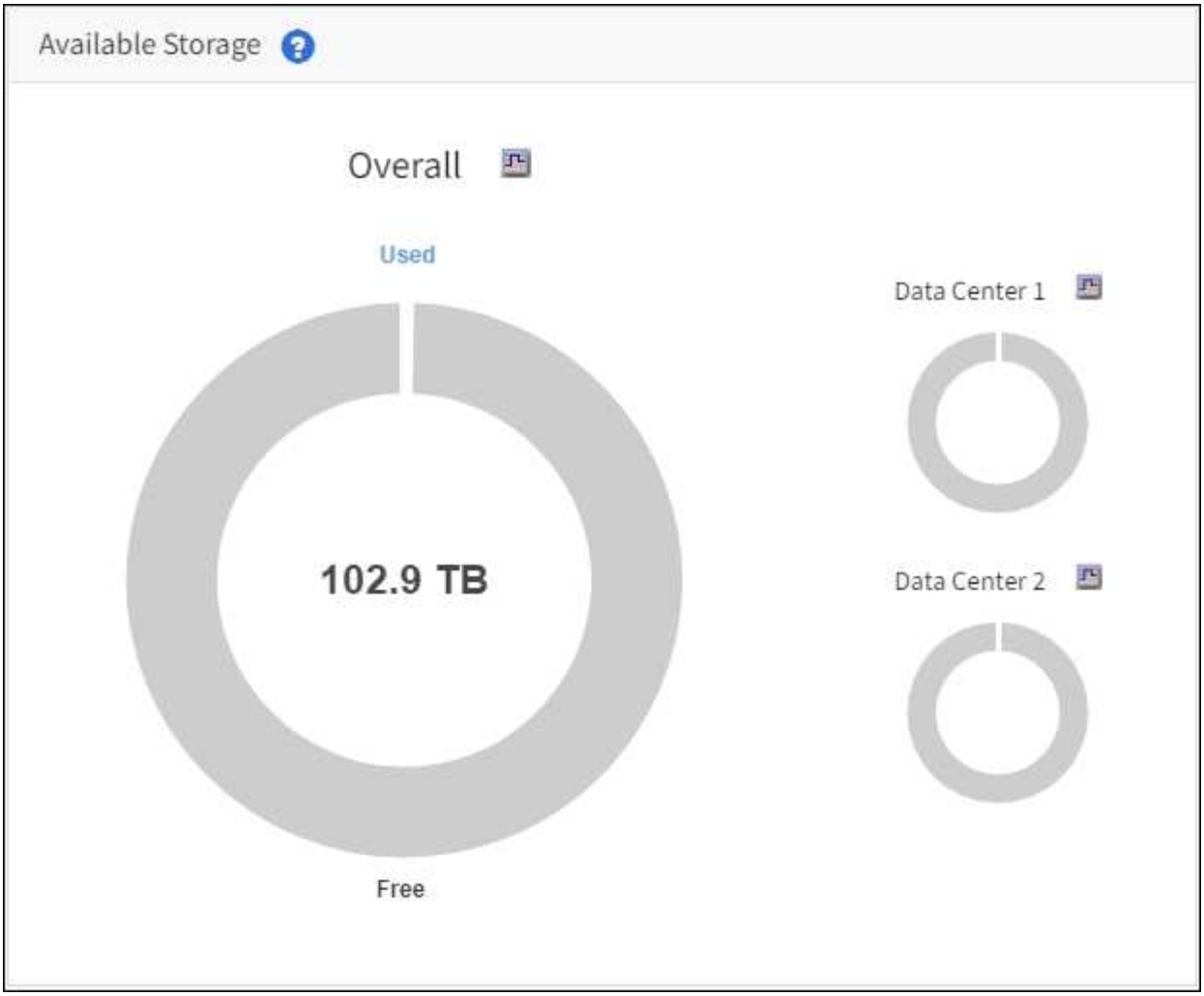
Utilizzare grafici e grafici

È possibile utilizzare grafici e report per monitorare lo stato del sistema StorageGRID e risolvere i problemi. I tipi di grafici e report disponibili in Grid Manager includono grafici a ciambella (solo nella dashboard), grafici e report di testo.

Tipi di grafici

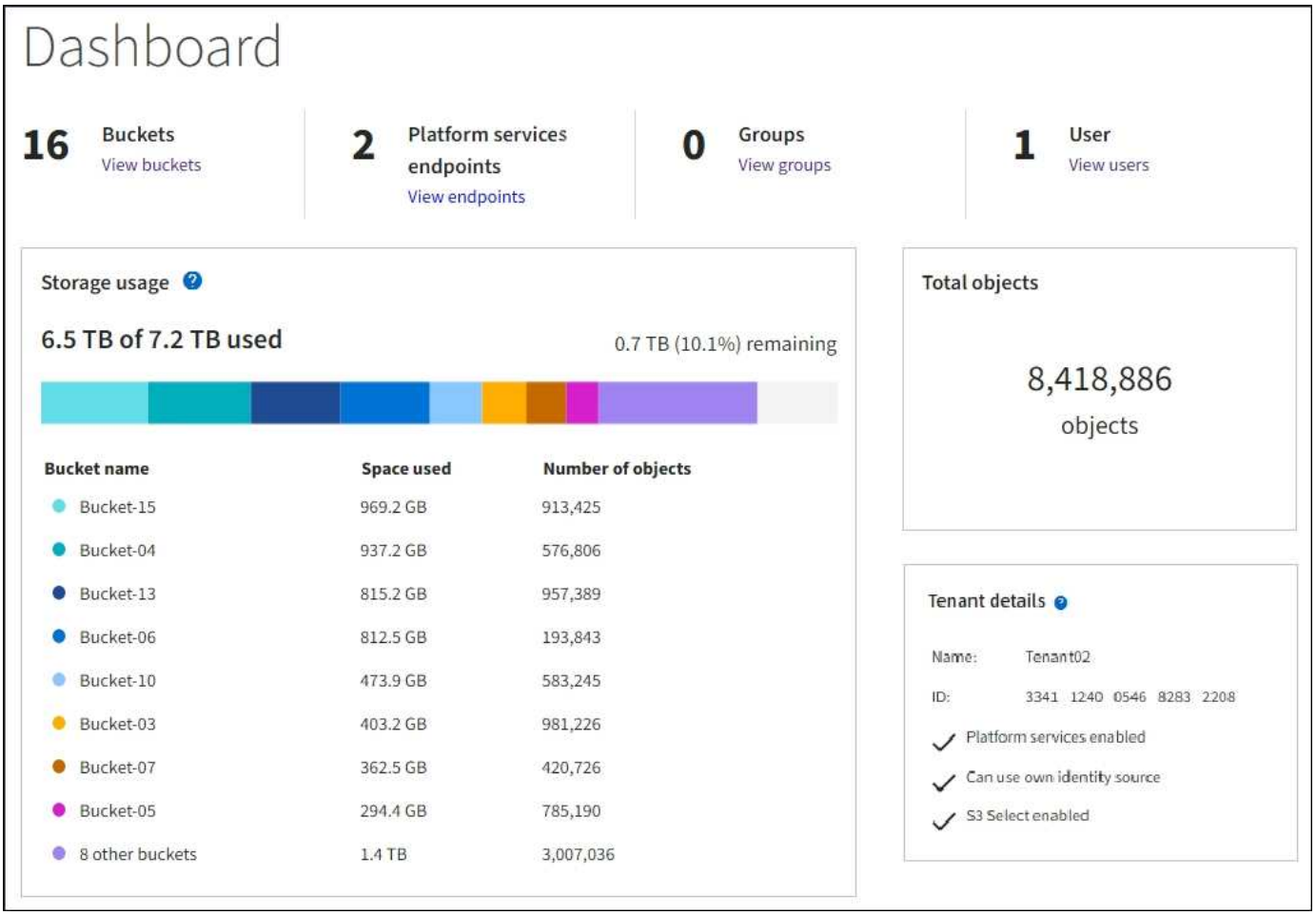
I grafici e i grafici riassumono i valori delle metriche e degli attributi specifici di StorageGRID.

Il pannello di controllo di Grid Manager include grafici a ciambella per riepilogare lo storage disponibile per la griglia e per ciascun sito.



Il pannello Storage Use (utilizzo dello storage) del pannello di controllo di Tenant Manager visualizza quanto segue:

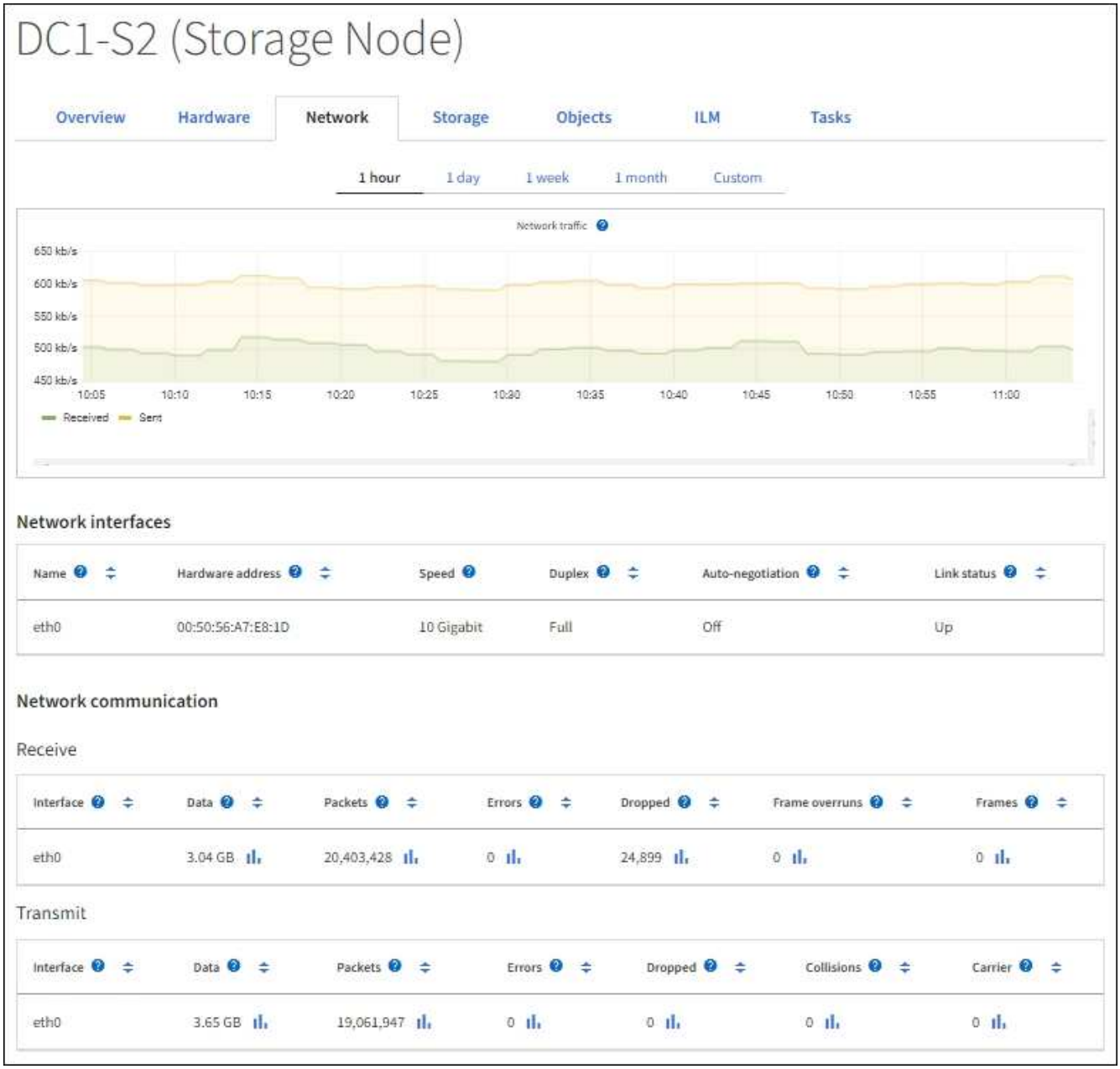
- Un elenco dei bucket più grandi (S3) o container (Swift) per il tenant
- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi
- La quantità totale di spazio utilizzato e, se viene impostata una quota, la quantità e la percentuale di spazio rimanente



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**.

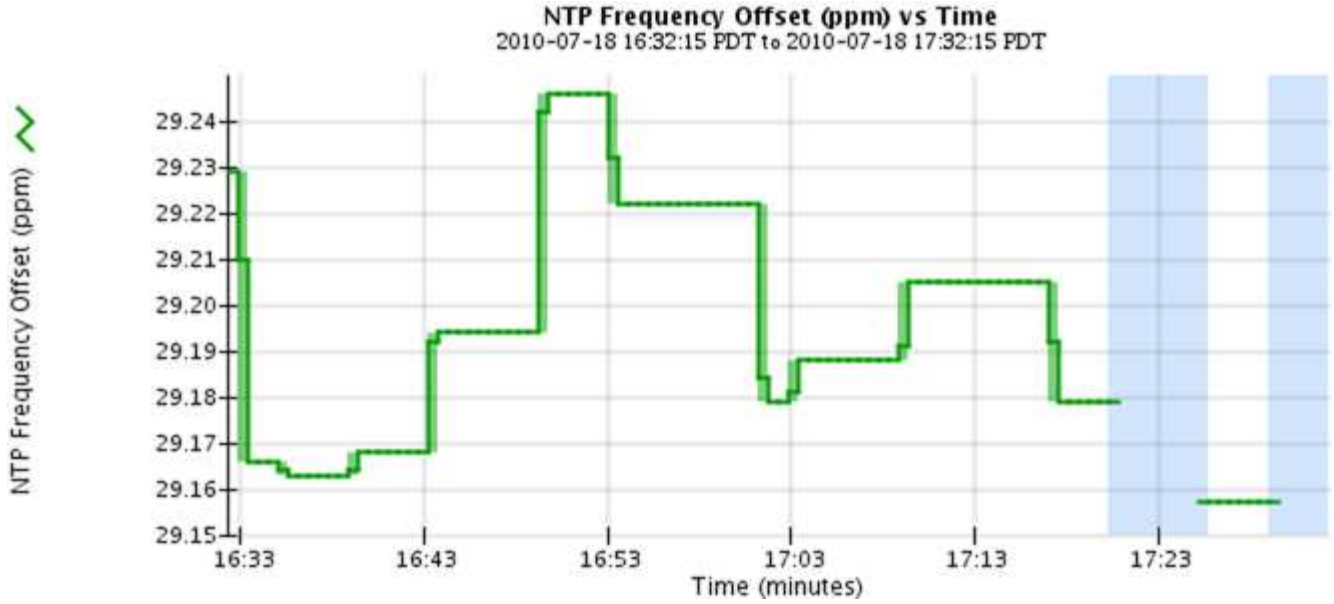
Esistono quattro tipi di grafici:

- **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 **NODES Network** di un nodo di storage include un grafico Grafana per il traffico di rete.

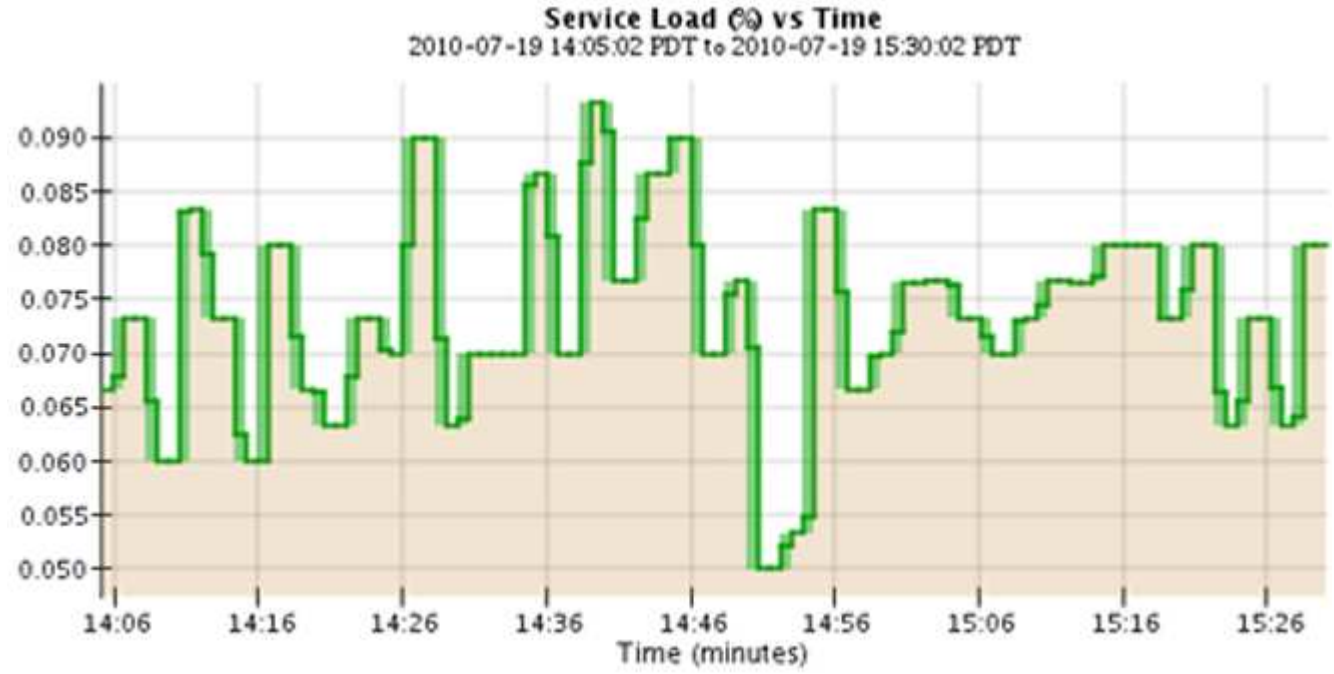


I grafici Grafana sono inclusi anche nelle dashboard predefinite disponibili nella pagina **SUPPORT Tools Metrics**.

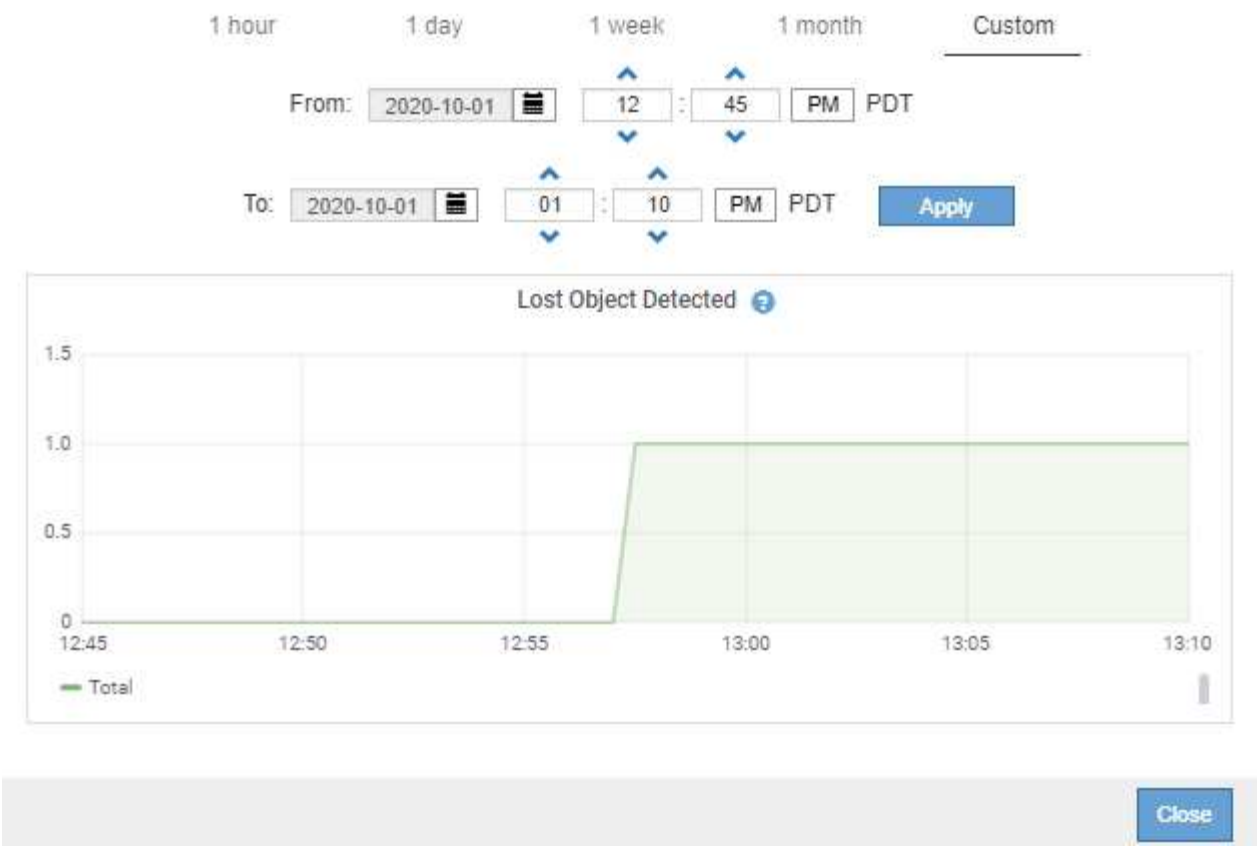
- **Grafici di linea**: Disponibili dalla pagina nodi e dalla pagina **SUPPORTO Strumenti topologia di griglia** (selezionare l'icona del grafico Dopo un valore di dati), i grafici a linee vengono utilizzati per rappresentare graficamente i valori degli attributi StorageGRID che hanno un valore unitario (ad esempio, offset di frequenza NTP, in ppm). Le modifiche al valore vengono tracciate a intervalli di dati regolari (bin) nel tempo.



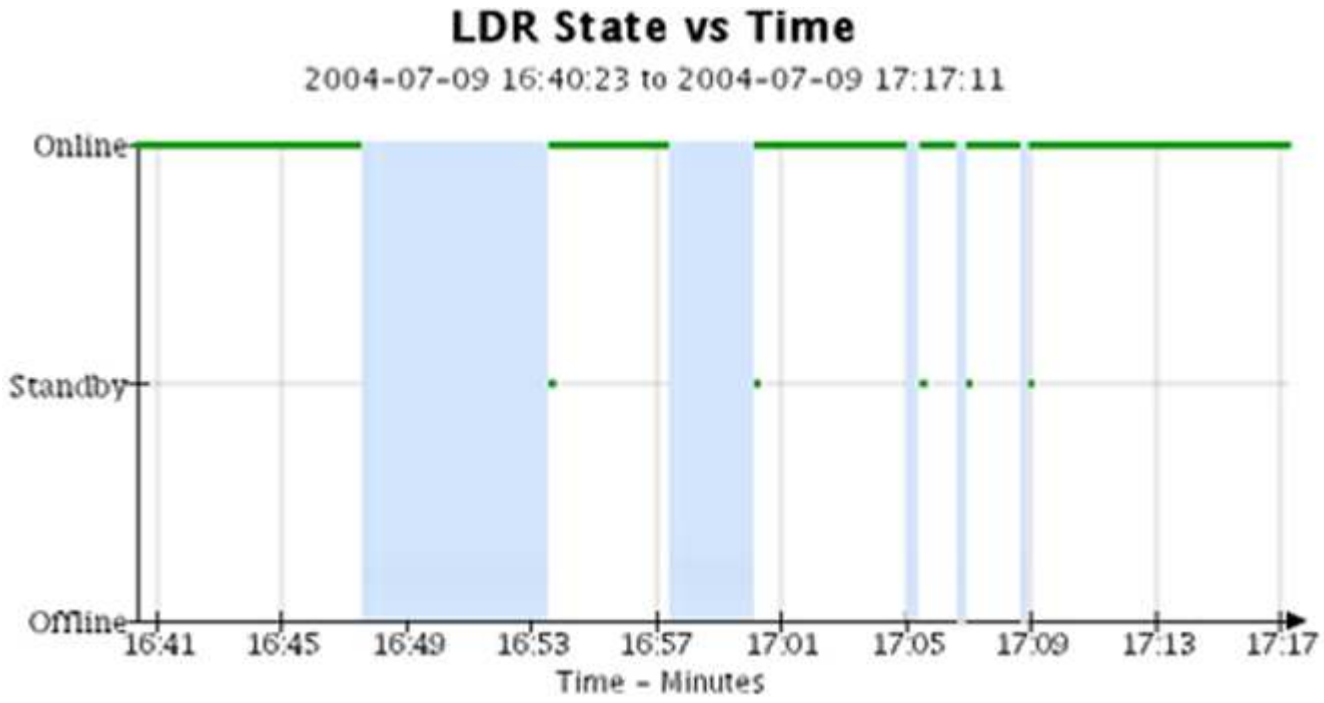
- **Area Graphs**: Disponibile dalla pagina Nodes e dalla pagina **SUPPORT Tools Grid topology** (selezionare l'icona del grafico) dopo un valore di dati), i grafici di area vengono utilizzati per rappresentare graficamente le quantità di attributi volumetrici, come i conteggi di oggetti o i valori di 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

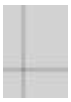
Visualizzare la pagina nodi

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 chiara intorno alle linee di colore verde scuro indica che i valori effettivi in quell'intervallo di tempo variano e sono stati "binned" per un plotting più rapido. 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.

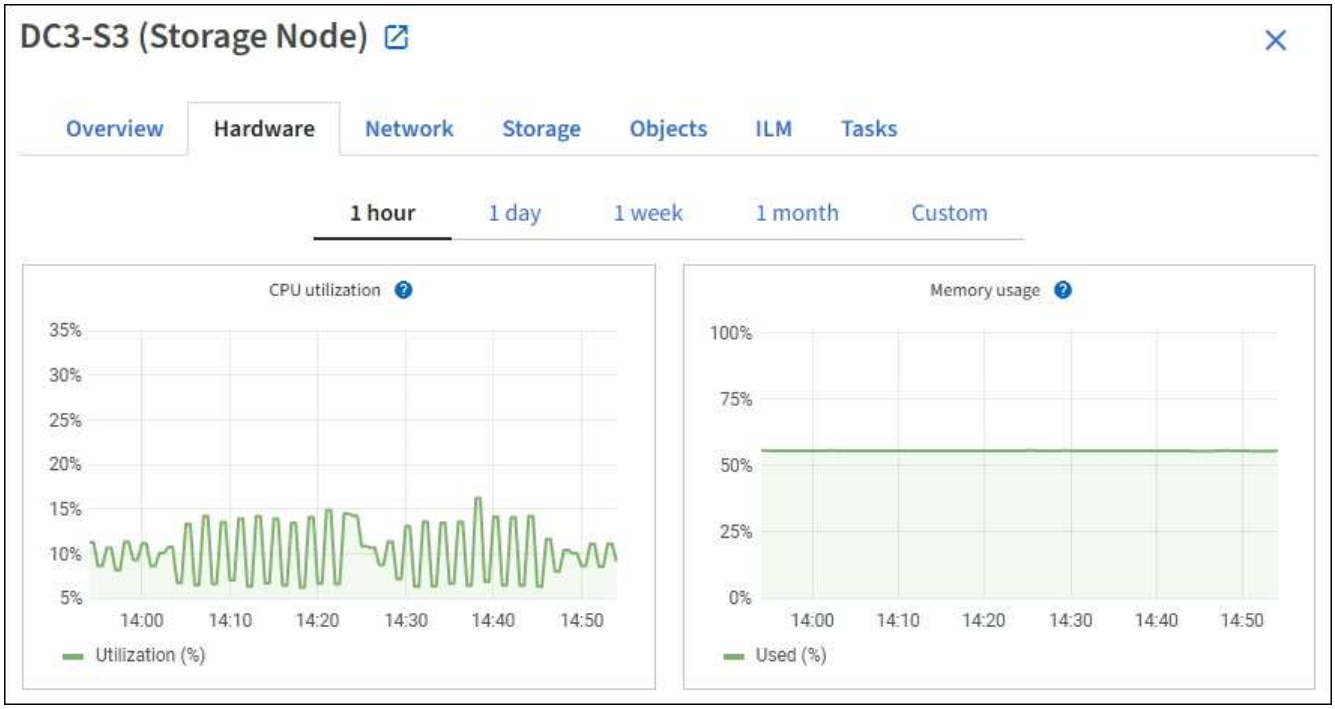
Di cosa hai bisogno

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

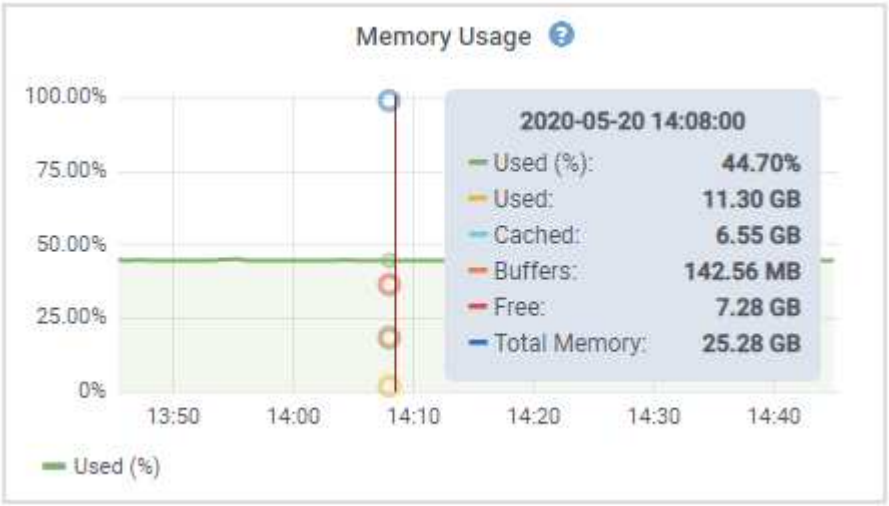
Fasi

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. In alternativa, spostare il cursore sul grafico per visualizzare valori più dettagliati per un determinato punto temporale.

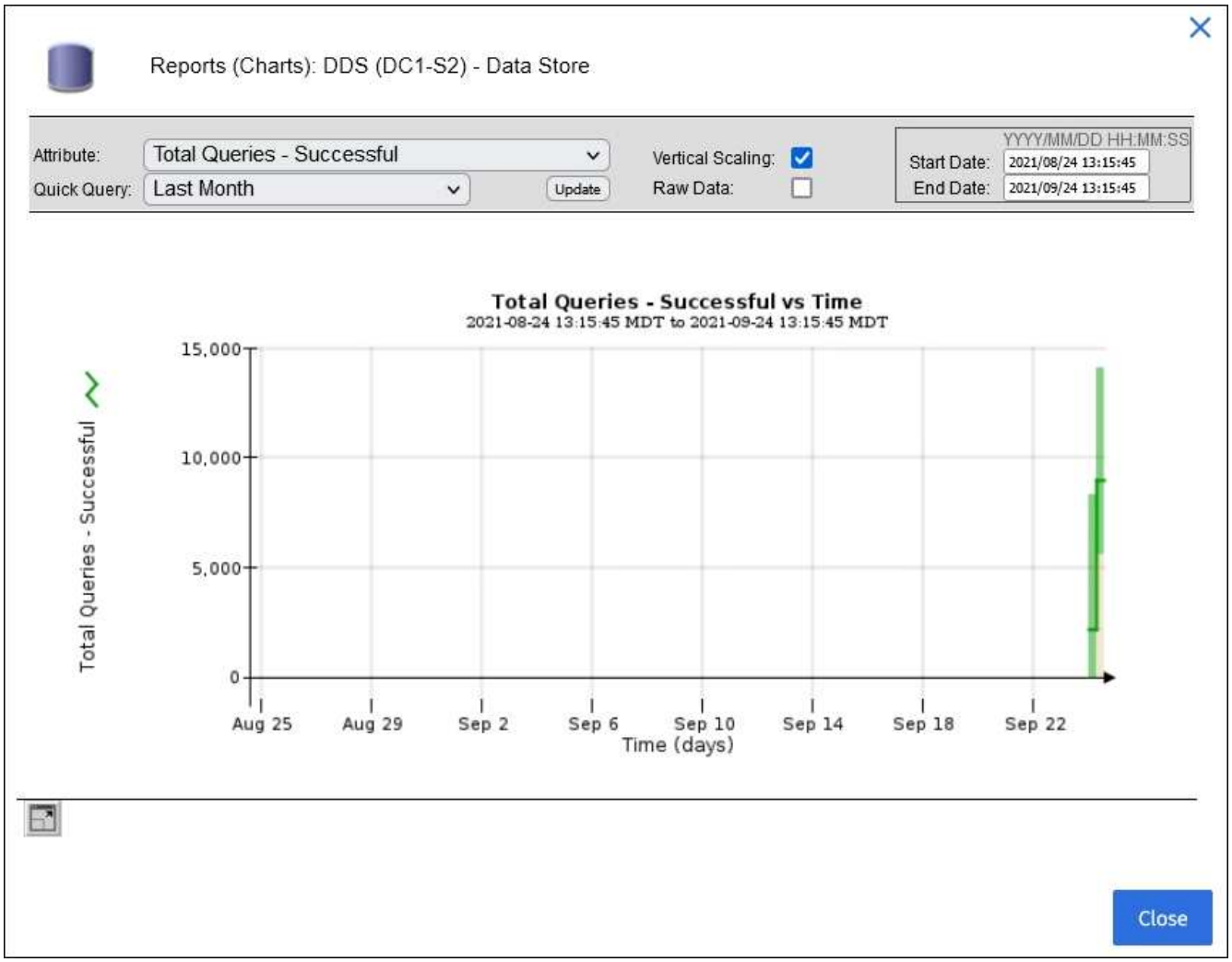


4. In base alle esigenze, spesso è possibile visualizzare un grafico per un attributo o una metrica specifici. Nella tabella della pagina nodi, selezionare l'icona del grafico a destra del nome dell'attributo.

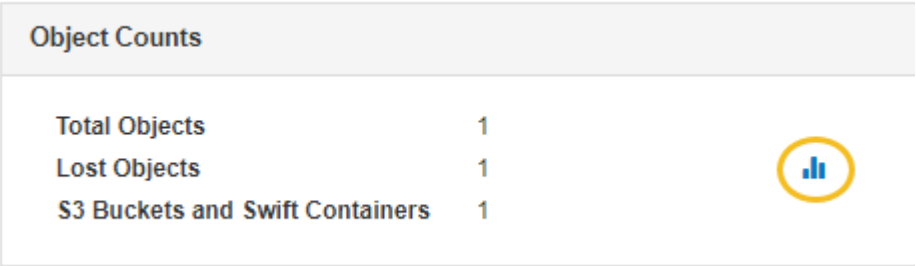
> I grafici non sono disponibili per tutte le metriche e gli attributi.

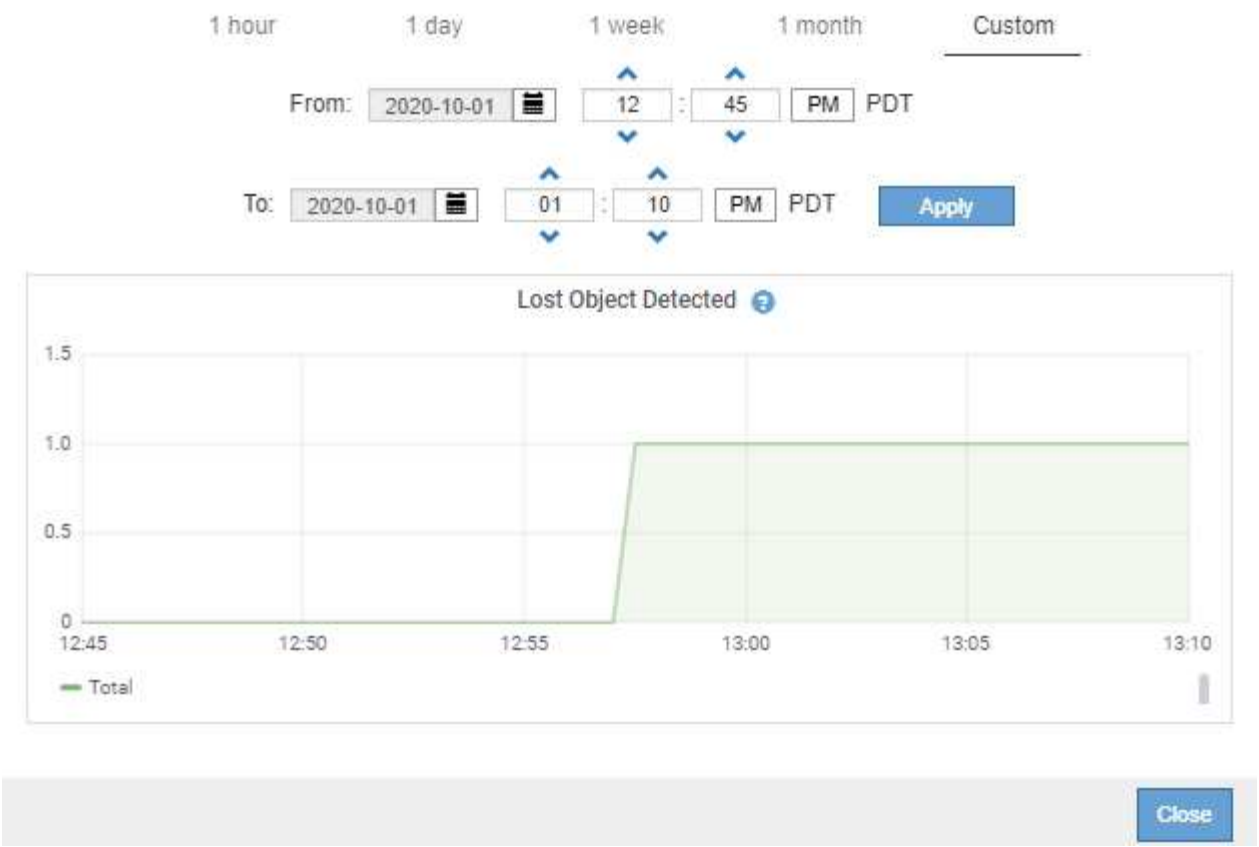
Esempio 1: Dalla scheda oggetti di un nodo di storage, è possibile selezionare l'icona del grafico Per visualizzare il numero totale di query di archiviazione dei metadati riuscite per il nodo di storage.

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

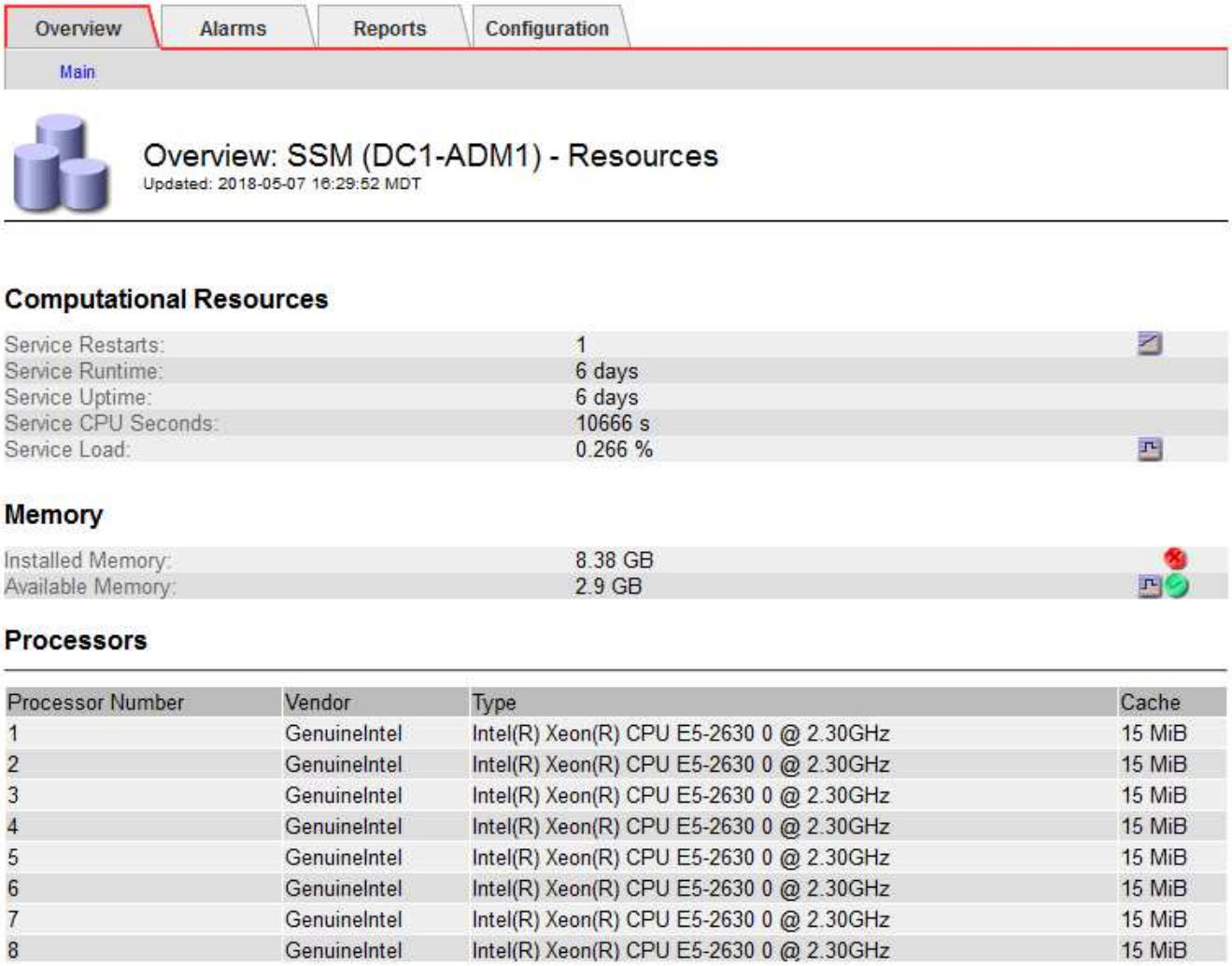


Esempio 2: Dalla scheda oggetti di un nodo di storage, è possibile selezionare l'icona del grafico Per visualizzare il grafico Grafana del numero di oggetti persi rilevati nel tempo.





