Monitorare e gestire StorageGRID

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-116/monitor/index.html on April 10, 2024. Always check docs.netapp.com for the latest.

Sommario

Monitorare e gestire StorageGRID . . . 1
Monitorare e risolvere i problemi . . . 1
Espandi il tuo grid . . . 350
Ripristino e manutenzione . . . 406
Esaminare i registri di audit . . . 657

Monitorare e gestire StorageGRID

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

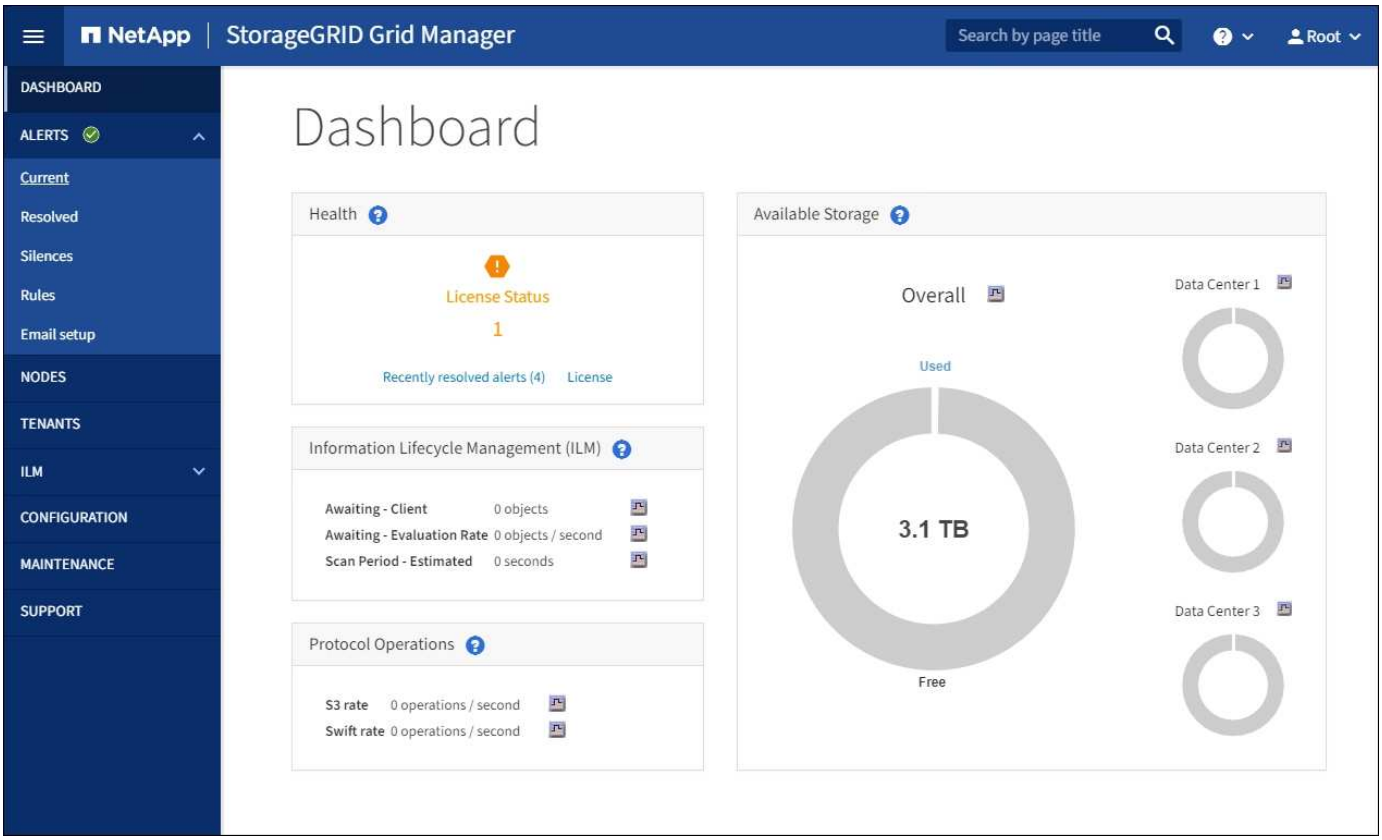
Queste istruzioni descrivono come utilizzare Grid Manager per monitorare un sistema StorageGRID. Verranno fornite informazioni su quali informazioni monitorare regolarmente, su come gestire gli avvisi e gli allarmi legacy, su come utilizzare SNMP per il monitoraggio e su come ottenere dati StorageGRID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

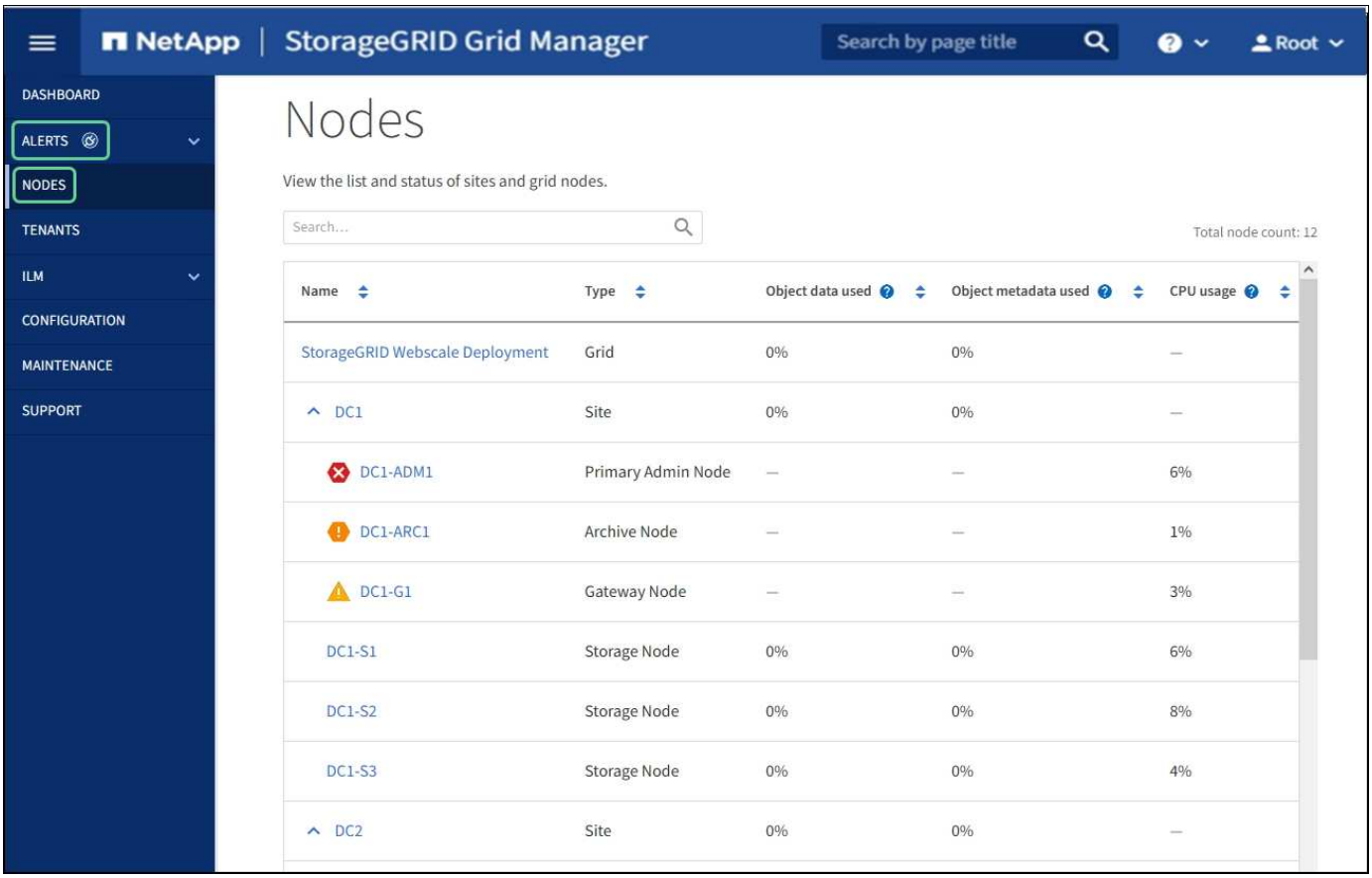
Descrizione	Visualizza ulteriori dettagli	Scopri di più
Visualizza le operazioni ILM correnti e le code ILM per il sistema. È possibile utilizzare queste informazioni per monitorare il carico di lavoro del sistema. • **In attesa - Client**: Il numero totale di oggetti in attesa di valutazione ILM dalle 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

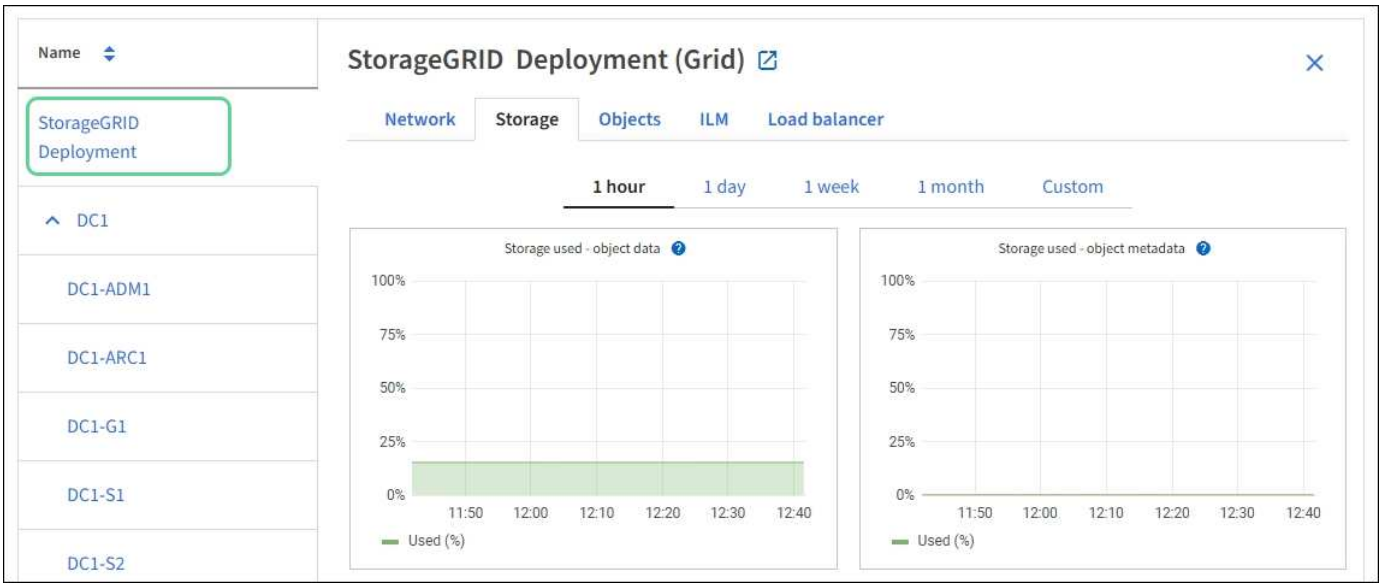
Se è presente un avviso attivo per un nodo, accanto al nome del nodo viene visualizzata una delle seguenti icone:

- **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.



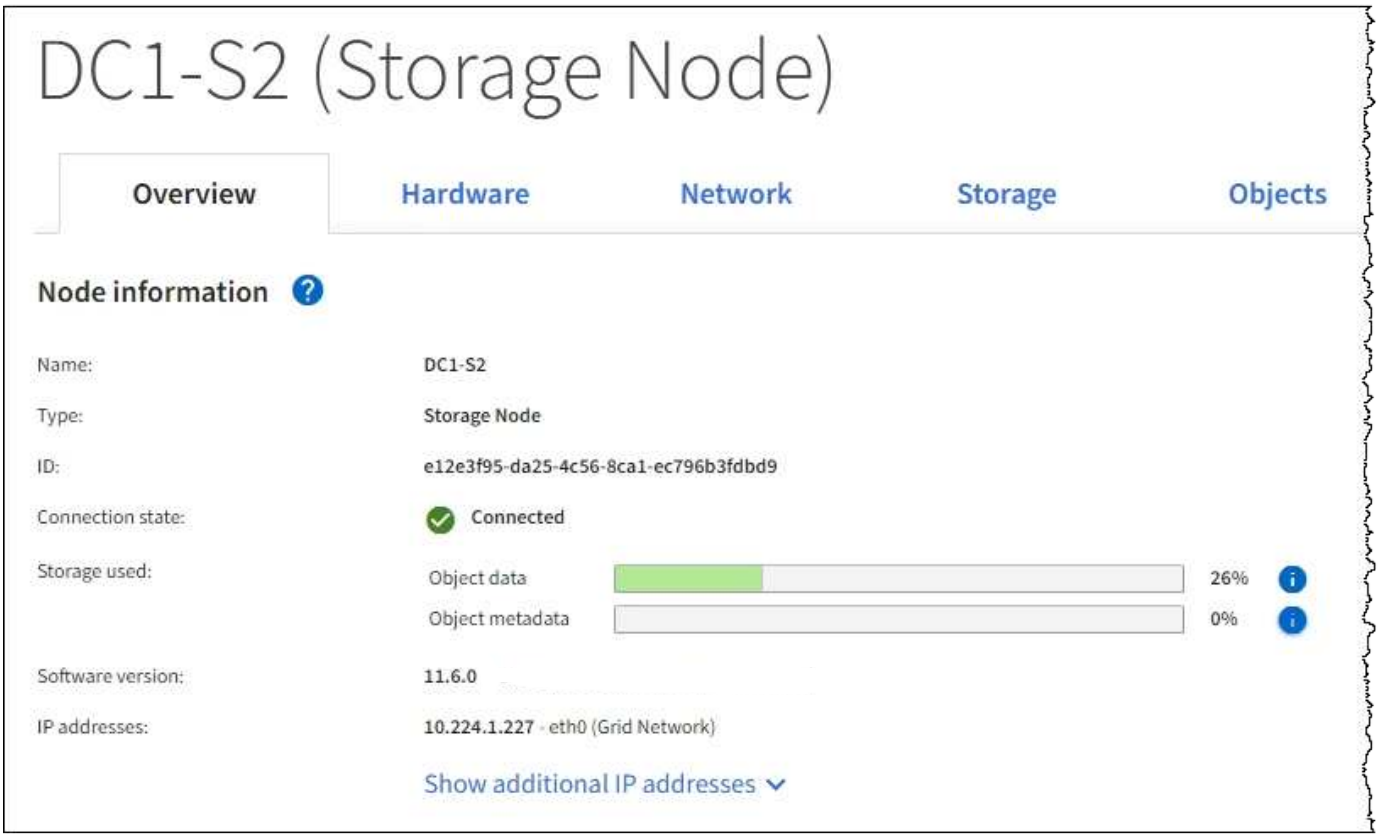
Visualizzare la scheda Panoramica

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

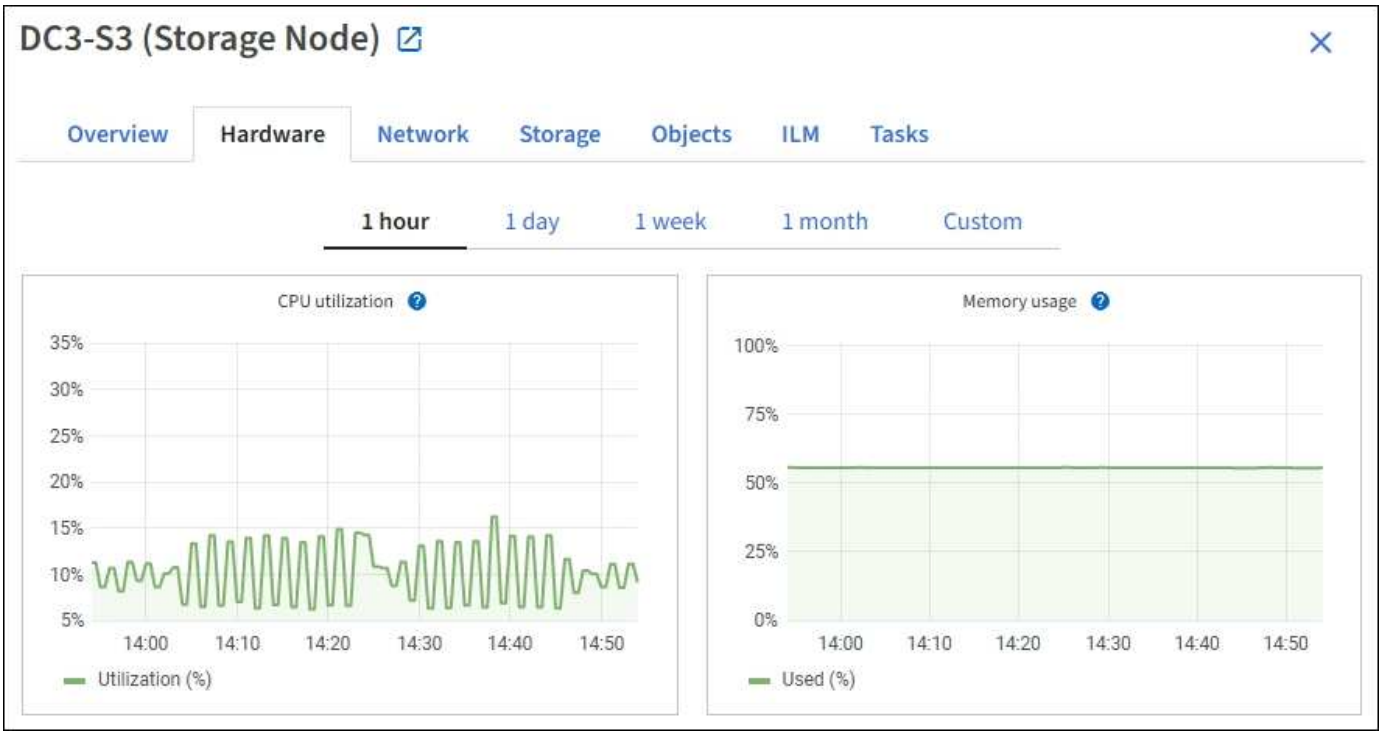
Visualizzare gli avvisi correnti

Visualizzare un avviso specifico

Visualizzare la scheda hardware

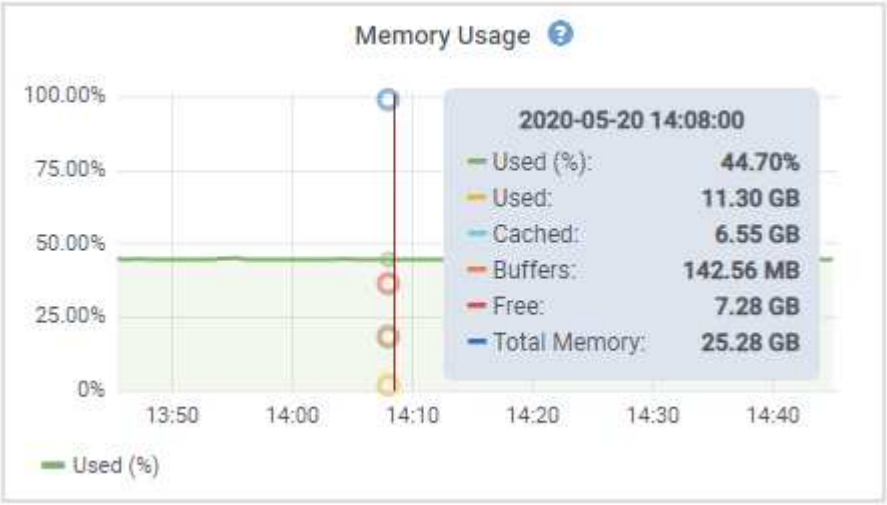
La scheda hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo, oltre a informazioni aggiuntive sull'hardware delle appliance.

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

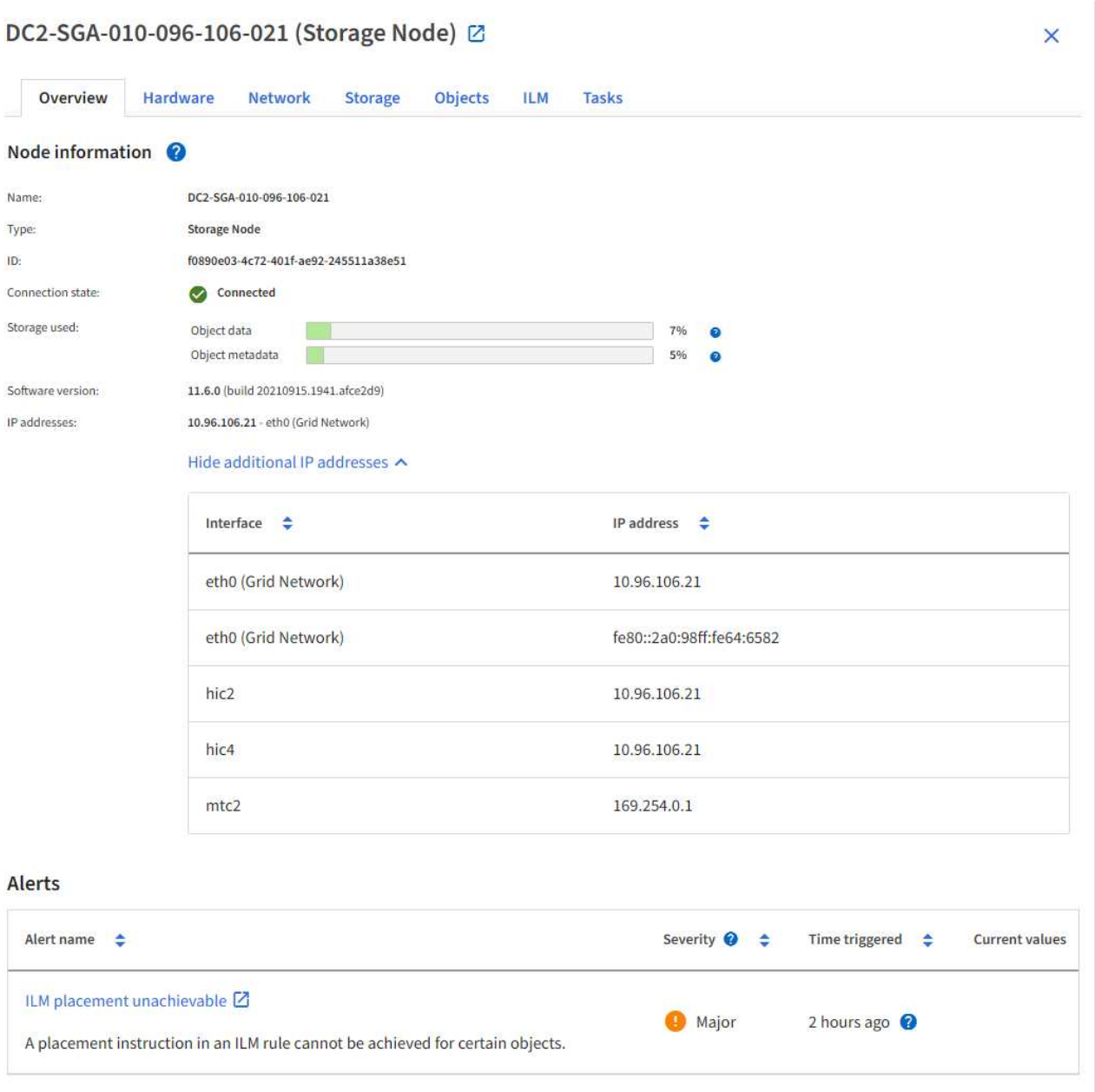
La pagina Nodes (nodi) elenca le informazioni sullo stato di salute del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ciascun nodo di storage dell'appliance. È inoltre possibile visualizzare memoria, hardware di storage, versione del firmware del controller, risorse di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