5. Per visualizzare i grafici degli attributi non visualizzati nella pagina nodo, selezionare **SUPPORT Tools Grid topology**.
6. Selezionare ***grid node component o 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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node component o 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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per i dati degli attributi che si prevede siano in continuo cambiamento, questi dati degli attributi vengono campionati dal servizio NMS (all'origine) a intervalli regolari. Per i dati degli attributi che cambiano di rado (ad esempio, dati basati su eventi come cambiamenti di stato o stato), un valore di attributo viene inviato al servizio NMS quando il valore cambia.

Il tipo di report visualizzato dipende dal periodo di tempo configurato. Per impostazione predefinita, i report di testo aggregati vengono generati per periodi di tempo superiori a una settimana.

Il testo grigio indica che il servizio è stato amministrativamente inattivo durante il campionamento. Il testo blu indica che il servizio si trova in uno stato sconosciuto.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node component o service*** **Report testo**.
3. Selezionare l'attributo da segnalare dall'elenco a discesa **attributo**.
4. Selezionare il numero di risultati per pagina dall'elenco a discesa **risultati per pagina**.
5. Per arrotondare i valori a un massimo di tre cifre decimali (ad esempio, per gli attributi riportati come percentuali), deselezionare la casella di controllo **dati non elaborati**.
6. Selezionare il periodo di tempo per il quale si desidera creare un report dall'elenco a discesa **Query rapida**.

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

Il report viene visualizzato dopo alcuni istanti. Attendere alcuni minuti per la tabulazione di intervalli di tempo lunghi.

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

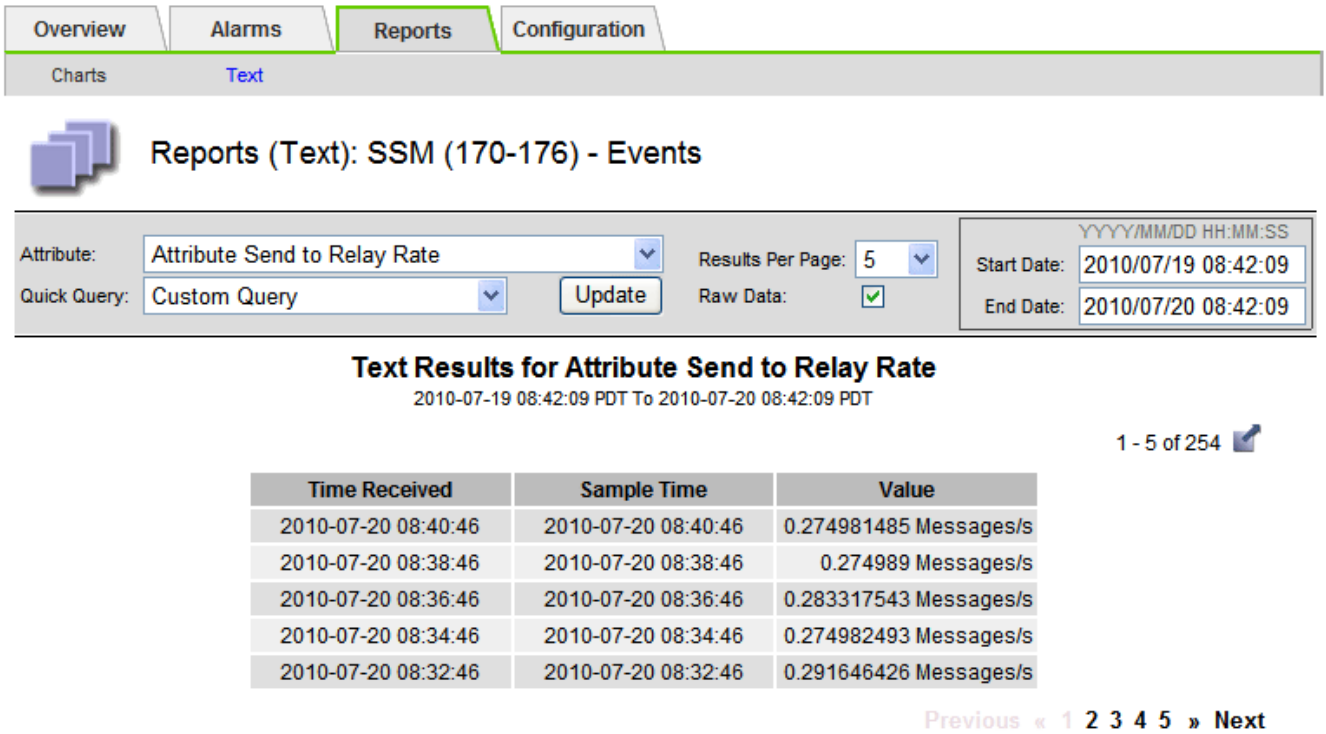
I report di testo esportati aprono una nuova scheda del browser che consente di selezionare e copiare i dati.

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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Maintenance (manutenzione) o Root Access (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.

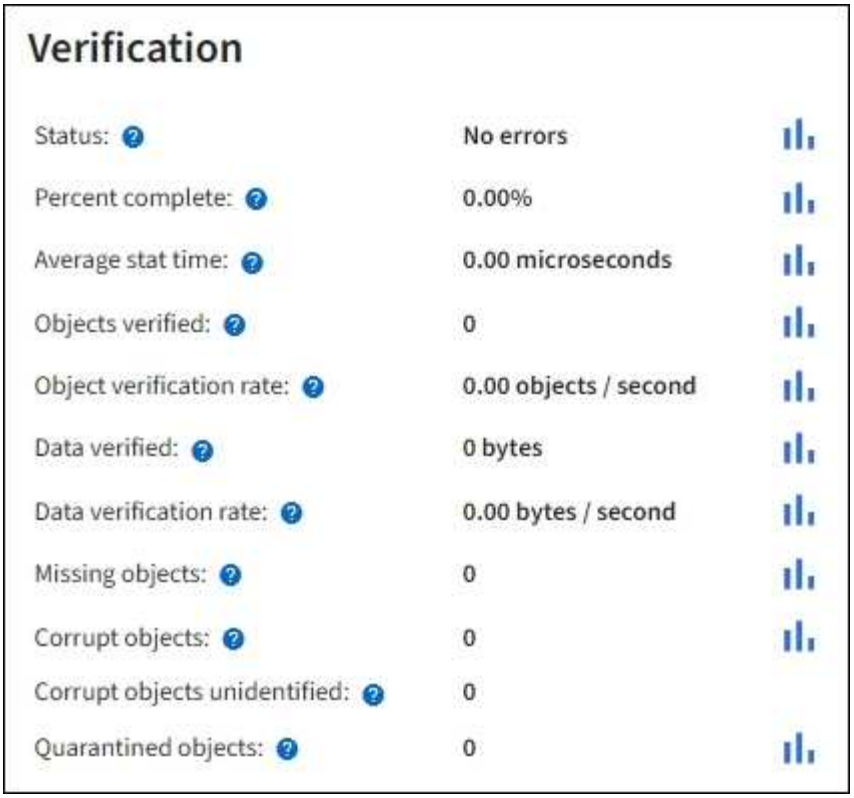
Fasi

1. Esaminare i risultati delle verifiche in background:

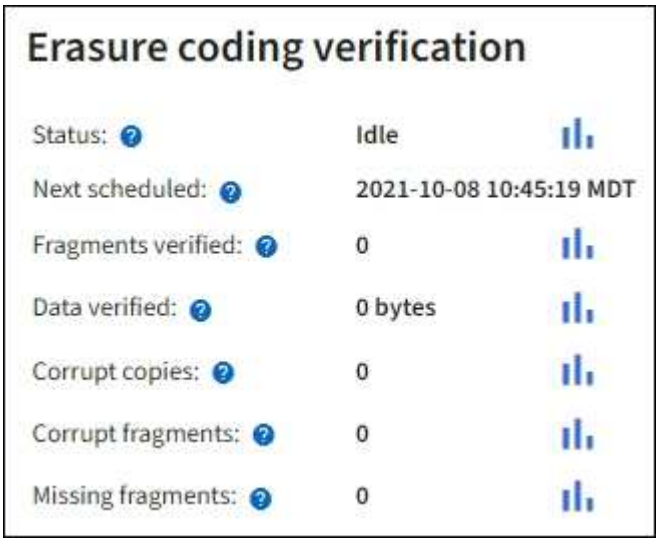
   a. Selezionare **NODI *nodo di storage* oggetti**.

   b. Verificare i risultati della verifica:

      - Per controllare la verifica dei dati degli oggetti replicati, esaminare gli attributi nella sezione verifica.

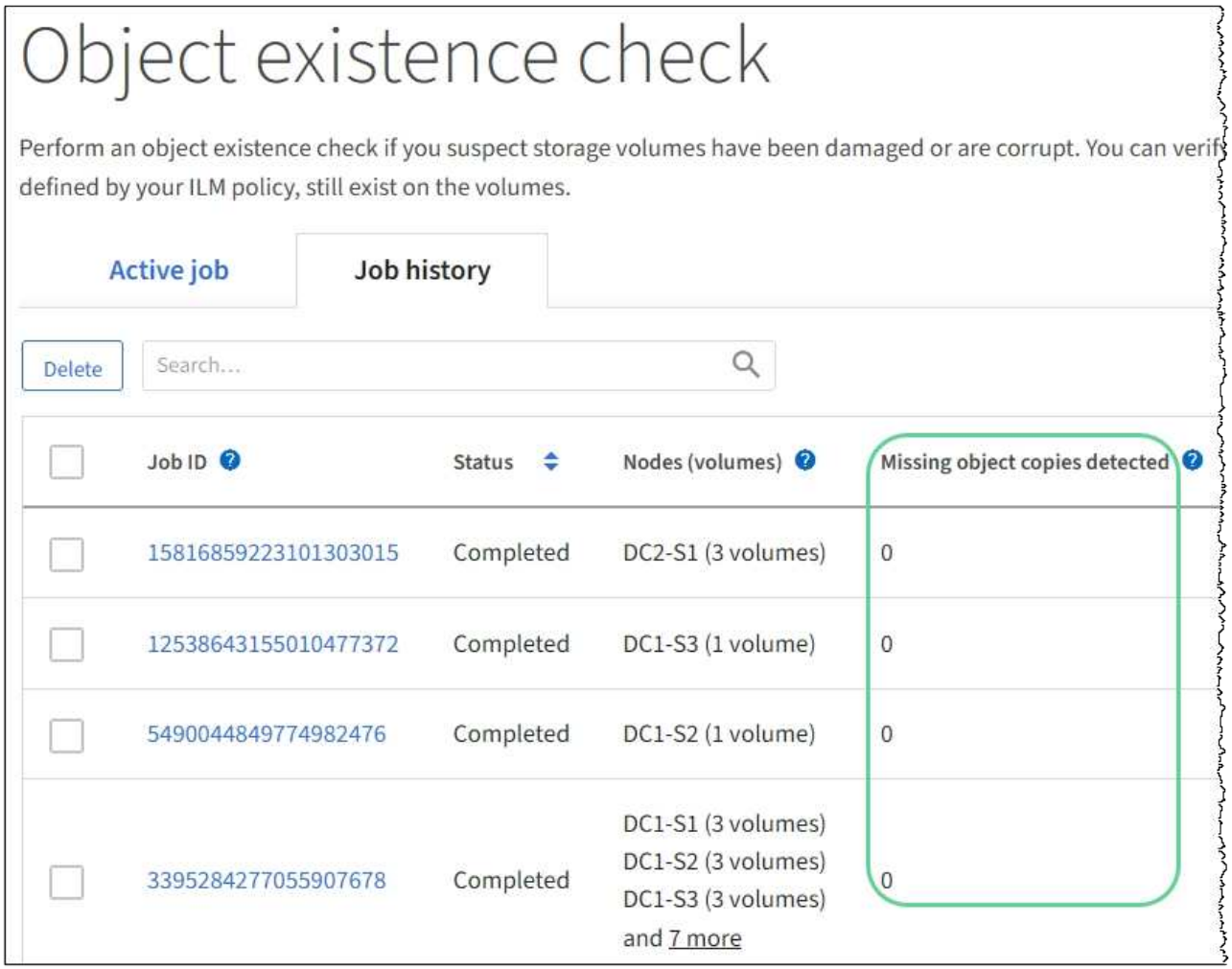


- Per controllare la verifica dei frammenti con codifica di cancellazione, selezionare ***Storage Node* ILM** e controllare gli attributi nella sezione Erasure coding verifcation.



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 alcuni lavori hanno causato 100 o più copie di oggetti mancanti e l' Avviso di perdita di oggetti 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**.

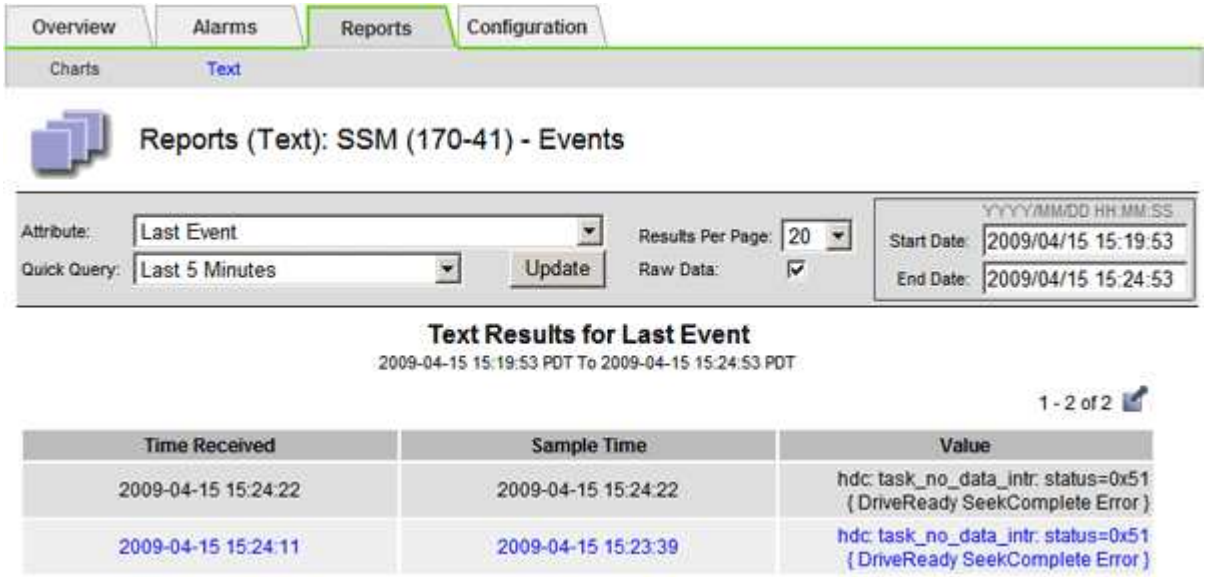
c. Selezionare **testo**.

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.

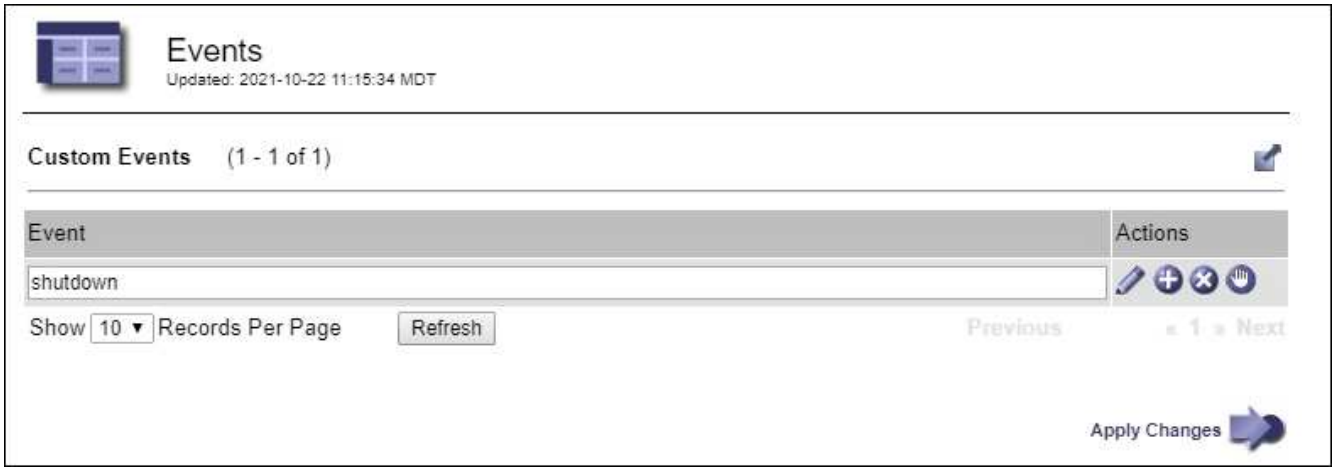
- Dopo la creazione di un evento personalizzato, viene monitorata ogni occorrenza.
- Per creare un evento personalizzato in base alle parole chiave in `/var/local/log/messages` i log in questi file devono essere:
  - Generato dal kernel
  - Generato da daemon o programma utente a livello di errore o 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

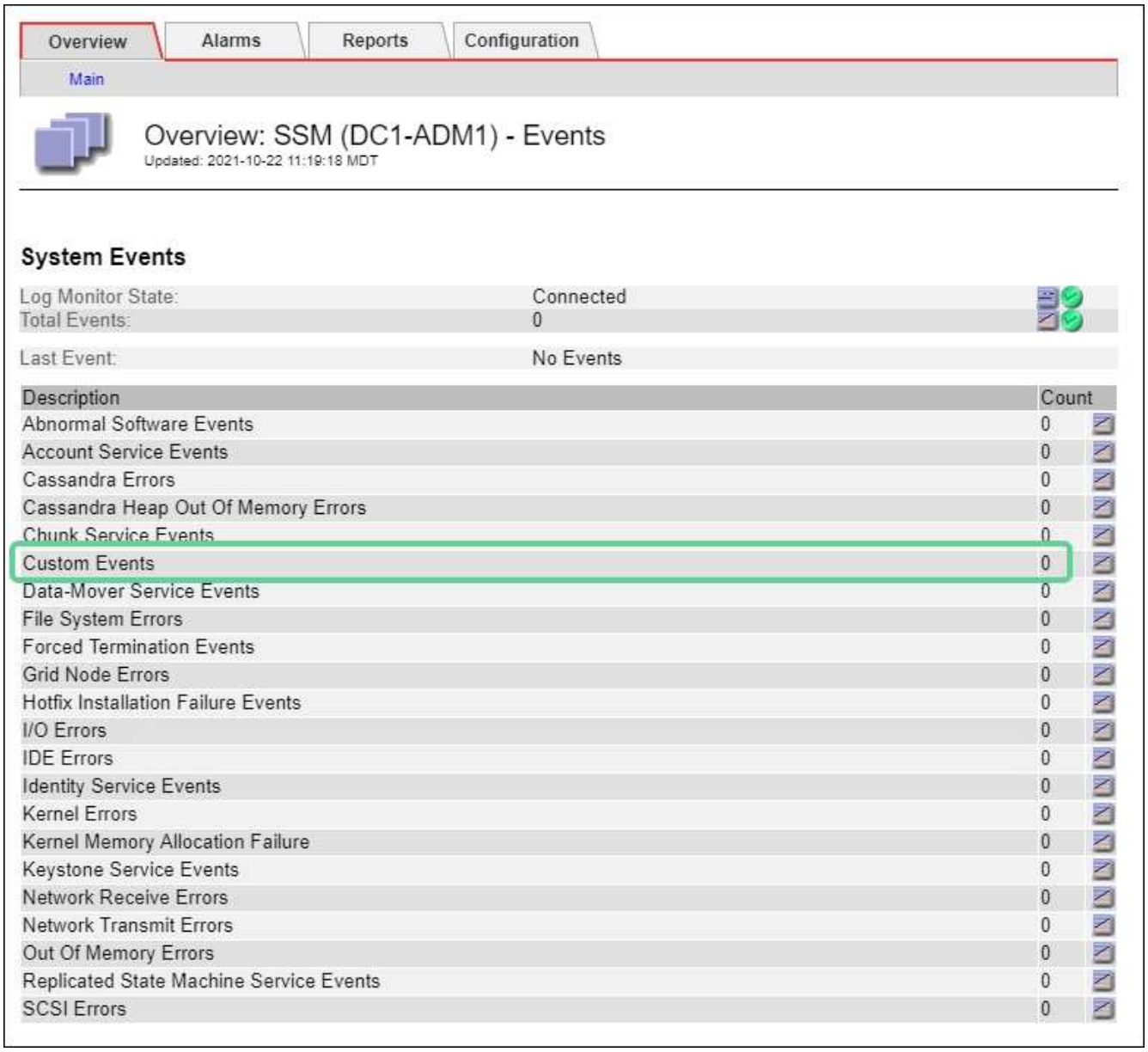
1. Selezionare **SUPPORT Alarms (legacy) Custom events**.
2. Fare clic su **Edit** (Modifica) (O **Inserisci** se questo non è il primo evento).

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.



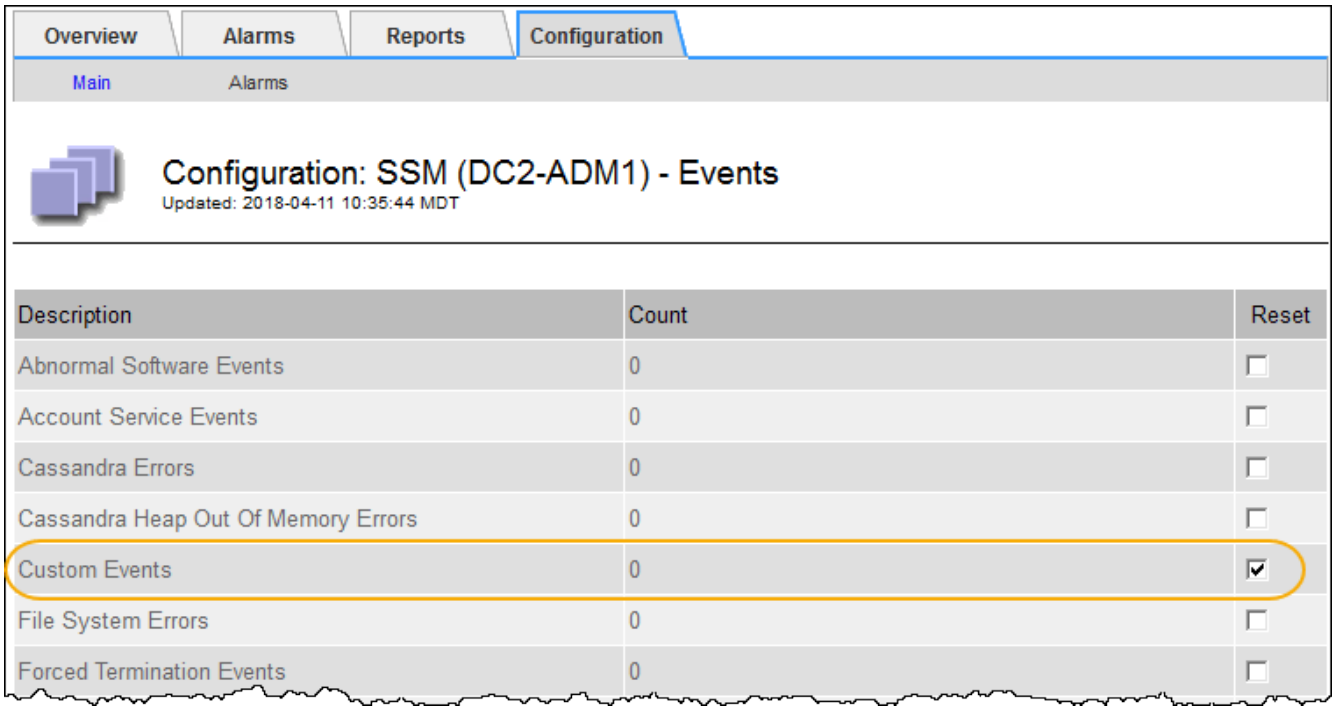
Azzerare il numero di eventi personalizzati

Se si desidera reimpostare il contatore solo per eventi personalizzati, è necessario utilizzare la pagina Grid Topology (topologia griglia) nel menu Support (supporto).

A proposito di questa attività

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.

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***grid node*** **SSM Eventi Configurazione principale**.
3. Selezionare la casella di controllo **Reset** per gli 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 audit, è possibile configurare l'accesso client alla condivisione di audit sia per NFS che per CIFS (CIFS è obsoleto). È inoltre possibile accedere ai file di log di audit direttamente dalla riga di comando del nodo di amministrazione.

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.

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, consultare le istruzioni relative ai messaggi di audit. Per informazioni su come configurare l'accesso al client di controllo, consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

Esaminare i registri di audit

Amministrare StorageGRID

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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre della passphrase di provisioning.

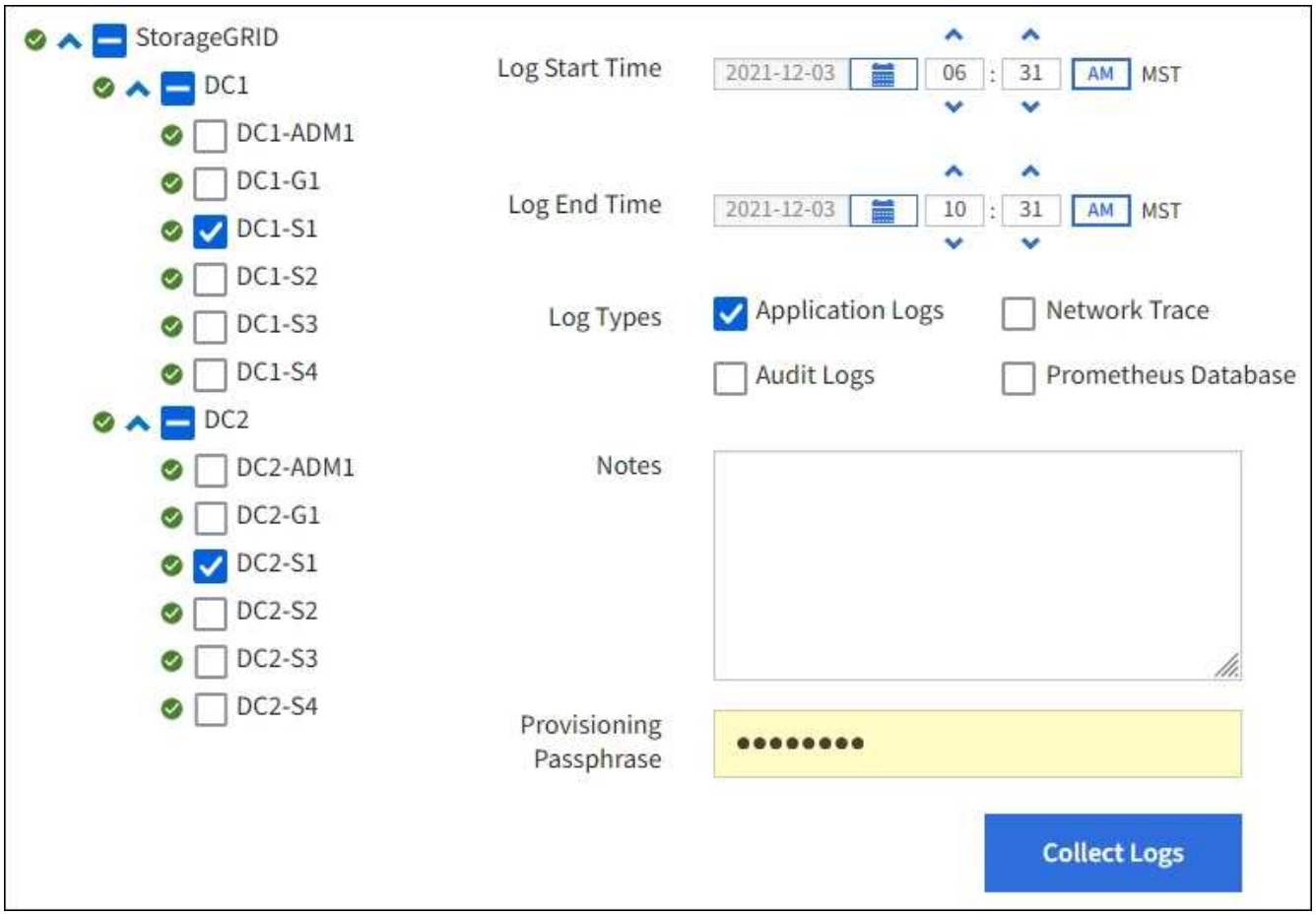
A proposito di questa attività

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 messaggio AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi relativi al sistema StorageGRID, è possibile attivare manualmente l'invio di un messaggio AutoSupport.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Root Access o Other Grid Configuration.

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.

   Viene visualizzata la pagina AutoSupport (Impostazioni) con la scheda **Settings** (Impostazioni) selezionata.

2. Selezionare **Invia AutoSupport attivato dall'utente**.

   StorageGRID tenta di inviare un messaggio AutoSupport al supporto tecnico. Se il tentativo ha esito positivo, i valori **risultato più recente** e **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. In caso di problemi, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il messaggio AutoSupport.

Dopo aver inviato un messaggio AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport del browser dopo 1 minuto per accedere ai risultati più recenti.

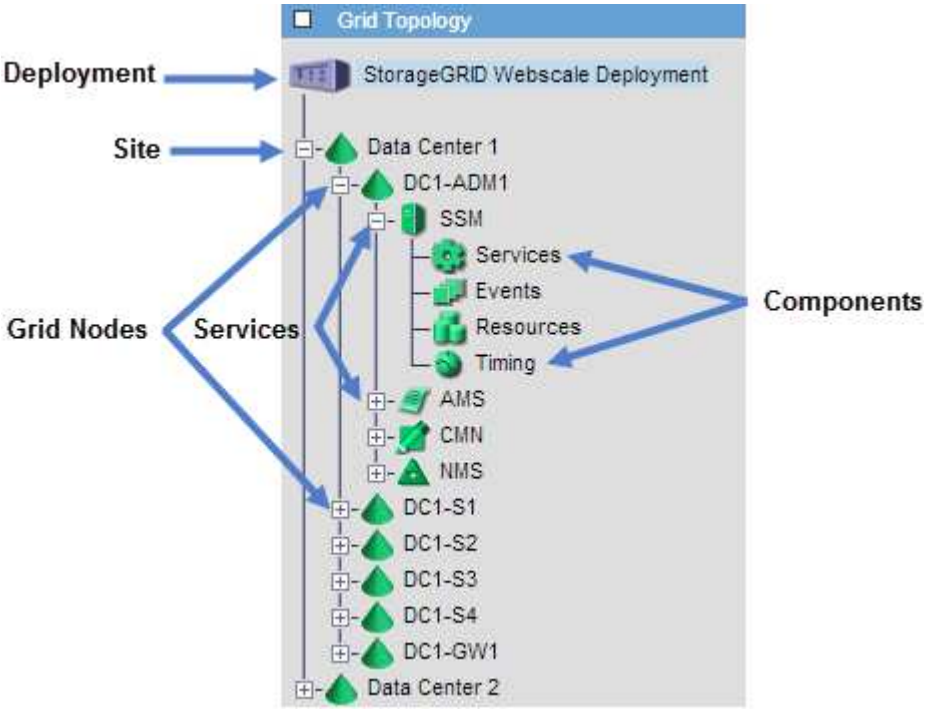
Informazioni correlate

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

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 alla struttura Grid Topology, selezionare **SUPPORT Tools Grid Topology**.



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 nell'intero sito o in ciascun nodo, tenere premuto il tasto **Ctrl** e fare clic su.

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.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

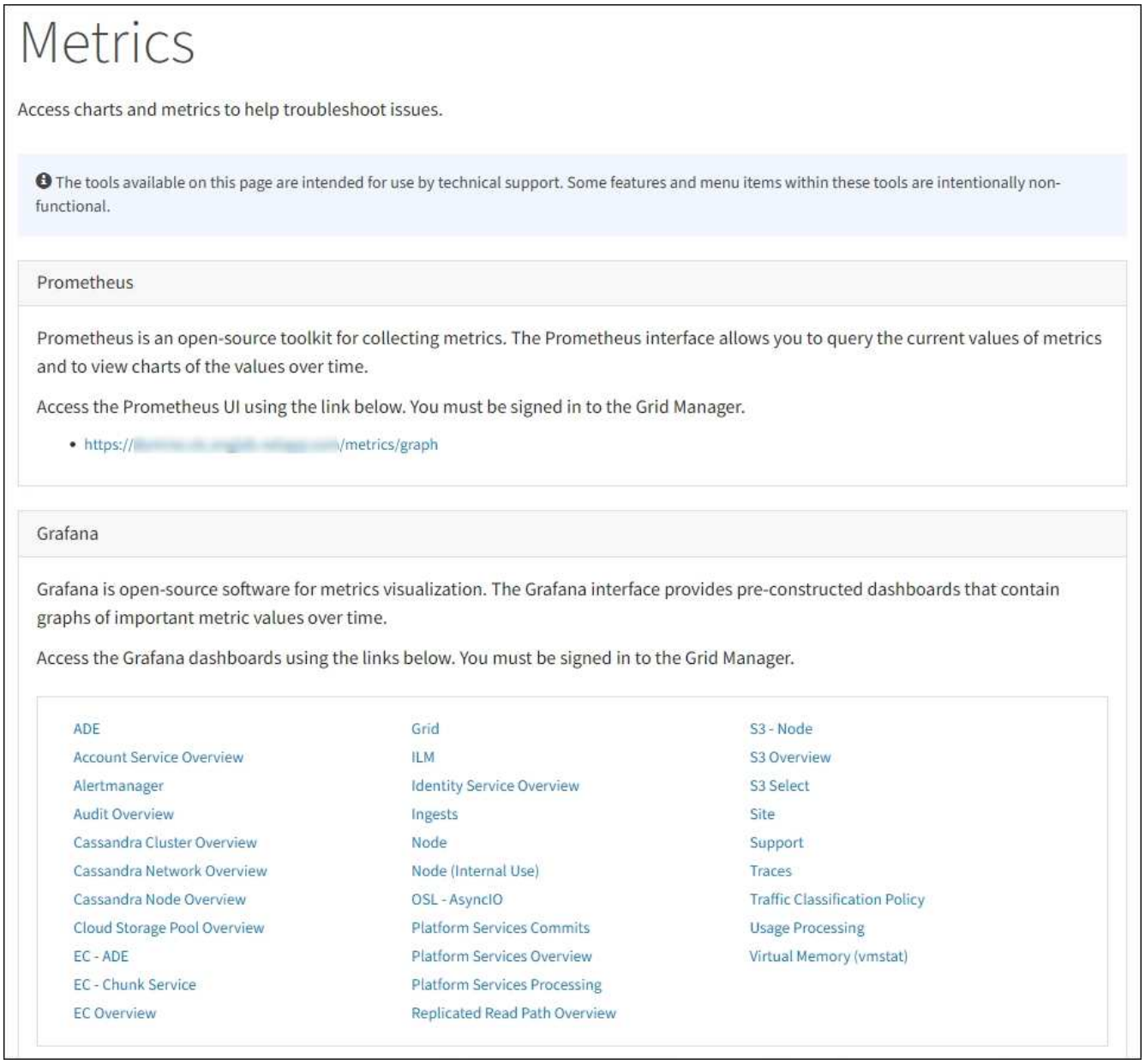
La pagina metriche consente di accedere alle interfacce utente Prometheus e Grafana. Prometheus è un software open-source per la raccolta di metriche. Grafana è un software open-source per la visualizzazione delle metriche.

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

Fasi

1. Come indicato dal supporto tecnico, selezionare **SUPPORTO Strumenti metriche**.

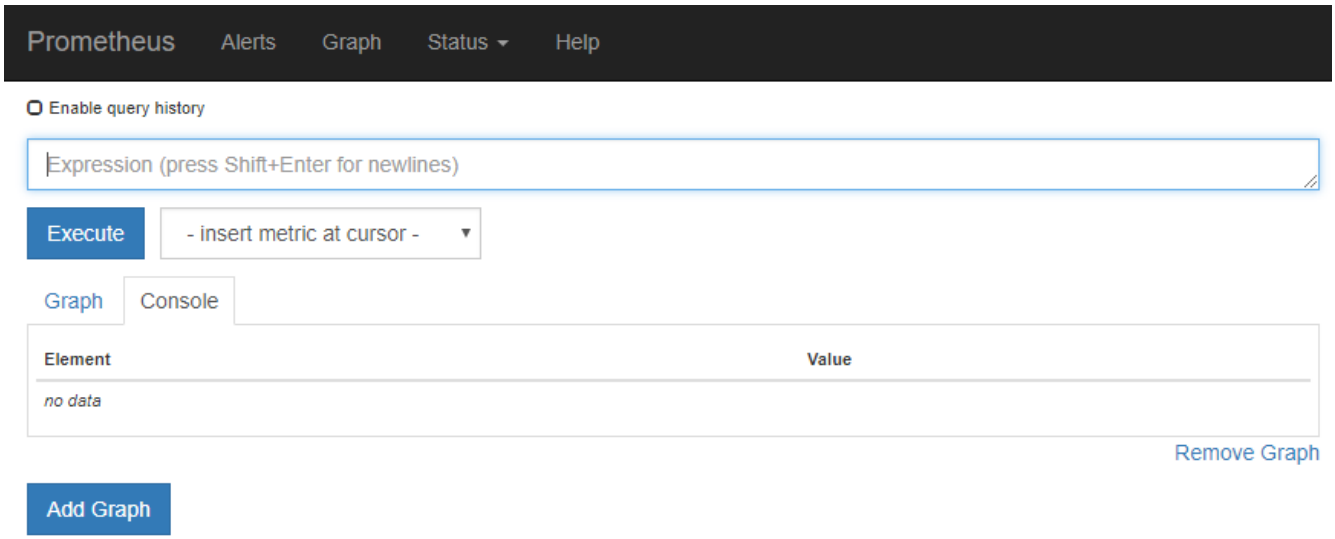
   Di seguito è riportato un esempio della pagina Metrics (metriche):



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

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

La pagina Diagnostics (Diagnostica) esegue una serie di controlli diagnostici sullo stato corrente della griglia. Ogni controllo diagnostico può avere uno dei tre stati seguenti:

- **Normale**: Tutti i valori rientrano nell'intervallo normale.
- **Attenzione**: Uno o più valori non rientrano nell'intervallo normale.
- **Attenzione**: Uno o più valori sono significativamente al di fuori dell'intervallo normale.