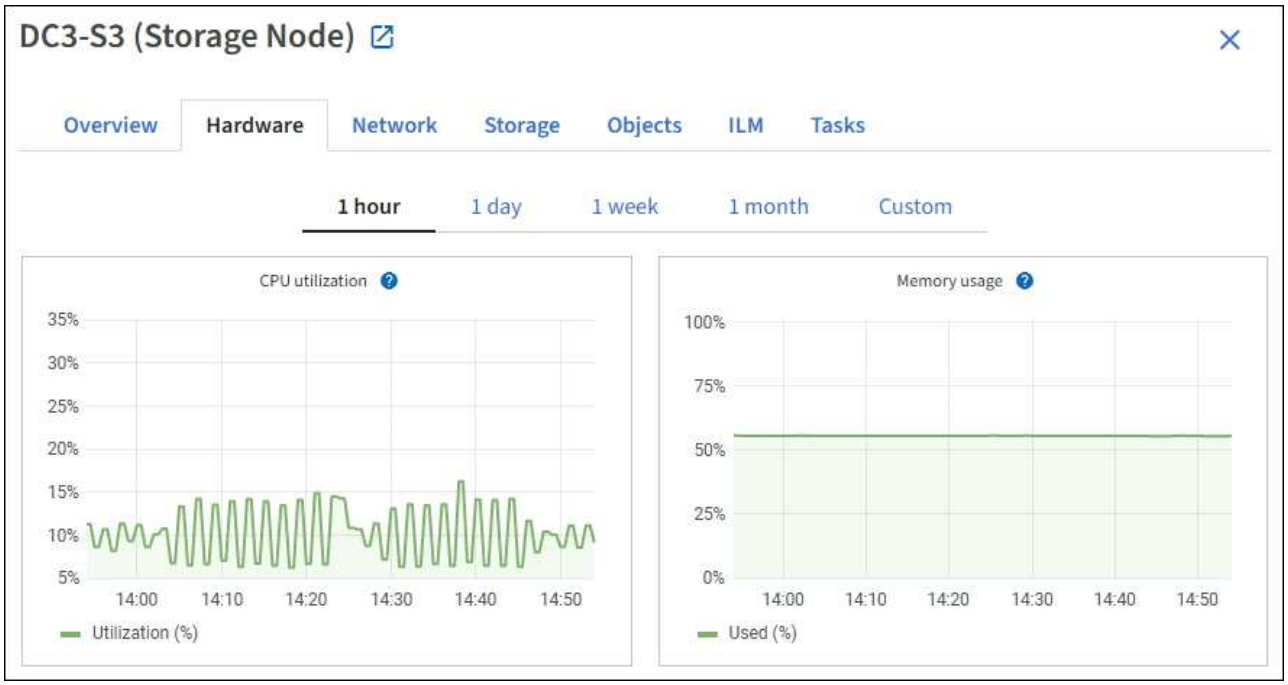
   - **eth**: Rete griglia, rete amministrativa o rete client.
   - **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
   - **mtc**: Una delle porte 1 GbE fisiche dell'appliance.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

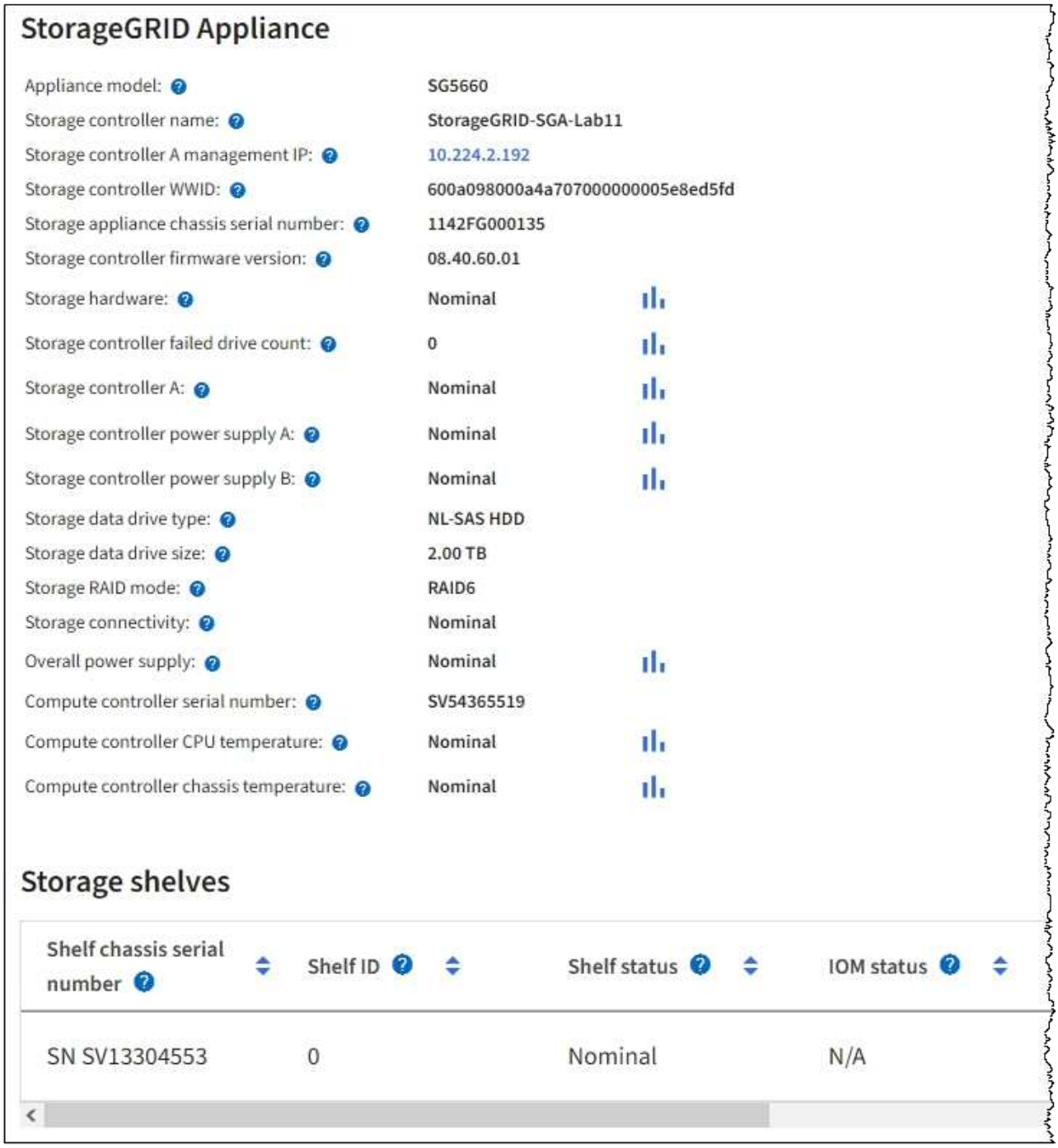
   a. Visualizzare i grafici relativi all'utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni 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.

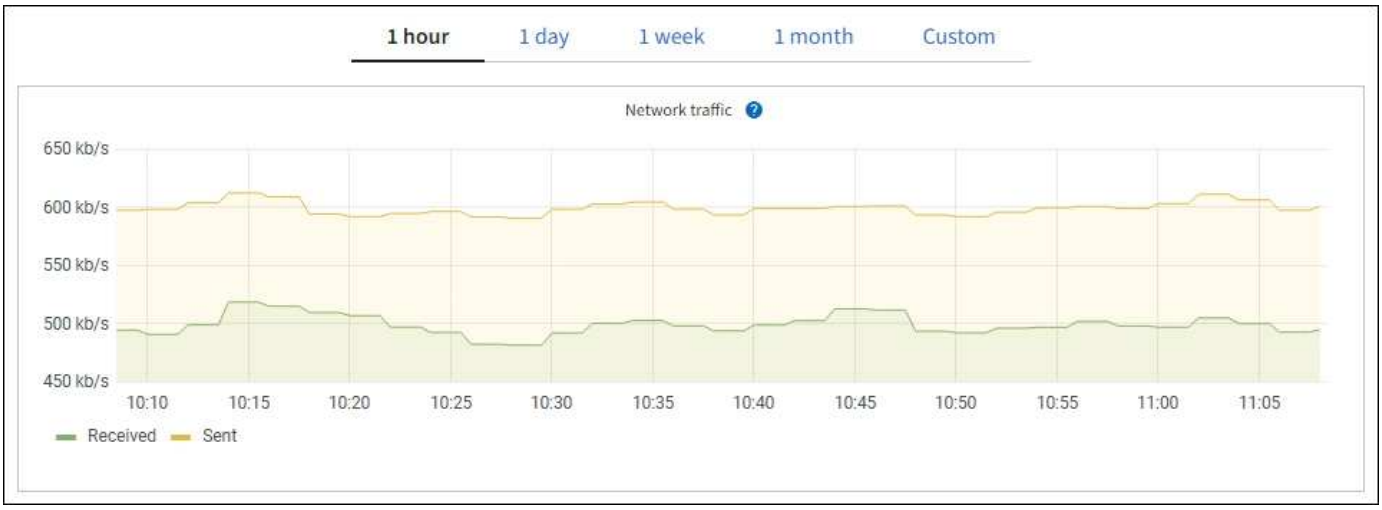
Nella tabella Storage shelf	Descrizione
Stato IOM	Lo stato dei moduli di input/output (IOM) in qualsiasi shelf di espansione. N/D se non si tratta di uno shelf di espansione.
Stato dell'alimentatore	Lo stato generale degli alimentatori per lo shelf di storage.
Stato del cassetto	Lo stato dei cassetti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

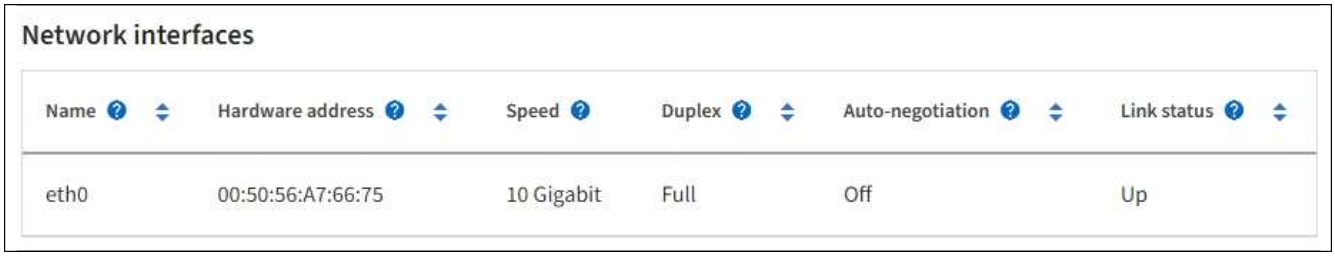
   Se uno stato non è "nominale", rivedere gli avvisi correnti. Puoi anche utilizzare Gestione di sistema di SANtricity per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

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

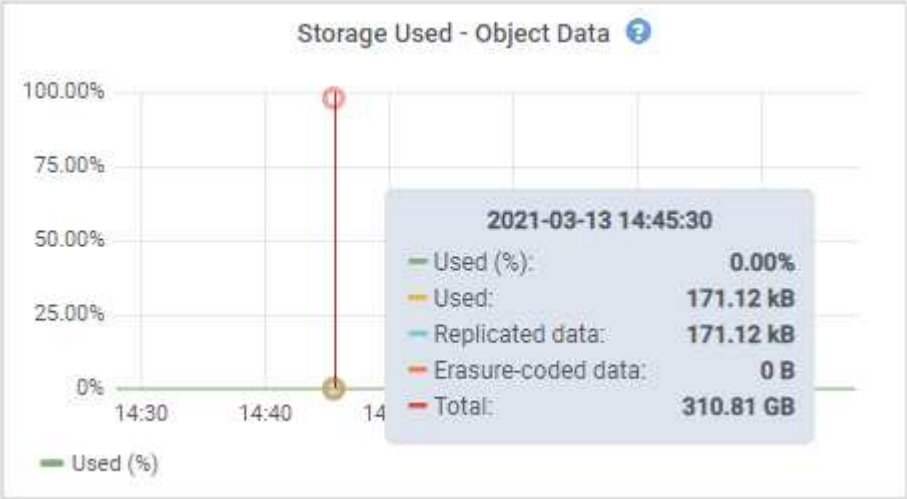
Receive

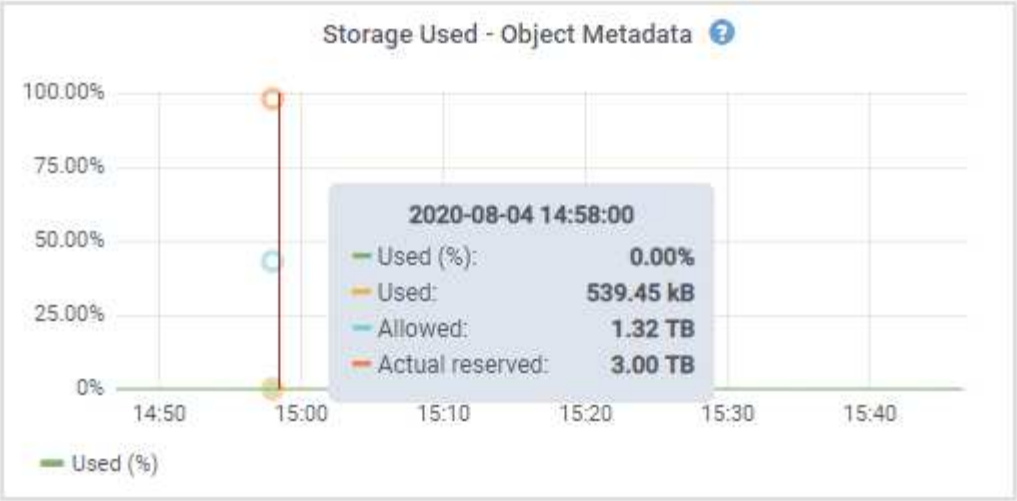
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

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

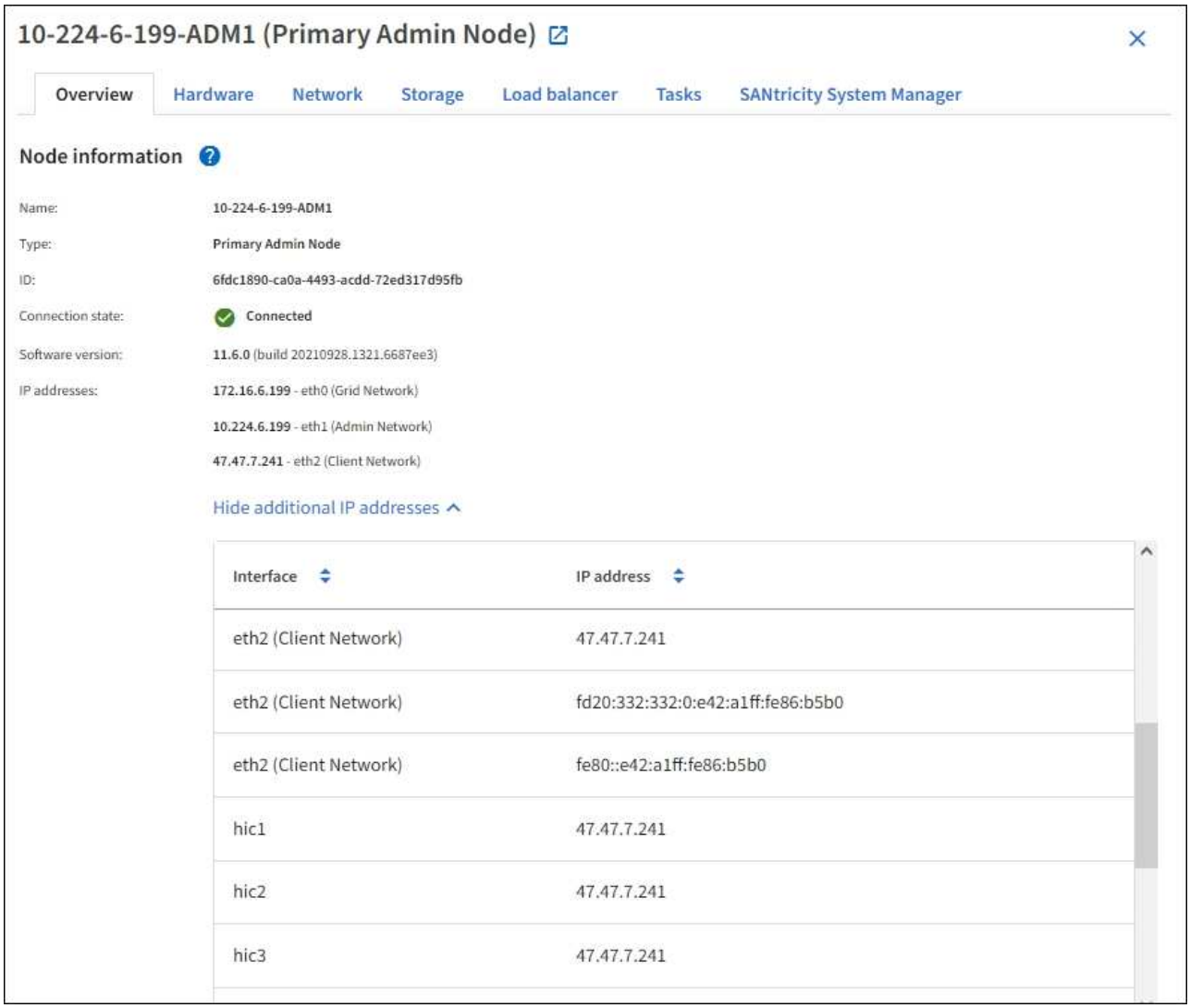
La pagina Nodes (nodi) elenca le informazioni sullo stato del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ogni appliance di servizi utilizzata come nodo di amministrazione o nodo gateway. È inoltre possibile visualizzare memoria, hardware di storage, risorse di rete,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

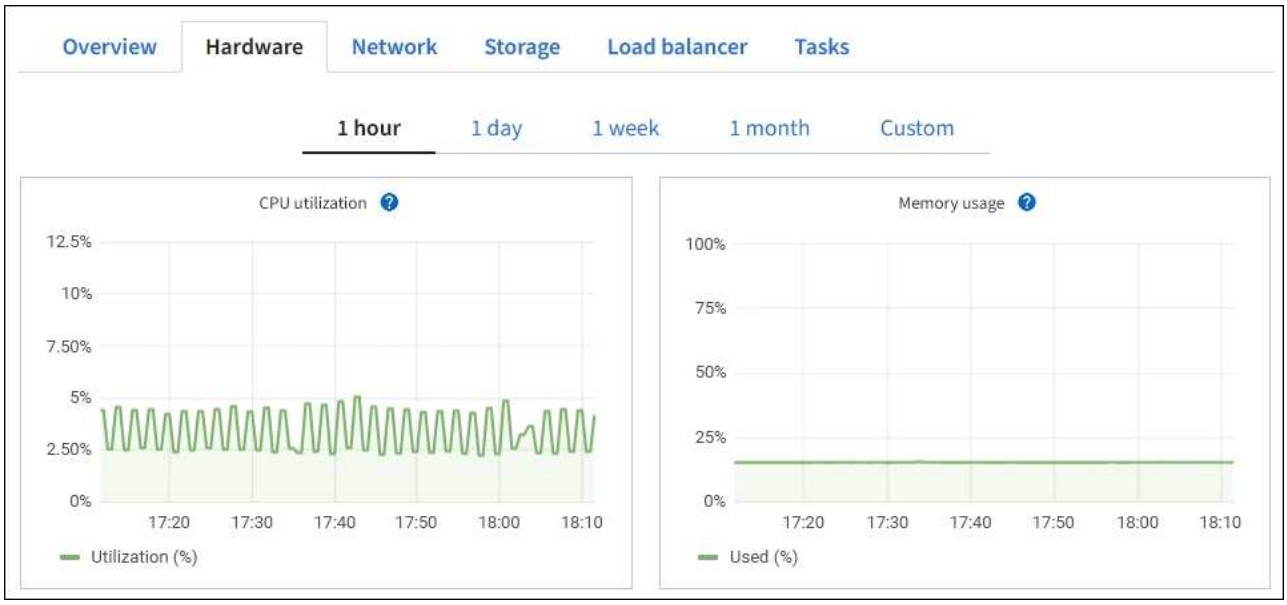
   - **Adllb** e **adlli**: Visualizzato se si utilizza il bonding Active/backup per l'interfaccia di Admin Network
   - **eth**: Rete griglia, rete amministrativa o rete client.
   - **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate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