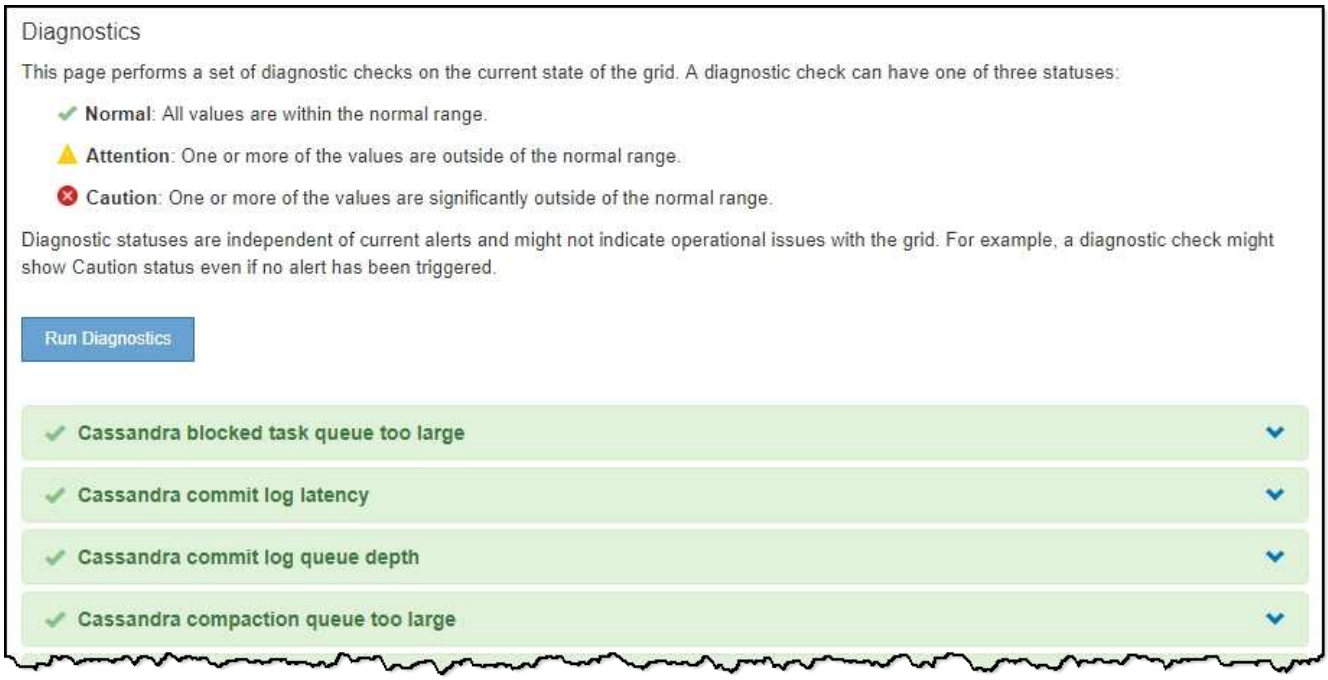
Gli stati di diagnostica sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la griglia. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato di attenzione anche se non è stato attivato alcun allarme.

Fasi

1. Selezionare **SUPPORT Tools Diagnostics**.

   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.



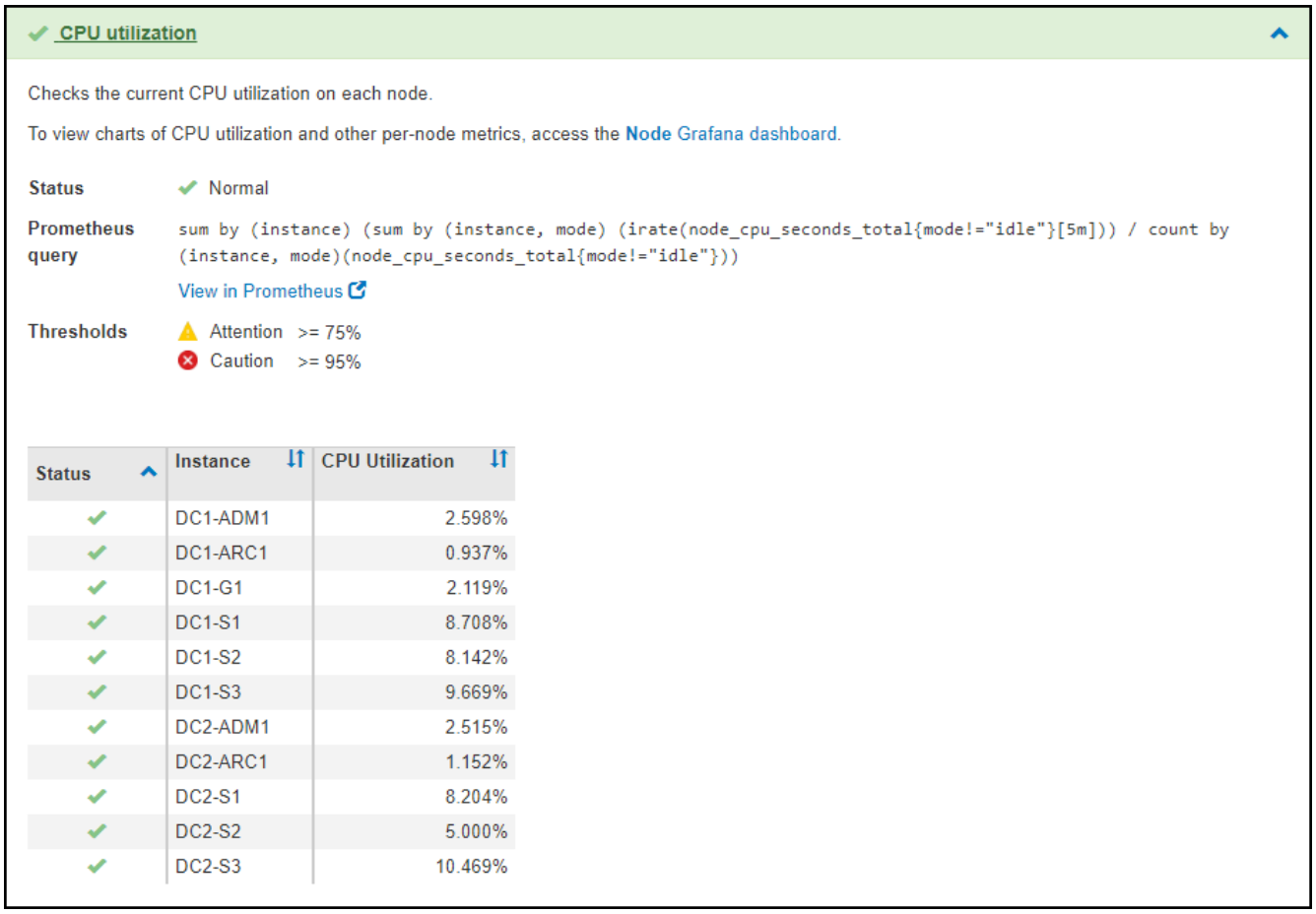
2. Per ulteriori informazioni su una diagnostica specifica, fare clic in un punto qualsiasi della riga.

   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 è possibile 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**.

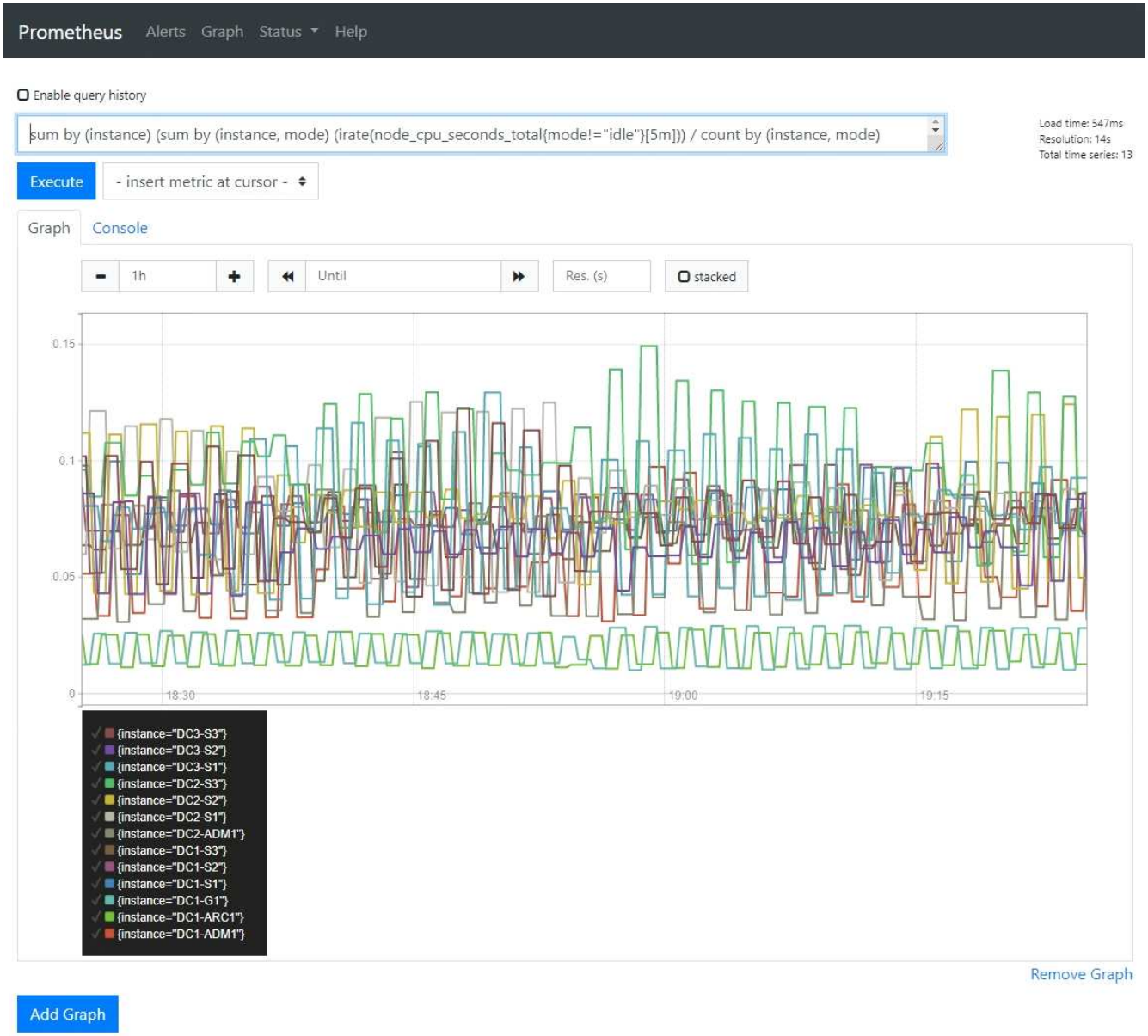
   Questo collegamento non viene visualizzato per tutte le diagnostiche.

   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.

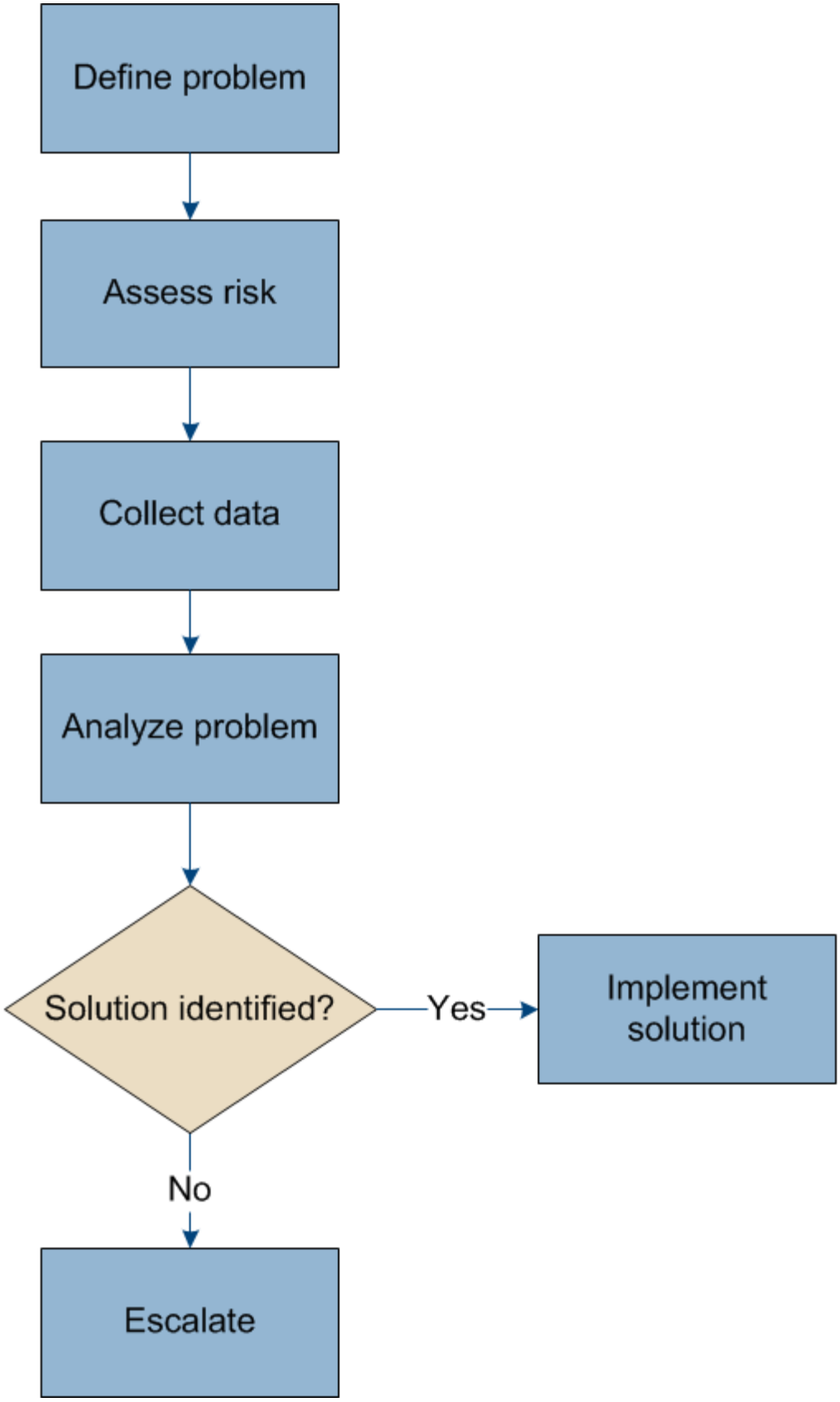
Risolvere i problemi di un sistema StorageGRID

Risolvere i problemi di un sistema StorageGRID

Se si riscontrano problemi durante l'utilizzo di un sistema StorageGRID, consultare i suggerimenti e le linee guida di questa sezione per ottenere assistenza nella determinazione e nella risoluzione del problema.

Panoramica della determinazione del problema

Se si verifica un problema quando Amministrazione di un sistema StorageGRID, è possibile utilizzare il processo descritto in questa figura per identificare e analizzare il problema. In molti casi, è possibile risolvere i problemi da soli; tuttavia, potrebbe essere necessario eseguire l'escalation di alcuni problemi al supporto tecnico.



Definire il problema

Il primo passo per risolvere un problema è definire il problema in modo chiaro.

Questa tabella fornisce esempi dei tipi di informazioni che è possibile raccogliere per definire un problema:

Domanda	Esempio di risposta
Cosa fa o non fa il sistema StorageGRID? Quali sono i suoi sintomi?	Le applicazioni client segnalano che non è possibile acquisire oggetti in StorageGRID.
Quando è iniziato il problema?	L'acquisizione di oggetti è stata negata per la prima volta alle 14:50 dell'8 gennaio 2020.
Come hai notato il problema per la prima volta?	Notificato dall'applicazione client. Ha ricevuto anche notifiche email di avviso.
Il problema si verifica in modo coerente o solo a volte?	Il problema è in corso.
Se il problema si verifica regolarmente, quali passaggi lo causano	Il problema si verifica ogni volta che un client tenta di acquisire un oggetto.
Se il problema si verifica in modo intermittente, quando si verifica? Registrare i tempi di ciascun incidente di cui si è a conoscenza.	Il problema non è intermittente.
Hai già visto questo problema? Con quale frequenza avete avuto questo problema in passato?	Questa è la prima volta che vedo questo problema.

Valutare i rischi e l'impatto sul sistema

Una volta definito il problema, valutarne il rischio e l'impatto sul sistema StorageGRID. Ad esempio, la presenza di avvisi critici non significa necessariamente che il sistema non stia fornendo servizi di base.

Questa tabella riassume l'impatto del problema di esempio sulle operazioni del sistema:

Domanda	Esempio di risposta
Il sistema StorageGRID è in grado di acquisire contenuti?	No
Le applicazioni client possono recuperare il contenuto?	Alcuni oggetti possono essere recuperati e altri no.
I dati sono a rischio?	No
La capacità di condurre il business è gravemente compromessa?	Sì, perché le applicazioni client non possono memorizzare oggetti nel sistema StorageGRID e i dati non possono essere recuperati in modo coerente.

Raccogliere i dati

Dopo aver definito il problema e averne valutato il rischio e l'impatto, raccogliere i dati per l'analisi. Il tipo di dati più utili da raccogliere dipende dalla natura del problema.

Tipo di dati da raccogliere	Perché raccogliere questo dat	Istruzioni
Creare una tempistica delle modifiche recenti	Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	• Creare una tempistica delle modifiche recenti
Consente di rivedere avvisi e allarmi	Gli avvisi e gli allarmi possono aiutare a determinare rapidamente la causa principale di un problema fornendo importanti indizi sui problemi sottostanti che potrebbero causarlo. Consultare l'elenco degli avvisi e degli allarmi correnti per verificare se StorageGRID ha identificato la causa principale di un problema. Per ulteriori informazioni, rivedere gli avvisi e gli allarmi attivati in passato.	• Visualizzare gli avvisi correnti • Visualizzare gli allarmi legacy • Visualizzare gli avvisi risolti • Rivedere la cronologia degli allarmi e la frequenza degli allarmi (sistema precedente)
Monitorare gli eventi	Gli eventi includono qualsiasi errore di sistema o evento di guasto per un nodo, inclusi errori come gli errori di rete. Monitorare gli eventi per ottenere ulteriori informazioni sui problemi o per la risoluzione dei problemi.	• Monitorare gli eventi
Identificare i trend utilizzando grafici e report di testo	Le tendenze possono fornire indizi preziosi su quando sono comparsi i problemi per la prima volta e possono aiutarti a capire quanto rapidamente le cose stanno cambiando.	• Utilizzare grafici e grafici • Utilizzare report di testo
Stabilire le linee di base	Raccogliere informazioni sui livelli normali dei vari valori operativi. Questi valori di riferimento, e le deviazioni da queste linee di base, possono fornire indizi preziosi.	• Stabilire le linee di base
Eseguire test di acquisizione e recupero	Per risolvere i problemi di performance con acquisizione e recupero, utilizzare una workstation per memorizzare e recuperare gli oggetti. Confrontare i risultati con quelli osservati durante l'utilizzo dell'applicazione client.	• Monitorare L'EFFICIENZA e OTTENERE le performance
Esaminare i messaggi di audit	Esaminare i messaggi di audit per seguire in dettaglio le operazioni di StorageGRID. I dettagli nei messaggi di audit possono essere utili per la risoluzione di molti tipi di problemi, inclusi quelli relativi alle performance.	• Esaminare i messaggi di audit

Tipo di dati da raccogliere	Perché raccogliere questo dat	Istruzioni
Controllare le posizioni degli oggetti e l'integrità dello storage	In caso di problemi di storage, verificare che gli oggetti siano posizionati nel punto previsto. Verificare l'integrità dei dati dell'oggetto su un nodo di storage.	• Monitorare le operazioni di verifica degli oggetti • Confermare le posizioni dei dati degli oggetti • Verificare l'integrità dell'oggetto
Raccogliere i dati per il supporto tecnico	Il supporto tecnico potrebbe richiedere di raccogliere dati o rivedere informazioni specifiche per risolvere i problemi.	• Raccogliere i file di log e i dati di sistema • Attivare manualmente un messaggio AutoSupport • Rivedere le metriche di supporto

Crea una timeline di modifiche recenti

Quando si verifica un problema, è necessario prendere in considerazione le modifiche apportate di recente e il momento in cui si sono verificate tali modifiche.

- Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.
- Una tempistica delle modifiche può aiutarti a identificare quali modifiche potrebbero essere responsabili di un problema e in che modo ciascuna modifica potrebbe avere influenzato il suo sviluppo.

Creare una tabella di modifiche recenti al sistema che includa informazioni su quando si è verificata ogni modifica e su eventuali dettagli rilevanti relativi alla modifica, ad esempio informazioni su ciò che è accaduto durante l'esecuzione della modifica:

Tempo di cambiamento	Tipo di cambiamento	Dettagli
Ad esempio: • Quando è stato avviato il ripristino del nodo? • Quando è stato completato l'aggiornamento del software? • Hai interrotto il processo?	Che cosa è successo? Cosa hai fatto?	Documentare i dettagli relativi alla modifica. Ad esempio: • Dettagli delle modifiche di rete. • Quale hotfix è stato installato. • Come sono cambiati i carichi di lavoro dei client. Assicurarsi di notare se più di una modifica si è verificata contemporaneamente. Ad esempio, questa modifica è stata apportata mentre era in corso un aggiornamento?

Esempi di modifiche recenti significative

Ecco alcuni esempi di modifiche potenzialmente significative:

- Il sistema StorageGRID è stato recentemente installato, ampliato o ripristinato?
- Il sistema è stato aggiornato di recente? È stata applicata una correzione rapida?
- L'hardware è stato riparato o modificato di recente?
- La policy ILM è stata aggiornata?
- Il carico di lavoro del client è cambiato?
- L'applicazione client o il suo comportamento sono cambiati?
- Hai modificato i bilanciatori di carico o aggiunto o rimosso un gruppo ad alta disponibilità di nodi di amministrazione o nodi gateway?
- Sono state avviate attività che potrebbero richiedere molto tempo? Alcuni esempi sono:
  - Ripristino di un nodo di storage guasto
  - Disattivazione del nodo di storage
- Sono state apportate modifiche all'autenticazione dell'utente, ad esempio l'aggiunta di un tenant o la modifica della configurazione LDAP?
- La migrazione dei dati è in corso?
- I servizi della piattaforma sono stati abilitati o modificati di recente?
- La compliance è stata abilitata di recente?
- I pool di storage cloud sono stati aggiunti o rimossi?
- Sono state apportate modifiche alla compressione o alla crittografia dello storage?
- Sono state apportate modifiche all'infrastruttura di rete? Ad esempio, VLAN, router o DNS.
- Sono state apportate modifiche alle origini NTP?
- Sono state apportate modifiche alle interfacce Grid, Admin o Client Network?
- Sono state apportate modifiche alla configurazione del nodo di archiviazione?

- Sono state apportate altre modifiche al sistema StorageGRID o al suo ambiente?

stabilire le linee di base

È possibile stabilire linee di base per il sistema registrando i livelli normali di diversi valori operativi. In futuro, è possibile confrontare i valori correnti con queste linee di base per rilevare e risolvere i valori anomali.

Proprietà	Valore	Come ottenere
Consumo medio di storage	GB consumati al giorno Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione). Nel grafico Storage used - Object Data (Storage utilizzato - dati oggetto), individuare un periodo in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare la quantità di storage consumata ogni giorno È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Consumo medio di metadati	GB consumati al giorno Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione). Nel grafico Storage used - Object Metadata (Storage utilizzato - metadati oggetto), individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per valutare la quantità di storage dei metadati consumata ogni giorno È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.

Proprietà	Valore	Come ottenere
Tasso di operazioni S3/Swift	Operazioni/secondo	Accedere alla dashboard in Grid Manager. Nella sezione Protocol Operations (operazioni protocollo), visualizzare i valori per la velocità S3 e la velocità Swift. Per visualizzare i tassi di acquisizione e recupero e i conteggi per un sito o nodo specifico, selezionare **NODES *Site o Storage Node* Objects**. Spostare il cursore sul grafico Ingest e Retrieve per S3 o Swift.
Operazioni S3/Swift non riuscite	Operazioni	Selezionare **SUPPORT Tools Grid topology**. Nella scheda Overview (Panoramica) della sezione API Operations (operazioni API), visualizzare il valore di S3 Operations - Failed (operazioni S3 - non riuscite) o Swift Operations - Failed (operazioni Swift - non riuscite).
Tasso di valutazione ILM	Oggetti/secondo	Dalla pagina nodi, selezionare ***grid* ILM**. Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare un valore di riferimento per **tasso di valutazione** per il sistema.
Velocità di scansione ILM	Oggetti/secondo	Selezionare **NODI *grid* ILM**. Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare un valore di riferimento per **velocità di scansione** per il sistema.

Proprietà	Valore	Come ottenere
Oggetti accodati dalle operazioni del client	Oggetti/secondo	Selezionare **NODI *grid* ILM**. Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore del mouse sul grafico per stimare un valore di riferimento per **oggetti accodati (dalle operazioni client)** per il sistema.
Latenza media delle query	Millisecondi	Selezionare **NODI *nodo di storage* oggetti**. Nella tabella Query, visualizzare il valore della latenza media.

Analizzare i dati

Utilizzare le informazioni raccolte per determinare la causa del problema e le potenziali soluzioni.

-analisi dipende dal problema, ma in generale:

- Individuare i punti di guasto e i colli di bottiglia utilizzando gli allarmi.
- Ricostruire la cronologia dei problemi utilizzando la cronologia degli allarmi e i grafici.
- Utilizzare i grafici per individuare le anomalie e confrontare la situazione del problema con il normale funzionamento.

Lista di controllo per le informazioni di escalation

Se non si riesce a risolvere il problema da solo, contattare il supporto tecnico. Prima di contattare il supporto tecnico, raccogliere le informazioni elencate nella seguente tabella per facilitare la risoluzione del problema.

✔	Elemento	Note
	Dichiarazione del problema	Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo coerente o intermittente? In caso di intermittenza, quali sono le volte in cui si è verificato il problema? Definire il problema
	Valutazione dell'impatto	Qual è la gravità del problema? Qual è l'impatto sull'applicazione client? • Il client si è connesso correttamente in precedenza? • Il client è in grado di acquisire, recuperare ed eliminare i dati?

✔	Elemento	Note
	ID sistema StorageGRID	Selezionare **MANUTENZIONE sistema licenza**. L'ID di sistema StorageGRID viene visualizzato come parte della licenza corrente.
	Versione del software	Nella parte superiore di Gestione griglia, selezionare l'icona della guida e selezionare **About** (informazioni su) per visualizzare la versione di StorageGRID.
	Personalizzazione	Riepilogare la configurazione del sistema StorageGRID. Ad esempio, elencare quanto segue: • Il grid utilizza la compressione dello storage, la crittografia dello storage o la conformità? • ILM esegue la replica o la cancellazione di oggetti codificati? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano comportamenti di ingest rigorosi, bilanciati o doppi?
	File di log e dati di sistema	Raccogliere i file di log e i dati di sistema per il sistema. Selezionare **SUPPORT Tools Logs**. È possibile raccogliere i log per l'intera griglia o per i nodi selezionati. Se si stanno raccogliendo registri solo per i nodi selezionati, assicurarsi di includere almeno un nodo di storage che dispone del servizio ADC. I primi tre nodi di storage di un sito includono il servizio ADC. Raccogliere i file di log e i dati di sistema
	Informazioni di riferimento	Raccogliere informazioni di riferimento relative alle operazioni di acquisizione, alle operazioni di recupero e al consumo dello storage. Stabilire le linee di base
	Tempistiche delle modifiche recenti	Creare una timeline che riepiloga le modifiche recenti apportate al sistema o al suo ambiente. Creare una tempistica delle modifiche recenti
	Cronologia degli sforzi per diagnosticare il problema	Se sono state adottate misure per diagnosticare o risolvere il problema da soli, assicurarsi di registrare i passaggi e il risultato.

Risolvere i problemi relativi a oggetti e storage

Confermare le posizioni dei dati degli oggetti

A seconda del problema, potrebbe essere necessario confermare la posizione in cui vengono memorizzati i dati dell'oggetto. Ad esempio, è possibile verificare che il criterio ILM funzioni come previsto e che i dati degli oggetti vengano memorizzati dove previsto.

Di cosa hai bisogno

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
  - **UUID**: Identificativo universalamente univoco dell'oggetto. Inserire l'UUID in tutte le lettere maiuscole.
  - **CBID**: Identificatore univoco dell'oggetto all'interno di StorageGRID . È possibile ottenere il CBID di un oggetto dal log di audit. Inserire il CBID in tutte le lettere maiuscole.
  - **S3 bucket e chiave oggetto**: Quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto.
  - **Swift container and object name**: Quando un oggetto viene acquisito tramite l'interfaccia Swift, l'applicazione client utilizza una combinazione di container e object name per memorizzare e identificare l'oggetto.

Fasi

1. Selezionare **ILM** > **Object metadata lookup**.
2. Digitare l'identificativo dell'oggetto nel campo **Identifier**.

   È possibile immettere UUID, CBID, S3 bucket/object-key o Swift container/object-name.

3. Se si desidera cercare una versione specifica dell'oggetto, inserire l'ID versione (facoltativo).

4. Selezionare **Cerca**.

   Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

   - Metadati di sistema, tra cui l'ID oggetto (UUID), l'ID versione (facoltativo), il nome dell'oggetto, il nome del contenitore, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.

- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
- Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

  Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```

Informazioni correlate

Gestire gli oggetti con ILM

Utilizzare S3

USA Swift

Errori dell'archivio di oggetti (volume di storage)

Lo storage sottostante su un nodo di storage è diviso in archivi di oggetti. Gli archivi di oggetti sono anche noti come volumi di storage.

È possibile visualizzare le informazioni sull'archivio di oggetti per ciascun nodo di storage. Gli archivi di oggetti sono visualizzati nella parte inferiore della pagina **NODE *Storage Node* Storage**.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

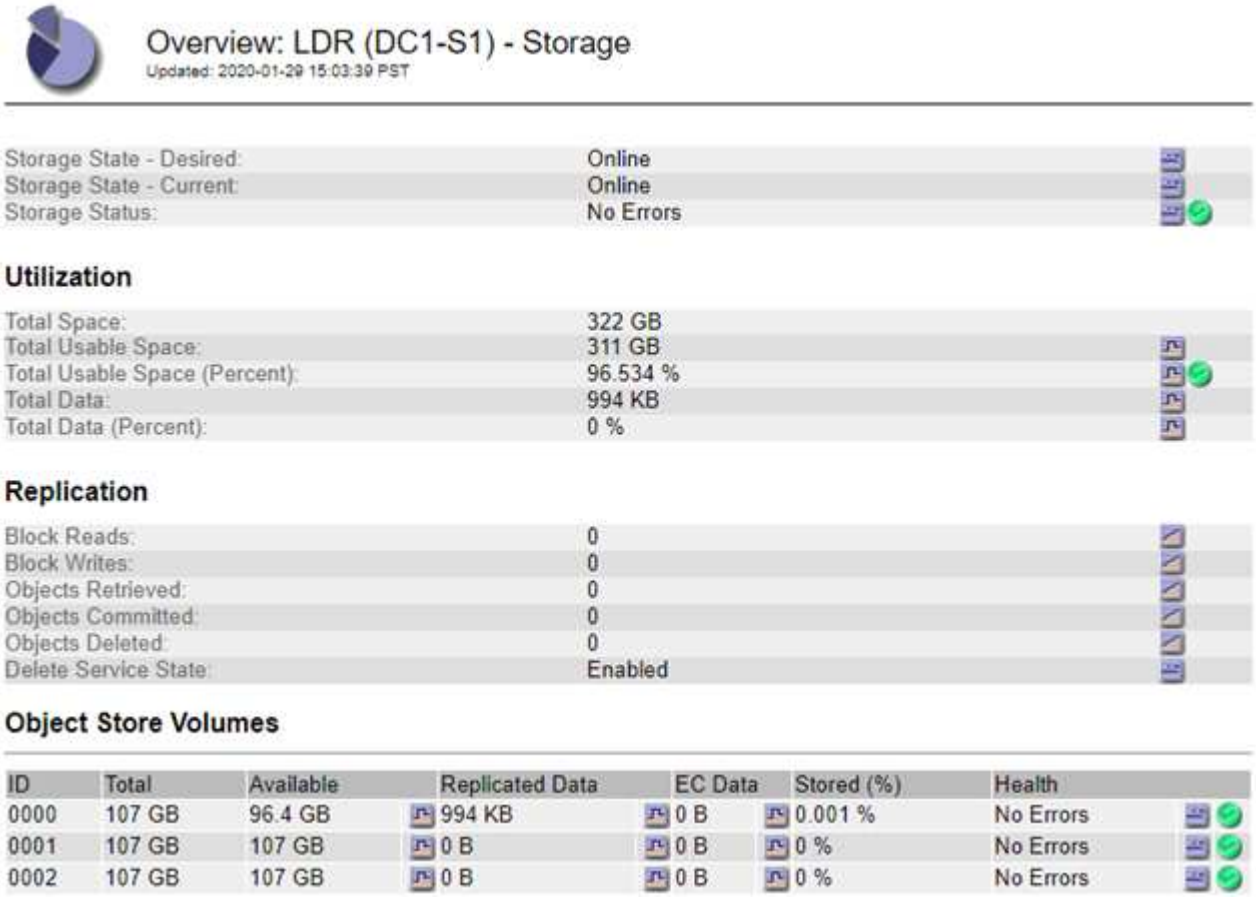
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Per ulteriori informazioni su ciascun nodo di storage, attenersi alla seguente procedura:

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site Storage Node*** **LDR Storage Overview Main**.



A seconda della natura del guasto, gli errori di un volume di storage potrebbero essere riflessi in un allarme sullo stato di storage o sullo stato di un archivio di oggetti. In caso di guasto di un volume di storage, è necessario riparare il volume di storage guasto per ripristinare la funzionalità completa del nodo di storage il prima possibile. Se necessario, accedere alla scheda **Configurazione** e posizionare il nodo di storage in uno stato di sola lettura-in modo che il sistema StorageGRID possa utilizzarlo per il recupero dei dati mentre si prepara per un ripristino completo del server.

Informazioni correlate

Ripristino e manutenzione

Verificare l'integrità dell'oggetto

Il sistema StorageGRID verifica l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti corrotti e mancanti.

Esistono due processi di verifica: Verifica in background e verifica dell'esistenza degli oggetti (in precedenza chiamata verifica in primo piano). Lavorano insieme per garantire l'integrità dei dati. La verifica in background viene eseguita automaticamente e verifica continuamente la correttezza dei dati dell'oggetto. Il controllo dell'esistenza degli oggetti può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) degli oggetti.

Che cos'è la verifica in background?

Il processo di verifica in background verifica automaticamente e continuamente la presenza di copie corrotte dei dati degli oggetti nei nodi di storage e tenta automaticamente di risolvere eventuali problemi rilevati.

La verifica in background verifica l'integrità degli oggetti replicati e degli oggetti con codifica in cancellazione, come segue:

- **Oggetti replicati**: Se il processo di verifica in background trova un oggetto replicato corrotto, la copia corrotta viene rimossa dalla sua posizione e messa in quarantena in un altro punto del nodo di storage. Quindi, viene generata una nuova copia non corrotta e posizionata per soddisfare il criterio ILM attivo. La nuova copia potrebbe non essere inserita nel nodo di storage utilizzato per la copia originale.

  > I dati degli oggetti corrotti vengono messi in quarantena invece che cancellati dal sistema, in modo che sia ancora possibile accedervi. Per ulteriori informazioni sull'accesso ai dati degli oggetti in quarantena, contattare il supporto tecnico.

- **Oggetti con codifica di cancellazione**: Se il processo di verifica in background rileva che un frammento di un oggetto con codifica di cancellazione è corrotto, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage, utilizzando i dati rimanenti e i frammenti di parità. Se il frammento danneggiato non può essere ricostruito, si tenta di recuperare un'altra copia dell'oggetto. Se il recupero ha esito positivo, viene eseguita una valutazione ILM per creare una copia sostitutiva dell'oggetto con codice di cancellazione.

  Il processo di verifica in background controlla solo gli oggetti sui nodi di storage. Non controlla gli oggetti nei nodi di archiviazione o in un pool di storage cloud. Gli oggetti devono avere più di quattro giorni di età per poter essere qualificati per la verifica in background.

La verifica in background viene eseguita a una velocità continua che non interferisce con le normali attività del sistema. Impossibile interrompere la verifica in background. Tuttavia, se si sospetta un problema, è possibile aumentare il tasso di verifica in background per verificare più rapidamente il contenuto di un nodo di storage.

Avvisi e allarmi (legacy) relativi alla verifica in background

Se il sistema rileva un oggetto corrotto che non è in grado di correggere automaticamente (perché il danneggiamento impedisce l'identificazione dell'oggetto), viene attivato l'avviso **rilevato oggetto corrotto non identificato**.

Se la verifica in background non riesce a sostituire un oggetto corrotto perché non riesce a individuare un'altra copia, viene attivato l'avviso **oggetti persi**.

Modificare il tasso di verifica in background

È possibile modificare la velocità con cui la verifica in background controlla i dati degli oggetti replicati su un nodo di storage in caso di dubbi sull'integrità dei dati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

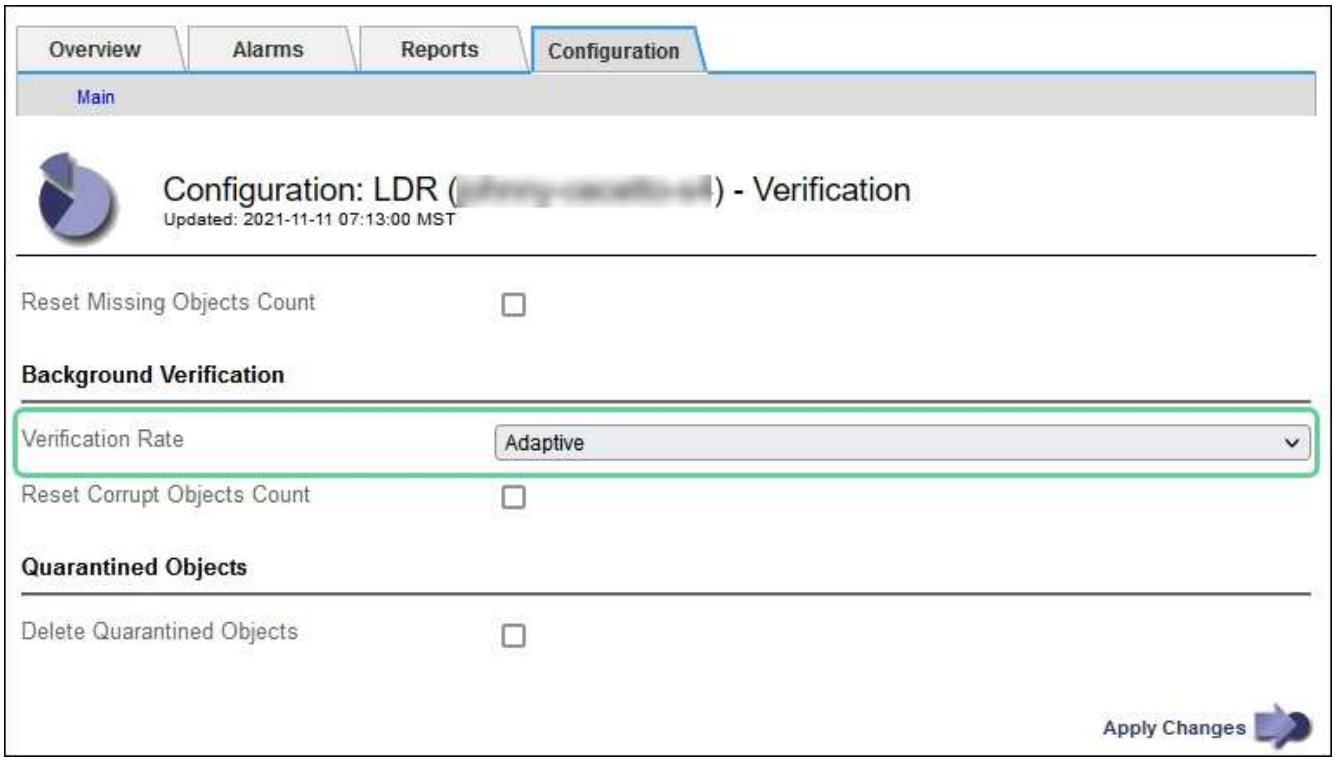
È possibile modificare il tasso di verifica per la verifica in background su un nodo di storage:

- Adattivo: Impostazione predefinita. L'attività è progettata per la verifica a un massimo di 4 MB/s o 10 oggetti/s (a seconda di quale valore viene superato per primo).
- Elevato: La verifica dello storage procede rapidamente, a una velocità che può rallentare le normali attività del sistema.

Utilizzare la frequenza di verifica alta solo quando si sospetta che un errore hardware o software possa avere dati oggetto corrotti. Una volta completata la verifica in background con priorità alta, la velocità di verifica viene ripristinata automaticamente su Adaptive.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Storage Node* LDR Verification**.
3. Selezionare **Configurazione principale**.
4. Accedere a **LDR verifica Configurazione principale**.
5. In background Verification (verifica in background), selezionare **Verification Rate High** (tasso di verifica) o **Verification Rate Adaptive** (tasso di verifica).



> Impostando la frequenza di verifica su alta, si attiva l'allarme VPRI (tasso di verifica) legacy a livello di avviso.

6. Fare clic su **Applica modifiche**.
7. Monitorare i risultati della verifica in background per gli oggetti replicati.
   a. Andare a **NODES *Storage Node* Objects**.
   b. Nella sezione verifica, monitorare i valori per **oggetti corrotti** e **oggetti corrotti non identificati**.