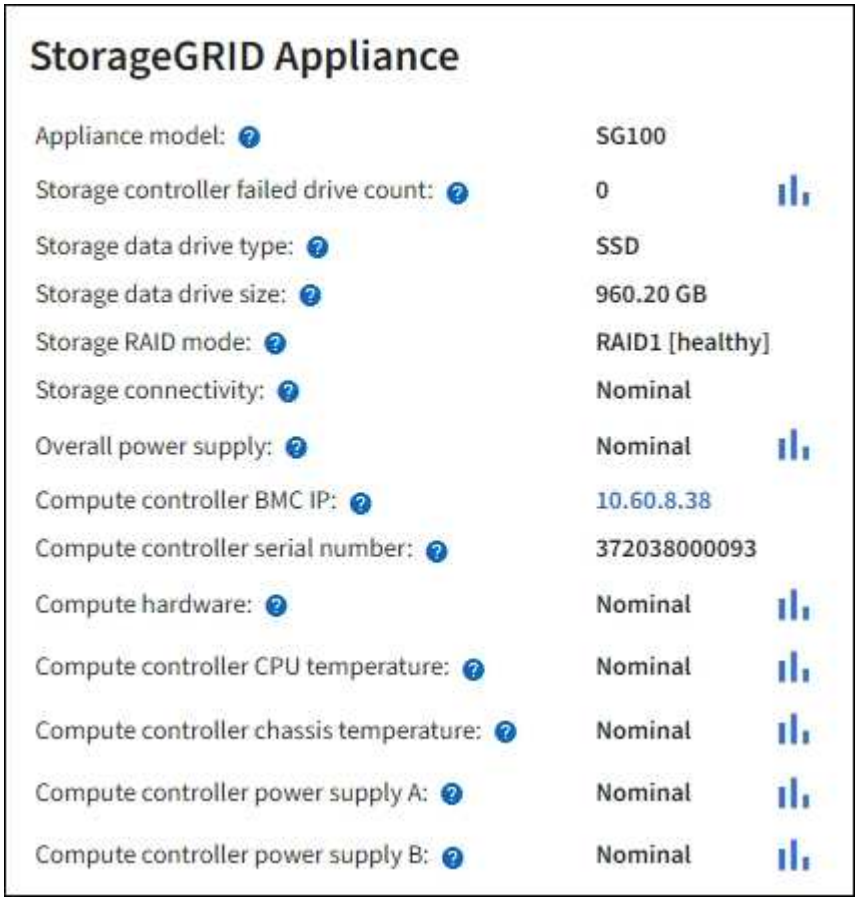
   La sezione Avvisi della scheda Panoramica visualizza gli avvisi attivi per il nodo.

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.



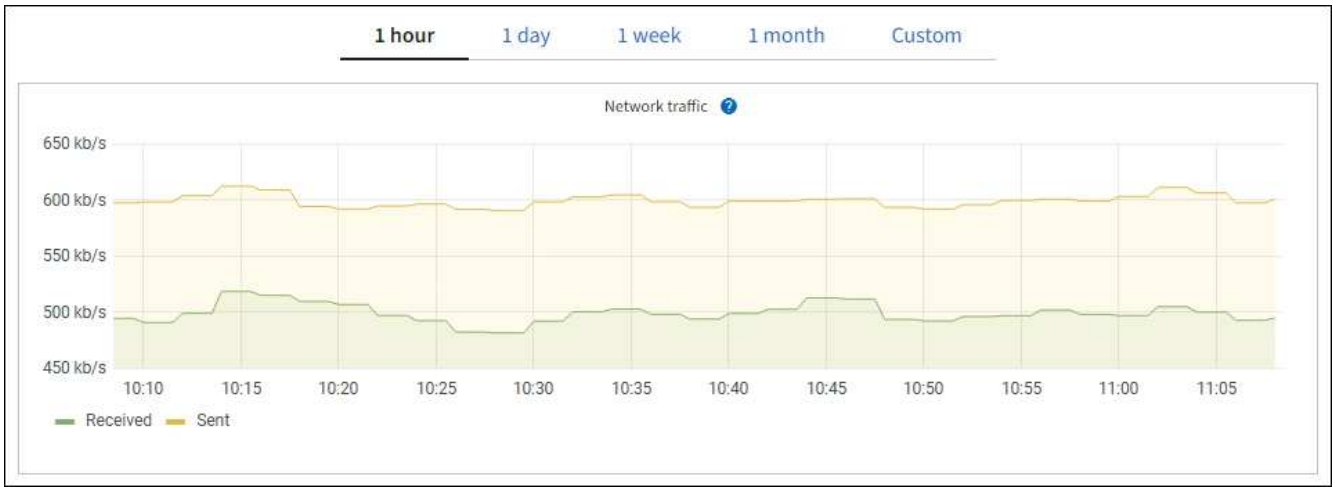
Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello dell'appliance StorageGRID.
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato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

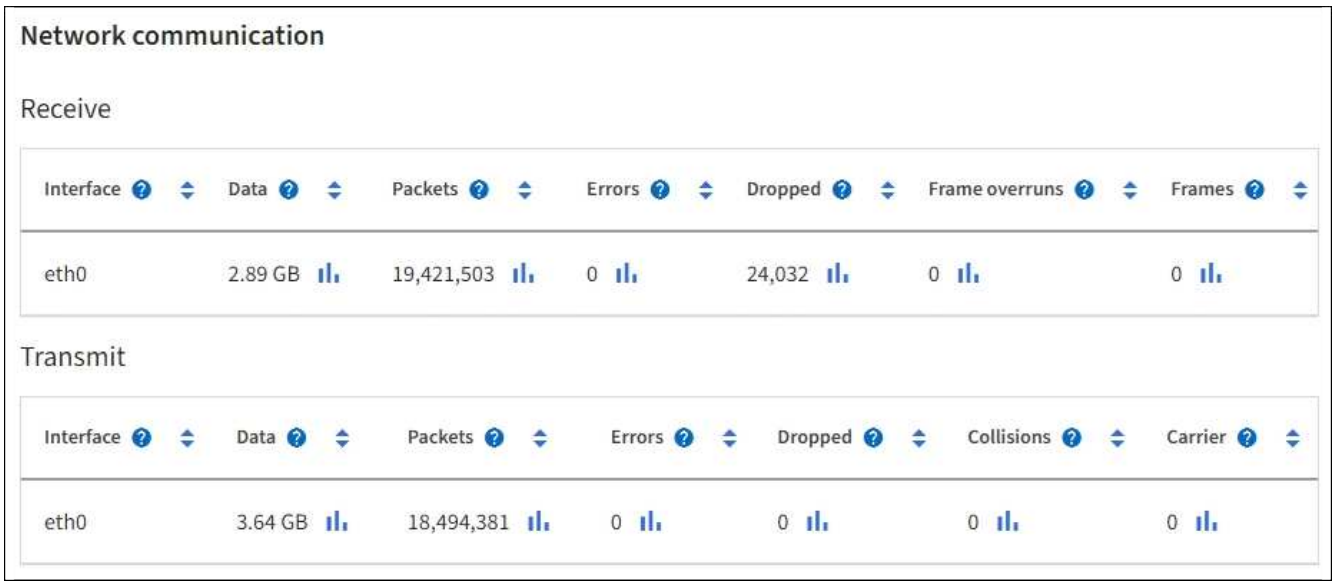
Utilizzare la seguente tabella con i valori nella colonna **Speed** della tabella Network Interfaces (interfacce di rete) per determinare se le quattro porte di rete 40/100-GbE dell'appliance sono state configurate per l'utilizzo della modalità Active/backup o LACP.

> 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

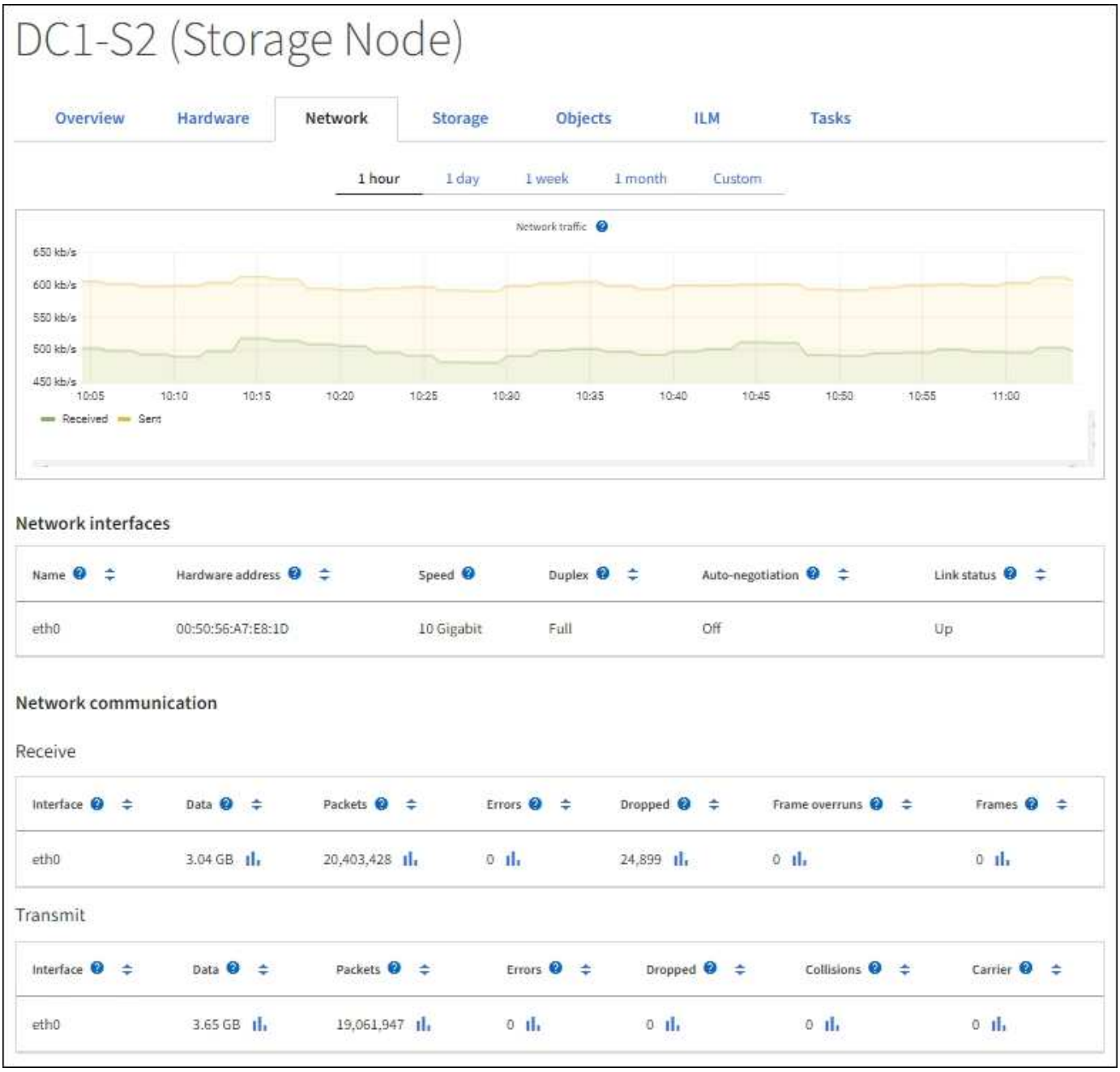
Visualizzare la scheda rete

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)