      Se la verifica in background trova dati di oggetti replicati corrotti, la metrica **Corrupt Objects** viene incrementata e StorageGRID tenta di estrarre l'identificatore di oggetti dai dati, come segue:

- Se è possibile estrarre l'identificativo dell'oggetto, StorageGRID crea automaticamente una nuova copia dei dati dell'oggetto. La nuova copia può essere eseguita in qualsiasi punto del sistema StorageGRID che soddisfi la policy ILM attiva.
- Se l'identificatore dell'oggetto non può essere estratto (perché è stato danneggiato), la metrica **Corrupt Objects Unidentified** viene incrementata e viene attivato l'avviso **Unidentified corrotto Object Detected**.

c. Se vengono rilevati dati di oggetti replicati corrotti, contattare il supporto tecnico per determinare la causa principale del danneggiamento.

8. Monitorare i risultati della verifica in background per gli oggetti con codifica erasure.

   Se la verifica in background trova frammenti corrotti di dati di oggetti con codifica di cancellazione, l'attributo corrotto Fragments Detected (frammenti corrotti rilevati) viene incrementato. StorageGRID esegue il ripristino ricostruendo il frammento corrotto in posizione sullo stesso nodo di storage.

   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Storage Node* LDR Erasure Coding**.
   c. Nella tabella Verification Results (risultati verifica), monitorare l'attributo corrotto Fragments Detected (ECCD).

9. Una volta ripristinati automaticamente gli oggetti corrotti dal sistema StorageGRID, ripristinare il numero di oggetti corrotti.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Storage Node* LDR Verification Configuration**.
   c. Selezionare **Ripristina conteggio oggetti corrotti**.
   d. Fare clic su **Applica modifiche**.

10. Se si è certi che gli oggetti in quarantena non sono necessari, è possibile eliminarli.

    > Se viene attivato l'allarme **oggetti persi** o l'allarme legacy PERSI (oggetti persi), il supporto tecnico potrebbe voler accedere agli oggetti in quarantena per eseguire il debug del problema sottostante o tentare il ripristino dei dati.

    a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
    b. Selezionare ***Storage Node* LDR Verification Configuration**.
    c. Selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).
    d. Selezionare **Applica modifiche**.

Che cos'è il controllo dell'esistenza di un oggetto?

Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti non verifica i dati degli oggetti stessi (la verifica in background lo fa), ma fornisce un modo per verificare l'integrità dei dispositivi di storage, soprattutto se un recente problema hardware potrebbe avere influenzato l'integrità dei dati.

A differenza della verifica in background, che si verifica automaticamente, è necessario avviare manualmente un lavoro di verifica dell'esistenza di un oggetto.

Il controllo dell'esistenza degli oggetti legge i metadati di ogni oggetto memorizzato in StorageGRID e verifica l'esistenza di copie di oggetti replicate e frammenti di oggetti codificati per la cancellazione. I dati mancanti

vengono gestiti come segue:

- **Copie replicate**: Se manca una copia dei dati degli oggetti replicati, StorageGRID tenta automaticamente di sostituire la copia da una copia memorizzata altrove nel sistema. Il nodo di storage esegue una copia esistente attraverso una valutazione ILM, che determina che il criterio ILM corrente non è più soddisfatto per questo oggetto perché manca un'altra copia. Viene generata una nuova copia per soddisfare la policy ILM attiva del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa posizione in cui è stata memorizzata la copia mancante.
- **Frammenti con codifica di cancellazione**: Se manca un frammento di un oggetto con codifica di cancellazione, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage utilizzando i frammenti rimanenti. Se il frammento mancante non può essere ricostruito (perché sono stati persi troppi frammenti), ILM tenta di trovare un'altra copia dell'oggetto, che può utilizzare per generare un nuovo frammento con codifica di cancellazione.

Eseguire il controllo dell'esistenza dell'oggetto

Viene creato ed eseguito un job di controllo dell'esistenza di un oggetto alla volta. Quando si crea un lavoro, selezionare i nodi di storage e i volumi che si desidera verificare. È inoltre possibile selezionare il controllo di coerenza per il lavoro.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Maintenance (manutenzione) o Root Access (accesso root).
- Hai garantito che i nodi di storage che desideri controllare siano online. Selezionare **NODES** per visualizzare la tabella dei nodi. Assicurarsi che non venga visualizzata alcuna icona di avviso accanto al nome del nodo per i nodi che si desidera controllare.
- Si è verificato che le seguenti procedure siano **non** in esecuzione sui nodi che si desidera controllare:
  - Espansione della griglia per aggiungere un nodo di storage
  - Decommissionare il nodo di storage
  - Ripristino di un volume di storage guasto
  - Ripristino di un nodo di storage con un disco di sistema guasto
  - Ribilanciamento EC
  - Clone del nodo dell'appliance

Il controllo dell'esistenza degli oggetti non fornisce informazioni utili durante l'esecuzione di queste procedure.

A proposito di questa attività

Il completamento di un processo di verifica dell'esistenza di un oggetto può richiedere giorni o settimane, a seconda del numero di oggetti nella griglia, dei nodi e dei volumi di storage selezionati e del controllo di coerenza selezionato. È possibile eseguire un solo processo alla volta, ma è possibile selezionare più nodi e volumi di storage contemporaneamente.

Fasi

1. Selezionare **MANUTENZIONE attività controllo dell'esistenza dell'oggetto**.
2. Selezionare **Crea job**. Viene visualizzata la procedura guidata Crea un processo di verifica dell'esistenza di un oggetto.
3. Selezionare i nodi contenenti i volumi che si desidera verificare. Per selezionare tutti i nodi online, selezionare la casella di controllo **Node name** (Nome nodo) nell'intestazione della colonna.

È possibile eseguire la ricerca in base al nome del nodo o al sito.

Non è possibile selezionare nodi non connessi alla griglia.

4. Selezionare **continua**.
5. Selezionare uno o più volumi per ciascun nodo dell'elenco. È possibile cercare i volumi utilizzando il numero del volume di storage o il nome del nodo.

   Per selezionare tutti i volumi per ciascun nodo selezionato, selezionare la casella di controllo **Storage volume** nell'intestazione della colonna.

6. Selezionare **continua**.
7. Selezionare il controllo di coerenza per il lavoro.

   Il controllo di coerenza determina il numero di copie dei metadati degli oggetti utilizzate per il controllo dell'esistenza degli oggetti.

   - **Strong-site**: Due copie di metadati in un singolo sito.
   - **Strong-Global**: Due copie di metadati in ogni sito.
   - **Tutti** (impostazione predefinita): Tutte e tre le copie dei metadati di ciascun sito.

     Per ulteriori informazioni sul controllo di coerenza, vedere le descrizioni nella procedura guidata.

8. Selezionare **continua**.
9. Controllare e verificare le selezioni. È possibile selezionare **Previous** (precedente) per passare a una fase precedente della procedura guidata e aggiornare le selezioni.

   Viene generato un job di controllo dell'esistenza di un oggetto che viene eseguito fino a quando non si verifica una delle seguenti condizioni:

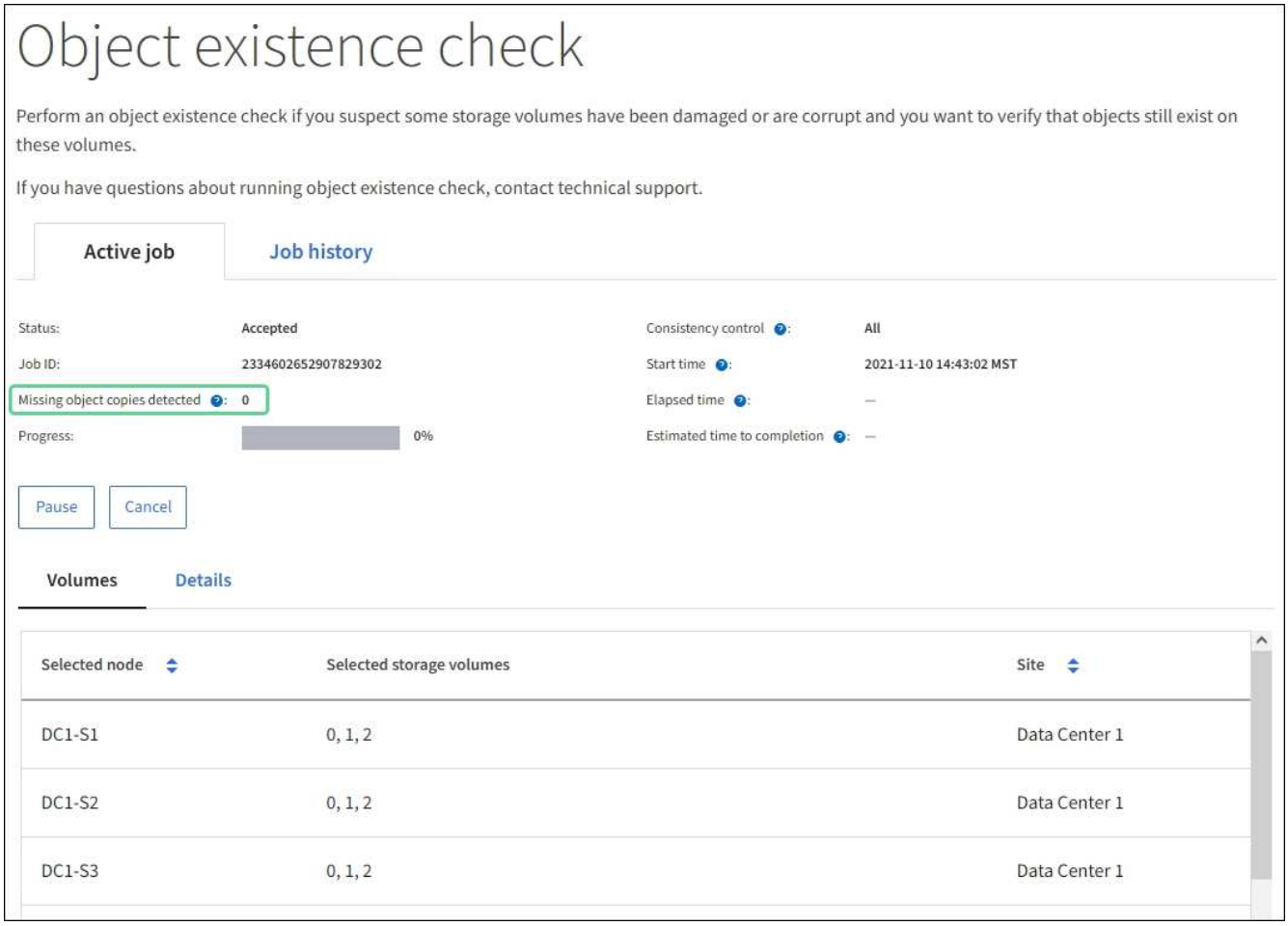
   - Il lavoro viene completato.
   - Il processo viene sospeso o annullato. È possibile riprendere un lavoro che è stato messo in pausa, ma non è possibile riprendere un lavoro che è stato annullato.
   - Il lavoro si blocca. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto bloccato**. Seguire le azioni correttive specificate per l'avviso.
   - Il lavoro non riesce. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto non riuscito**. Seguire le azioni correttive specificate per l'avviso.
   - Viene visualizzato il messaggio "Sservizio non disponibile" o "errore interno del server". Dopo un minuto, aggiornare la pagina per continuare a monitorare il lavoro.

   > Se necessario, è possibile allontanarsi dalla pagina di controllo dell'esistenza dell'oggetto e tornare indietro per continuare a monitorare il lavoro.

10. Durante l'esecuzione del processo, visualizzare la scheda **lavoro attivo** e annotare il valore di copie oggetto mancanti rilevate.

    Questo valore rappresenta il numero totale di copie mancanti di oggetti replicati e di oggetti con codifica di cancellazione con uno o più frammenti mancanti.

    Se il numero di copie di oggetti mancanti rilevate è superiore a 100, potrebbe esserci un problema con lo storage del nodo di storage.



11. Una volta completato il lavoro, eseguire eventuali azioni aggiuntive richieste:
    - Se le copie oggetto mancanti rilevate sono pari a zero, non sono stati rilevati problemi. Non è richiesta alcuna azione.
    - Se vengono rilevate copie di oggetti mancanti maggiori di zero e l'avviso **oggetti persi** non è stato attivato, tutte le copie mancanti sono state riparate dal sistema. Verificare che eventuali problemi hardware siano stati corretti per evitare danni futuri alle copie degli oggetti.
    - Se le copie degli oggetti mancanti rilevate sono superiori a zero e viene attivato l'avviso **oggetti persi**, l'integrità dei dati potrebbe risentirne. Contattare il supporto tecnico.
    - È possibile analizzare le copie degli oggetti persi utilizzando grep per estrarre i messaggi di audit LLST: `grep LLST audit_file_name`.

      Questa procedura è simile a quella per analisi degli oggetti smarriti, anche se per le copie di oggetto cercate `LLST` invece di `OLST`.

12. Se è stato selezionato il controllo di coerenza strong-site o strong-Global per il processo, attendere circa tre settimane per la coerenza dei metadati ed eseguire nuovamente il processo sugli stessi volumi.

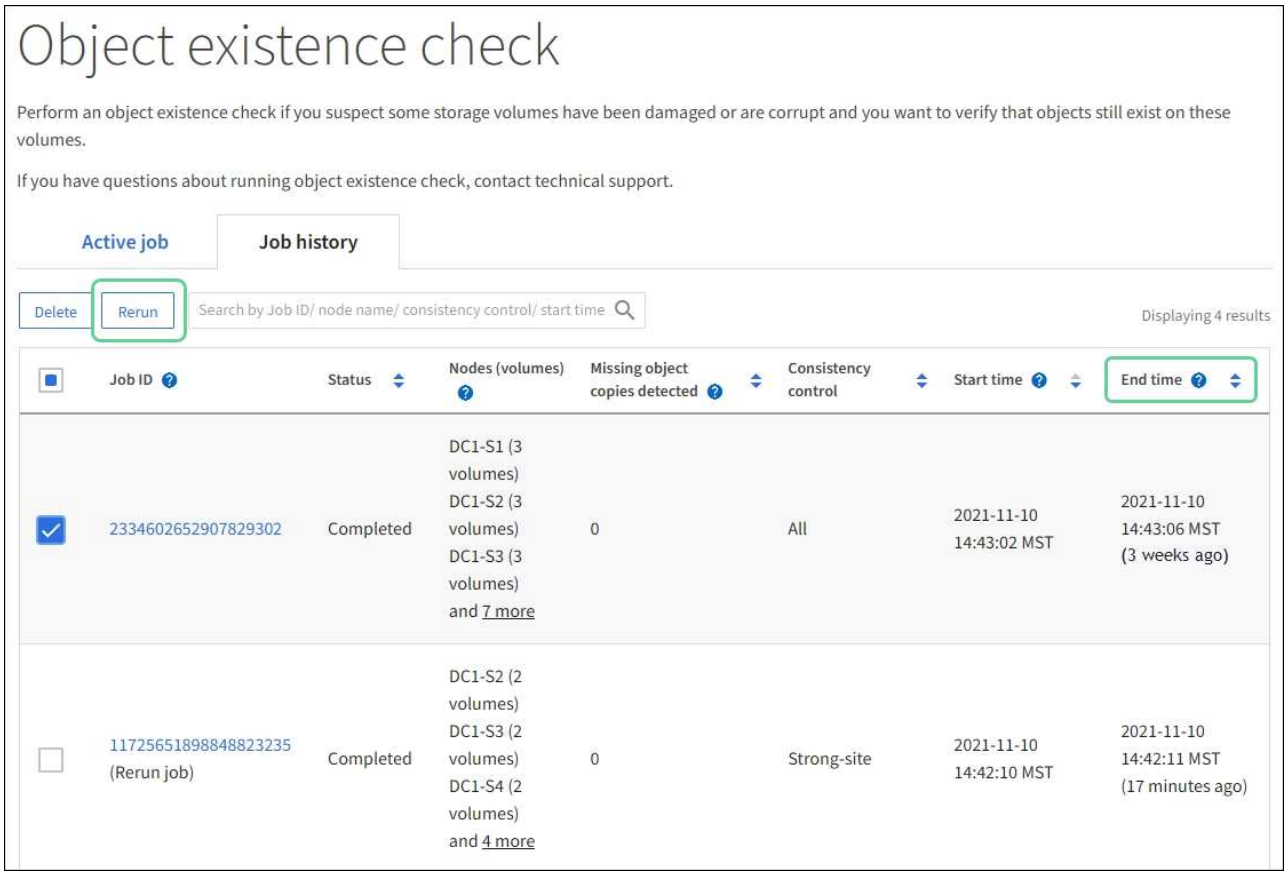
    Quando StorageGRID ha avuto il tempo di ottenere la coerenza dei metadati per i nodi e i volumi inclusi nel processo, la riesecuzione del processo potrebbe eliminare le copie degli oggetti mancanti segnalate erroneamente o causare il controllo di altre copie degli oggetti in caso di mancata esecuzione.

    a. Selezionare **MANUTENZIONE verifica dell'esistenza dell'oggetto Cronologia lavori**.
    b. Determinare quali lavori sono pronti per essere rieseguiti:

i. Esaminare la colonna **ora di fine** per determinare quali lavori sono stati eseguiti più di tre settimane fa.

ii. Per questi lavori, eseguire la scansione della colonna di controllo della coerenza per individuare la presenza di un sito forte o globale forte.

c. Selezionare la casella di controllo per ciascun processo che si desidera rieseguire, quindi selezionare **Rerun**.



d. Nella procedura guidata Riesegui job, esaminare i nodi e i volumi selezionati e il controllo di coerenza.

e. Quando si è pronti per rieseguire i lavori, selezionare **Rerun**.

Viene visualizzata la scheda lavoro attivo. Tutti i lavori selezionati vengono rieseguiti come un unico lavoro con un controllo di coerenza del sito sicuro. Un campo **lavori correlati** nella sezione Dettagli elenca gli ID lavoro per i lavori originali.

Al termine

Se hai ancora dubbi sull'integrità dei dati, vai a **SUPPORT Tools Grid topology *Site Storage Node* LDR Verification Configuration Main** e aumenta il tasso di verifica in background. La verifica in background verifica la correttezza di tutti i dati degli oggetti memorizzati e ripara eventuali problemi rilevati. L'individuazione e la riparazione di potenziali problemi il più rapidamente possibile riduce il rischio di perdita di dati.

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Gli oggetti possono essere recuperati per diversi motivi, tra cui le richieste di lettura da un'applicazione client, le verifiche in background dei dati degli oggetti replicati, le rivalutazioni ILM e il ripristino dei dati degli oggetti durante il ripristino di un nodo di storage.

Il sistema StorageGRID utilizza le informazioni sulla posizione nei metadati di un oggetto per determinare da quale posizione recuperare l'oggetto. Se una copia dell'oggetto non viene trovata nella posizione prevista, il sistema tenta di recuperare un'altra copia dell'oggetto da un'altra parte del sistema, supponendo che il criterio ILM contenga una regola per eseguire due o più copie dell'oggetto.

Se il recupero riesce, il sistema StorageGRID sostituisce la copia mancante dell'oggetto. In caso contrario, viene attivato l'avviso **oggetti persi**, come segue:

- Per le copie replicate, se non è possibile recuperare un'altra copia, l'oggetto viene considerato perso e viene attivato l'avviso.
- Per le copie codificate erasure, se una copia non può essere recuperata dalla posizione prevista, l'attributo Corrupt Copies Detected (ECOR) viene incrementato di uno prima di tentare di recuperare una copia da un'altra posizione. Se non viene trovata alcuna altra copia, viene attivato l'avviso.

Esaminare immediatamente tutti gli avvisi **oggetti persi** per determinare la causa principale della perdita e determinare se l'oggetto potrebbe ancora esistere in un nodo di storage o in un nodo di archivio offline o al momento non disponibile.

Nel caso in cui i dati degli oggetti senza copie vadano persi, non esiste una soluzione di recovery. Tuttavia, è necessario reimpostare il contatore Lost Objects (oggetti persi) per evitare che oggetti persi noti mascherino eventuali nuovi oggetti persi.

Informazioni correlate

Esaminare gli oggetti persi

Ripristinare i conteggi degli oggetti persi e mancanti

Esaminare gli oggetti persi

Quando viene attivato l'avviso **oggetti persi**, è necessario eseguire un'analisi immediata. Raccogliere informazioni sugli oggetti interessati e contattare il supporto tecnico.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

L'avviso **oggetti persi** indica che StorageGRID ritiene che non vi siano copie di un oggetto nella griglia. I dati potrebbero essere stati persi in modo permanente.

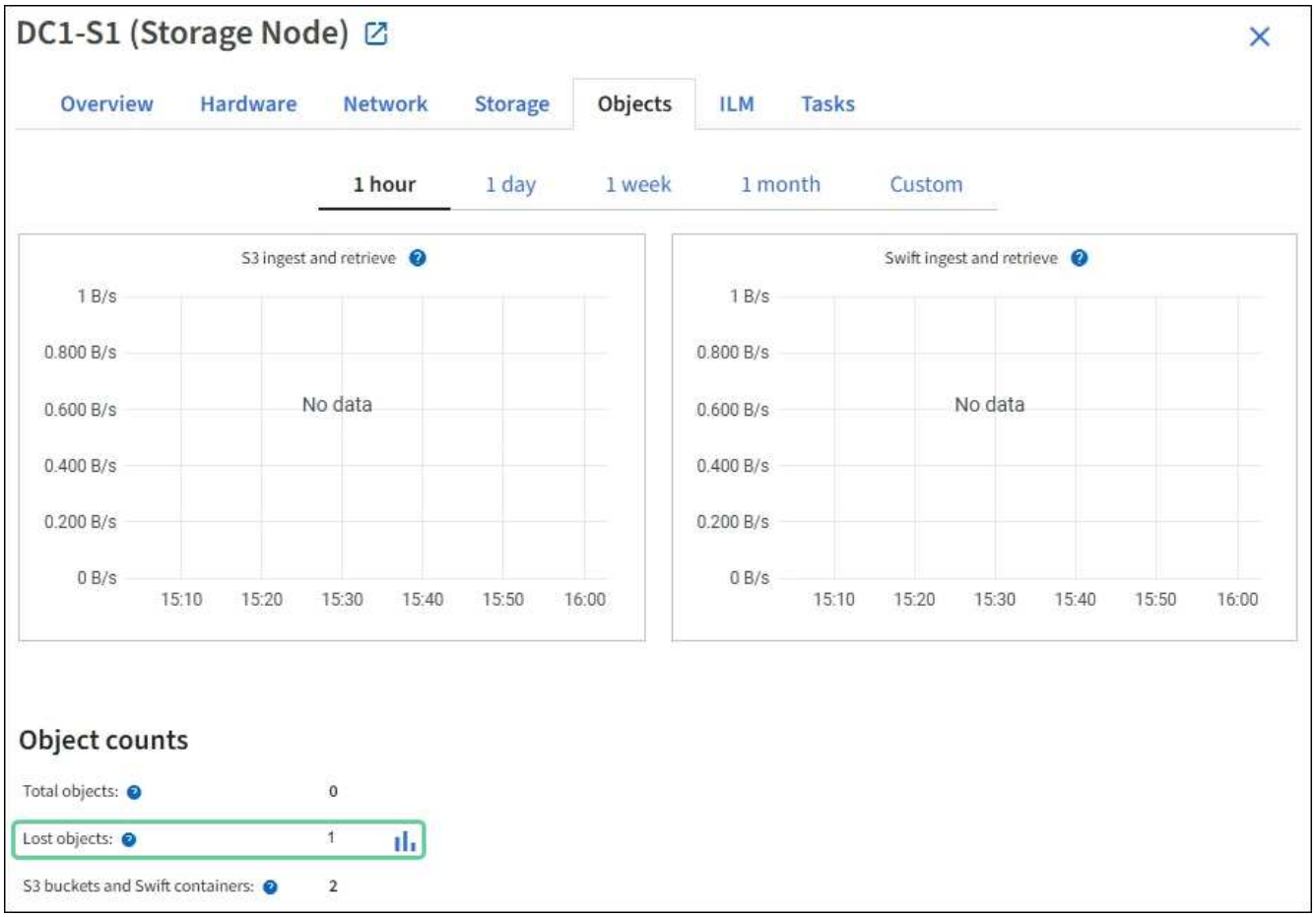
Esaminare immediatamente gli avvisi di oggetti smarriti. Potrebbe essere necessario intervenire per evitare ulteriori perdite di dati. In alcuni casi, potrebbe essere possibile ripristinare un oggetto perso se si esegue un'azione rapida.

Fasi

1. Selezionare **NODI**.
2. Selezionare ***Storage Node* Objects**.
3. Esaminare il numero di oggetti persi visualizzato nella tabella dei conteggi degli oggetti.

   Questo numero indica il numero totale di oggetti che il nodo della griglia rileva come mancanti dall'intero

sistema StorageGRID. Il valore è la somma dei contatori Lost Objects del componente Data Store all'interno dei servizi LDR e DDS.



4. Da un nodo amministratore, accedere al registro di controllo per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **oggetti persi**:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
   b. Passare alla directory in cui si trovano i registri di controllo. Inserire: `cd /var/local/audit/export/`
   c. Utilizzare grep per estrarre i messaggi di audit OLST (Object Lost). Inserire: `grep OLST audit_file_name`
   d. Annotare il valore UUID incluso nel messaggio.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Utilizzare `ObjectByUUID` Comando per trovare l'oggetto in base al relativo identificatore (UUID), quindi determinare se i dati sono a rischio.

   a. Telnet all'host locale 1402 per accedere alla console LDR.

   b. Inserire: `/proc/OBRP/ObjectByUUID UUID_value`

      In questo primo esempio, l'oggetto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` ha due posizioni elencate.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
```

```
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```


Nel secondo esempio, l’oggetto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` non ha posizioni elencate.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Esaminare l’output di /proc/OBRP/ObjectByUUID e intraprendere l’azione appropriata:

Metadati	Conclusione
Nessun oggetto trovato ("ERRORE":"")	Se l'oggetto non viene trovato, viene visualizzato il messaggio "ERROR":". Se l'oggetto non viene trovato, è possibile azzerare il numero di **oggetti persi** per eliminare l'avviso. La mancanza di un oggetto indica che l'oggetto è stato intenzionalmente cancellato.
Posizioni 0	Se nell'output sono presenti posizioni, l'avviso **oggetti persi** potrebbe essere un falso positivo. Verificare che gli oggetti esistano. Utilizzare l'ID nodo e il percorso del file elencati nell'output per confermare che il file a oggetti si trova nella posizione indicata. (La procedura per ricerca di oggetti potenzialmente persi Spiega come utilizzare l'ID nodo per trovare il nodo di storage corretto). Se gli oggetti sono presenti, è possibile ripristinare il numero di **oggetti persi** per cancellare l'avviso.
Posizioni = 0	Se nell'output non sono presenti posizioni, l'oggetto potrebbe essere mancante. Puoi provare cercare e ripristinare l'oggetto oppure puoi contattare il supporto tecnico. Il supporto tecnico potrebbe richiedere di determinare se è in corso una procedura di ripristino dello storage. Vale a dire, è stato emesso un comando *repair-data* su qualsiasi nodo di storage e il ripristino è ancora in corso? Consultare le informazioni su ripristino dei dati degli oggetti in un volume di storage.

Informazioni correlate

Esaminare i registri di audit

Cercare e ripristinare oggetti potenzialmente persi

Potrebbe essere possibile trovare e ripristinare oggetti che hanno attivato un allarme Lost Objects (LOST Objects, oggetti persi) e un avviso **Object Lost** e che sono stati identificati come potenzialmente persi.

Di cosa hai bisogno

- È necessario disporre dell'UUID di qualsiasi oggetto perso, come indicato in "analisi degli oggetti persi".
- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

È possibile seguire questa procedura per cercare copie replicate dell'oggetto perso in un altro punto della griglia. Nella maggior parte dei casi, l'oggetto perso non viene trovato. Tuttavia, in alcuni casi, potrebbe essere possibile trovare e ripristinare un oggetto replicato perso se si esegue un'azione rapida.

Contattare il supporto tecnico per assistenza con questa procedura.

Fasi

1. Da un nodo amministratore, cercare nei registri di controllo le posizioni possibili degli oggetti:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
   b. Passare alla directory in cui si trovano i registri di controllo: `cd /var/local/audit/export/`
   c. Utilizzare grep per estrarre i messaggi di controllo associati all'oggetto potenzialmente perso e inviarli a un file di output. Inserire: `grep uuid-valueaudit_file_name > output_file_name`

      Ad esempio:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. Utilizzare grep per estrarre i messaggi di controllo LLST (Location Lost) da questo file di output. Inserire: `grep LLST output_file_name`

      Ad esempio:

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      Un messaggio di audit LLST è simile a questo messaggio di esempio.

      ```
      [AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
      [UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
      [PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
      [TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
      1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
      SM]
      [ATID(UI64):7086871083190743409]]
      ```

   e. Individuare il campo PCLD e IL campo NOID nel messaggio LLST.

      Se presente, il valore di PCLD è il percorso completo sul disco verso la copia dell'oggetto replicato mancante. IL valore DI NOID è l'id del nodo dell'LDR in cui è possibile trovare una copia dell'oggetto.

      Se si trova una posizione dell'oggetto, potrebbe essere possibile ripristinarlo.

f. Individuare il nodo di storage per questo ID nodo LDR.

Esistono due modi per utilizzare l'ID del nodo per trovare il nodo di storage:

- In Grid Manager, selezionare **SUPPORT Tools Grid topology**. Quindi selezionare ***Data Center Storage Node* LDR**. L'ID del nodo LDR si trova nella tabella Node Information (informazioni nodo). Esaminare le informazioni relative a ciascun nodo di storage fino a individuare quello che ospita questo LDR.
- Scaricare e decomprimere il pacchetto di ripristino per la griglia. Esiste una directory */docs* nel pacchetto SUDDETTO. Se si apre il file index.html, il Riepilogo server mostra tutti gli ID dei nodi per tutti i nodi della griglia.

2. Determinare se l'oggetto esiste sul nodo di storage indicato nel messaggio di audit:

a. Accedere al nodo Grid:

i. Immettere il seguente comando: `ssh admin@grid_node_IP`

ii. Immettere la password elencata in `Passwords.txt` file.

iii. Immettere il seguente comando per passare a root: `su -`

iv. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

1. Determinare se il percorso del file per l'oggetto esiste.

Per il percorso file dell'oggetto, utilizzare il valore PCLD del messaggio di audit LLST.

Ad esempio, immettere:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Nota: Racchiudere sempre il percorso del file oggetto tra virgolette singole nei comandi per escapire eventuali caratteri speciali.

- Se il percorso dell'oggetto non viene trovato, l'oggetto viene perso e non può essere ripristinato utilizzando questa procedura. Contattare il supporto tecnico.
- Se viene trovato il percorso dell'oggetto, andare al passo Ripristinare l'oggetto su StorageGRID. È possibile tentare di ripristinare l'oggetto trovato in StorageGRID.

a. se il percorso dell'oggetto è stato trovato, tentare di ripristinare l'oggetto su StorageGRID:

i. Dallo stesso nodo di storage, modificare la proprietà del file a oggetti in modo che possa essere gestito da StorageGRID. Inserire: `chown ldr-user:bycast 'file_path_of_object'`

ii. Telnet all'host locale 1402 per accedere alla console LDR. Inserire: `telnet 0 1402`

iii. Inserire: `cd /proc/STOR`

iv. Inserire: `Object_Found 'file_path_of_object'`

Ad esempio, immettere:

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Emissione di `Object\_Found` il comando notifica alla griglia la posizione dell'oggetto. Attiva anche il criterio ILM attivo, che crea copie aggiuntive come specificato nel criterio.

Nota: Se il nodo di storage in cui è stato trovato l'oggetto non è in linea, è possibile copiare l'oggetto in qualsiasi nodo di storage in linea. Posizionare l'oggetto in qualsiasi directory /var/local/rangedb del nodo di storage online. Quindi, eseguire il `Object\_Found` utilizzando il percorso del file all'oggetto.

- Se l'oggetto non può essere ripristinato, il `Object\_Found` comando non riuscito. Contattare il supporto tecnico.
- Se l'oggetto è stato ripristinato correttamente in StorageGRID, viene visualizzato un messaggio di esito positivo. Ad esempio:

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Andare al passo Verificare che siano state create nuove posizioni

v. se l'oggetto è stato ripristinato in StorageGRID, verificare che siano state create nuove posizioni.

A. Inserire: `cd /proc/OBRP`

B. Inserire: `ObjectByUUID UUID_value`

L'esempio seguente mostra che sono presenti due posizioni per l'oggetto con UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
```

```
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```


1. Disconnettersi dalla console LDR. Inserire: `exit`

   a. Da un nodo di amministrazione, cercare nei registri di controllo il messaggio di audit ORLM relativo a questo oggetto per confermare che ILM (Information Lifecycle Management) ha inserito le copie come richiesto.

2. Accedere al nodo Grid:
   a. Immettere il seguente comando: `ssh admin@grid_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. Passare alla directory in cui si trovano i registri di controllo: `cd /var/local/audit/export/`
4. Utilizzare grep per estrarre i messaggi di audit associati all'oggetto in un file di output. Inserire: `grep uuid-valueaudit_file_name > output_file_name`

   Ad esempio:

   ```
   Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
   messages_about_restored_object.txt
   ```

5. Utilizzare grep per estrarre i messaggi di audit ORLM (Object Rules Met) da questo file di output. Inserire: `grep ORLM output_file_name`

   Ad esempio:

   ```
   Admin: # grep ORLM messages_about_restored_object.txt
   ```

   Un messaggio di audit ORLM è simile a questo messaggio di esempio.

   ```
   [AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
   [STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
   BCCA72DD1311"]
   [LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
   [RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
   69]
   [ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
   ```

6. Individuare il campo LOCS (POSIZIONI) nel messaggio di audit.

   Se presente, il valore di CLDI in LOCS è l'ID del nodo e l'ID del volume in cui è stata creata una copia dell'oggetto. Questo messaggio indica che l'ILM è stato applicato e che sono state create due copie di oggetti in due posizioni nella griglia. . Ripristinare il numero di oggetti persi in Grid Manager.

Informazioni correlate

Esaminare gli oggetti persi

Ripristinare i conteggi degli oggetti persi e mancanti

Esaminare i registri di audit

Dopo aver esaminato il sistema StorageGRID e aver verificato che tutti gli oggetti persi registrati vengano persi in modo permanente o che si tratti di un falso allarme, è possibile azzerare il valore dell'attributo oggetti persi.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

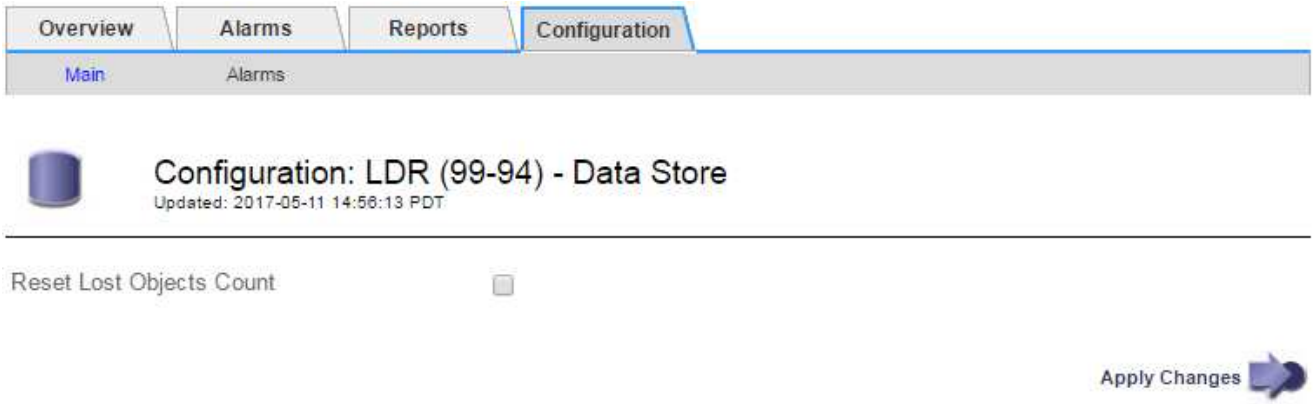
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

- **SUPPORTO Strumenti topologia griglia *Sito nodo di storage* LDR Archivio dati Panoramica principale**
- **SUPPORTO Strumenti topologia griglia *Sito nodo di storage* DDS Archivio dati Panoramica principale**

Queste istruzioni mostrano come azzerare il contatore dalla pagina **LDR Data Store**.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site Storage Node* LDR Data Store Configuration** per il nodo di storage con l'avviso **Objects Lost** o L'allarme LOST.
3. Selezionare **Reset Lost Objects Count** (Ripristina conteggio oggetti persi).



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

   L'attributo Lost Objects (oggetti persi) viene reimpostato su 0 e l'avviso **Objects lost** (oggetti persi) e l'allarme LOST (PERSO) vengono eliminati, che possono richiedere alcuni minuti.

5. Facoltativamente, reimpostare altri valori degli attributi correlati che potrebbero essere stati incrementati durante il processo di identificazione dell'oggetto perso.

   a. Selezionare ***Site Storage Node* LDR Erasure Coding Configuration**.
   b. Selezionare **Reset Reads Failure Count** e **Reset corrotto copies Detected Count**.
   c. Fare clic su **Applica modifiche**.

d. Selezionare ***Site Storage Node* LDR Verification Configuration**.

e. Selezionare **Reset Missing Objects Count** e **Reset Corrupt Objects Count**.

f. Se si è certi che gli oggetti in quarantena non siano necessari, selezionare **Delete Quarantined Objects** (Elimina oggetti in quarantena).

   Gli oggetti in quarantena vengono creati quando la verifica in background identifica una copia di oggetti replicati corrotta. Nella maggior parte dei casi, StorageGRID sostituisce automaticamente l'oggetto corrotto ed è sicuro eliminare gli oggetti in quarantena. Tuttavia, se viene attivato l'allarme **oggetti persi** o L'allarme PERSO, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena.

g. Fare clic su **Applica modifiche**.

Dopo aver fatto clic su **Apply Changes** (Applica modifiche), il ripristino degli attributi può richiedere alcuni istanti.

Risolvere i problemi relativi all'avviso di storage dei dati a oggetti in esaurimento

L'avviso **Low Object Data Storage** monitora lo spazio disponibile per memorizzare i dati degli oggetti su ciascun nodo di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

L'avviso **Low Object Data Storage** viene attivato quando la quantità totale di dati di oggetti codificati replicati ed erasure su un nodo di storage soddisfa una delle condizioni configurate nella regola di avviso.

Per impostazione predefinita, viene attivato un avviso importante quando questa condizione viene valutata come true:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In questa condizione:

- `storagegrid_storage_utilization_data_bytes` È una stima della dimensione totale dei dati degli oggetti replicati ed erasure coded per un nodo di storage.
- `storagegrid_storage_utilization_usable_space_bytes` È la quantità totale di spazio di storage a oggetti rimanente per un nodo di storage.

Se viene attivato un avviso **Low Object Data Storage** maggiore o minore, è necessario eseguire una procedura di espansione il prima possibile.

Fasi

1. Selezionare **ALERTS current**.

   Viene visualizzata la pagina Avvisi.

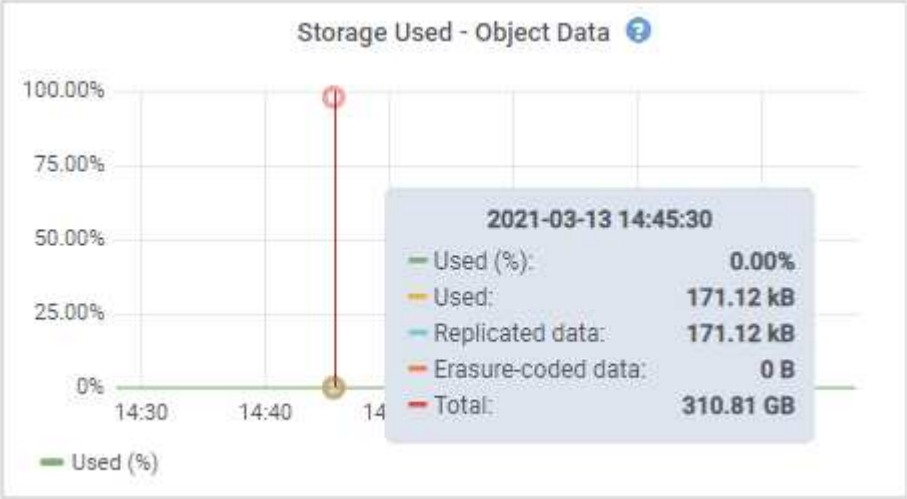
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low Object Data Storage**, se necessario, e selezionare l'avviso che si desidera visualizzare.

   Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.

3. Esaminare i dettagli nella finestra di dialogo e prendere nota di quanto segue:
   - Tempo di attivazione
   - Il nome del sito e del nodo
   - I valori correnti delle metriche per questo avviso
4. Selezionare **NODES *Storage Node o Site* Storage**.
5. Spostare 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.



6. Selezionare i controlli dell'ora sopra il grafico per visualizzare l'utilizzo dello storage in diversi periodi di tempo.

   L'utilizzo dello storage nel tempo può aiutarti a capire la quantità di storage utilizzata prima e dopo l'attivazione dell'avviso e può aiutarti a stimare il tempo necessario per lo spazio rimanente del nodo.

7. Non appena possibile, eseguire una procedura di espansione per aggiungere capacità di storage.

   È possibile aggiungere volumi di storage (LUN) ai nodi di storage esistenti oppure aggiungere nuovi nodi di storage.

Per gestire un nodo di storage completo, consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

Risolvere i problemi relativi all'allarme Storage Status (SST)

Espandi il tuo grid

Amministrare StorageGRID

Risolvere i problemi relativi agli avvisi di override del watermark di sola lettura bassa

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, potrebbe essere necessario risolvere l'avviso **bassa sostituzione filigrana di sola lettura**. Se possibile, aggiornare il sistema per iniziare a utilizzare i valori ottimizzati.

Nelle release precedenti, le tre filigrane dei volumi di storage Erano impostazioni globali n. 8212; gli stessi valori applicati a ogni volume di storage su ogni nodo di storage. A partire da StorageGRID 11.6, il software può ottimizzare queste filigrane per ogni volume di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

Quando si esegue l'aggiornamento a StorageGRID 11.6, le filigrane ottimizzate di sola lettura e di lettura/scrittura vengono applicate automaticamente a tutti i volumi di storage, a meno che non si verifichino le seguenti condizioni:

- Il sistema è vicino alla capacità e non è in grado di accettare nuovi dati se sono state applicate filigrane ottimizzate. In questo caso, StorageGRID non modificherà le impostazioni della filigrana.
- In precedenza, le filigrane dei volumi di storage sono state impostate su un valore personalizzato. StorageGRID non sovrascrive le impostazioni personalizzate del watermark con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso **override filigrana di sola lettura bassa** se il valore personalizzato per la filigrana di sola lettura morbida del volume di storage è troppo piccolo.

Comprendere l'avviso

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, l'avviso **Low Read-only watermark override** potrebbe essere attivato per uno o più nodi di storage.

Ogni istanza dell'avviso indica che il valore personalizzato di **Storage Volume Soft Read-Only Watermark** è inferiore al valore minimo ottimizzato per quel nodo di storage. Se si continua a utilizzare l'impostazione personalizzata, lo spazio del nodo di storage potrebbe essere molto basso prima di poter passare in sicurezza allo stato di sola lettura. Alcuni volumi di storage potrebbero diventare inaccessibili (automaticamente smontati) quando il nodo raggiunge la capacità.

Ad esempio, si supponga di aver precedentemente impostato la filigrana di sola lettura **Storage Volume Soft** su 5 GB. Supponiamo ora che StorageGRID abbia calcolato i seguenti valori ottimizzati per i quattro volumi di storage nel nodo di storage A:

Volume 0	12 GB
Volume 1	12 GB

Volume 2	11 GB
Volume 3	15 GB

L'avviso **Low Read-only watermark override** viene attivato per il nodo di storage A perché il watermark personalizzato (5 GB) è inferiore al valore minimo ottimizzato per tutti i volumi in quel nodo (11 GB). Se si continua a utilizzare l'impostazione personalizzata, lo spazio del nodo potrebbe essere estremamente ridotto prima di poter passare in sicurezza allo stato di sola lettura.

Risolvere l'avviso

Seguire questa procedura se sono stati attivati uno o più avvisi **Low Read-only watermark override**. È inoltre possibile utilizzare queste istruzioni se si utilizzano impostazioni personalizzate per la filigrana e si desidera iniziare a utilizzare impostazioni ottimizzate anche se non sono stati attivati avvisi.

Di cosa hai bisogno

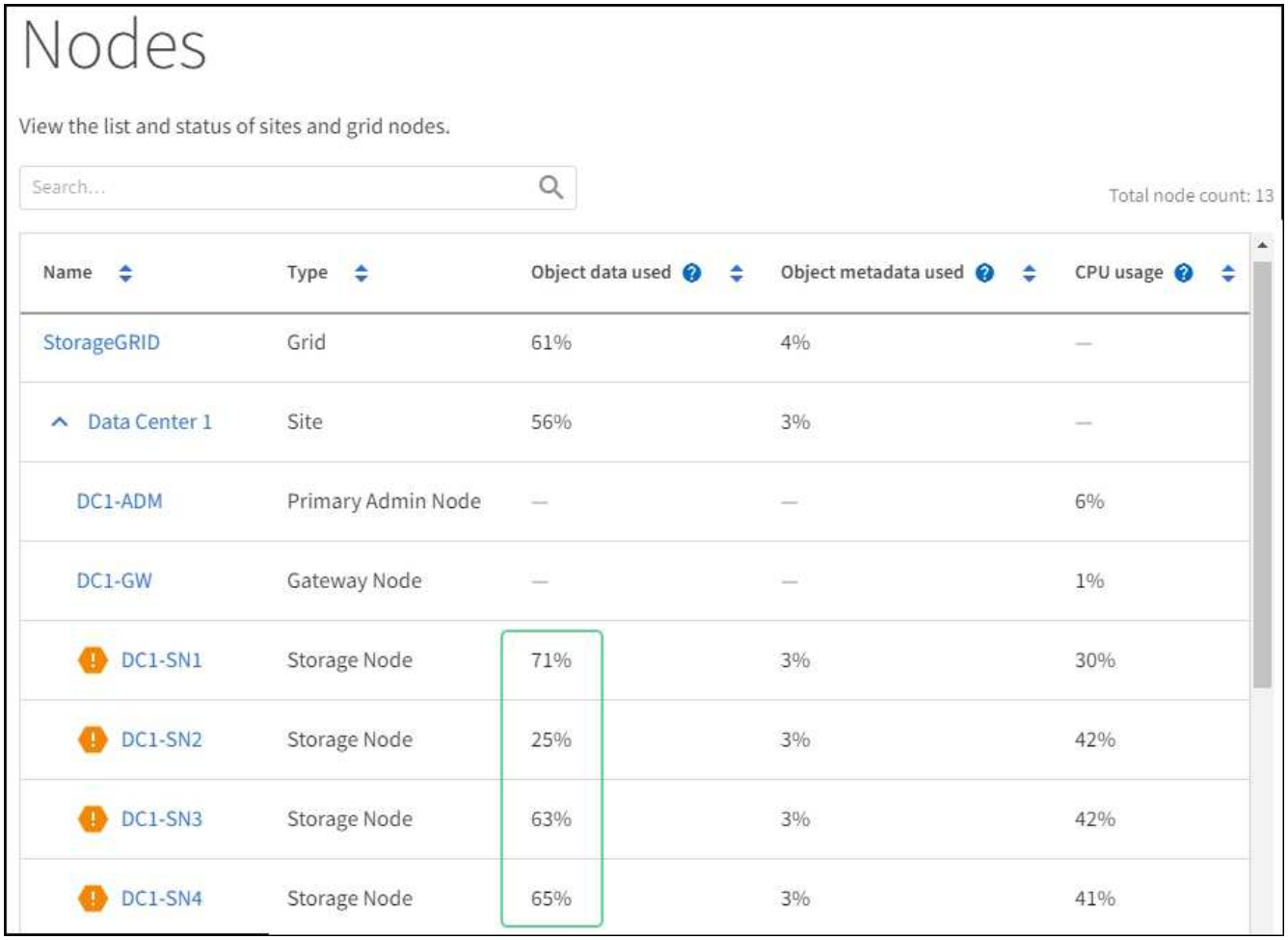
- L'aggiornamento a StorageGRID 11.6 è stato completato.
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root.

A proposito di questa attività

È possibile risolvere l'avviso **deroga filigrana di sola lettura bassa** aggiornando le impostazioni di filigrana personalizzate con le nuove sostituzioni della filigrana. Tuttavia, se uno o più nodi di storage sono quasi pieni o si hanno requisiti ILM speciali, è necessario prima visualizzare le filigrane di storage ottimizzate e determinare se è sicuro utilizzarle.

Valutare l'utilizzo dei dati a oggetti per l'intero grid

1. Selezionare **NODI**.
2. Per ogni sito nella griglia, espandere l'elenco dei nodi.
3. Esaminare i valori percentuali mostrati nella colonna **dati oggetto utilizzati** per ciascun nodo di storage in ogni sito.



4. Se nessuno dei nodi di storage è quasi pieno (ad esempio, tutti i valori **dati oggetto utilizzati** sono inferiori al 80%), è possibile iniziare a utilizzare le impostazioni di override. Passare a. Utilizzare filigrane ottimizzate.

> Esistono alcune eccezioni a questa regola generale. Ad esempio, se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se i pool di storage specifici sono quasi pieni, è necessario eseguire prima i passaggi descritti in Visualizza filigrane di storage ottimizzate e. Determinare se è possibile utilizzare filigrane ottimizzate.

5. Se uno o più nodi di storage sono quasi pieni, eseguire le operazioni descritte in Visualizza filigrane di storage ottimizzate e. Determinare se è possibile utilizzare filigrane ottimizzate.

Visualizza filigrane di storage ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati che ha calcolato per la filigrana di sola lettura del volume di storage **Soft Read-only**. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

1. Selezionare **SUPPORT Tools Metrics**.
2. Nella sezione Prometheus, selezionare il collegamento per accedere all'interfaccia utente Prometheus.
3. Per visualizzare la filigrana minima di sola lettura soft consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage. Se questo valore è superiore all'impostazione personalizzata per **Storage Volume Soft Read-Only Watermark**, viene attivato l'avviso **Low Read-only watermark override** per il nodo di storage.

4. Per visualizzare la filigrana di sola lettura soft massima consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore massimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage.

5. Nota sul valore massimo ottimizzato per ciascun nodo di storage.

Determinare se è possibile utilizzare filigrane ottimizzate

1. Selezionare **NODI**.
2. Ripetere questi passaggi per ogni nodo di storage online:
   a. Selezionare ***Storage Node* Storage**.
   b. Scorrere verso il basso fino alla tabella degli archivi di oggetti.
   c. Confrontare il valore **Available** per ciascun archivio di oggetti (volume) con il watermark ottimizzato massimo annotato per quel nodo di storage.
3. Se almeno un volume su ogni nodo di storage online ha più spazio disponibile rispetto al watermark ottimizzato massimo per quel nodo, visitare il sito Web Utilizzare filigrane ottimizzate per iniziare a utilizzare le filigrane ottimizzate.

   In caso contrario, espandi il tuo grid il più presto possibile. Aggiungere volumi di storage a un nodo esistente o aggiungere nuovi nodi di storage. Quindi, passare a. Utilizzare filigrane ottimizzate per aggiornare le impostazioni della filigrana.

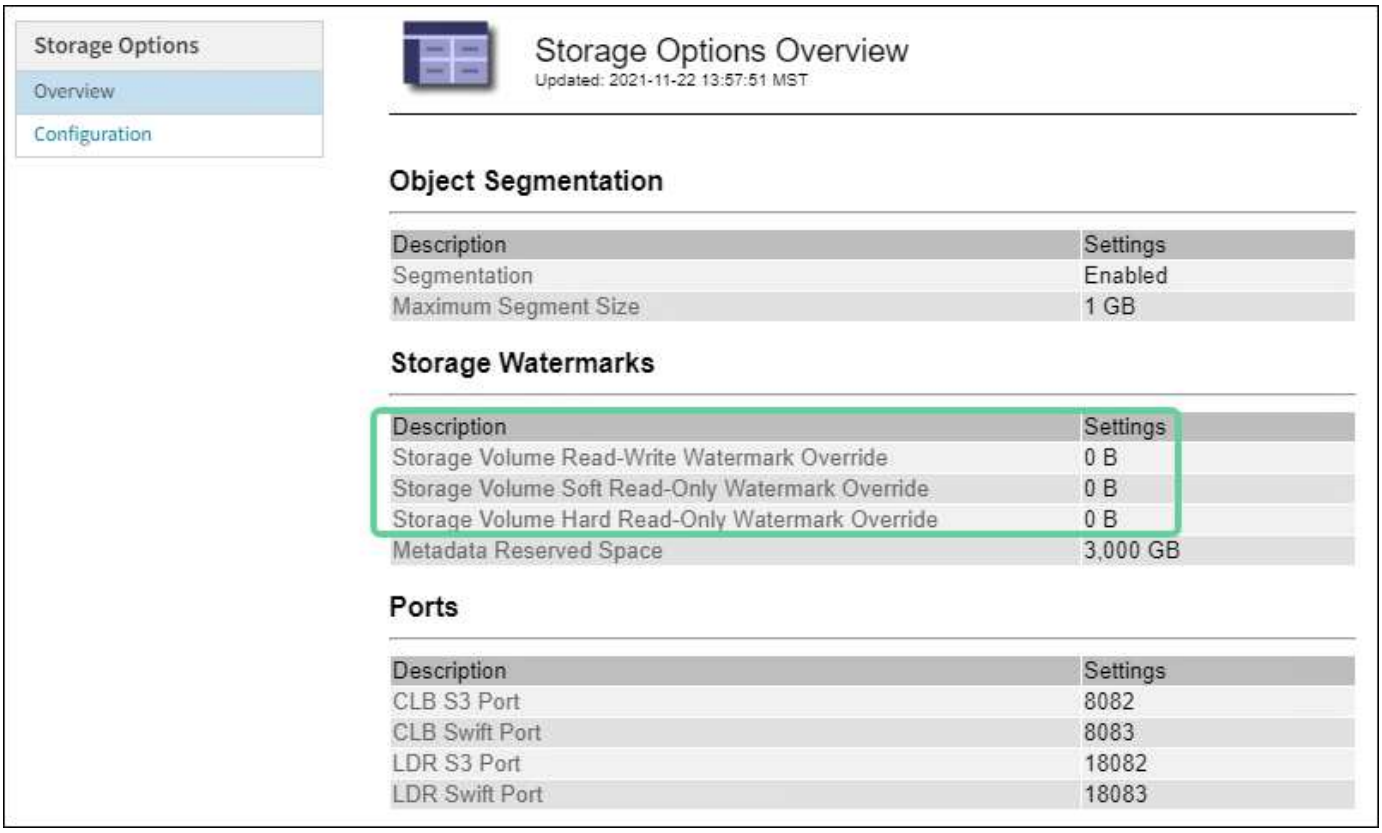
4. Se è necessario continuare a utilizzare valori personalizzati per le filigrane del volume di storage, silenzio oppure disattiva L'avviso **deroga filigrana di sola lettura bassa**.

   > Gli stessi valori di watermark personalizzati vengono applicati a ogni volume di storage su ogni nodo di storage. L'utilizzo di valori inferiori a quelli consigliati per le filigrane dei volumi di storage potrebbe causare l'inaccessibilità di alcuni volumi di storage (automaticamente smontati) quando il nodo raggiunge la capacità.

Utilizzare filigrane ottimizzate

1. Accedere a **CONFIGURAZIONE sistema Opzioni di storage**.
2. Selezionare **Configuration** (Configurazione) dal menu Storage Options (Opzioni storage).
3. Impostare tutte e tre le sostituzioni filigrana su 0.
4. Selezionare **Applica modifiche**.

Le impostazioni ottimizzate del watermark del volume di storage sono ora attive per ciascun volume di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.



Risolvere i problemi relativi all'allarme Storage Status (SST)

L'allarme Storage Status (SST) viene attivato se un nodo di storage non dispone di spazio libero sufficiente per lo storage a oggetti.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

L'allarme SSTS (Storage Status) viene attivato a livello Notice quando la quantità di spazio libero su ogni volume in un nodo di storage scende al di sotto del valore del watermark di sola lettura del volume di storage (**CONFIGURAZIONE sistema Opzioni di storage**).

Storage Options Overview
Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

Ad esempio, si supponga che la filigrana Storage Volume Soft Read-Only sia impostata su 10 GB, che è il valore predefinito. L'allarme SSTS viene attivato se su ciascun volume di storage nel nodo di storage rimangono meno di 10 GB di spazio utilizzabile. Se uno dei volumi dispone di almeno 10 GB di spazio disponibile, l'allarme non viene attivato.

Se è stato attivato un allarme SSTS, è possibile seguire questa procedura per comprendere meglio il problema.

Fasi

1. Selezionare **SUPPORTO Allarmi (legacy) Allarmi correnti**.
2. Dalla colonna Service (Servizio), selezionare il data center, il nodo e il servizio associati all'allarme SSTS.

   Viene visualizzata la pagina Grid Topology (topologia griglia). La scheda Allarmi mostra gli allarmi attivi per il nodo e il servizio selezionato.

Overview | Alarms | Reports | Configuration
Main | History

Alarms: LDR (DC1-S3-101-195) - Storage
Updated: 2019-10-09 12:52:43 MDT

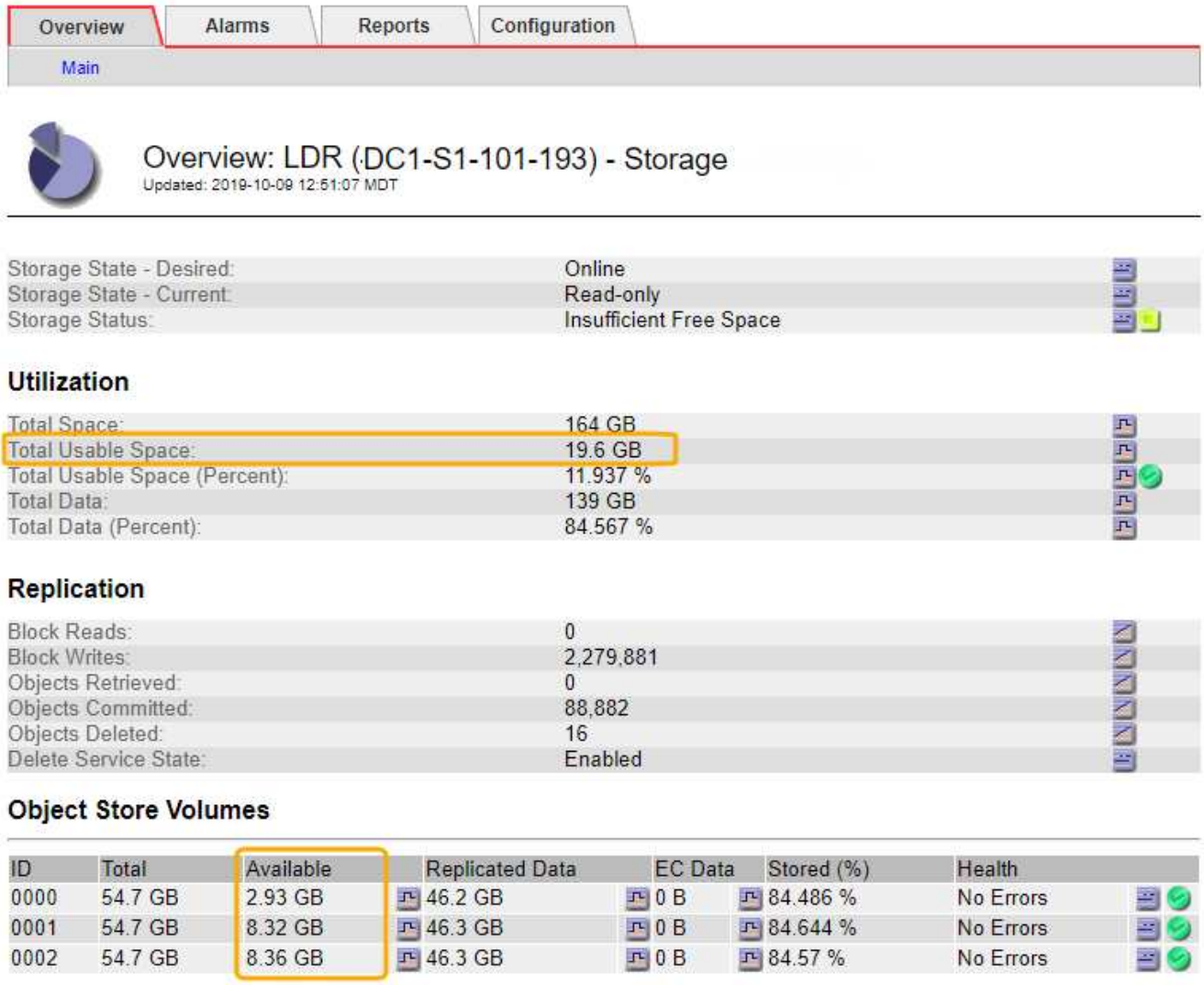
Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		
Normal	SHLH (Health)						

Apply Changes

   In questo esempio, gli allarmi SST (Storage Status) e SAVP (Total usable Space (Percent)) sono stati attivati a livello di notifica.

In genere, sia l'allarme SSTS che l'allarme SAVP vengono attivati circa contemporaneamente; tuttavia, l'attivazione di entrambi gli allarmi dipende dall'impostazione del watermark in GB e dall'impostazione dell'allarme SAVP in percentuale.

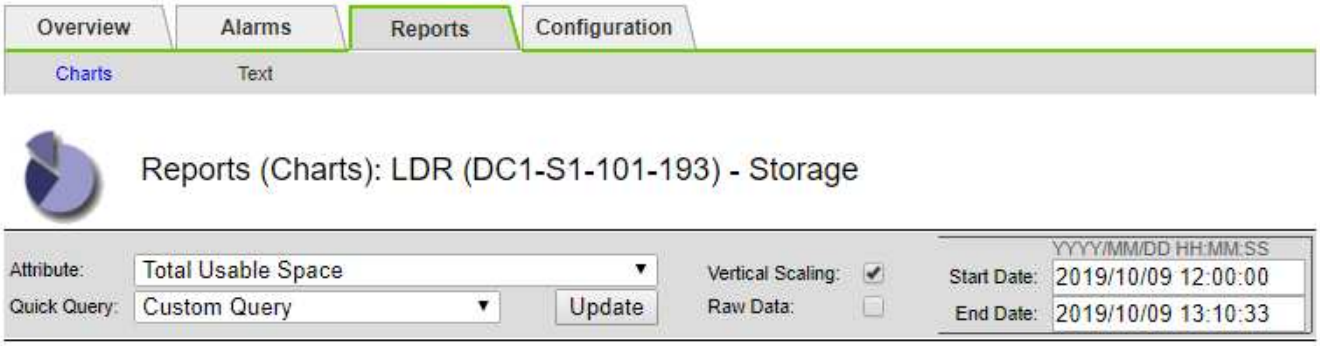
3. Per determinare la quantità di spazio utilizzabile effettivamente disponibile, selezionare **LDR Storage Overview** e individuare l'attributo Total Usable Space (STAS).

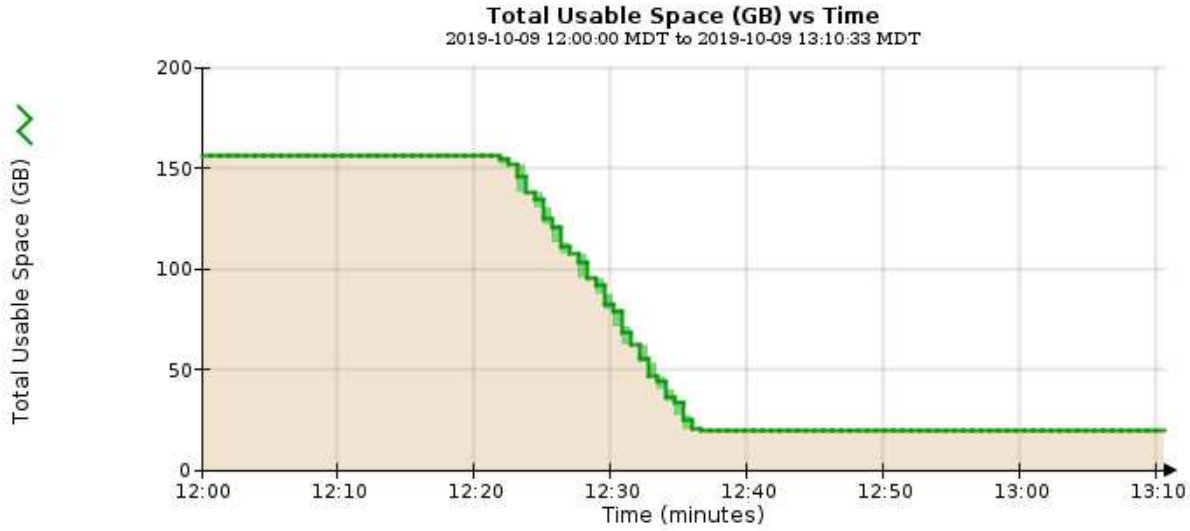


In questo esempio, rimangono disponibili solo 19.6 GB dei 164 GB di spazio su questo nodo di storage. Si noti che il valore totale è la somma dei valori **Available** per i tre volumi dell'archivio di oggetti. L'allarme SSTS è stato attivato perché ciascuno dei tre volumi di storage aveva meno di 10 GB di spazio disponibile.

4. Per capire come lo storage è stato utilizzato nel tempo, selezionare la scheda **Report** e tracciare lo spazio utilizzabile totale nelle ultime ore.

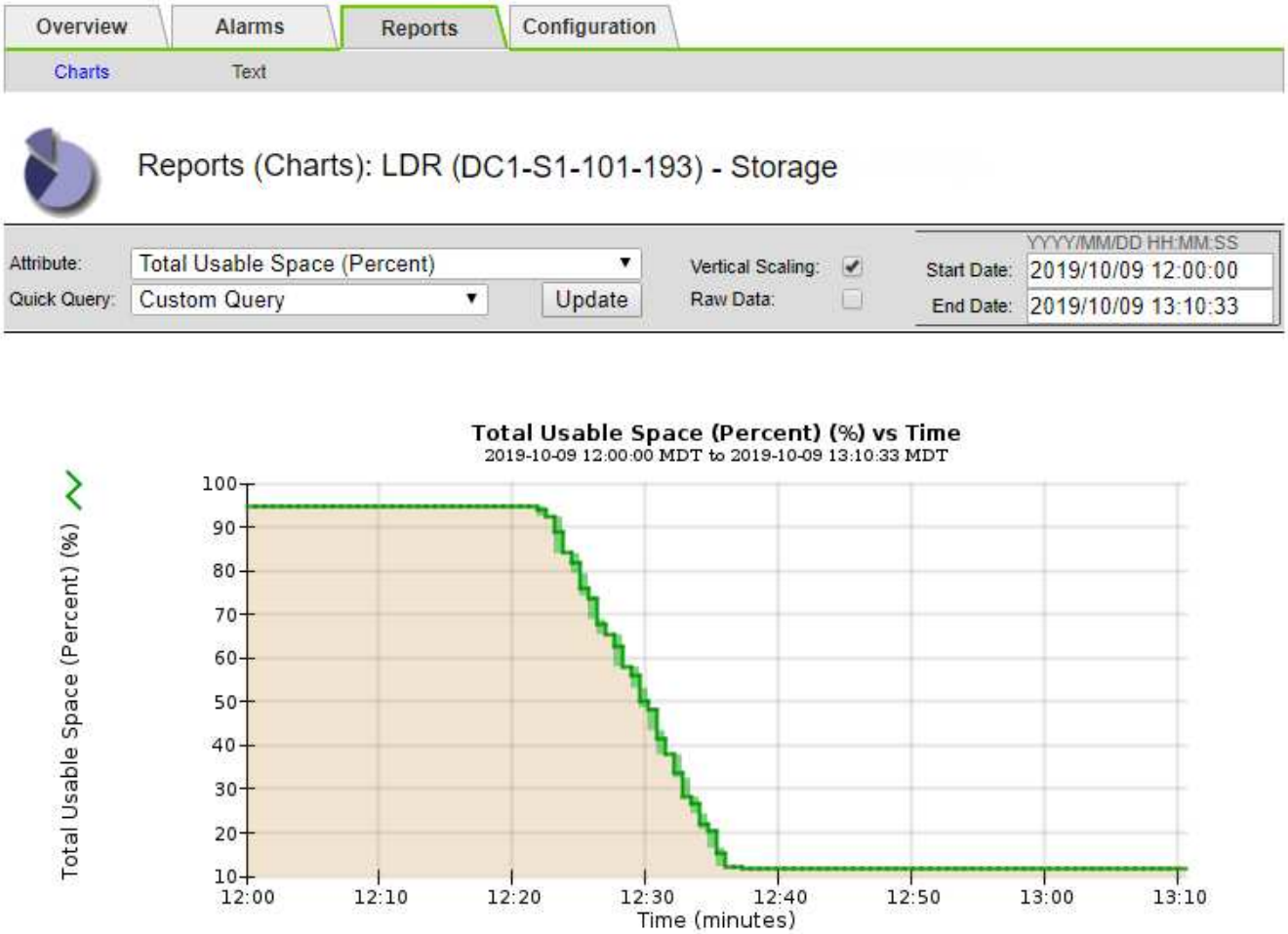
   In questo esempio, lo spazio utilizzabile totale è sceso da circa 155 GB a 12:00 a 20 GB a 12:35, il che corrisponde al momento in cui è stato attivato l'allarme SSTS.





5. Per comprendere come lo storage viene utilizzato come percentuale del totale, tracciare lo spazio utilizzabile totale (percentuale) nelle ultime ore.

   In questo esempio, lo spazio utilizzabile totale è sceso dal 95% a poco più del 10% circa contemporaneamente.



6. Se necessario, aggiungere capacità di storage Espansione del sistema StorageGRID.

   Per le procedure su come gestire un nodo di storage completo, vedere Istruzioni per l'amministrazione di StorageGRID.

Risoluzione dei problemi relativi all'erogazione dei messaggi dei servizi della piattaforma (allarme SMTT)

L'allarme SMTT (Total Events) viene attivato in Grid Manager se un messaggio di servizio della piattaforma viene inviato a una destinazione che non può accettare i dati.

A proposito di questa attività

Ad esempio, un caricamento di S3 multiparte può avere successo anche se la replica o il messaggio di notifica associati non possono essere inviati all'endpoint configurato. In alternativa, un messaggio per la replica di CloudMirror potrebbe non essere recapitato se i metadati sono troppo lunghi.

L'allarme SMTT contiene un messaggio Last Event (ultimo evento) che indica: `Failed to publish notifications for` *`bucket-name object key`* per l'ultimo oggetto la cui notifica non è riuscita.

I messaggi degli eventi sono elencati anche in `/var/local/log/bycast-err.log` file di log. Vedere Riferimenti ai file di log.

Per ulteriori informazioni sulla risoluzione dei problemi relativi ai servizi della piattaforma, consultare Istruzioni per l'amministrazione di StorageGRID. Potrebbe essere necessario Accedere al tenant dal tenant manager per

eseguire il debug di un errore del servizio della piattaforma.

Fasi

1. Per visualizzare l'allarme, selezionare **NODES** ***Site Grid Node*** **Events**.
2. Visualizza ultimo evento nella parte superiore della tabella.

   I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

3. Seguire le indicazioni fornite nel contenuto degli allarmi SMTT per correggere il problema.
4. Selezionare **Reset event count** (Ripristina conteggi eventi).
5. Notificare al tenant gli oggetti i cui messaggi dei servizi della piattaforma non sono stati recapitati.
6. Chiedere al tenant di attivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto.

Risolvere i problemi relativi ai metadati

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi ai metadati.

Risolvere i problemi relativi all'avviso di storage metadati in esaurimento

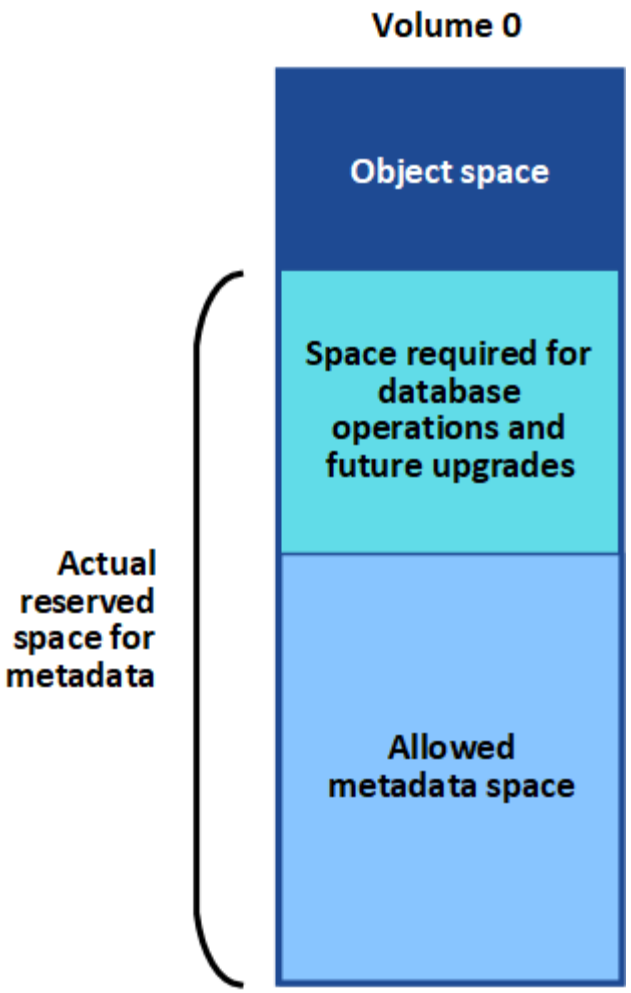
Se viene attivato l'avviso **Low metadata storage**, è necessario aggiungere nuovi nodi di storage.

Di cosa hai bisogno

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

A proposito di questa attività

StorageGRID riserva una certa quantità di spazio sul volume 0 di ciascun nodo di storage per i metadati dell'oggetto. Questo spazio è noto come spazio riservato effettivo e viene suddiviso nello spazio consentito per i metadati dell'oggetto (lo spazio consentito per i metadati) e nello spazio richiesto per le operazioni essenziali del database, come la compattazione e la riparazione. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



Se i metadati degli oggetti consumano più del 100% dello spazio consentito per i metadati, le operazioni del database non possono essere eseguite in modo efficiente e si verificano errori.

È possibile Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage per aiutarti a prevenire gli errori e correggerli prima che si verifichino.

StorageGRID utilizza la seguente metrica Prometheus per misurare la quantità di spazio consentito per i metadati:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

Quando l'espressione Prometheus raggiunge determinate soglie, viene attivato l'avviso **Low metadata storage**.

- **Minore**: I metadati degli oggetti utilizzano almeno il 70% dello spazio consentito per i metadati. È necessario aggiungere nuovi nodi di storage il prima possibile.
- **Major**: I metadati degli oggetti utilizzano almeno il 90% dello spazio consentito per i metadati. È necessario aggiungere immediatamente nuovi nodi di storage.

> Quando i metadati dell'oggetto utilizzano almeno il 90% dello spazio consentito per i metadati, viene visualizzato un avviso nella dashboard. Se viene visualizzato questo avviso, è necessario aggiungere immediatamente nuovi nodi di storage. Non è mai necessario consentire ai metadati degli oggetti di utilizzare più del 100% dello spazio consentito.

- **Critico**: I metadati degli oggetti utilizzano almeno il 100% dello spazio consentito e stanno iniziando a consumare lo spazio necessario per le operazioni essenziali del database. È necessario interrompere l'acquisizione di nuovi oggetti e aggiungere immediatamente nuovi nodi di storage.

Nell'esempio seguente, i metadati degli oggetti utilizzano oltre il 100% dello spazio consentito per i metadati. Si tratta di una situazione critica, che può causare errori e operazioni inefficienti del database.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

> Se la dimensione del volume 0 è inferiore all'opzione di storage Metadata Reserved Space (ad esempio, in un ambiente non in produzione), il calcolo dell'avviso **Low metadata storage** potrebbe essere impreciso.

Fasi

1. Selezionare **ALERTS current**.
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low metadata storage**, se necessario, e selezionare l'avviso specifico che si desidera visualizzare.
3. Esaminare i dettagli nella finestra di dialogo degli avvisi.
4. Se è stato attivato un avviso importante o critico **Low metadata storage**, eseguire un'espansione per aggiungere immediatamente i nodi di storage.

   > Poiché StorageGRID conserva copie complete di tutti i metadati degli oggetti in ogni sito, la capacità dei metadati dell'intera griglia è limitata dalla capacità dei metadati del sito più piccolo. Se devi aggiungere capacità di metadati a un sito, dovresti anche espandere qualsiasi altro sito Dello stesso numero di nodi di storage.

   Dopo aver eseguito l'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti nei nuovi nodi, aumentando così la capacità complessiva dei metadati della griglia. Non è richiesta alcuna azione da parte dell'utente. L'avviso **Low metadata storage** viene cancellato.

Risolvere i problemi relativi all'allarme Services: Status - Cassandra (SVST)

L'allarme servizi: Stato - Cassandra (SVST) indica che potrebbe essere necessario ricostruire il database Cassandra per un nodo di storage. Cassandra viene utilizzato come archivio di metadati per StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

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

A proposito di questa attività

Se Cassandra viene arrestato per più di 15 giorni (ad esempio, il nodo di storage viene spento), Cassandra non si avvia quando il nodo viene riportato in linea. È necessario ricostruire il database Cassandra per il servizio DDS interessato.

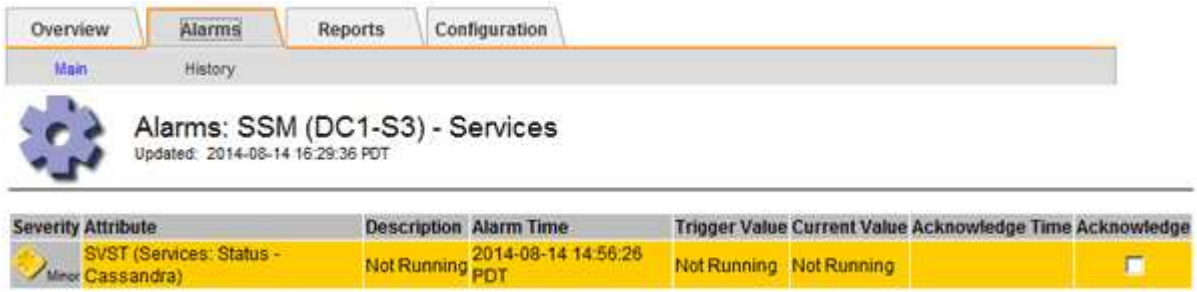
È possibile eseguire la diagnostica per ottenere ulteriori informazioni sullo stato corrente della griglia.

> Se due o più servizi di database Cassandra rimangono inutilizzati per più di 15 giorni, contattare il supporto tecnico e non procedere con la procedura riportata di seguito.

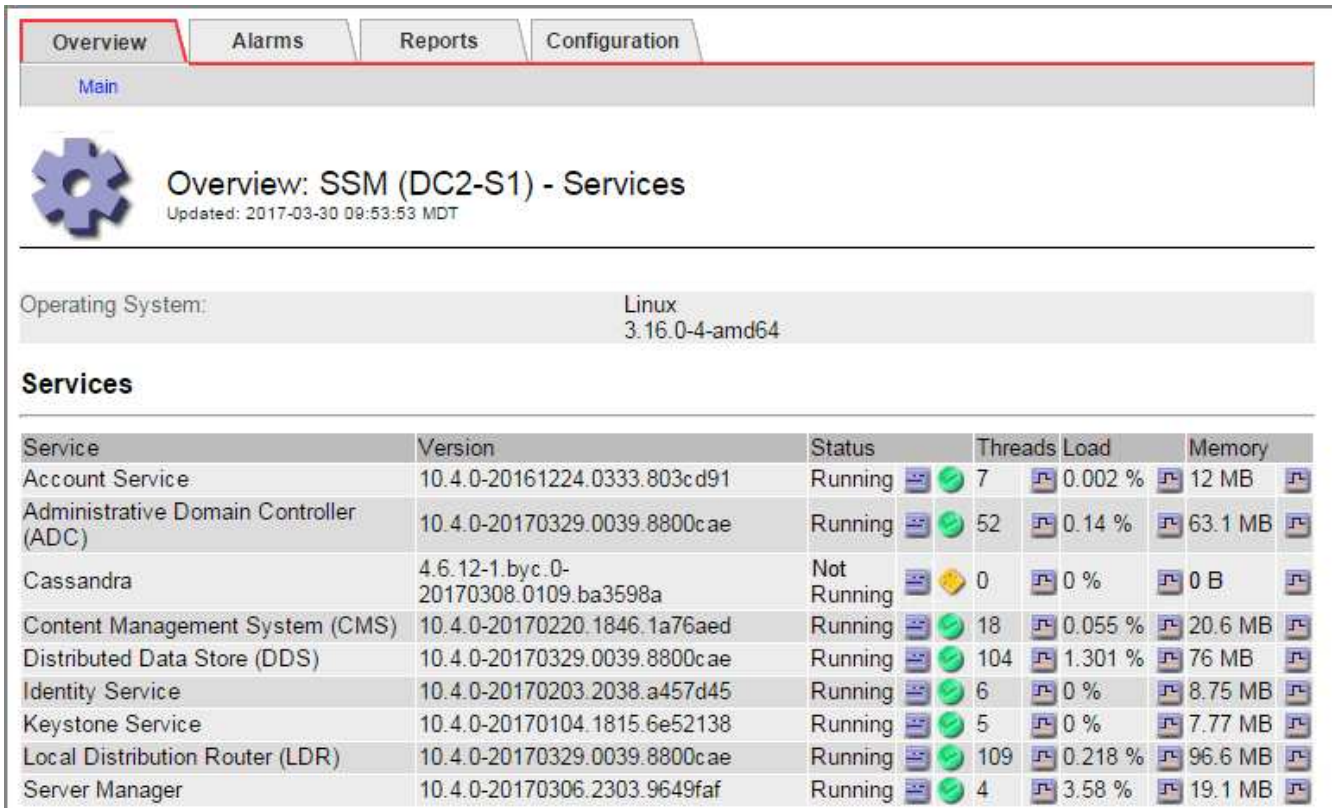
Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site Storage Node*** **SSM Services Alarms Main** per visualizzare gli allarmi.