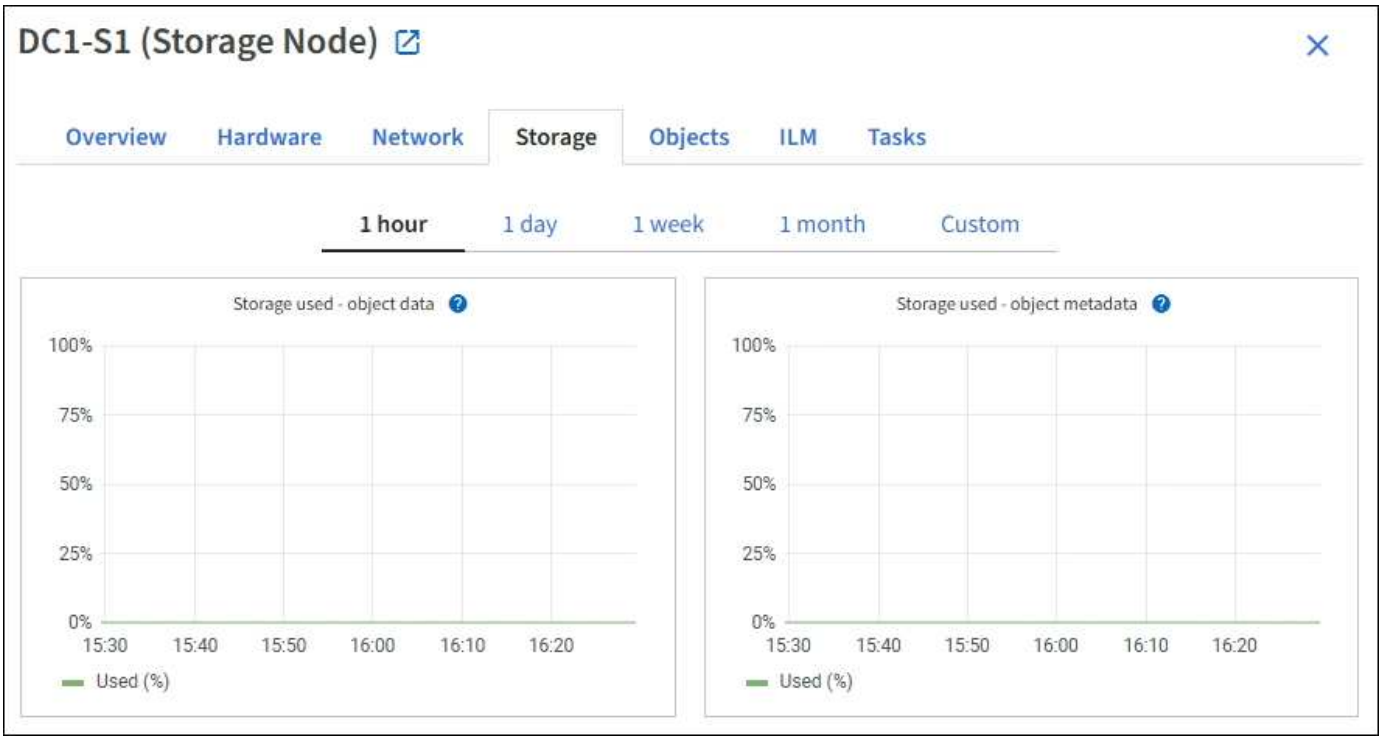
La scheda Storage riepiloga la disponibilità dello storage e altre metriche di storage.

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.

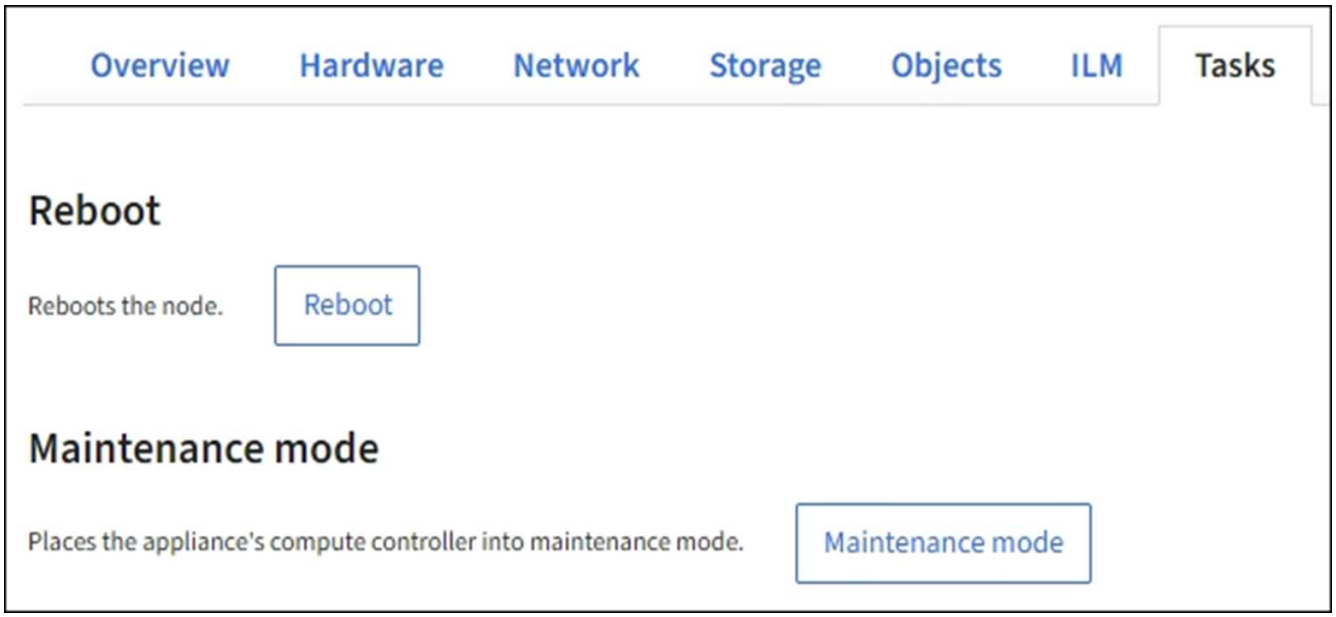
  Se si intende riavviare un nodo di storage, tenere presente quanto segue:

  - 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.

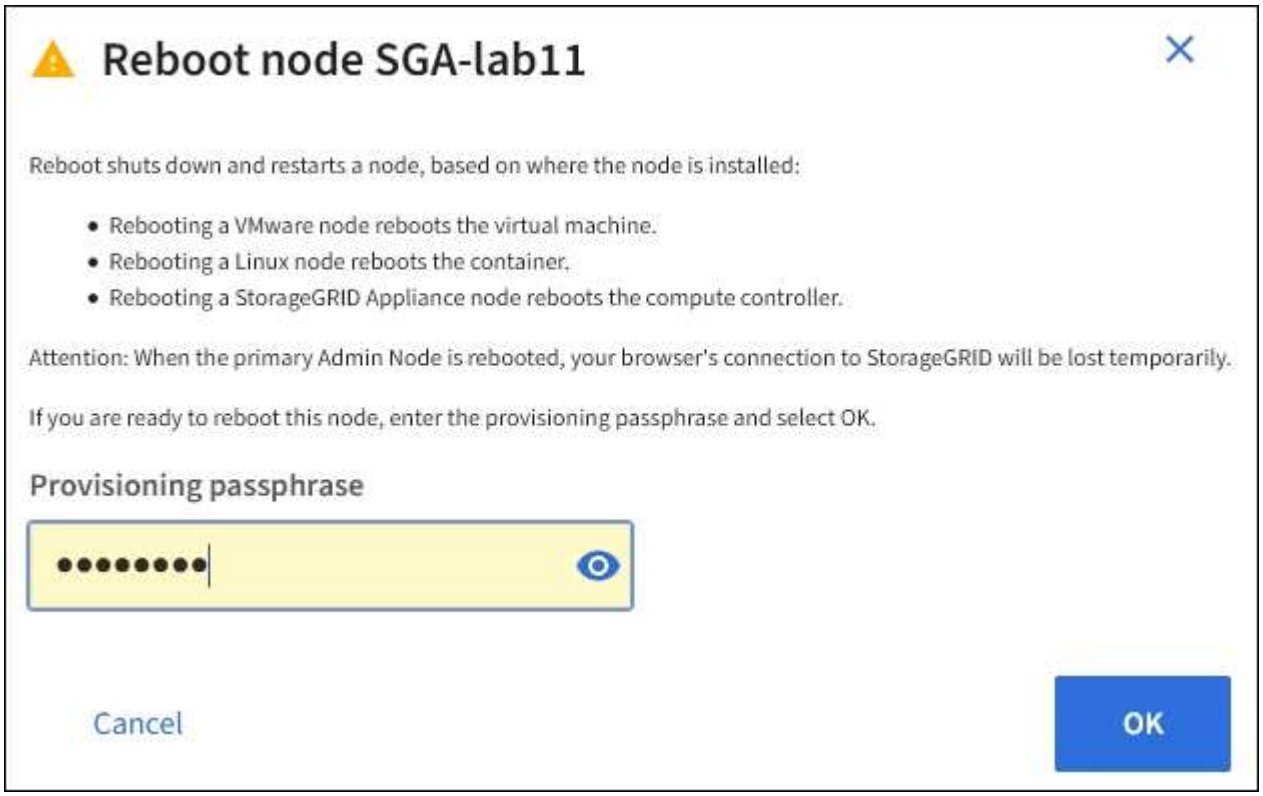
Fasi

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

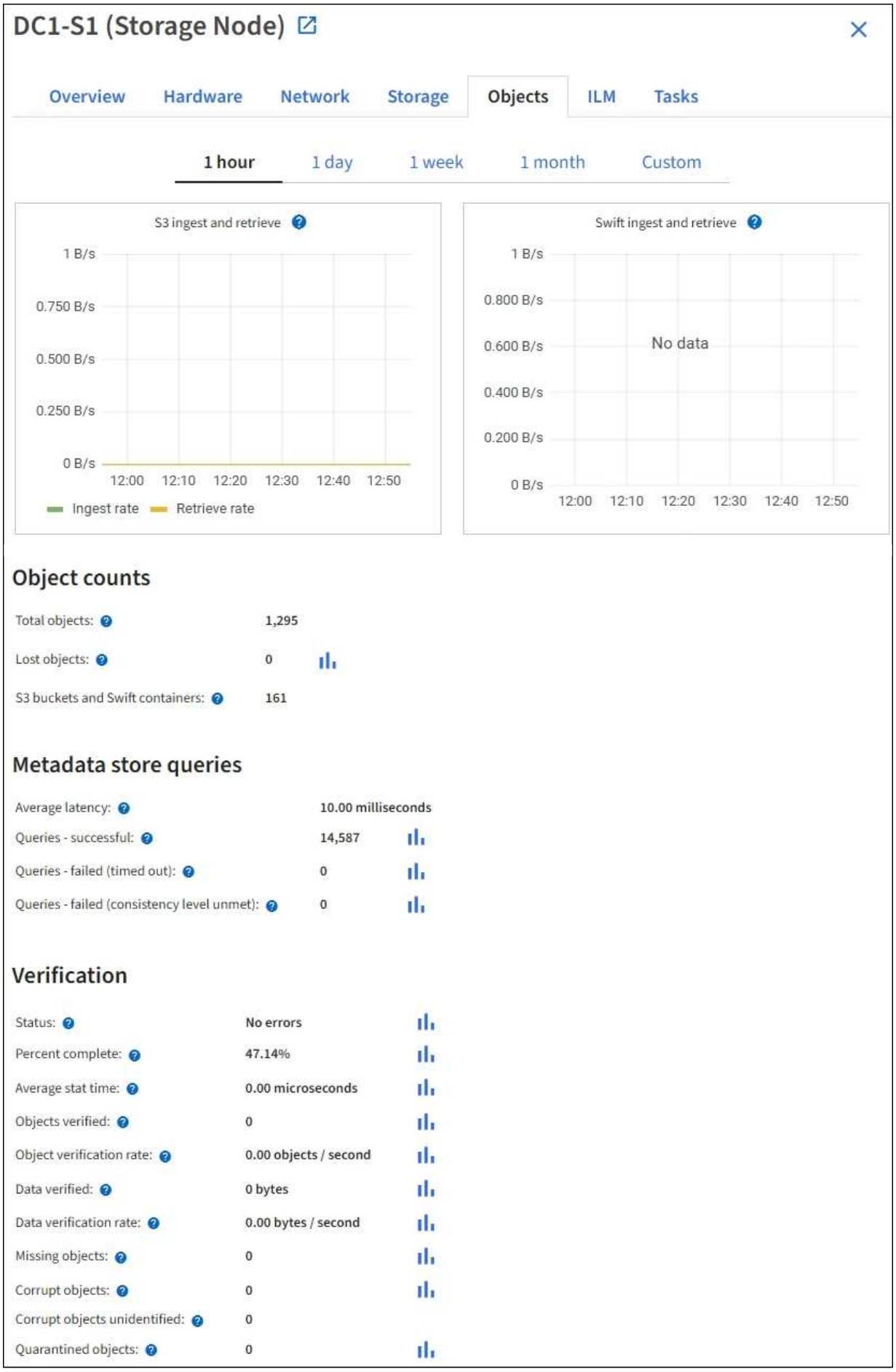
Appliance di storage SG5600

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.