   Questo esempio mostra che l'allarme SVST è stato attivato.



   La pagina principale dei servizi SSM indica inoltre che Cassandra non è in esecuzione.



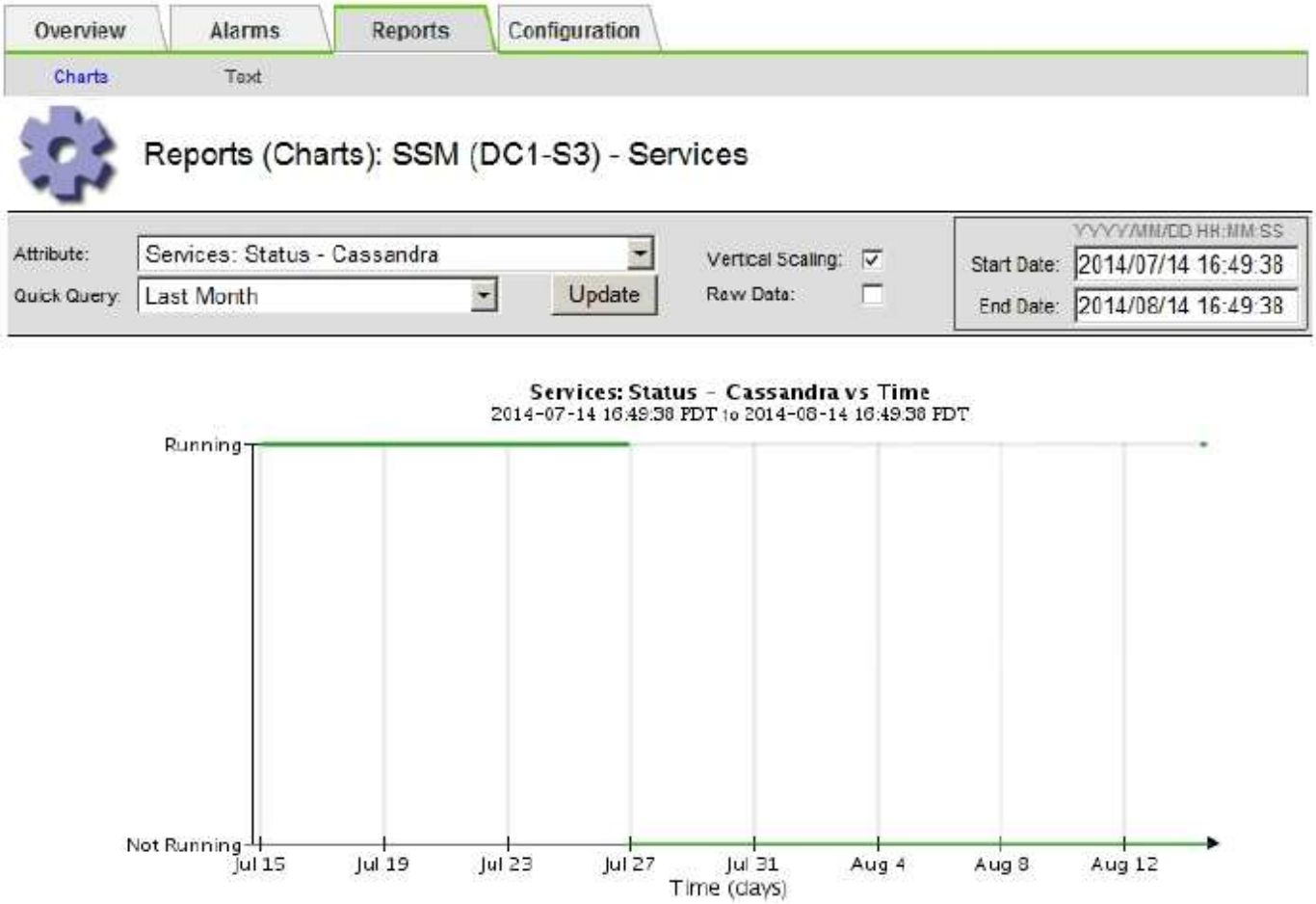
3. prova a riavviare Cassandra dal nodo di storage:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
   b. Inserire: `/etc/init.d/cassandra status`
   c. Se Cassandra non è in esecuzione, riavviarlo: `/etc/init.d/cassandra restart`
4. Se Cassandra non si riavvia, determinare per quanto tempo Cassandra è rimasto inattivo. Se Cassandra è rimasto inattivo per più di 15 giorni, è necessario ricostruire il database Cassandra.

   > Se due o più servizi di database Cassandra non sono disponibili, contattare il supporto tecnico e non procedere con i passaggi riportati di seguito.

   È possibile determinare per quanto tempo Cassandra è rimasta inattiva, inserendolo nella cartella o esaminando il file servermanager.log.

5. Per inserire il grafico Cassandra:
   a. Selezionare **SUPPORT Tools Grid topology**. Quindi selezionare ***Site Storage Node* SSM servizi Report grafici**.
   b. Selezionare **attributo Servizio: Stato - Cassandra**.
   c. Per **Data di inizio**, immettere una data che sia almeno 16 giorni prima della data corrente. Per **Data di fine**, inserire la data corrente.
   d. Fare clic su **Aggiorna**.
   e. Se il grafico mostra Cassandra come inattivo per più di 15 giorni, ricostruire il database Cassandra.

L'esempio seguente mostra che Cassandra è rimasta inattiva per almeno 17 giorni.



1. Per esaminare il file servermanager.log sul nodo di storage:

   a. Accedere al nodo Grid:

      i. Immettere il seguente comando: `ssh admin@grid_node_IP`

      ii. Immettere la password elencata in `Passwords.txt` file.

      iii. Immettere il seguente comando per passare a root: `su -`

      iv. Immettere la password elencata in `Passwords.txt` file. Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

   b. Inserire: `cat /var/local/log/servermanager.log`

      Viene visualizzato il contenuto del file servermanager.log.

      Se Cassandra rimane inattivo per più di 15 giorni, nel file servermanager.log viene visualizzato il seguente messaggio:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

   a. Assicurarsi che la data e l'ora del messaggio siano quelle in cui si è tentato di riavviare Cassandra, come indicato al punto Riavviare Cassandra dal nodo di storage.

Per Cassandra possono essere presenti più voci; è necessario individuare la voce più recente.

b. Se Cassandra è rimasto inattivo per più di 15 giorni, è necessario ricostruire il database Cassandra.

   Per istruzioni, vedere Recovery Storage Node Down per più di 15 giorni.

c. Contattare il supporto tecnico se gli allarmi non vengono disattivati dopo la ricostruzione di Cassandra.

Risolvere i problemi relativi agli errori di memoria esaurita di Cassandra (allarme SMTT)

Un allarme SMTT (Total Events) viene attivato quando il database Cassandra presenta un errore di memoria esaurita. Se si verifica questo errore, contattare il supporto tecnico per risolvere il problema.

A proposito di questa attività

Se si verifica un errore di memoria insufficiente per il database Cassandra, viene creato un dump heap, viene attivato un allarme SMTT (Total Events) e il conteggio degli errori Cassandra Heap out of Memory viene incrementato di uno.

Fasi

1. Per visualizzare l'evento, selezionare **SUPPORT Tools Grid topology Configuration**.
2. Verificare che il conteggio degli errori di memoria esaurita di Cassandra sia pari o superiore a 1.

   È possibile eseguire la diagnostica per ottenere ulteriori informazioni sullo stato corrente della griglia.

3. Passare a. `/var/local/core/`, comprimere `Cassandra.hprof` e inviarla al supporto tecnico.
4. Eseguire un backup di `Cassandra.hprof` ed eliminarlo da `/var/local/core/ directory`.

   Questo file può avere una dimensione massima di 24 GB, quindi è necessario rimuoverlo per liberare spazio.

5. Una volta risolto il problema, selezionare la casella di controllo **Reset** per il conteggio degli errori di memoria esaurita di Cassandra Heap. Quindi selezionare **Apply Changes** (Applica modifiche).

   Per reimpostare i conteggi degli eventi, è necessario disporre dell'autorizzazione Grid Topology Page Configuration (Configurazione pagina topologia griglia).

Risolvere gli errori del certificato

Se si verifica un problema di sicurezza o certificato quando si tenta di connettersi a StorageGRID utilizzando un browser Web, un client S3 o Swift o uno strumento di monitoraggio esterno, controllare il certificato.

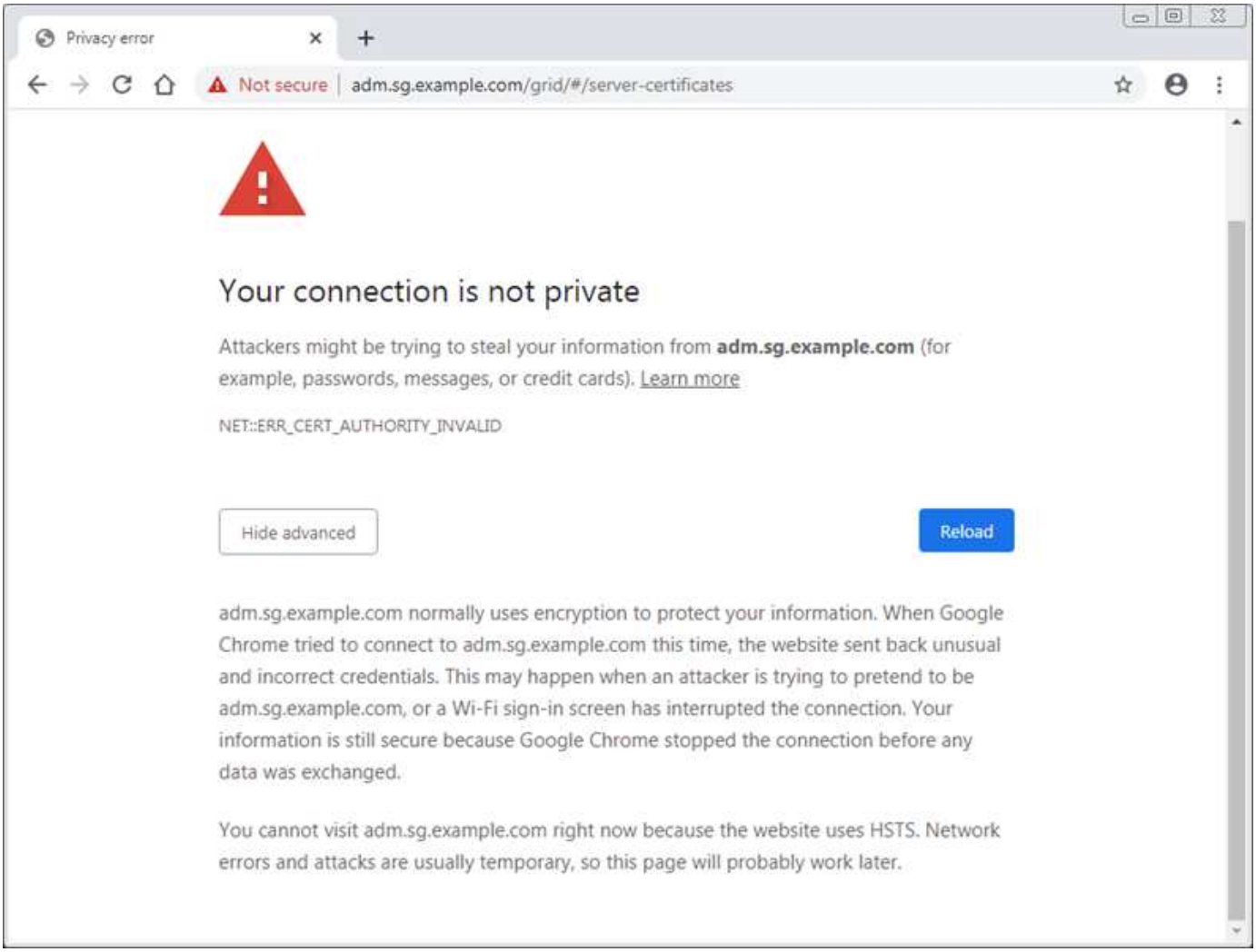
A proposito di questa attività

Gli errori dei certificati possono causare problemi quando si tenta di connettersi a StorageGRID utilizzando Gestione griglia, API di gestione griglia, Gestore tenant o API di gestione tenant. Gli errori di certificato possono verificarsi anche quando si tenta di connettersi a un client S3 o Swift o a uno strumento di monitoraggio esterno.

Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Viene ripristinato da un certificato dell'interfaccia di gestione personalizzata al certificato del server predefinito.

L'esempio seguente mostra un errore di certificato quando il certificato dell'interfaccia di gestione personalizzata è scaduto:



Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** viene attivato quando il certificato del server sta per scadere.

Quando si utilizzano certificati client per l'integrazione esterna di Prometheus, gli errori dei certificati possono essere causati dal certificato dell'interfaccia di gestione di StorageGRID o dai certificati client. L'avviso **scadenza dei certificati client configurati nella pagina certificati** viene attivato quando un certificato client sta per scadere.

Fasi

Se si riceve una notifica di avviso relativa a un certificato scaduto, accedere ai dettagli del certificato: . Selezionare **CONFIGURAZIONE sicurezza certificati**, quindi selezionare la scheda del certificato appropriata.

1. Controllare il periodo di validità del certificato. + alcuni browser Web e client S3 o Swift non accettano certificati con un periodo di validità superiore a 398 giorni.

2. Se il certificato è scaduto o scadrà a breve, caricare o generare un nuovo certificato.
   - Per un certificato del server, consultare la procedura per Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager.
   - Per un certificato client, vedere la procedura per configurazione di un certificato client.
3. In caso di errori del certificato del server, provare una o entrambe le seguenti opzioni:
   - Assicurarsi che il campo Subject alternative Name (SAN) del certificato sia compilato e che LA SAN corrisponda all'indirizzo IP o al nome host del nodo a cui si sta effettuando la connessione.
   - Se si sta tentando di connettersi a StorageGRID utilizzando un nome di dominio:
     i. Inserire l'indirizzo IP del nodo di amministrazione invece del nome di dominio per evitare l'errore di connessione e accedere a Grid Manager.
     ii. Da Grid Manager, selezionare **CONFIGURAZIONE sicurezza certificati**, quindi selezionare la scheda del certificato appropriata per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
     iii. Nelle istruzioni per l'amministrazione di StorageGRID, vedere la procedura per Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager.

Risolvere i problemi relativi al nodo di amministrazione e all'interfaccia utente

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi ai nodi di amministrazione e all'interfaccia utente di StorageGRID.

Risoluzione dei problemi relativi agli errori di accesso

Se si verifica un errore durante l'accesso a un nodo amministrativo StorageGRID, il sistema potrebbe avere un problema con la configurazione della federazione delle identità, un problema di rete o hardware, un problema con i servizi del nodo amministrativo o un problema con il database Cassandra sui nodi di storage connessi.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` file.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Utilizzare queste linee guida per la risoluzione dei problemi se viene visualizzato uno dei seguenti messaggi di errore quando si tenta di accedere a un nodo amministratore:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Fasi

1. Attendere 10 minuti e riprovare a effettuare l'accesso.

   Se l'errore non viene risolto automaticamente, passare alla fase successiva.

2. Se il sistema StorageGRID dispone di più di un nodo amministratore, provare ad accedere al gestore della griglia da un altro nodo amministratore.
   - Se sei in grado di effettuare l'accesso, puoi utilizzare le opzioni **Dashboard**, **NODES**, **Alerts** e **SUPPORT** per determinare la causa dell'errore.
   - Se si dispone di un solo nodo di amministrazione o non si riesce ancora ad accedere, passare alla fase successiva.
3. Determinare se l'hardware del nodo non è in linea.
4. Se il sistema StorageGRID è abilitato per l'accesso singolo (SSO), fare riferimento alla procedura per la configurazione dell'accesso singolo nelle istruzioni per l'amministrazione di StorageGRID.

   Potrebbe essere necessario disattivare temporaneamente e riattivare SSO per un singolo nodo di amministrazione per risolvere eventuali problemi.

   > Se SSO è attivato, non è possibile accedere utilizzando una porta con restrizioni. È necessario utilizzare la porta 443.

5. Determinare se l'account in uso appartiene a un utente federato.

   Se l'account utente federated non funziona, provare ad accedere a Grid Manager come utente locale, ad esempio root.

   - Se l'utente locale può effettuare l'accesso:
     i. Esaminare gli eventuali allarmi visualizzati.
     ii. Selezionare **CONFIGURATION Access Control Identity Federation**.
     iii. Fare clic su **Test Connection** (verifica connessione) per convalidare le impostazioni di connessione per il server LDAP.
     iv. Se il test non riesce, risolvere eventuali errori di configurazione.
   - Se l'utente locale non riesce ad accedere e si è certi che le credenziali siano corrette, passare alla fase successiva.
6. Utilizzare Secure Shell (ssh) per accedere al nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@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. `#`.

7. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

   Assicurarsi che i servizi api nms, mi, nginx e mgmt siano tutti in esecuzione.

   L'output viene aggiornato immediatamente se lo stato di un servizio cambia.

```
$ storagegrid-status
Host Name                       99-211
IP Address                      10.96.99.211
Operating System Kernel         4.19.0         Verified
Operating System Environment    Debian 10.1    Verified
StorageGRID Webscale Release    11.4.0         Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                 5.5.9999+default Running
Network Monitoring              11.4.0         Running
Time Synchronization            1:4.2.8p10+dfsg Running
ams                             11.4.0         Running
cmn                             11.4.0         Running
nms                             11.4.0         Running
ssm                             11.4.0         Running
mi                              11.4.0         Running
dynip                           11.4.0         Running
nginx                           1.10.3         Running
tomcat                          9.0.27         Running
grafana                         6.4.3          Running
mgmt api                        11.4.0         Running
prometheus                      11.4.0         Running
persistence                     11.4.0         Running
ade exporter                    11.4.0         Running
alertmanager                    11.4.0         Running
attrDownPurge                   11.4.0         Running
attrDownSamp1                   11.4.0         Running
attrDownSamp2                   11.4.0         Running
node exporter                   0.17.0+ds      Running
sg snmp agent                   11.4.0         Running
```

8. Verificare che il servizio nginx-gw sia in esecuzione `# service nginx-gw status`
9. Usa Lumberjack per raccogliere i log: `# /usr/local/sbin/lumberjack.rb`

   Se l'autenticazione non è riuscita in passato, è possibile utilizzare le opzioni di script --start e --end Lumberjack per specificare l'intervallo di tempo appropriato. Utilizzare lumberjack -h per i dettagli su queste opzioni.

   L'output sul terminale indica dove è stato copiato l'archivio di log.

10. Rivedi i seguenti log:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`

- `**/*commands.txt`

11. Se non si riesce a identificare alcun problema con il nodo di amministrazione, eseguire uno dei seguenti comandi per determinare gli indirizzi IP dei tre nodi di storage che eseguono il servizio ADC presso la propria sede. In genere, si tratta dei primi tre nodi di storage installati nel sito.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

I nodi di amministrazione utilizzano il servizio ADC durante il processo di autenticazione.

12. Dal nodo di amministrazione, accedere a ciascuno dei nodi di storage ADC, utilizzando gli indirizzi IP identificati.
    a. Immettere il seguente comando: `ssh admin@grid_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. `#`.

13. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

    Assicurarsi che i servizi idnt, acct, nginx e cassandra siano tutti in esecuzione.

14. Ripetere i passaggi Utilizzare Lumberjack per raccogliere i registri e. Esaminare i registri Per rivedere i log sui nodi di storage.
15. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

    Fornire al supporto tecnico i registri raccolti. Vedere anche Riferimenti ai file di log.

Risolvere i problemi dell'interfaccia utente

Dopo l'aggiornamento a una nuova versione del software StorageGRID, potrebbero verificarsi problemi con Grid Manager o con il tenant manager.

L'interfaccia Web non risponde come previsto

Dopo l'aggiornamento del software StorageGRID, il gestore di rete o il tenant manager potrebbero non rispondere come previsto.

In caso di problemi con l'interfaccia Web:

- Assicurarsi di utilizzare un browser web supportato.

> Il supporto del browser è cambiato per StorageGRID 11.5. Confermare che si sta utilizzando una versione supportata.

- Cancellare la cache del browser Web.

  La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare nuovamente correttamente. Per istruzioni, consultare la documentazione del browser Web.

Controllare lo stato di un nodo amministratore non disponibile

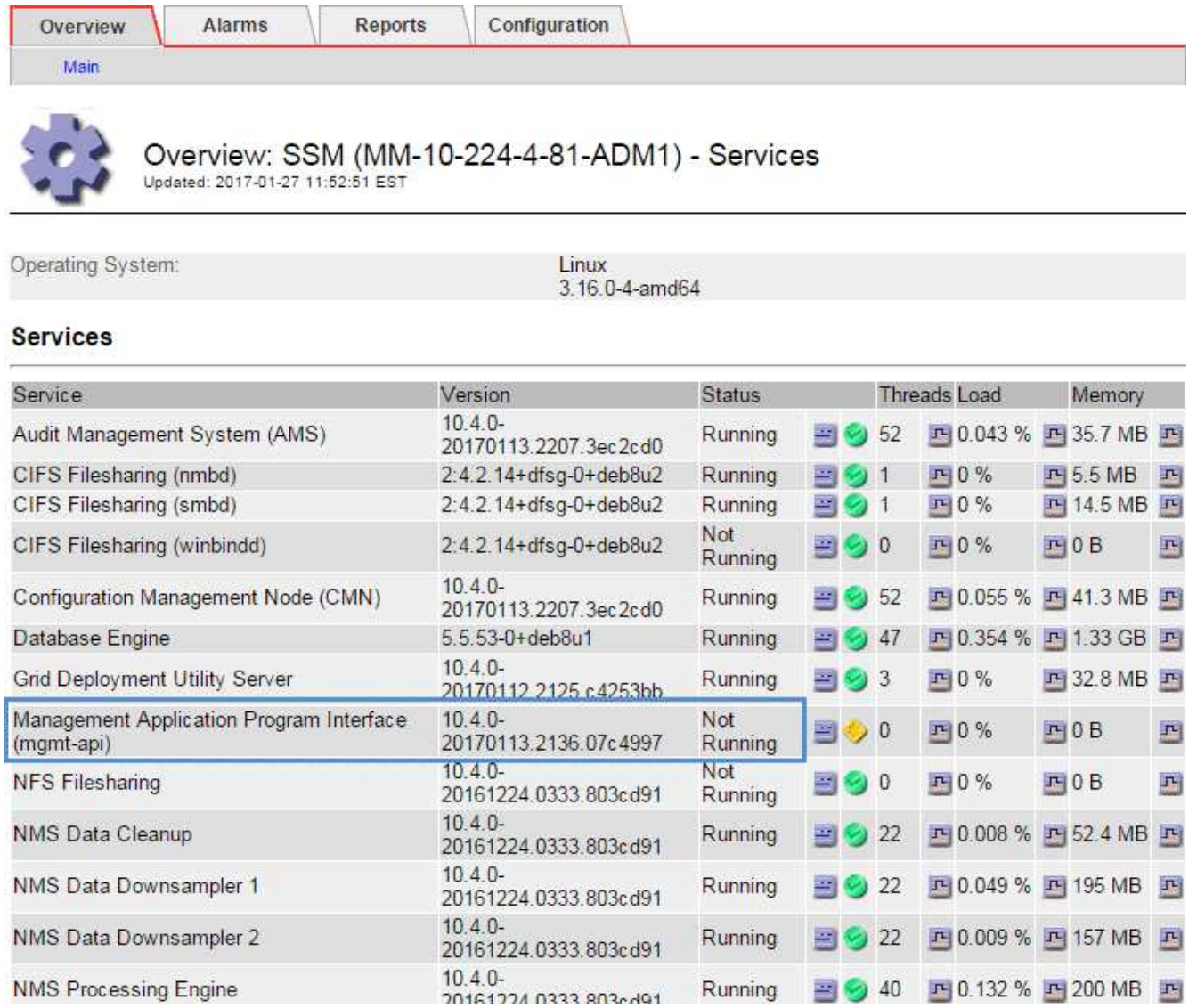
Se il sistema StorageGRID include più nodi di amministrazione, è possibile utilizzare un altro nodo di amministrazione per controllare lo stato di un nodo di amministrazione non disponibile.

Di cosa hai bisogno

È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Da un nodo Admin disponibile, accedere a Grid Manager utilizzando un browser web supportato.
2. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
3. Selezionare ***Site* non disponibile Admin Node SSM servizi Panoramica principale**.
4. Cercare i servizi con stato non in esecuzione e che potrebbero essere visualizzati anche in blu.



5. Determinare se gli allarmi sono stati attivati.
6. Intraprendere le azioni appropriate per risolvere il problema.

Informazioni correlate

Amministrare StorageGRID

Risolvere i problemi di rete, hardware e piattaforma

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi a problemi di rete, hardware e piattaforma StorageGRID.

Risolvere gli errori "422: Unprocessable Entity"

L'errore 422: Unprocessable Entity può verificarsi in diverse circostanze. Controllare il messaggio di errore per determinare la causa del problema.

Se viene visualizzato uno dei messaggi di errore elencati, eseguire l'azione consigliata.

Messaggio di errore	Causa principale e azione correttiva

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Questo messaggio potrebbe essere visualizzato se si seleziona l'opzione **non utilizzare TLS** per Transport Layer Security (TLS) durante la configurazione della federazione delle identità utilizzando Windows Active Directory (ad).
	
	L'utilizzo dell'opzione **non utilizzare TLS** non è supportato per l'utilizzo con i server ad che applicano la firma LDAP. Selezionare l'opzione **Use STARTTLS** (Usa STARTTLS*) o l'opzione **Use LDAPS** (Usa LDAPS* per TLS).

Messaggio di errore	Causa principale e azione correttiva

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Questo messaggio viene visualizzato se si tenta di utilizzare una crittografia non supportata per stabilire una connessione TLS (Transport Layer Security) da StorageGRID a un sistema esterno utilizzato per identificare la federazione o i pool di storage cloud.
	
	Controllare le cifre offerte dal sistema esterno. Il sistema deve utilizzare uno dei cifrari supportati da StorageGRID per le connessioni TLS in uscita, come illustrato nelle istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

Amministrare StorageGRID

risoluzione dei problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia

L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato quando l'impostazione Maximum Transmission Unit (MTU) per l'interfaccia Grid Network (eth0) differisce significativamente tra i nodi della griglia.

A proposito di questa attività

Le differenze nelle impostazioni MTU potrebbero indicare che alcune, ma non tutte, reti eth0 sono configurate per i frame jumbo. Una mancata corrispondenza delle dimensioni MTU superiore a 1000 potrebbe causare problemi di performance di rete.

Fasi

1. Elencare le impostazioni MTU per eth0 su tutti i nodi.
   - Utilizzare la query fornita in Grid Manager.
   - Selezionare *`primary Admin Node IP address`*`/metrics/graph` e immettere la seguente query: `node_network_mtu_bytes{interface='eth0'}`
2. Modificare le impostazioni MTU in base alle necessità per assicurarsi che siano le stesse per l'interfaccia Grid Network (eth0) su tutti i nodi.
   - Per i nodi dell'appliance, consultare le istruzioni di installazione e manutenzione dell'appliance.
   - Per i nodi basati su Linux e VMware, utilizzare il seguente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Esempio: `change-ip.py -n node 1500 grid admin`

     Nota: Nei nodi basati su Linux, se il valore MTU desiderato per la rete nel container supera il valore già configurato sull'interfaccia host, è necessario prima configurare l'interfaccia host in modo che abbia il

valore MTU desiderato, quindi utilizzare `change-ip.py` Script per modificare il valore MTU della rete nel container.

Utilizzare i seguenti argomenti per modificare la MTU su nodi basati su Linux o VMware.

Argomenti di posizione	Descrizione
`mtu`	MTU da impostare. Deve essere compreso tra 1280 e 9216.
`network`	Le reti a cui applicare la MTU. Includere uno o più dei seguenti tipi di rete: • griglia • amministratore • client

+

Argomenti facoltativi	Descrizione
`-h, - help`	Visualizzare il messaggio della guida e uscire.
`-n node, --node node`	Il nodo. L'impostazione predefinita è il nodo locale.

Informazioni correlate

Appliance di servizi SG100 e SG1000

Appliance di storage SG6000

Appliance di storage SG5700

Appliance di storage SG5600

Risolvere i problemi relativi all'allarme NRER (Network Receive Error)

Gli allarmi NRER (Network Receive Error) possono essere causati da problemi di connettività tra StorageGRID e l'hardware di rete. In alcuni casi, gli errori NRER possono essere corretti senza l'intervento manuale. Se gli errori non si cancellano, eseguire le azioni consigliate.

A proposito di questa attività

Gli allarmi NRER possono essere causati dai seguenti problemi relativi all'hardware di rete che si collega a StorageGRID:

- La funzione FEC (Forward Error Correction) è obbligatoria e non in uso
- Mancata corrispondenza tra porta dello switch e MTU della scheda NIC
- Elevati tassi di errore di collegamento
- Buffer di anello NIC scaduto

Fasi

1. Seguire i passaggi per la risoluzione dei problemi relativi a tutte le potenziali cause dell'allarme NRER in base alla configurazione di rete.

   - Se l'errore è causato da una mancata corrispondenza FEC, attenersi alla seguente procedura:

     Nota: Questi passaggi sono applicabili solo per gli errori NRER causati dalla mancata corrispondenza FEC sulle appliance StorageGRID.

     i. Controllare lo stato FEC della porta dello switch collegato all'appliance StorageGRID.

     ii. Controllare l'integrità fisica dei cavi che collegano l'apparecchio allo switch.

     iii. Se si desidera modificare le impostazioni FEC per tentare di risolvere l'allarme NRER, assicurarsi innanzitutto che l'appliance sia configurata per la modalità **auto** nella pagina di configurazione del collegamento del programma di installazione dell'appliance StorageGRID (consultare le istruzioni di installazione e manutenzione dell'appliance). Quindi, modificare le impostazioni FEC sulle porte dello switch. Le porte dell'appliance StorageGRID regoleranno le impostazioni FEC in modo che corrispondano, se possibile.

     Non è possibile configurare le impostazioni FEC sulle appliance StorageGRID. Le appliance tentano invece di rilevare e duplicare le impostazioni FEC sulle porte dello switch a cui sono collegate. Se i collegamenti sono forzati a velocità di rete 25-GbE o 100-GbE, lo switch e la NIC potrebbero non riuscire a negoziare un'impostazione FEC comune. Senza un'impostazione FEC comune, la rete torna alla modalità "no-FEC". Quando la funzione FEC non è attivata, le connessioni sono più soggette a errori causati da disturbi elettrici.

     Nota: Le appliance StorageGRID supportano Firecode (FC) e Reed Solomon (RS) FEC, oltre che FEC.

   - Se l'errore è causato da una mancata corrispondenza tra la porta dello switch e la MTU della NIC, verificare che le dimensioni MTU configurate sul nodo corrispondano all'impostazione MTU per la porta dello switch.

     La dimensione MTU configurata sul nodo potrebbe essere inferiore all'impostazione sulla porta dello switch a cui è connesso il nodo. Se un nodo StorageGRID riceve un frame Ethernet più grande del relativo MTU, cosa possibile con questa configurazione, potrebbe essere segnalato l'allarme NRER. Se si ritiene che questo sia quanto accade, modificare la MTU della porta dello switch in modo che corrisponda alla MTU dell'interfaccia di rete StorageGRID oppure modificare la MTU dell'interfaccia di rete StorageGRID in modo che corrisponda alla porta dello switch, in base agli obiettivi o ai requisiti della MTU end-to-end.

     > Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.

     > Per modificare l'impostazione MTU, consultare la guida all'installazione e alla manutenzione dell'appliance.

   - Se l'errore è causato da un elevato tasso di errori di collegamento, attenersi alla seguente procedura:

     i. Attivare FEC, se non è già attivato.

     ii. Verificare che il cablaggio di rete sia di buona qualità e non sia danneggiato o collegato in modo

errato.

iii. Se i cavi non sembrano essere il problema, contattare il supporto tecnico.

> In un ambiente con elevati livelli di rumore elettrico, potrebbero verificarsi errori elevati.

- Se l'errore è un buffer di anello della scheda di rete in eccesso, contattare il supporto tecnico.

  Il buffer circolare può essere sovraccarico quando il sistema StorageGRID è sovraccarico e non è in grado di elaborare gli eventi di rete in modo tempestivo.

2. Dopo aver risolto il problema sottostante, reimpostare il contatore degli errori.
   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   b. Selezionare ***Site Grid Node*** **SSM risorse Configurazione principale**.
   c. Selezionare **Ripristina conteggio errori di ricezione** e fare clic su **Applica modifiche**.

Informazioni correlate

Risolvere i problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia

Riferimento allarmi (sistema legacy)

Appliance di storage SG6000

Appliance di storage SG5700

Appliance di storage SG5600

Appliance di servizi SG100 e SG1000

Risoluzione dei problemi relativi agli errori di sincronizzazione dell'ora

Potrebbero verificarsi problemi con la sincronizzazione dell'ora nella griglia.

Se si verificano problemi di sincronizzazione dell'ora, verificare di aver specificato almeno quattro origini NTP esterne, ciascuna con uno strato 3 o un riferimento migliore, e che tutte le origini NTP esterne funzionino normalmente e siano accessibili dai nodi StorageGRID.

> Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time sulle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'utilizzo in ambienti ad alta precisione, come StorageGRID.

Informazioni correlate

Ripristino e manutenzione

Linux: Problemi di connettività di rete

Potrebbero verificarsi problemi con la connettività di rete per i grid node StorageGRID ospitati su host Linux.

Clonazione indirizzo MAC

In alcuni casi, i problemi di rete possono essere risolti utilizzando la clonazione dell'indirizzo MAC. Se si utilizzano host virtuali, impostare il valore della chiave di clonazione dell'indirizzo MAC per ciascuna rete su "true" nel file di configurazione del nodo. Questa impostazione fa in modo che l'indirizzo MAC del container StorageGRID utilizzi l'indirizzo MAC dell'host. Per creare i file di configurazione dei nodi, consultare le istruzioni nella guida all'installazione della piattaforma in uso.

> Creare interfacce di rete virtuali separate per l'utilizzo da parte del sistema operativo host Linux. L'utilizzo delle stesse interfacce di rete per il sistema operativo host Linux e per il container StorageGRID potrebbe rendere il sistema operativo host irraggiungibile se la modalità promiscua non è stata attivata sull'hypervisor.

Per ulteriori informazioni sull'attivazione della clonazione MAC, consultare le istruzioni nella guida all'installazione della piattaforma.

Modalità promiscua

Se non si desidera utilizzare la clonazione dell'indirizzo MAC e si desidera consentire a tutte le interfacce di ricevere e trasmettere dati per indirizzi MAC diversi da quelli assegnati dall'hypervisor, Assicurarsi che le proprietà di sicurezza a livello di switch virtuale e gruppo di porte siano impostate su **Accept** per modalità promiscuous, modifiche indirizzo MAC e trasmissione forgiata. I valori impostati sullo switch virtuale possono essere sovrascritti dai valori a livello di gruppo di porte, quindi assicurarsi che le impostazioni siano le stesse in entrambe le posizioni.

Informazioni correlate

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Linux: Stato del nodo "orfano"

Un nodo Linux in uno stato orfano di solito indica che il servizio StorageGRID o il daemon del nodo StorageGRID che controlla il contenitore del nodo sono morti inaspettatamente.

A proposito di questa attività

Se un nodo Linux segnala che si trova in uno stato orfano, è necessario:

- Controllare i registri per verificare la presenza di errori e messaggi.
- Tentare di riavviare il nodo.
- Se necessario, utilizzare i comandi del motore dei container per arrestare il contenitore di nodi esistente.
- Riavviare il nodo.

Fasi

1. Controllare i log sia per il daemon di servizio che per il nodo orfano per verificare la presenza di errori evidenti o messaggi relativi all'uscita imprevista.
2. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
3. Tentare di riavviare il nodo eseguendo il seguente comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Se il nodo è orfano, la risposta è

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Da Linux, arrestare il motore dei container e qualsiasi processo di controllo del nodo storagegrid. Ad esempio:`sudo docker stop --time secondscontainer-name`

   Per `seconds`, immettere il numero di secondi che si desidera attendere per l'arresto del container (in genere 15 minuti o meno). Ad esempio:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Riavviare il nodo: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

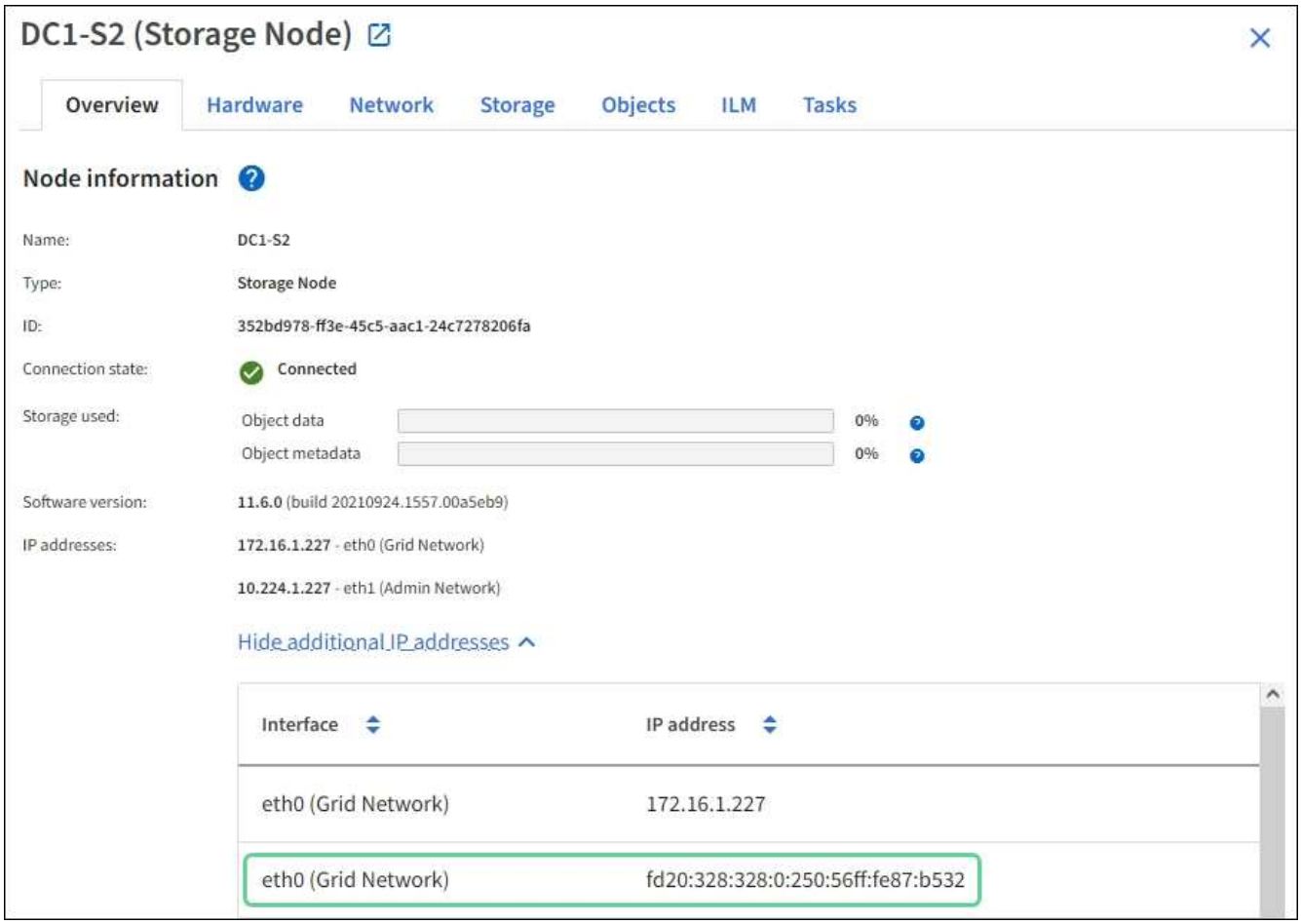
Linux: Risoluzione dei problemi relativi al supporto IPv6

Potrebbe essere necessario abilitare il supporto IPv6 nel kernel se sono stati installati nodi StorageGRID su host Linux e si nota che gli indirizzi IPv6 non sono stati assegnati ai contenitori di nodi come previsto.