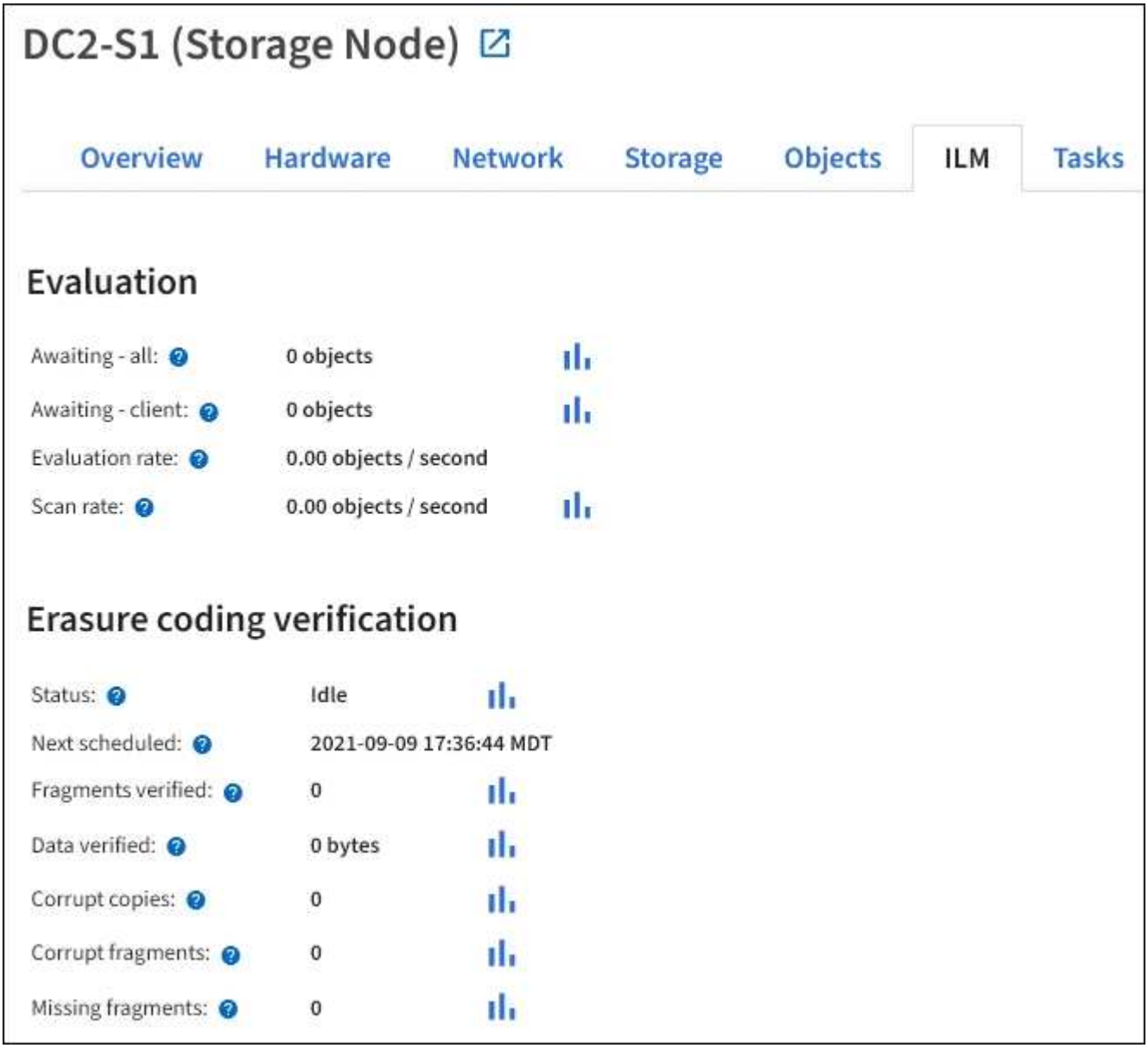

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

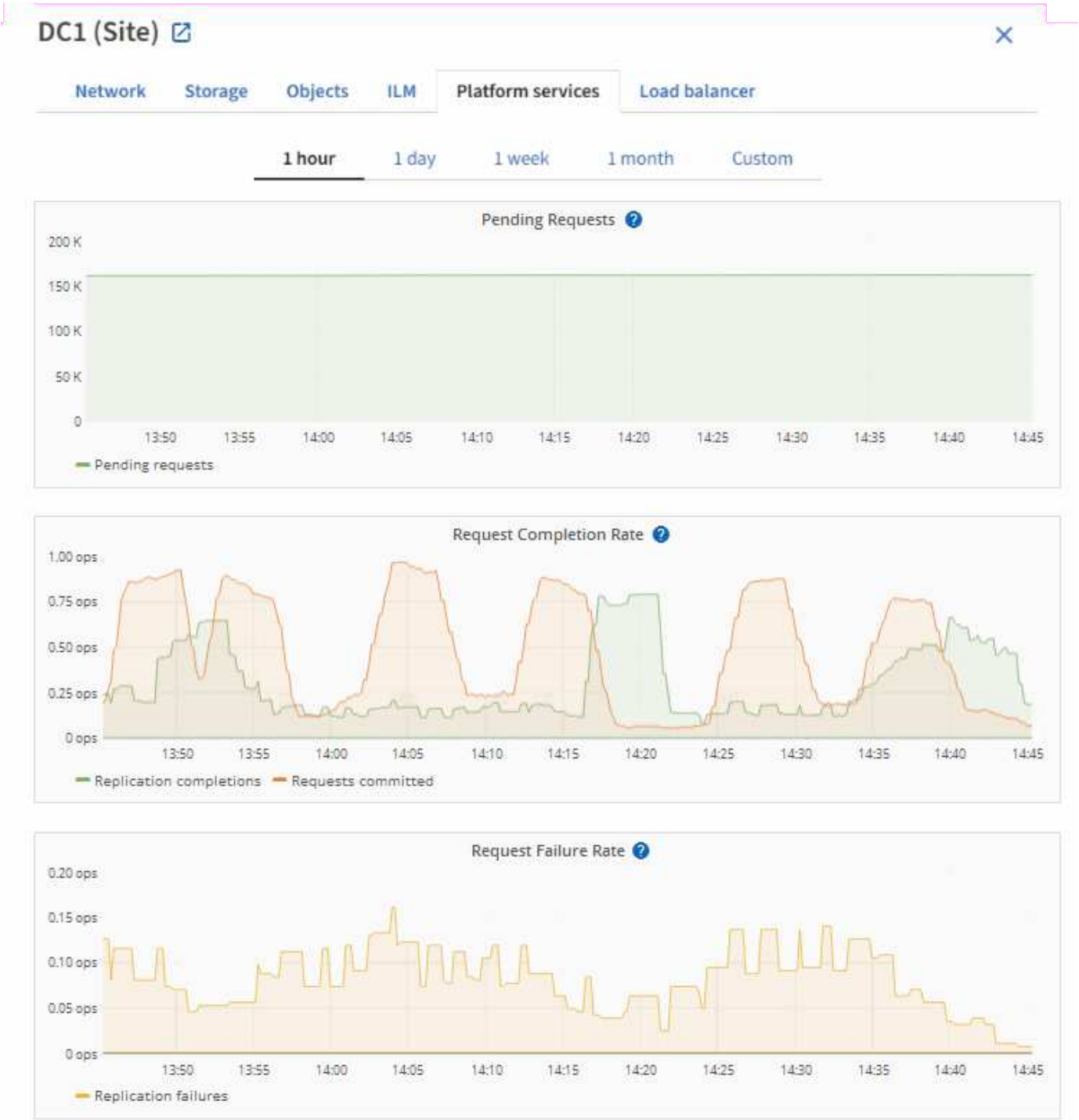
Monitorare le operazioni di bilanciamento del carico

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.

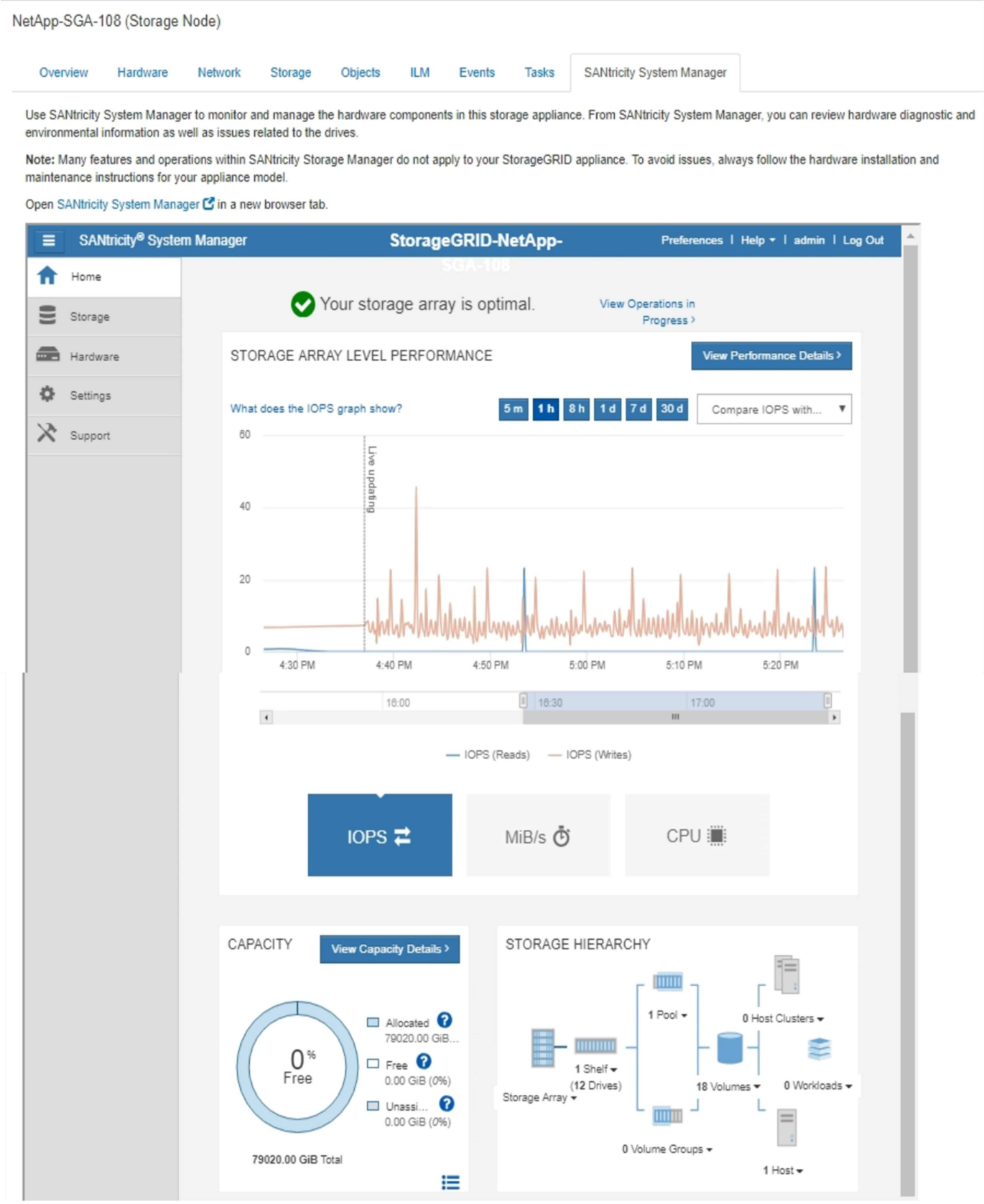
Amministrare StorageGRID

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).