A proposito di questa attività

È possibile visualizzare l'indirizzo IPv6 assegnato a un nodo Grid nelle seguenti posizioni in Grid Manager:

- Selezionare **NODI** e selezionare il nodo. Quindi, selezionare **Mostra altri** accanto a **indirizzi IP** nella scheda Panoramica.



- Selezionare **SUPPORT Tools Grid topology**. Quindi, selezionare ***node* SSM Resources**. Se è stato assegnato un indirizzo IPv6, questo viene elencato sotto l'indirizzo IPv4 nella sezione **indirizzi di rete**.

Se l'indirizzo IPv6 non viene visualizzato e il nodo è installato su un host Linux, seguire questa procedura per abilitare il supporto IPv6 nel kernel.

Fasi

1. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
2. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

   Il risultato deve essere 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

   Se il risultato non è 0, consultare la documentazione relativa al sistema operativo in uso per le modifiche `sysctl` impostazioni. Quindi, modificare il valore su 0 prima di continuare.

3. Inserire il contenitore di nodi StorageGRID: `storagegrid node enter node-name`

4. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Il risultato deve essere 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> Se il risultato non è 1, questa procedura non si applica. Contattare il supporto tecnico.

5. Uscire dal container: `exit`

```
root@DC1-S1:~ # exit
```

6. Come root, modificare il seguente file: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Individuare le due righe seguenti e rimuovere i tag di commento. Quindi, salvare e chiudere il file.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Eseguire questi comandi per riavviare il container StorageGRID:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Risolvere i problemi di un server syslog esterno

La seguente tabella descrive i messaggi di errore del server syslog esterno ed elenca le azioni correttive.

Messaggio di errore	Descrizione e azioni consigliate
Impossibile risolvere il nome host	Impossibile risolvere l'FQDN immesso per il server syslog in un indirizzo IP. 1. Controllare il nome host immesso. Se è stato immesso un indirizzo IP, assicurarsi che sia un indirizzo IP valido con la notazione W.X.Y.Z ("decimale separato da punti"). 2. Verificare che i server DNS siano configurati correttamente. 3. Verificare che ciascun nodo possa accedere agli indirizzi IP del server DNS.
Connessione rifiutata	Una connessione TCP o TLS al server syslog è stata rifiutata. Sulla porta TCP o TLS dell'host potrebbe non essere presente alcun servizio o un firewall potrebbe bloccare l'accesso. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Verificare che l'host del servizio syslog stia eseguendo un daemon syslog in attesa sulla porta specificata. 3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi all'IP e alla porta del server syslog.
Rete non raggiungibile	Il server syslog non si trova su una subnet collegata direttamente. Un router ha restituito un messaggio di errore ICMP per indicare che non è stato possibile inoltrare i messaggi di test dai nodi elencati al server syslog. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per instradare il traffico al server syslog attraverso l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host non raggiungibile	Il server syslog si trova su una subnet collegata direttamente (subnet utilizzata dai nodi elencati per gli indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di test, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del server syslog. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Verificare che l'host che esegue il servizio syslog sia attivo.

Messaggio di errore	Descrizione e azioni consigliate
Timeout della connessione	È stato eseguito un tentativo di connessione TCP/TLS, ma non è stata ricevuta alcuna risposta dal server syslog per molto tempo. Potrebbe esserci un errore di configurazione del routing o un firewall potrebbe interrompere il traffico senza inviare alcuna risposta (una configurazione comune). 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per indirizzare il traffico al server syslog tramite l'interfaccia di rete e il gateway (Grid, Admin o Client) su cui si prevede di raggiungere il server syslog. 3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi elencati all'IP e alla porta del server syslog.
Connessione chiusa dal partner	Una connessione TCP al server syslog è stata stabilita correttamente, ma in seguito è stata chiusa. I motivi potrebbero includere: • Il server syslog potrebbe essere stato riavviato o riavviato. • Il nodo e il server syslog potrebbero avere impostazioni TCP/TLS diverse. • Un firewall intermedio potrebbe chiudere le connessioni TCP inattive. • Un server non syslog in ascolto sulla porta del server syslog potrebbe aver chiuso la connessione. a. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. b. Se si utilizza TLS, verificare che anche il server syslog utilizzi TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. c. Verificare che un firewall intermedio non sia configurato per chiudere le connessioni TCP inattive.
Errore certificato TLS	Il certificato del server ricevuto dal server syslog non era compatibile con il bundle di certificati CA e con il certificato client forniti. 1. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server sul server syslog. 2. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.

Messaggio di errore	Descrizione e azioni consigliate
Inoltro sospeso	I record syslog non vengono più inoltrati al server syslog e StorageGRID non è in grado di rilevare il motivo. Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale.
Sessione TLS terminata	Il server syslog ha terminato la sessione TLS e StorageGRID non è in grado di rilevare il motivo. 1. Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale. 2. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 3. Se si utilizza TLS, verificare che anche il server syslog utilizzi TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. 4. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server dal server syslog. 5. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.
Query dei risultati non riuscita	Il nodo di amministrazione utilizzato per la configurazione e il test del server syslog non è in grado di richiedere i risultati del test dai nodi elencati. Uno o più nodi potrebbero non essere attivi. 1. Seguire le procedure standard per la risoluzione dei problemi per assicurarsi che i nodi siano online e che tutti i servizi previsti siano in esecuzione. 2. Riavviare il servizio miscd sui nodi elencati.

Riferimenti agli avvisi

La tabella seguente elenca tutti gli avvisi StorageGRID predefiniti. Se necessario, è possibile creare regole di avviso personalizzate per adattarsi al proprio approccio di gestione del sistema.

Consultare le informazioni su Metriche Prometheus comunemente utilizzate per informazioni sulle metriche utilizzate in alcuni di questi avvisi.

Nome dell'avviso	Descrizione e azioni consigliate
Batteria dell'appliance scaduta	La batteria del controller di storage dell'appliance è scaduta. 1. Sostituire la batteria. La procedura per la sostituzione di un controller di storage include la procedura per la rimozione e la sostituzione della batteria. Consultare le istruzioni relative all'appliance di storage: ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000 2. Se l'avviso persiste, contattare il supporto tecnico.
Batteria dell'appliance guasta	La batteria del controller di storage dell'appliance si è guastata. 1. Sostituire la batteria. La procedura per la sostituzione di un controller di storage include la procedura per la rimozione e la sostituzione della batteria. Consultare le istruzioni relative all'appliance di storage: ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000 2. Se l'avviso persiste, contattare il supporto tecnico.
La capacità appresa della batteria dell'appliance non è sufficiente	La capacità appresa della batteria nel controller di storage dell'appliance non è sufficiente. 1. Sostituire la batteria. La procedura per la sostituzione di un controller di storage include la procedura per la rimozione e la sostituzione della batteria. Consultare le istruzioni relative all'appliance di storage: ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000 2. Se l'avviso persiste, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Batteria dell'apparecchio quasi scaduta	La batteria del controller di storage dell'appliance sta per scadere. 1. Sostituire la batteria al più presto. La procedura per la sostituzione di un controller di storage include la procedura per la rimozione e la sostituzione della batteria. Consultare le istruzioni relative all'appliance di storage: ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000 2. Se l'avviso persiste, contattare il supporto tecnico.
Batteria dell'apparecchio rimossa	La batteria nel controller di storage dell'appliance non è presente. 1. Installare una batteria. La procedura per la sostituzione di un controller di storage include la procedura per la rimozione e la sostituzione della batteria. Consultare le istruzioni relative all'appliance di storage: ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000 2. Se l'avviso persiste, contattare il supporto tecnico.
Batteria dell'apparecchio troppo calda	La batteria del controller di storage dell'apparecchio è surriscaldata. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Esaminare i possibili motivi dell'aumento della temperatura, ad esempio un guasto alla ventola o all'HVAC. 3. Se l'avviso persiste, contattare il supporto tecnico.
Errore di comunicazione BMC dell'appliance	La comunicazione con il BMC (Baseboard Management Controller) è stata persa. 1. Verificare che il BMC funzioni correttamente. Selezionare **NODES**, quindi selezionare la scheda **hardware** per il nodo dell'appliance. Individuare il campo Compute Controller BMC IP (IP BMC controller di calcolo) e individuare l'IP desiderato. 2. Tentare di ripristinare le comunicazioni BMC posizionando il nodo in modalità di manutenzione, quindi spegnendo e riaccendendo l'appliance. Consultare le istruzioni per l'apparecchio: ◦ Appliance di servizi SG100 e SG1000 ◦ Appliance di storage SG6000 3. Se l'avviso persiste, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Periferica di backup della cache dell'appliance non riuscita	Si è verificato un errore in una periferica di backup della cache persistente. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Contattare il supporto tecnico.
Capacità insufficiente del dispositivo di backup della cache dell'appliance	La capacità della periferica di backup della cache è insufficiente. Contattare il supporto tecnico.
Dispositivo di backup cache dell'appliance protetto da scrittura	Una periferica di backup della cache è protetta da scrittura. Contattare il supporto tecnico.
Mancata corrispondenza delle dimensioni della memoria cache dell'appliance	I due controller dell'appliance hanno dimensioni della cache diverse. Contattare il supporto tecnico.
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. 1. Verificare l'eventuale presenza di condizioni di surriscaldamento dei componenti hardware e seguire le azioni consigliate: ◦ Se si dispone di SG100, SG1000 o SG6000, utilizzare BMC. ◦ Se si dispone di un sistema SG5600 o SG5700, utilizzare Gestore di sistema di SANtricity. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di servizi SG100 e SG1000 ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600

Nome dell'avviso	Descrizione e azioni consigliate
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. 1. Verificare l'eventuale presenza di condizioni di surriscaldamento dei componenti hardware e seguire le azioni consigliate: ◦ Se si dispone di SG100, SG1000 o SG6000, utilizzare BMC. ◦ Se si dispone di un sistema SG5600 o SG5700, utilizzare Gestore di sistema di SANtricity. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di servizi SG100 e SG1000 ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000
Il controller di calcolo dell'appliance richiede attenzione	È stato rilevato un guasto hardware nel controller di calcolo di un'appliance StorageGRID. 1. Verificare la presenza di errori nei componenti hardware e seguire le azioni consigliate: ◦ Se si dispone di SG100, SG1000 o SG6000, utilizzare BMC. ◦ Se si dispone di un sistema SG5600 o SG5700, utilizzare Gestore di sistema di SANtricity. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di servizi SG100 e SG1000 ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000

Nome dell'avviso	Descrizione e azioni consigliate
Si è verificato un problema nell'alimentatore A del controller di calcolo dell'appliance	Si è verificato un problema nell'alimentatore A del controller di calcolo. Questo avviso potrebbe indicare che l'alimentatore è guasto o che si è verificato un problema nell'alimentazione. 1. Verificare la presenza di errori nei componenti hardware e seguire le azioni consigliate: ◦ Se si dispone di SG100, SG1000 o SG6000, utilizzare BMC. ◦ Se si dispone di un sistema SG5600 o SG5700, utilizzare Gestore di sistema di SANtricity. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di servizi SG100 e SG1000 ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000
Si è verificato un problema nell'alimentatore B del controller di calcolo dell'appliance	L'alimentazione B nel controller di calcolo presenta un problema. Questo avviso potrebbe indicare che l'alimentatore è guasto o che si è verificato un problema di alimentazione. 1. Verificare la presenza di errori nei componenti hardware e seguire le azioni consigliate: ◦ Se si dispone di SG100, SG1000 o SG6000, utilizzare BMC. ◦ Se si dispone di un sistema SG5600 o SG5700, utilizzare Gestore di sistema di SANtricity. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di servizi SG100 e SG1000 ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000
Il servizio di monitoraggio dell'hardware di calcolo dell'appliance si è bloccato	Il servizio che monitora lo stato dell'hardware dello storage ha smesso di riportare i dati. 1. Controllare lo stato del servizio di stato del sistema eos nel sistema operativo di base. 2. Se il servizio si trova in uno stato di arresto o di errore, riavviarlo. 3. Se l'avviso persiste, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate

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.
	
	Questo avviso potrebbe indicare la presenza di un problema relativo alla connessione Fibre Channel tra lo storage e i controller di calcolo nell'appliance.
	
	1. Verificare la presenza di errori nei componenti hardware (**NODI *nodo appliance* hardware**). Se lo stato di uno dei componenti non è "nominale", eseguire le seguenti operazioni:
	  a. Verificare che i cavi Fibre Channel tra i controller siano collegati correttamente.
	  b. Assicurarsi che i cavi Fibre Channel siano privi di piegature eccessive.
	  c. Verificare che i moduli SFP+ siano inseriti correttamente.
	
	  Nota: se il problema persiste, il sistema StorageGRID potrebbe disattivare automaticamente la connessione problematica.
	
	2. Se necessario, sostituire i componenti. Consultare le istruzioni per l'apparecchio:
	  ◦ Appliance di storage SG5700
	  ◦ Appliance di storage SG6000

Errore della porta HBA Fibre Channel dell'appliance	Una porta HBA Fibre Channel si sta guastando o si è guastata. Contattare il supporto tecnico.

Unità flash cache dell'appliance non ottimali	I dischi utilizzati per la cache SSD non sono ottimali.
	
	1. Sostituire le unità cache SSD. Consultare le istruzioni per l'apparecchio:
	  ◦ Appliance di storage SG5600
	  ◦ Appliance di storage SG5700
	  ◦ Appliance di storage SG6000
	2. Se l'avviso persiste, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Interconnessione dell'appliance/contenitore della batteria rimosso	Il contenitore di interconnessione/batteria non è presente. 1. Sostituire la batteria. La procedura per la sostituzione di un controller di storage include la procedura per la rimozione e la sostituzione della batteria. Consultare le istruzioni relative all'appliance di storage. ◦ Appliance di storage SG5600 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG6000 2. Se l'avviso persiste, contattare il supporto tecnico.
Porta LACP dell'appliance mancante	Una porta su un'appliance StorageGRID non partecipa al bond LACP. 1. Controllare la configurazione dello switch. Assicurarsi che l'interfaccia sia configurata nel gruppo di aggregazione dei collegamenti corretto. 2. Se l'avviso persiste, contattare il supporto tecnico.
Alimentatore generale dell'appliance degradato	La potenza di un'appliance StorageGRID è diversa dalla tensione di esercizio consigliata. 1. Controllare lo stato degli alimentatori A e B per determinare quale alimentatore funziona in modo anomalo e seguire le azioni consigliate: ◦ Se si dispone di SG100, SG1000 o SG6000, utilizzare BMC. ◦ Se si dispone di un sistema SG5600 o SG5700, utilizzare Gestore di sistema di SANtricity. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600 ◦ Appliance di servizi SG100 e SG1000

Nome dell'avviso	Descrizione e azioni consigliate
Guasto del controller dello storage dell'appliance A.	Si è verificato un errore nel controller storage A di un'appliance StorageGRID. 1. Utilizzare Gestione di sistema di SANtricity per controllare i componenti hardware e seguire le azioni consigliate. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600
Guasto del controller storage dell'appliance B.	Il controller dello storage B in un'appliance StorageGRID si è guastato. 1. Utilizzare Gestione di sistema di SANtricity per controllare i componenti hardware e seguire le azioni consigliate. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600
Guasto al disco del controller dello storage dell'appliance	Uno o più dischi di un'appliance StorageGRID si sono guastati o non sono ottimali. 1. Utilizzare Gestione di sistema di SANtricity per controllare i componenti hardware e seguire le azioni consigliate. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600
Problema hardware del controller dello storage dell'appliance	Il software SANtricity segnala "richiede attenzione" per un componente di un'appliance StorageGRID. 1. Utilizzare Gestione di sistema di SANtricity per controllare i componenti hardware e seguire le azioni consigliate. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600

Nome dell'avviso	Descrizione e azioni consigliate
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. 1. Utilizzare Gestione di sistema di SANtricity per controllare i componenti hardware e seguire le azioni consigliate. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600
Guasto all'alimentazione B del controller storage dell'appliance	L'alimentazione B di un apparecchio StorageGRID non è conforme alla tensione di esercizio consigliata. 1. Utilizzare Gestione di sistema di SANtricity per controllare i componenti hardware e seguire le azioni consigliate. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600
Il servizio di monitoraggio hardware dello storage dell'appliance si è bloccato	Il servizio che monitora lo stato dell'hardware dello storage ha smesso di riportare i dati. 1. Controllare lo stato del servizio di stato del sistema eos nel sistema operativo di base. 2. Se il servizio si trova in uno stato di arresto o di errore, riavviarlo. 3. Se l'avviso persiste, contattare il supporto tecnico.
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. 1. Utilizzare Gestione di sistema di SANtricity per controllare i componenti hardware e seguire le azioni consigliate. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600

Nome dell'avviso	Descrizione e azioni consigliate
Temperatura dell'apparecchio superata	La temperatura nominale o massima del controller di storage dell'appliance è stata superata. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Esaminare i possibili motivi dell'aumento della temperatura, ad esempio un guasto alla ventola o all'HVAC. 3. Se l'avviso persiste, contattare il supporto tecnico.
Sensore di temperatura dell'apparecchio rimosso	È stato rimosso un sensore di temperatura. Contattare il supporto tecnico.
Errore compattatore automatico Cassandra	Si è verificato un errore nel compattatore automatico Cassandra. Il compattatore automatico Cassandra è presente su tutti i nodi di storage e gestisce le dimensioni del database Cassandra per la sovrascrittura e l'eliminazione di carichi di lavoro pesanti. Anche se questa condizione persiste, alcuni carichi di lavoro sperimenteranno un consumo inaspettatamente elevato di metadati. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Contattare il supporto tecnico.
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. 1. Assicurarsi che il servizio rsyslog sia in esecuzione sul nodo. 2. Se necessario, riavviare il servizio rsyslog sul nodo utilizzando il comando `service rsyslog restart`. 3. Se non è possibile riavviare il servizio rsyslog e non si salvano messaggi di audit sui nodi di amministrazione, contattare il supporto tecnico. Se questa condizione non viene corretta, i registri di controllo andranno persi.

Nome dell'avviso	Descrizione e azioni consigliate
Metriche del compattatore automatico Cassandra non aggiornate	Le metriche che descrivono il compattatore automatico Cassandra non sono aggiornate. Il compattatore automatico Cassandra è presente su tutti i nodi di storage e gestisce le dimensioni del database Cassandra per la sovrascrittura e l'eliminazione di carichi di lavoro pesanti. Mentre questo avviso persiste, alcuni carichi di lavoro sperimenteranno un consumo inaspettatamente elevato di metadati. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Contattare il supporto tecnico.
Errore di comunicazione Cassandra	I nodi che eseguono il servizio Cassandra hanno problemi di comunicazione tra loro. Questo avviso indica che qualcosa sta interferendo con le comunicazioni da nodo a nodo. Potrebbe esserci un problema di rete o il servizio Cassandra potrebbe essere inattivo su uno o più nodi di storage. 1. Determinare se è presente un altro avviso che interessa uno o più nodi di storage. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Verificare la presenza di un problema di rete che potrebbe interessare uno o più nodi di storage. 3. Selezionare **SUPPORT** > **Tools** > **Grid topology**. 4. Per ciascun nodo di storage del sistema, selezionare **SSM servizi**. Assicurarsi che lo stato del servizio Cassandra sia "in esecuzione". 5. Se Cassandra non è in esecuzione, seguire la procedura descritta in avvio o riavvio di un servizio. 6. Se tutte le istanze del servizio Cassandra sono in esecuzione e l'avviso non viene risolto, contattare il supporto tecnico.
Le compaction di Cassandra sono sovraccaricate	Il processo di compattazione Cassandra è sovraccarico. In caso di sovraccarico del processo di compattazione, le prestazioni di lettura potrebbero essere ridotte e la RAM potrebbe essere consuicata. Anche il servizio Cassandra potrebbe non rispondere o bloccarsi. 1. Riavviare il servizio Cassandra seguendo la procedura descritta in riavvio di un servizio. 2. Se l'avviso persiste, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Metriche di riparazione Cassandra non aggiornate	Le metriche che descrivono i lavori di riparazione Cassandra non sono aggiornate. Se questa condizione persiste per più di 48 ore, le query del client, come gli elenchi dei bucket, potrebbero mostrare i dati cancellati. 1. Riavviare il nodo. Da Grid Manager, selezionare **NODES**, selezionare il nodo e selezionare la scheda Tasks (attività). 2. Se l'avviso persiste, contattare il supporto tecnico.
Il processo di riparazione di Cassandra è lento	Il progresso delle riparazioni del database Cassandra è lento. Quando le riparazioni del database sono lente, le operazioni di coerenza dei dati Cassandra vengono ostacolate. Se questa condizione persiste per più di 48 ore, le query del client, come gli elenchi dei bucket, potrebbero mostrare i dati cancellati. 1. Verificare che tutti i nodi di storage siano online e che non siano presenti avvisi relativi alla rete. 2. Monitorare questo avviso per un massimo di 2 giorni per verificare se il problema si risolve da solo. 3. Se le riparazioni del database continuano a procedere lentamente, contattare il supporto tecnico.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione Cassandra non è disponibile. Il servizio di riparazione Cassandra esiste su tutti i nodi di storage e fornisce funzioni di riparazione critiche per il database Cassandra. Se questa condizione persiste per più di 48 ore, le query del client, come gli elenchi dei bucket, potrebbero mostrare i dati cancellati. 1. Selezionare **SUPPORT** > **Tools** > **Grid topology**. 2. Per ciascun nodo di storage del sistema, selezionare **SSM servizi**. Assicurarsi che lo stato del servizio Cassandra Reaper sia "in esecuzione". 3. Se Cassandra Reaper non è in esecuzione, seguire la procedura descritta in avvio o riavvio di un servizio. 4. Se tutte le istanze del servizio Cassandra Reaper sono in esecuzione e l'avviso non viene risolto, contattare il supporto tecnico.
Tabella Cassandra corrotta	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva la corruzione della tabella. Contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
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. 1. Accedere alla sezione Cloud Storage Pools della pagina Storage Pools. 2. Esaminare la colonna Last Error (ultimo errore) per determinare quale pool di storage cloud presenta un errore. 3. Consultare le istruzioni per gestione degli oggetti con la gestione del ciclo di vita delle informazioni.
Lease DHCP scaduto	Il lease DHCP su un'interfaccia di rete è scaduto. Se il lease DHCP è scaduto, seguire le azioni consigliate: 1. Assicurarsi che vi sia connettività tra questo nodo e il server DHCP sull'interfaccia interessata. 2. Assicurarsi che siano disponibili indirizzi IP da assegnare nella subnet interessata sul server DHCP. 3. Assicurarsi che vi sia una prenotazione permanente per l'indirizzo IP configurato nel server DHCP. In alternativa, utilizzare lo strumento Modifica IP StorageGRID per assegnare un indirizzo IP statico esterno al pool di indirizzi DHCP. Vedere istruzioni per il ripristino e la manutenzione.
Il lease DHCP sta per scadere	Il lease DHCP su un'interfaccia di rete sta per scadere. Per impedire la scadenza del lease DHCP, seguire le azioni consigliate: 1. Assicurarsi che vi sia connettività tra questo nodo e il server DHCP sull'interfaccia interessata. 2. Assicurarsi che siano disponibili indirizzi IP da assegnare nella subnet interessata sul server DHCP. 3. Assicurarsi che vi sia una prenotazione permanente per l'indirizzo IP configurato nel server DHCP. In alternativa, utilizzare lo strumento Modifica IP StorageGRID per assegnare un indirizzo IP statico esterno al pool di indirizzi DHCP. Vedere istruzioni per il ripristino e la manutenzione.

Nome dell'avviso	Descrizione e azioni consigliate
Server DHCP non disponibile	Il server DHCP non è disponibile. Il nodo StorageGRID non è in grado di contattare il server DHCP. Il lease DHCP per l'indirizzo IP del nodo non può essere validato. 1. Assicurarsi che vi sia connettività tra questo nodo e il server DHCP sull'interfaccia interessata. 2. Assicurarsi che siano disponibili indirizzi IP da assegnare nella subnet interessata sul server DHCP. 3. Assicurarsi che vi sia una prenotazione permanente per l'indirizzo IP configurato nel server DHCP. In alternativa, utilizzare lo strumento Modifica IP StorageGRID per assegnare un indirizzo IP statico esterno al pool di indirizzi DHCP. Vedere istruzioni per il ripristino e la manutenzione.
L'i/o del disco è molto lento	L'i/o del disco molto lento potrebbe influire sulle prestazioni di StorageGRID. 1. Se il problema riguarda un nodo dell'appliance di storage, utilizzare Gestione di sistema di SANtricity per verificare la presenza di dischi difettosi, dischi con guasti previsti o riparazioni dei dischi in corso. Controllare inoltre lo stato dei collegamenti Fibre Channel o SAS tra i controller di calcolo e storage dell'appliance per verificare se i collegamenti sono inattivi o mostrano tassi di errore eccessivi. 2. Esaminare il sistema storage che ospita i volumi di questo nodo per determinare e correggere la causa principale del rallentamento dell'i/O. 3. Se l'avviso persiste, contattare il supporto tecnico. **Nota:** i nodi interessati potrebbero disattivare i servizi e riavviarsi per evitare di influire sulle prestazioni complessive della griglia. Quando la condizione sottostante viene cancellata e questi nodi rilevano le normali prestazioni i/o, tornano automaticamente al servizio completo.

Nome dell'avviso	Descrizione e azioni consigliate

Errore di ribilanciamento EC	Il processo di ribilanciamento dei dati con codifica di cancellazione tra i nodi di storage non è riuscito o è stato messo in pausa dall'utente.
	
	1. Assicurarsi che tutti i nodi di storage del sito da ribilanciare siano online e disponibili.
	2. Assicurarsi che non vi siano errori di volume nel sito in fase di ribilanciamento. In caso affermativo, terminare il lavoro di ribilanciamento EC in modo da poter eseguire un lavoro di riparazione.
	
	`'rebalance-data terminate --job-id <ID>'`
	
	3. Assicurarsi che non vi siano guasti al servizio sul sito in fase di ribilanciamento. Se un servizio non è in esecuzione, seguire la procedura per avviare o riavviare un servizio nelle istruzioni di ripristino e manutenzione.
	4. Dopo aver risolto eventuali problemi, riavviare il processo eseguendo il seguente comando sul nodo di amministrazione primario:
	
	`'rebalance-data start --job-id <ID>'`
	
	5. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

Errore di riparazione EC	Un lavoro di riparazione per i dati con codifica di cancellazione non è riuscito o è stato interrotto. 1. Assicurarsi che siano disponibili volumi o nodi di storage sufficienti per sostituire il nodo o il volume di storage guasto. 2. Assicurarsi che siano disponibili nodi di storage sufficienti per soddisfare la policy ILM attiva. 3. Assicurarsi che non vi siano problemi di connettività di rete. 4. Dopo aver risolto eventuali problemi, riavviare il processo eseguendo il seguente comando sul nodo di amministrazione primario: `'repair-data start-ec-node-repair --repair-id <ID>'` 5. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Riparazione EC in stallo	Un lavoro di riparazione per i dati con codifica di cancellazione si è bloccato. 1. Assicurarsi che siano disponibili volumi o nodi di storage sufficienti per sostituire il nodo o il volume di storage guasto. 2. Assicurarsi che non vi siano problemi di connettività di rete. 3. Dopo aver risolto eventuali problemi, controllare se l'avviso è stato risolto. Per visualizzare un report più dettagliato sull'avanzamento della riparazione, eseguire il seguente comando sul nodo di amministrazione principale: `'repair-data show-ec-repair-status --repair-id <ID>'` 4. Se non si riesce a risolvere il problema, contattare il supporto tecnico.
Errore di notifica e-mail	Impossibile inviare la notifica via email per un avviso. Questo avviso viene attivato quando una notifica e-mail di avviso non riesce o non è possibile inviare un'e-mail di prova (inviata dalla pagina **ALERTS Email setup**). 1. Accedere a Grid Manager dal nodo Admin elencato nella colonna **Sito/nodo** dell'avviso. 2. Accedere alla pagina **ALERTS email setup**, controllare le impostazioni e modificarle se necessario. 3. Fare clic su **Send Test Email** (Invia email di prova) e controllare la posta in arrivo di un destinatario del test. Se non è possibile inviare l'e-mail di prova, potrebbe essere attivata una nuova istanza di questo avviso. 4. Se non è stato possibile inviare l'e-mail di prova, verificare che il server e-mail sia in linea. 5. Se il server funziona, selezionare **SUPPORT Tools Logs** e raccogliere il log per il nodo di amministrazione. Specificare un periodo di tempo di 15 minuti prima e dopo l'ora dell'avviso. 6. Estrarre l'archivio scaricato ed esaminare il contenuto di `prometheus.log (_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log).` 7. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Scadenza dei certificati client configurati nella pagina certificati	Uno o più certificati client configurati nella pagina certificati stanno per scadere. 1. In Grid Manager, selezionare **CONFIGURATION Security Certificates**, quindi selezionare la scheda **Client**. 2. Seleziona un certificato che scadrà a breve. 3. Selezionare **Allega nuovo certificato** a. caricare o generare un nuovo certificato. 4. Ripetere questa procedura per ogni certificato che scadrà a breve.
Scadenza del certificato endpoint del bilanciamento del carico	Uno o più certificati endpoint per il bilanciamento del carico stanno per scadere. 1. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**. 2. Selezionare un endpoint con un certificato che scadrà a breve. 3. Selezionare **Edit endpoint** (Modifica endpoint) per caricare o generare un nuovo certificato. 4. Ripetere questi passaggi per ogni endpoint con un certificato scaduto o che scadrà a breve. Per ulteriori informazioni sulla gestione degli endpoint del bilanciamento del carico, vedere Istruzioni per l'amministrazione di StorageGRID.
Scadenza del certificato del server per l'interfaccia di gestione	Il certificato del server utilizzato per l'interfaccia di gestione sta per scadere. 1. Selezionare **CONFIGURAZIONE sicurezza certificati**. 2. Nella scheda **Global**, selezionare **Management interface certificate**. 3. Caricare un nuovo certificato dell'interfaccia di gestione.
Scadenza del certificato server globale per S3 e Swift API	Il certificato del server utilizzato per accedere 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.

Nome dell'avviso	Descrizione e azioni consigliate
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. 1. Aggiornare il certificato CA sul server syslog esterno. 2. Ottenere una copia del certificato CA aggiornato. 3. Da Grid Manager, andare a **CONFIGURAZIONE monitoraggio Audit e server syslog**. 4. Selezionare **Modifica server syslog esterno**. 5. Selezionare **Sfoglia** per caricare il nuovo certificato. 6. Completare la configurazione guidata per salvare il nuovo certificato e la nuova chiave.
Scadenza del certificato client syslog esterno	Il certificato client per un server syslog esterno sta per scadere. 1. Da Grid Manager, andare a **CONFIGURAZIONE monitoraggio Audit e server syslog**. 2. Selezionare **Modifica server syslog esterno**. 3. Selezionare **Sfoglia** per caricare il nuovo certificato. 4. Selezionare **Sfoglia** per caricare la nuova chiave privata. 5. Completare la configurazione guidata per salvare il nuovo certificato e la nuova chiave.
Scadenza del certificato del server syslog esterno	Il certificato del server presentato dal server syslog esterno sta per scadere. 1. Aggiornare il certificato del server sul server syslog esterno. 2. Se in precedenza si utilizzava l'API Grid Manager per fornire un certificato server per la convalida del certificato, caricare il certificato server aggiornato utilizzando l'API.
Errore di inoltro del server syslog esterno	Il nodo non può inoltrare i log al server syslog esterno. 1. Da Grid Manager, andare a **CONFIGURAZIONE monitoraggio Audit e server syslog**. 2. Selezionare **Modifica server syslog esterno**. 3. Avanzare attraverso la Configurazione guidata fino a quando non si è in grado di selezionare **Invia messaggi di prova**. 4. Selezionare **Send test messages** (Invia messaggi di test) per determinare perché i log non possono essere inoltrati al server syslog esterno. 5. Risolvere eventuali problemi segnalati.

Nome dell'avviso	Descrizione e azioni consigliate
Mancata corrispondenza MTU rete griglia	L'impostazione MTU (Maximum Transmission Unit) per l'interfaccia Grid Network (eth0) differisce significativamente tra i nodi della griglia. Le differenze nelle impostazioni MTU potrebbero indicare che alcune, ma non tutte, reti eth0 sono configurate per i frame jumbo. Una mancata corrispondenza delle dimensioni MTU superiore a 1000 potrebbe causare problemi di performance di rete. Consultare le istruzioni per l'avviso di mancata corrispondenza MTU della rete griglia in Risolvere i problemi di rete, hardware e piattaforma.
Elevato utilizzo di heap Java	Viene utilizzata una percentuale elevata di spazio heap Java. Se l'heap Java diventa pieno, i servizi di metadati potrebbero non essere disponibili e le richieste del client potrebbero non riuscire. 1. Esaminare l'attività ILM sulla dashboard. Questo avviso potrebbe essere risolto da solo quando il carico di lavoro ILM diminuisce. 2. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 3. Se l'avviso persiste, contattare il supporto tecnico.
Latenza elevata per le query sui metadati	Il tempo medio per le query dei metadati Cassandra è troppo lungo. Un aumento della latenza delle query può essere causato da una modifica dell'hardware, ad esempio la sostituzione di un disco, una modifica del carico di lavoro, ad esempio un aumento improvviso delle attività di acquisizione, o una modifica della rete, ad esempio un problema di comunicazione tra nodi e siti. 1. Determinare se sono state apportate modifiche all'hardware, al carico di lavoro o alla rete durante l'aumento della latenza della query. 2. Se non si riesce a risolvere il problema, contattare il supporto tecnico.
Errore di sincronizzazione della federazione delle identità	Impossibile sincronizzare utenti e gruppi federati dall'origine dell'identità. 1. Verificare che il server LDAP configurato sia in linea e disponibile. 2. Esaminare le impostazioni nella pagina Identity Federation (Federazione identità). Verificare che tutti i valori siano aggiornati. Vedere USA la federazione delle identità Nelle istruzioni per l'amministrazione di StorageGRID. 3. Fare clic su **Test Connection** (verifica connessione) per convalidare le impostazioni del server LDAP. 4. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Errore di sincronizzazione della federazione delle identità per un tenant	Impossibile sincronizzare utenti e gruppi federati dall'origine dell'identità configurata da un tenant. 1. Accedi al tenant manager. 2. Verificare che il server LDAP configurato dal tenant sia online e disponibile. 3. Esaminare le impostazioni nella pagina Identity Federation (Federazione identità). Verificare che tutti i valori siano aggiornati. Vedere USA la federazione delle identità nelle istruzioni per l'utilizzo di un account tenant. 4. Fare clic su **Test Connection** (verifica connessione) per convalidare le impostazioni del server LDAP. 5. Se non si riesce a risolvere il problema, contattare il supporto tecnico.
Posizionamento ILM non raggiungibile	Non è possibile ottenere un'istruzione di posizionamento in una regola ILM per determinati oggetti. Questo avviso indica che un nodo richiesto da un'istruzione di posizionamento non è disponibile o che una regola ILM non è configurata correttamente. Ad esempio, una regola potrebbe specificare un numero di copie replicate maggiore rispetto ai nodi di storage. 1. Assicurarsi che tutti i nodi siano online. 2. Se tutti i nodi sono in linea, rivedere le istruzioni di posizionamento in tutte le regole ILM che utilizzano il criterio ILM attivo. Verificare che siano presenti istruzioni valide per tutti gli oggetti. Vedere istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni. 3. Se necessario, aggiornare le impostazioni delle regole e attivare un nuovo criterio. **Nota:** l'eliminazione dell'avviso potrebbe richiedere fino a 1 giorno. 4. Se il problema persiste, contattare il supporto tecnico. **Nota:** questo avviso potrebbe essere visualizzato durante un aggiornamento e potrebbe persistere per 1 giorno dopo il completamento dell'aggiornamento. Quando questo avviso viene attivato da un aggiornamento, viene visualizzato da solo.

Nome dell'avviso	Descrizione e azioni consigliate
Periodo di scansione ILM troppo lungo	Il tempo necessario per eseguire la scansione, valutare gli oggetti e applicare ILM è troppo lungo. Se il tempo stimato per completare una scansione ILM completa di tutti gli oggetti è troppo lungo (vedere **periodo di scansione - stimato** nella dashboard), il criterio ILM attivo potrebbe non essere applicato ai nuovi oggetti acquisiti. Le modifiche al criterio ILM potrebbero non essere applicate agli oggetti esistenti. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Verificare che tutti i nodi di storage siano online. 3. Ridurre temporaneamente la quantità di traffico client. Ad esempio, in Grid Manager, selezionare **CONFIGURATION Network Traffic classification** e creare una policy che limiti la larghezza di banda o il numero di richieste. 4. Se l'i/o del disco o la CPU sono sovraccarichi, provare a ridurre il carico o aumentare la risorsa. 5. Se necessario, aggiornare le regole ILM per utilizzare il posizionamento sincrono (impostazione predefinita per le regole create dopo StorageGRID 11.3). 6. Se l'avviso persiste, contattare il supporto tecnico. Amministrare StorageGRID
Velocità di scansione ILM bassa	La velocità di scansione ILM è impostata su un valore inferiore a 100 oggetti/secondo. Questo avviso indica che la velocità di scansione ILM del sistema è stata modificata a meno di 100 oggetti/secondo (impostazione predefinita: 400 oggetti/secondo). Il criterio ILM attivo potrebbe non essere applicato ai nuovi oggetti acquisiti. Le modifiche successive al criterio ILM non verranno applicate agli oggetti esistenti. 1. Determinare se è stata apportata una modifica temporanea alla velocità di scansione ILM come parte di un'indagine di supporto in corso. 2. Contattare il supporto tecnico. Non modificare mai la velocità di scansione ILM senza contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
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. 1. Utilizzando il software KMS, aggiornare il certificato CA per il server di gestione delle chiavi. 2. Da Grid Manager, selezionare **CONFIGURATION Security Key management server**. 3. Selezionare il KMS che presenta un avviso di stato del certificato. 4. Selezionare **Modifica**. 5. Selezionare **Avanti** per passare alla fase 2 (carica certificato server). 6. Selezionare **Sfoglia** per caricare il nuovo certificato. 7. Selezionare **Salva**. Amministrare StorageGRID
Scadenza del certificato client KMS	Il certificato client per un server di gestione delle chiavi sta per scadere. 1. Da Grid Manager, selezionare **CONFIGURATION Security Key management server**. 2. Selezionare il KMS che presenta un avviso di stato del certificato. 3. Selezionare **Modifica**. 4. Selezionare **Avanti** per passare alla fase 3 (carica certificati client). 5. Selezionare **Sfoglia** per caricare il nuovo certificato. 6. Selezionare **Sfoglia** per caricare la nuova chiave privata. 7. Selezionare **Salva**. Amministrare StorageGRID
Impossibile caricare la configurazione KMS	La configurazione per il server di gestione delle chiavi esiste ma non è riuscita a caricarsi. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Se l'avviso persiste, contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Errore di connettività KMS	Un nodo appliance non è riuscito a connettersi al server di gestione delle chiavi del proprio sito. 1. Da Grid Manager, selezionare **CONFIGURATION Security Key management server**. 2. Verificare che le voci relative a porta e nome host siano corrette. 3. Verificare che il certificato del server, il certificato del client e la chiave privata del certificato del client siano corretti e non scaduti. 4. Assicurarsi che le impostazioni del firewall consentano al nodo dell'appliance di comunicare con il KMS specificato. 5. Correggere eventuali problemi di rete o DNS. 6. Se hai bisogno di assistenza o se l'avviso persiste, contatta il supporto tecnico.
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. 1. Verificare che il KMS assegnato al sito utilizzi il nome corretto per la chiave di crittografia e le versioni precedenti. 2. Se hai bisogno di assistenza o se l'avviso persiste, contatta il supporto tecnico.
Rotazione della chiave di crittografia KMS non riuscita	Tutti i volumi dell'appliance sono stati decifrati, ma uno o più volumi non sono stati ruotati sulla chiave più recente.contattare il supporto tecnico.
KMS non configurato	Non esiste alcun server di gestione delle chiavi per questo sito. 1. Da Grid Manager, selezionare **CONFIGURATION Security Key management server**. 2. Aggiungere un KMS per questo sito o un KMS predefinito. Amministrare StorageGRID
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. 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Assicurarsi che il server di gestione delle chiavi (KMS) disponga della chiave di crittografia configurata e di eventuali versioni precedenti. 3. Se hai bisogno di assistenza o se l'avviso persiste, contatta il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Scadenza del certificato del server KMS	Il certificato del server utilizzato dal server di gestione delle chiavi (KMS) sta per scadere. 1. Utilizzando il software KMS, aggiornare il certificato del server per il server di gestione delle chiavi. 2. Se hai bisogno di assistenza o se l'avviso persiste, contatta il supporto tecnico. Amministrare StorageGRID
Coda di audit di grandi dimensioni	La coda dei dischi per i messaggi di controllo è piena. 1. Controllare il carico sul sistema - se si è verificato un numero significativo di transazioni, l'avviso dovrebbe risolversi nel tempo e si può ignorare l'avviso. 2. Se l'avviso 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. 3. Ridurre il tasso di operazioni del client o diminuire il numero di messaggi di controllo registrati modificando il livello di controllo per le scritture del client e le letture del client su Error (errore) o Off (**CONFIGURATION Monitoring Audit and syslog server**). Esaminare i registri di audit
Rilevata attività di bilanciamento del carico CLB legacy	Alcuni client potrebbero connettersi al servizio di bilanciamento del carico CLB obsoleto utilizzando il certificato API S3 e Swift predefinito. 1. Per semplificare gli aggiornamenti futuri, installare un certificato S3 e Swift API personalizzato nella scheda **Global** della pagina **Certificates**. Quindi, assicurarsi che tutti i client S3 o Swift che si connettono alla CLB legacy abbiano il nuovo certificato. 2. Creare uno o più endpoint del bilanciamento del carico. Quindi, indirizzare tutti i client S3 e Swift esistenti a questi endpoint. Contattare il supporto tecnico se è necessario rimappare la porta del client. Altre attività potrebbero attivare questo avviso, incluse le scansioni delle porte. Per determinare se il servizio CLB obsoleto è attualmente in uso, consultare la `storagegrid_private_clb_http_connection_established_successful` Metrica Prometheus. Se necessario, disattivare o disattivare questa regola di avviso se il servizio CLB non è più in uso.

Nome dell'avviso	Descrizione e azioni consigliate
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. 1. Da Grid Manager, andare a **CONFIGURAZIONE monitoraggio Audit e server syslog**. 2. Selezionare **Modifica server syslog esterno**. 3. Avanzare attraverso la Configurazione guidata fino a quando non si è in grado di selezionare **Invia messaggi di prova**. 4. Selezionare **Send test messages** (Invia messaggi di test) per determinare perché i log non possono essere inoltrati al server syslog esterno. 5. Risolvere eventuali problemi segnalati.
Bassa capacità del disco di log di audit	Lo spazio disponibile per i registri di controllo è insufficiente. 1. Monitorare questo avviso per verificare se il problema si risolve da solo e se lo spazio su disco diventa nuovamente disponibile. 2. Contattare il supporto tecnico se lo spazio disponibile continua a diminuire.
Memoria del nodo a bassa disponibilità	La quantità di RAM disponibile su un nodo è bassa. Una RAM disponibile bassa potrebbe indicare un cambiamento nel carico di lavoro o una perdita di memoria con uno o più nodi. 1. Monitorare questo avviso per verificare se il problema si risolve da solo. 2. Se la memoria disponibile scende al di sotto della soglia di allarme principale, contattare il supporto tecnico.
Spazio libero ridotto per il pool di storage	La quantità di spazio disponibile per memorizzare i dati degli oggetti in un pool di storage è bassa. 1. Selezionare **ILM** > **Storage Pools**. 2. Selezionare il pool di storage elencato nell'avviso e selezionare **Visualizza dettagli**. 3. Determinare dove è richiesta ulteriore capacità di storage. È possibile aggiungere nodi di storage a ciascun sito del pool di storage o aggiungere volumi di storage (LUN) a uno o più nodi di storage esistenti. 4. Eseguire una procedura di espansione per aumentare la capacità dello storage. Espandi il tuo grid

Nome dell'avviso	Descrizione e azioni consigliate
Memoria del nodo installata insufficiente	La quantità di memoria installata su un nodo è bassa. Aumentare la quantità di RAM disponibile per la macchina virtuale o l'host Linux. Controllare il valore di soglia dell'avviso principale per determinare il requisito minimo predefinito per un nodo StorageGRID. Consultare le istruzioni per l'installazione della piattaforma: • Installare Red Hat Enterprise Linux o CentOS • Installare Ubuntu o Debian • Installare VMware
Storage dei metadati basso	Lo spazio disponibile per memorizzare i metadati degli oggetti è basso. **Allarme critico** 1. Interrompere l'acquisizione degli oggetti. 2. Aggiungere immediatamente nodi di storage in una procedura di espansione. **Allerta importante** Aggiungere immediatamente nodi di storage in una procedura di espansione. **Avviso minore** 1. Monitorare la velocità di utilizzo dello spazio di metadati dell'oggetto. Selezionare **NODES *Storage Node* Storage** e visualizzare il grafico Storage Used - Object Metadata. 2. Aggiungere nodi di storage in un procedura di espansione il più presto possibile. 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. Consultare le istruzioni per l'avviso di storage metadati in esaurimento in Risolvere i problemi relativi ai metadati.
Capacità disco di metriche ridotte	Lo spazio disponibile per il database delle metriche è basso. 1. Monitorare questo avviso per verificare se il problema si risolve da solo e se lo spazio su disco diventa nuovamente disponibile. 2. Contattare il supporto tecnico se lo spazio disponibile continua a diminuire.

Nome dell'avviso	Descrizione e azioni consigliate
Storage dei dati a oggetti basso	Lo spazio disponibile per memorizzare i dati degli oggetti è basso. Eseguire una procedura di espansione. È possibile aggiungere volumi di storage (LUN) ai nodi di storage esistenti oppure aggiungere nuovi nodi di storage. Risolvere i problemi relativi all'avviso di storage dei dati a oggetti in esaurimento Espandi il tuo grid
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. Per informazioni su come risolvere questo avviso, visitare il sito Web all'indirizzo Risolvere i problemi relativi agli avvisi di override del watermark di sola lettura bassa.
Bassa capacità del disco root	Lo spazio disponibile per il disco root è insufficiente. 1. Monitorare questo avviso per verificare se il problema si risolve da solo e se lo spazio su disco diventa nuovamente disponibile. 2. Contattare il supporto tecnico se lo spazio disponibile continua a diminuire.
Bassa capacità dei dati di sistema	Lo spazio disponibile per i dati di sistema StorageGRID su `/var/local` il file system è in esaurimento. 1. Monitorare questo avviso per verificare se il problema si risolve da solo e se lo spazio su disco diventa nuovamente disponibile. 2. Contattare il supporto tecnico se lo spazio disponibile continua a diminuire.
Spazio libero nella directory tmp basso	Lo spazio disponibile nella directory /tmp è insufficiente. 1. Monitorare questo avviso per verificare se il problema si risolve da solo e se lo spazio su disco diventa nuovamente disponibile. 2. Contattare il supporto tecnico se lo spazio disponibile continua a diminuire.
Errore di connettività di rete del nodo	Si sono verificati errori durante il trasferimento dei dati tra nodi. Gli errori di connettività di rete potrebbero essere stati corretti senza l'intervento manuale. Contattare il supporto tecnico se gli errori non sono chiari. Consultare le istruzioni relative all'allarme NRER (Network Receive Error) in Risolvere i problemi di rete, hardware e piattaforma.

Nome dell'avviso	Descrizione e azioni consigliate
Errore frame ricezione rete nodo	Un'elevata percentuale di frame di rete ricevuti da un nodo presenta errori. Questo avviso potrebbe indicare un problema hardware, ad esempio un cavo difettoso o un ricetrasmettitore guasto su entrambe le estremità della connessione Ethernet. 1. Se si utilizza un'appliance, provare a sostituire ogni ricetrasmettitore e cavo SFP+ o SFP28, uno alla volta, per verificare se l'avviso scompare. 2. Se l'avviso persiste, contattare il supporto tecnico.
Nodo non sincronizzato con il server NTP	L'ora del nodo non è sincronizzata con il server NTP (Network Time Protocol). 1. Verificare di aver specificato almeno quattro server NTP esterni, ciascuno dei quali fornisce un riferimento di livello 3 o superiore. 2. Verificare che tutti i server NTP funzionino correttamente. 3. Verificare le connessioni ai server NTP. Assicurarsi che non siano bloccati da un firewall.
Nodo non bloccato con server NTP	Il nodo non è bloccato su un server NTP (Network Time Protocol). 1. Verificare di aver specificato almeno quattro server NTP esterni, ciascuno dei quali fornisce un riferimento di livello 3 o superiore. 2. Verificare che tutti i server NTP funzionino correttamente. 3. Verificare le connessioni ai server NTP. Assicurarsi che non siano bloccati da un firewall.
Rete nodo non appliance non in funzione	Uno o più dispositivi di rete sono disconnessi o non attivi. Questo avviso indica che un'interfaccia di rete (eth) per un nodo installato su una macchina virtuale o su un host Linux non è accessibile. Contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Controllo dell'esistenza dell'oggetto non riuscito	Il processo di controllo dell'esistenza dell'oggetto non è riuscito. 1. Selezionare **MAINTENANCE object existence check**. 2. Annotare il messaggio di errore. Eseguire le azioni correttive appropriate: **Impossibile avviare**, **connessione persa**, **errore sconosciuto** a. Assicurarsi che i nodi di storage e i volumi inclusi nel processo siano online e disponibili. b. Assicurarsi che non vi siano errori di servizio o di volume sui nodi di storage. Se un servizio non è in esecuzione, avviare o riavviare il servizio. Vedere istruzioni per il ripristino e la manutenzione. c. Assicurarsi che il controllo di coerenza selezionato possa essere soddisfatto. d. Dopo aver risolto eventuali problemi, selezionare **Riprova**. Il lavoro riprenderà dall'ultimo stato valido. **Errore critico dello storage nel volume** e. Ripristinare il volume guasto. Vedere istruzioni per il ripristino e la manutenzione. f. Selezionare **Riprova**. g. Al termine del lavoro, creare un altro lavoro per i volumi rimanenti sul nodo per verificare la presenza di errori aggiuntivi. 3. Se non riesci a risolvere i problemi, contatta il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Controllo dell'esistenza dell'oggetto bloccato	Il lavoro di verifica dell'esistenza dell'oggetto si è bloccato. Impossibile continuare il lavoro di verifica dell'esistenza dell'oggetto. Uno o più nodi di storage o volumi inclusi nel processo non sono in linea o non rispondono, oppure il controllo di coerenza selezionato non può più essere soddisfatto perché troppi nodi sono inattivi o non disponibili. 1. Assicurarsi che tutti i nodi e i volumi di storage controllati siano online e disponibili (selezionare **NODI**). 2. Assicurarsi che siano disponibili e in linea un numero sufficiente di nodi di storage per consentire al nodo coordinatore corrente di leggere i metadati degli oggetti utilizzando il controllo di coerenza selezionato. Se necessario, avviare o riavviare un servizio. Vedere istruzioni per il ripristino e la manutenzione. Quando si risolvono i passi 1 e 2, il lavoro viene avviato automaticamente da dove è stato interrotto. 3. Se il controllo di coerenza selezionato non può essere soddisfatto, annullare il lavoro e avviare un altro lavoro utilizzando un controllo di coerenza inferiore. 4. Se non riesci a risolvere i problemi, contatta il supporto tecnico.
Oggetti persi	Uno o più oggetti sono stati persi dalla griglia. Questo avviso potrebbe indicare che i dati sono stati persi in modo permanente e non sono recuperabili. 1. Esaminare immediatamente questo avviso. Potrebbe essere necessario intervenire per evitare ulteriori perdite di dati. Inoltre, se si esegue un'azione rapida, potrebbe essere possibile ripristinare un oggetto perso. Risolvere i problemi relativi ai dati degli oggetti persi e mancanti 2. Una volta risolto il problema sottostante, azzerare il contatore: a. Selezionare **SUPPORT** > **Tools** > **Grid topology**. b. Per il nodo di storage che ha generato l'avviso, selezionare ***Site Grid Node*** **LDR Data Store Configuration Main**. c. Selezionare **Reset Lost Objects Count** e fare clic su **Apply Changes** (Applica modifiche).

Nome dell'avviso	Descrizione e azioni consigliate
Servizi della piattaforma non disponibili	In un sito sono in esecuzione o disponibili troppi nodi di storage con il servizio RSM. Assicurarsi che la maggior parte dei nodi di storage che dispongono del servizio RSM nel sito interessato sia in esecuzione e in stato non di errore. Consultare "Troubleshooting platform Services" in Istruzioni per l'amministrazione di StorageGRID.
S3 HA POSTO la dimensione dell'oggetto troppo grande	Un client S3 sta tentando di eseguire un'operazione PUT Object che supera i limiti di dimensione S3. 1. Utilizzare l'ID tenant mostrato nei dettagli dell'avviso per identificare l'account tenant. 2. Accedere a **Support Tools Logs** e raccogliere i registri delle applicazioni per il nodo di storage mostrato nei dettagli dell'avviso. Specificare un periodo di tempo di 15 minuti prima e dopo l'ora dell'avviso. 3. Estrarre l'archivio scaricato e accedere alla posizione di `bycast.log` (`/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log`). 4. Cercare il contenuto di `bycast.log` per `"method=PUT"` E identificare l'indirizzo IP del client S3 osservando il `clientIP` campo. 5. Informare tutti gli utenti client che la dimensione massima DELL'oggetto PUT è 5 GiB. 6. USA caricamenti multiparte per oggetti di dimensioni superiori a 5 GiB.

Collegamento dell'appliance di servizi alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa.
	
	1. Controllare il cavo e la connessione fisica alla porta di rete amministrativa 1.
	2. Risolvere eventuali problemi di connessione. Consultare le istruzioni di installazione e manutenzione dell'hardware dell'appliance.
	3. Se questa porta viene disconnessa in base allo scopo, disattivare questa regola. In Grid Manager, selezionare **ALERTS Rules**, selezionare la regola e fare clic su **Edit rule** (Modifica regola). Quindi, deselezionare la casella di controllo **Enabled**.
	  ◦ Appliance di servizi SG100 e SG1000
	  ◦ Disattiva le regole di avviso

Nome dell'avviso	Descrizione e azioni consigliate
Collegamento dell'appliance di servizi su Admin Network (o Client Network)	L'interfaccia dell'appliance alla rete di amministrazione (eth1) o alla rete client (eth2) è inattiva o disconnessa. 1. Controllare i cavi, gli SFP e le connessioni fisiche alla rete StorageGRID. 2. Risolvere eventuali problemi di connessione. Consultare le istruzioni di installazione e manutenzione dell'hardware dell'appliance. 3. Se questa porta viene disconnessa in base allo scopo, disattivare questa regola. In Grid Manager, selezionare **ALERTS Rules**, selezionare la regola e fare clic su **Edit rule** (Modifica regola). Quindi, deselezionare la casella di controllo **Enabled**. ◦ Appliance di servizi SG100 e SG1000 ◦ Disattiva le regole di avviso
Collegamento dell'appliance di servizi alla porta di rete 1, 2, 3 o 4	La porta di rete 1, 2, 3 o 4 dell'appliance è inattiva o scollegata. 1. Controllare i cavi, gli SFP e le connessioni fisiche alla rete StorageGRID. 2. Risolvere eventuali problemi di connessione. Consultare le istruzioni di installazione e manutenzione dell'hardware dell'appliance. 3. Se questa porta viene disconnessa in base allo scopo, disattivare questa regola. In Grid Manager, selezionare **ALERTS Rules**, selezionare la regola e fare clic su **Edit rule** (Modifica regola). Quindi, deselezionare la casella di controllo **Enabled**. ◦ Appliance di servizi SG100 e SG1000 ◦ Disattiva le regole di avviso

Nome dell'avviso	Descrizione e azioni consigliate
Connettività dello storage dell'appliance di servizi degradata	Uno dei due SSD di un'appliance di servizi si è guastato o non è sincronizzato con l'altro. La funzionalità dell'appliance non viene influenzata, ma il problema deve essere risolto immediatamente. Se entrambi i dischi si guastano, l'apparecchio non funzionerà più. 1. Da Grid Manager, selezionare **NODES** ***Services appliance*****, quindi selezionare la scheda hardware**. 2. Esaminare il messaggio nel campo **Storage RAID Mode** (modalità RAID storage). 3. Se il messaggio indica lo stato di avanzamento di un'operazione di risincronizzazione, attendere il completamento dell'operazione, quindi confermare che l'avviso è stato risolto. Un messaggio di risincronizzazione indica che l'unità SSD è stata sostituita di recente o che viene risincronizzata per un altro motivo. 4. Se il messaggio indica che uno degli SSD è guasto, sostituire il disco guasto non appena possibile. Per istruzioni su come sostituire un disco in un'appliance di servizi, consultare la guida all'installazione e alla manutenzione delle appliance SG100 e SG1000. Appliance di servizi SG100 e SG1000
Collegamento dell'appliance di storage alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa. 1. Controllare il cavo e la connessione fisica alla porta di rete amministrativa 1. 2. Risolvere eventuali problemi di connessione. Consultare le istruzioni di installazione e manutenzione dell'hardware dell'appliance. 3. Se questa porta viene disconnessa in base allo scopo, disattivare questa regola. In Grid Manager, selezionare **ALERTS Rules**, selezionare la regola e fare clic su **Edit rule** (Modifica regola). Quindi, deselezionare la casella di controllo **Enabled**. ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600 ◦ Disattiva le regole di avviso

Nome dell'avviso	Descrizione e azioni consigliate
Collegamento dell'appliance di storage su Admin Network (o Client Network)	L'interfaccia dell'appliance alla rete di amministrazione (eth1) o alla rete client (eth2) è inattiva o disconnessa. 1. Controllare i cavi, gli SFP e le connessioni fisiche alla rete StorageGRID. 2. Risolvere eventuali problemi di connessione. Consultare le istruzioni di installazione e manutenzione dell'hardware dell'appliance. 3. Se questa porta viene disconnessa in base allo scopo, disattivare questa regola. In Grid Manager, selezionare **ALERTS Rules**, selezionare la regola e fare clic su **Edit rule** (Modifica regola). Quindi, deselezionare la casella di controllo **Enabled**. ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600 ◦ Disattiva le regole di avviso
Collegamento dell'appliance di storage alla porta di rete 1, 2, 3 o 4	La porta di rete 1, 2, 3 o 4 dell'appliance è inattiva o scollegata. 1. Controllare i cavi, gli SFP e le connessioni fisiche alla rete StorageGRID. 2. Risolvere eventuali problemi di connessione. Consultare le istruzioni di installazione e manutenzione dell'hardware dell'appliance. 3. Se questa porta viene disconnessa in base allo scopo, disattivare questa regola. In Grid Manager, selezionare **ALERTS Rules**, selezionare la regola e fare clic su **Edit rule** (Modifica regola). Quindi, deselezionare la casella di controllo **Enabled**. ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600 ◦ Disattiva le regole di avviso

Nome dell'avviso	Descrizione e azioni consigliate
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. 1. Controllare le spie degli indicatori di porta dall'apparecchio. 2. Se le spie di una porta sono spente, verificare che il cavo sia collegato correttamente. Se necessario, sostituire il cavo. 3. Attendere fino a cinque minuti. **Nota:** se è necessario sostituire un secondo cavo, non scollegarlo per almeno 5 minuti. In caso contrario, il volume root potrebbe diventare di sola lettura, il che richiede un riavvio hardware. 4. Da Grid Manager, selezionare **NODES**. Quindi, selezionare la scheda hardware del nodo che ha riscontrato il problema. Verificare che la condizione di avviso sia stata risolta.
Dispositivo di storage inaccessibile	Impossibile accedere a un dispositivo di storage. Questo avviso indica che non è possibile montare o accedere a un volume a causa di un problema con un dispositivo di storage sottostante. 1. Controllare lo stato di tutti i dispositivi di storage utilizzati per il nodo: ◦ Se il nodo è installato su una macchina virtuale o su un host Linux, seguire le istruzioni del sistema operativo per eseguire la diagnostica hardware o eseguire un controllo del file system. ▪ Installare Red Hat Enterprise Linux o CentOS ▪ Installare Ubuntu o Debian ▪ Installare VMware ◦ Se il nodo è installato su un'appliance SG100, SG1000 o SG6000, utilizzare BMC. ◦ Se il nodo è installato su un'appliance SG5600 o SG5700, utilizzare Gestione di sistema di SANtricity. 2. Se necessario, sostituire il componente. Consultare le istruzioni per l'apparecchio: ◦ Appliance di storage SG6000 ◦ Appliance di storage SG5700 ◦ Appliance di storage SG5600

Nome dell'avviso	Descrizione e azioni consigliate
Utilizzo elevato della quota del tenant	Viene utilizzata una percentuale elevata di spazio di quota tenant. Se un tenant supera la quota, i nuovi ingest vengono rifiutati. **Nota:** questa regola di avviso è disattivata per impostazione predefinita perché potrebbe generare numerose notifiche. 1. In Grid Manager, selezionare **TENANT**. 2. Ordinare la tabella in base a **quota Utilization**. 3. Selezionare un tenant il cui utilizzo della quota è prossimo al 100%. 4. Eseguire una o entrambe le operazioni seguenti: ◦ Selezionare **Edit** (Modifica) per aumentare la quota di storage per il tenant. ◦ Avvisare il tenant che l'utilizzo delle quote è elevato.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono o non è possibile raggiungere il nodo. Questo avviso indica che un nodo è disconnesso per un motivo sconosciuto. 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. Monitorare questo avviso per verificare se il problema si risolve da solo. Se il problema persiste: 1. Determinare se è presente un altro avviso che interessa questo nodo. Questo avviso potrebbe essere risolto quando si risolve l'altro avviso. 2. Verificare che tutti i servizi su questo nodo siano in esecuzione. Se un servizio viene arrestato, provare ad avviarlo. Vedere istruzioni per il ripristino e la manutenzione. 3. Assicurarsi che l'host del nodo sia acceso. In caso contrario, avviare l'host. **Nota:** se più host sono spenti, consultare la istruzioni per il ripristino e la manutenzione. 4. Determinare se si è verificato un problema di connettività di rete tra questo nodo e il nodo di amministrazione. 5. Se non si riesce a risolvere l'avviso, contattare il supporto tecnico.
Riavvio del nodo imprevisto	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore. 1. Monitorare questo avviso. L'avviso viene cancellato dopo 24 ore. Tuttavia, se il nodo si riavvia di nuovo inaspettatamente, questo avviso viene attivato di nuovo. 2. Se non si riesce a risolvere l'avviso, potrebbe esserci un guasto hardware. Contattare il supporto tecnico.

Nome dell'avviso	Descrizione e azioni consigliate
Rilevato oggetto corrotto non identificato	È stato trovato un file nello storage a oggetti replicato che non è stato possibile identificare come oggetto replicato. 1. Determinare se vi sono problemi con lo storage sottostante su un nodo di storage. Ad esempio, eseguire la diagnostica hardware o eseguire un controllo del file system. 2. Dopo aver risolto eventuali problemi di storage, eseguire il controllo dell'esistenza dell'oggetto Per determinare se le copie replicate, come definito dalla policy ILM, sono mancanti. 3. Monitorare questo avviso. L'avviso verrà visualizzato dopo 24 ore, ma verrà nuovamente attivato se il problema non è stato risolto. 4. Se non si riesce a risolvere l'avviso, contattare il supporto tecnico.

Metriche Prometheus comunemente utilizzate

Il servizio Prometheus sui nodi di amministrazione raccoglie le metriche delle serie temporali dai servizi su tutti i nodi. Mentre Prometheus raccoglie più di mille metriche, un numero relativamente piccolo è necessario per monitorare le operazioni StorageGRID più critiche.

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.

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.

La seguente tabella elenca le metriche Prometheus più comunemente utilizzate. È possibile fare riferimento a questo elenco per comprendere meglio le condizioni nelle regole di avviso predefinite o per creare le condizioni per le regole di avviso personalizzate.

> 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.

Metrica Prometheus	Descrizione
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.

Metrica Prometheus	Descrizione
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	Network Device statytics receive_errs.
node_network_transmit_errs_total	Network Device statytics 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.

Metrica Prometheus	Descrizione
storagegrid_http_sessions_incoming_failed	Il numero totale di sessioni HTTP che non sono riuscite a completare correttamente, a causa di una richiesta HTTP non valida o di un errore durante l'elaborazione di un'operazione.
storagegrid_http_sessions_incoming_successful	Il numero totale di sessioni HTTP completate correttamente.
storagegrid_ilm_waiting_background_objects	Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalla scansione.
storagegrid_ilm_waiting_client_evaluation_objects_per_second	La velocità corrente alla quale gli oggetti vengono valutati in base al criterio ILM su questo nodo.
storagegrid_ilm_waiting_client_objects	Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalle operazioni del client (ad esempio, acquisizione).
storagegrid_ilm_waiting_total_objects	Il numero totale di oggetti in attesa di valutazione ILM.
storagegrid_ilm_scan_objects_per_second	La velocità con cui gli oggetti di proprietà di questo nodo vengono sottoposti a scansione e messi in coda per ILM.
storagegrid_ilm_scan_period_estimated_minutes	Il tempo stimato per completare una scansione ILM completa su questo nodo. **Nota:** Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti di proprietà di questo nodo.
storagegrid_load_balancer_endpoint_cert_expiry_time	Il tempo di scadenza del certificato endpoint del bilanciamento del carico in secondi dall'epoca.
storagegrid_metadata_queries_average_latency_milliseconds	Il tempo medio richiesto per eseguire una query sull'archivio di metadati tramite questo servizio.
storagegrid_network_received_bytes	La quantità totale di dati ricevuti dall'installazione.
storagegrid_network_transmitted_bytes	La quantità totale di dati inviati dall'installazione.
storagegrid_node_cpu_utilization_percent	La percentuale di tempo CPU disponibile attualmente utilizzata da questo servizio. Indica la disponibilità del servizio. La quantità di tempo CPU disponibile dipende dal numero di CPU del server.

Metrica Prometheus	Descrizione
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.

Metrica Prometheus	Descrizione
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_bytes	Una stima della dimensione totale dei dati degli oggetti replicati ed erasure coded sul nodo di 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.

Metrica Prometheus	Descrizione
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.

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, non è possibile elaborare le transazioni di acquisizione o recupero. 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.
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.

Codice	Nome	Servizio	Azione consigliata
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 multipath viene visualizzato come "Dvoto" (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 percorso multiplo "Ddegradato" sia stato modificato in "nominale" nella sezione relativa all'hardware di storage.
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. 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 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 ristabilito 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.
CAIH	Numero di destinazioni Ingest disponibili	CLB	Questo allarme è obsoleto.
CAQH	Numero di destinazioni disponibili	CLB	Questo allarme viene cancellato quando vengono corretti i problemi sottostanti dei servizi LDR disponibili. Assicurarsi che il componente HTTP dei servizi LDR sia in linea e in esecuzione normalmente. 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.
CCES	Sessioni in entrata - stabilite	CLB	Questo allarme viene attivato se sono attive (aperte) 20,000 o più sessioni HTTP sul nodo gateway. Se un client dispone di troppe connessioni, potrebbero verificarsi errori di connessione. È necessario ridurre il carico di lavoro.
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 pannello di controllo in Grid Manager. È necessario eseguire una procedura di espansione per aggiungere nuovi nodi di storage il prima possibile. Vedere Espandi il tuo grid. 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.
CLBA	Stato CLB	CLB	Se viene attivato un allarme, selezionare **SUPPORTO Strumenti topologia griglia**, quindi selezionare ***sito nodo griglia*** **CLB Panoramica principale** e **CLB Allarmi principale** per determinare la causa dell'allarme e risolvere il problema. Se il problema persiste, contattare il supporto tecnico.
CLBE	Stato CLB	CLB	Se il valore di CLB state (Stato CLB) è Standby, continuare a monitorare la situazione e, se il problema persiste, contattare il supporto tecnico. Se lo stato è Offline e non sono noti problemi hardware del server (ad esempio, il server è scollegato) o un downtime pianificato, riavviare il servizio. Se il problema persiste, contattare il supporto tecnico.

Codice	Nome	Servizio	Azione consigliata
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.
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.

Codice	Nome	Servizio	Azione consigliata
DNST	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.
ECCD	Rilevati frammenti corrotti	LDR	Viene attivato un allarme quando il processo di verifica in background rileva un frammento corrotto con codifica di cancellazione. 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 dell'oggetto con codifica di cancellazione 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 frammenti corrotti e continuare a 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 l'eliminazione dei dati dell'oggetto codificato 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	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 al protocollo 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: • Il protocollo 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 il protocollo HTTP non è in linea, metterlo in linea. Verificare che l'attributo Avvio automatico HTTP sia attivato. Se il protocollo 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**.

Codice	Nome	Servizio	Azione consigliata
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.
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

Codice	Nome	Servizio	Azione consigliata
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. In Grid Manager, selezionare **CONFIGURAZIONE sicurezza certificati**. 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)
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.

Codice	Nome	Servizio	Azione consigliata
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.
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.

Codice	Nome	Servizio	Azione consigliata
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.
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 risorse Configurazione principale**, 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	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 non è possibile recuperare gli oggetti. 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 Grid task visualizza informazioni sull'errore (ad esempio, "check failed on node 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 ad interrompere 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 risorse Report grafici**. 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 Grid Topology Page Configuration (Configurazione 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	Viene attivato un allarme se il software SANtricity indica la presenza di un problema di "intervento richiesto" in un componente di un'appliance StorageGRID. Selezionare **NODI**. Quindi selezionare **Appliance Storage Node hardware**. Scorrere verso il basso per visualizzare lo stato di ciascun componente. Nel software SANtricity, 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.

Allarmi che generano notifiche SNMP (sistema legacy)

La tabella seguente elenca gli allarmi legacy che generano notifiche SNMP. A differenza degli avvisi, non tutti gli allarmi generano notifiche SNMP. Solo gli allarmi elencati generano notifiche SNMP e solo con la severità indicata o superiore.

> 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	Severità
ACMS	Servizi metadati disponibili	Critico
AITE	Recupera stato	Minore
AITU	Recupera stato	Maggiore
AMQS	Messaggi di controllo in coda	Avviso
AOTE	Store state (Stato archiviazione)	Minore
AOTU	Stato del negozio	Maggiore
AROQ	Oggetti in coda	Minore
ARRF	Errori della richiesta	Maggiore
ARRV	Errori di verifica	Maggiore
ARVF	Guasti del negozio	Maggiore
ASXP	Controlla le condivisioni	Minore
AUMA	Stato AMS	Minore
AUXS	Audit Export Status (Stato esportazione audit)	Minore
BTOF	Offset	Avviso
CAHP	Percentuale di utilizzo di Java Heap	Maggiore
CAQH	Numero di destinazioni disponibili	Avviso
CASA	Data Store Status (Stato archivio dati)	Maggiore
CDLP	Spazio utilizzato metadati (percentuale)	Maggiore

Codice	Nome	Severità
CLBE	Stato CLB	Critico
DNST	Stato DNS	Critico
ECST	Stato di verifica	Maggiore
HSTE	Stato HTTP	Maggiore
HTA	Avvio automatico HTTP	Avviso
PERSO	Oggetti persi	Maggiore
MINQ	Notifiche e-mail in coda	Avviso
MIN	Email Notifications Status (Stato notifiche e-mail)	Minore
NANG	Network Auto Negotiate (negoziazione automatica di rete	Avviso
NUP	Impostazione fronte/retro di rete	Minore
NLNK	Network link Detect (rilevamento collegamento di rete	Minore
NRER	Errori di ricezione	Avviso
NSPD	Velocità	Avviso
NTER.A.	Errori di trasmissione	Avviso
NTFQ	Offset frequenza NTP	Minore
NTLK	Blocco NTP	Minore
NTOF	Offset ora NTP	Minore
NTSJ	Jitter di origine temporale selezionato	Minore
NTSU	Stato NTP	Maggiore
OPST	Stato generale dell’alimentazione	Maggiore
ORSU	Stato della replica in uscita	Avviso

Codice	Nome	Severità
PSA	Power Supply A Status (Stato alimentatore A)	Maggiore
PSB	Stato dell'alimentatore B.	Maggiore
RDTE	Stato di Tivoli Storage Manager	Avviso
RDTU	Stato di Tivoli Storage Manager	Maggiore
SAVP	Spazio totale utilizzabile (percentuale)	Avviso
SHLH	Salute	Avviso
SLSA	Media carico CPU	Avviso
SMTT	Eventi totali	Avviso
SNST	Stato	
SOSS	Stato del sistema operativo per lo storage	Avviso
SST	Stato dello storage	Avviso
SVST	Stato	Avviso
TMEM	Memoria installata	Minore
UMEM	Memoria disponibile	Minore
VMST	Stato	Minore
VPRI	Priorità di verifica	Avviso
VSTU	Stato di verifica dell'oggetto	Avviso

Riferimenti ai file di log

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

I log sono classificati come segue:

- Log del software StorageGRID

- Log di implementazione e manutenzione
- 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.

Per accedere ai registri, è possibile raccogliere i file di log e i dati di sistema da uno o più nodi come un singolo archivio di file di log (**SUPPORT Tools Logs**). 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.

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).
cassandra	Informazioni sul database Cassandra e registri di riparazione Reaper.
ce	Informazioni sui VCSs sul 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.

Percorso di archiviazione	Descrizione
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. Include anche i log di traffico di Grid Manager e Tenant Manager.
nginx-gw	File e log di configurazione del bilanciamento del carico.
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` non 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.
provisioning	Log relativi al processo di provisioning della griglia.
zattera	Log dal cluster Raft utilizzato nei servizi della piattaforma.
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.

Informazioni correlate

Raccogliere i file di log e i dati di sistema

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 Eventi**.	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 Eventi**.	Tutti i nodi
`/var/local/core/`	Contiene tutti i file core dump creati se il programma termina in modo anomalo. Le possibili cause includono errori di asserzione, violazioni o timeout di thread. Il file `` `/var/local/core/kexec_cmd `` di solito esiste sui nodi appliance e non indica un errore.	Tutti i nodi

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

Registri per i 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/clb.errlog`	Informazioni sugli errori per il servizio CLB. **Nota:** il servizio CLB è obsoleto.	Nodi gateway
`/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

Nome del file	Note	Trovato in
`/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
`/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

Nome del file	Note	Trovato in
`/var/local/log/miscd/*.log`	Contiene i log per il servizio MISCd (Information Service Control Daemon), che fornisce un'interfaccia per eseguire query e gestire servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio per eseguire query sullo stato dei servizi in esecuzione su altri nodi.	Tutti i nodi
`/var/local/log/nginx/*.log`	Contiene i log per il servizio nginx, che funge da meccanismo di autenticazione e comunicazione sicura per diversi servizi grid (come Prometheus e Dynip) per poter comunicare con servizi su altri nodi tramite API HTTPS.	Tutti i nodi
`/var/local/log/nginx-gw/*.log`	Contiene i log per le porte amministrative limitate sui nodi di amministrazione e 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

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

Nome del file	Note	Trovato in
`/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

Informazioni correlate

A proposito di bycast.log

Utilizzare 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/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. Il file `mysql.err` acquisisce errori e eventi del database, come avvii e arresti. Il file `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
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. Il `/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
Samba	/var/local/log/samba/	La directory di log di Samba include un file di log per ogni processo Samba (smb, nmb e winbind) e per ogni nome host/IP del client.	Nodo di amministrazione configurato per esportare la condivisione di controllo su CIFS

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

Codice di errore	Significato
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
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

Numero di errore	Codice di errore	Significato
010	ECHILD	Nessun processo figlio
011	EAGAIN	Riprovare
012	ENOMEM	Memoria esaurita
013	EACCES	Permesso negato
014	EFAULT	Indirizzo non valido
015	ENOTBLK	Dispositivo a blocchi richiesto
016	EBUSY	Periferica o risorsa occupata
017	EEXIST	Il file esiste
018	ESCLUDI	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo di questo tipo
020	ENOTDIR	Non una directory
021	EISDIR	È una directory
022	EINVAL	Argomento non valido
023	ENFILE	Overflow della tabella dei file
024	EMFILE	Troppi file aperti
025	ENOTTY	Non è una macchina da scrivere
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

Numero di errore	Codice di errore	Significato
031	EMSINK	Troppi collegamenti
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dominio della funzione
034	ERANGE	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un deadlock delle risorse
036	ENAMETOLONG	Nome file troppo lungo
037	ENOLCK	Nessun blocco di record disponibile
038	ENOSYS	Funzione non implementata
039	ENOTEMPTY	Directory non vuota
040	ELOOP	Sono stati rilevati troppi collegamenti simbolici
041		
042	ENOMSG	Nessun messaggio del tipo desiderato
043	EIDRM	Identificatore rimosso
044	ECHRNG	Numero di canale fuori intervallo
045	EL2NSYNC	Livello 2 non sincronizzato
046	EL3HLT	Livello 3 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 interrotto

Numero di errore	Codice di errore	Significato
052	EBADE	Scambio non valido
053	EBADR	Descrittore della richiesta non valido
054	ESCLUDI	Exchange pieno
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato del file di font non valido
060	ENOSTR	Il dispositivo non è un flusso
061	ENODATA	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse out of Streams
064	ENONET	La macchina non è in rete
065	ENOPKG	Pacchetto non installato
066	EREMOTE	L'oggetto è remoto
067	ENOLINK	Il collegamento è stato separato
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

Numero di errore	Codice di errore	Significato
073	EDOTDOT	Errore specifico RFS
074	EBADMSG	Non è un messaggio dati
075	EOVERFLOW	Valore troppo grande per il tipo di dati definito
076	ENOTUNIQ	Nome non univoco sulla rete
077	EBADFD	Descrittore del file in stato non valido
078	EREMCHG	Indirizzo remoto modificato
079	ELIBACC	Impossibile accedere a una libreria condivisa necessaria
080	ELIBBAD	Accesso a una libreria condivisa danneggiata
081	ELIBSCN	
082	ELIBMAX	Tentativo di collegamento in troppe librerie condivise
083	ELIBEXEC	Impossibile eseguire direttamente una libreria condivisa
084	EILSEQ	Sequenza di byte non valida
085	ERESTART	La chiamata di sistema interrotta deve essere riavviata
086	ESTRPIPE	Errore pipe flussi
087	EUSERS	Troppi utenti
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

Numero di errore	Codice di errore	Significato
093	EPROTONOSUPPORT	Protocollo non supportato
094	SESOCKTNOSUPPORT	Tipo di socket non supportato
095	EOPNOTSUPP	Operazione non supportata sull'endpoint di trasporto
096	EPFNOSUPPORT	Famiglia di protocolli non supportata
097	EAFNOSUPPORT	Famiglia di indirizzi non supportata dal protocollo
098	EADDRINUSE	Indirizzo già in uso
099	EADDRNOTAVAIL	Impossibile assegnare l'indirizzo richiesto
100	ENETDOWN	La rete non è disponibile
101	ENETUNREACH	La rete non è raggiungibile
102	ENETRESET	Connessione di rete interrotta a causa del ripristino
103	PRONTO	Il software ha causato l'interruzione della connessione
104	ECONNRESET	Connessione ripristinata da peer
105	ENOBUFS	Spazio buffer non disponibile
106	EISCONN	Endpoint di trasporto già connesso
107	ENOTCONN	Endpoint di trasporto non connesso
108	ESHUTDOWN	Impossibile inviare dopo l'arresto dell'endpoint di trasporto
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

Numero di errore	Codice di errore	Significato
114	EALREADY	Operazione già in corso
115	EINPROGRESS	Operazione in corso
116		
117	EUCLEAN	La struttura deve essere pulita
118	ENOTNAM	Non è un file XENIX denominato
119	ENAVAIL	Nessun semaphore XENIX disponibile
120	EISNAM	È un file di tipo denominato
121	EREMOTEIO	Errore i/o remoto
122	EDQUOT	Quota superata
123	ENOMEDIUM	Nessun supporto trovato
124	EMPDIUMTYPE	Tipo di supporto errato
125	LED ECANCELED	Operazione annullata
126	ENOKEY	Chiave richiesta non disponibile
127	EKEYEXPIRED	Chiave scaduta
128	EKEYREVOKED	Chiave revocata
129	EKEYREJECTED	Chiave rifiutata dal servizio
130	EOWNERDEAD	Per i mutex più forti: Il proprietario è morto
131	ENOTRECOVERABILE	Per mutex affidabili: Stato non ripristinabile

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI 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.