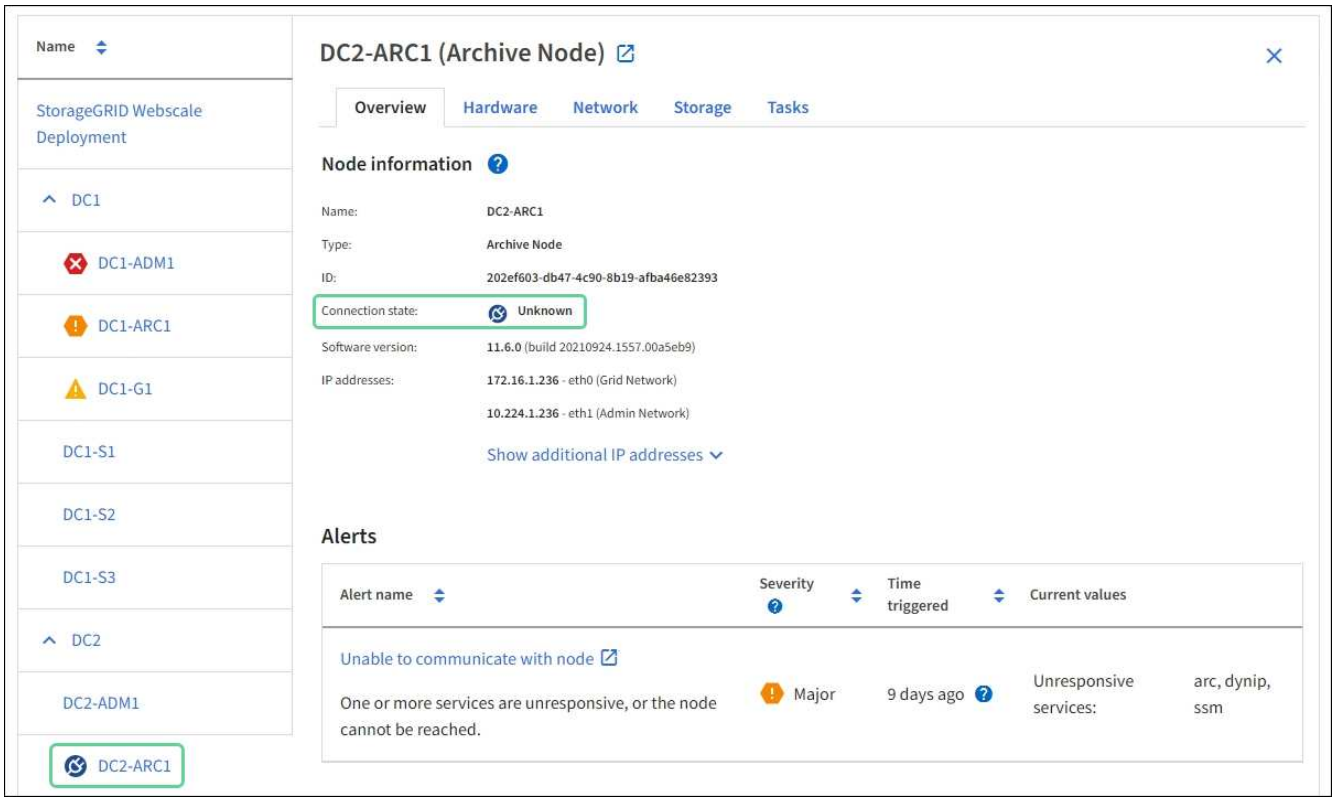
- **Non connesso - amministrazione non attiva** : Il nodo non è connesso alla rete per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.
-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

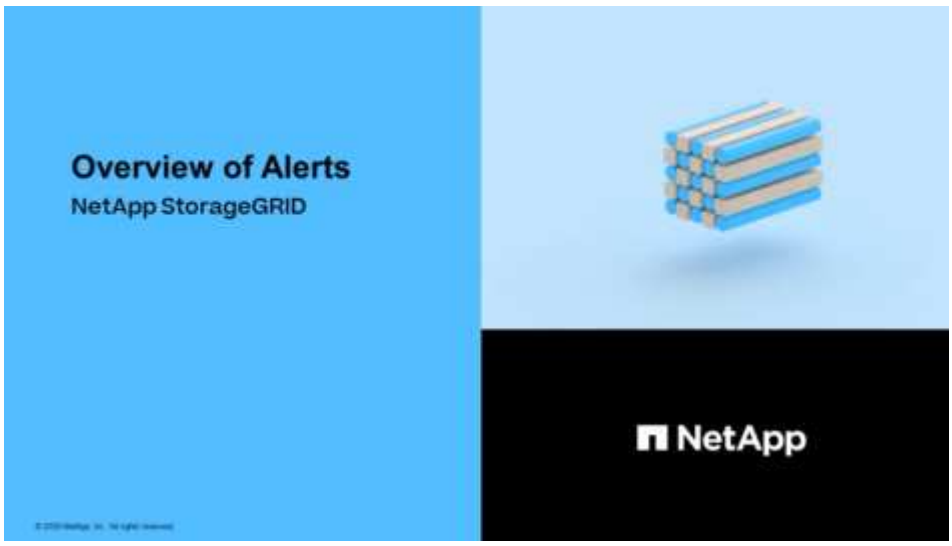
Ripristino e manutenzione

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".

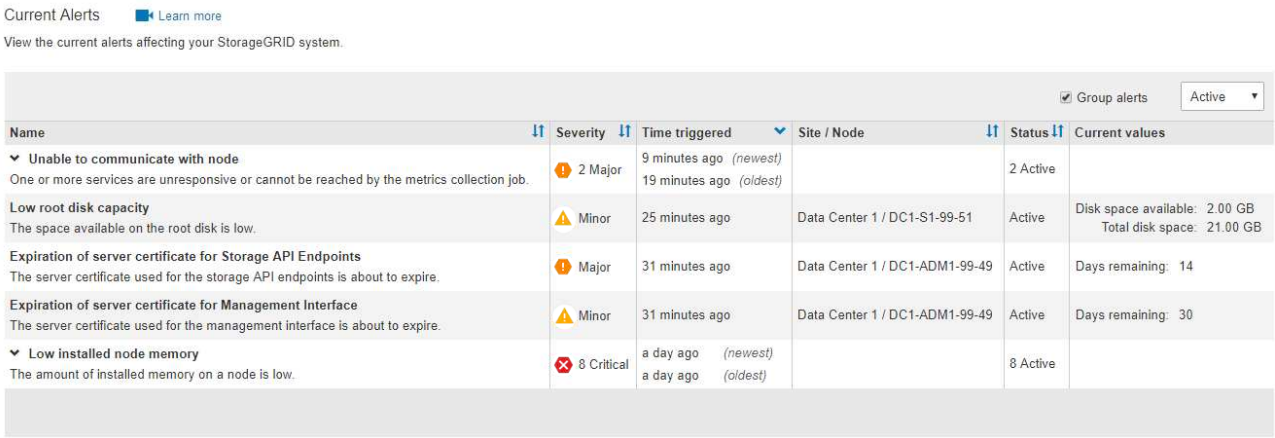


Fasi

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.

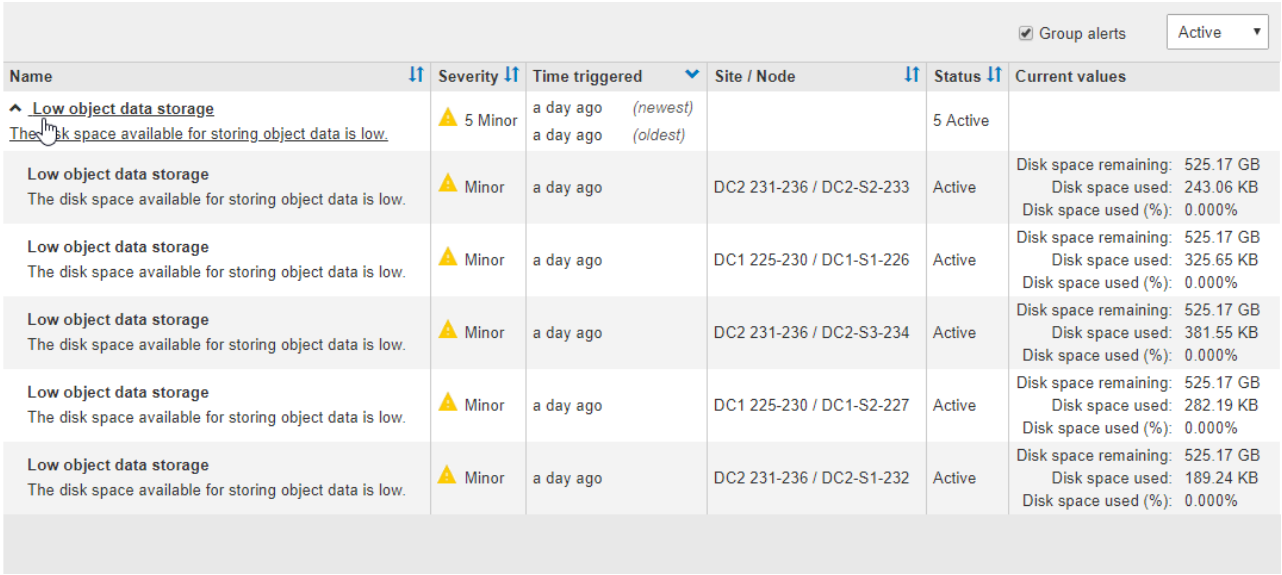
La pagina Current Alerts (Avvisi correnti) viene aggiornata ogni due minuti.

2. Esaminare le informazioni contenute nella tabella.

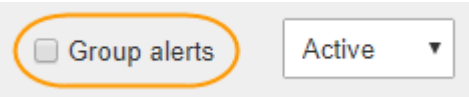
Intestazione di colonna	Descrizione
Nome	Il nome dell'avviso e la relativa descrizione.
Severità	La severità dell'avviso. Se vengono raggruppati più avvisi, la riga del titolo mostra il numero di istanze di tale avviso che si verificano a ogni livello di gravità. • **Critico** : Si verifica una condizione 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

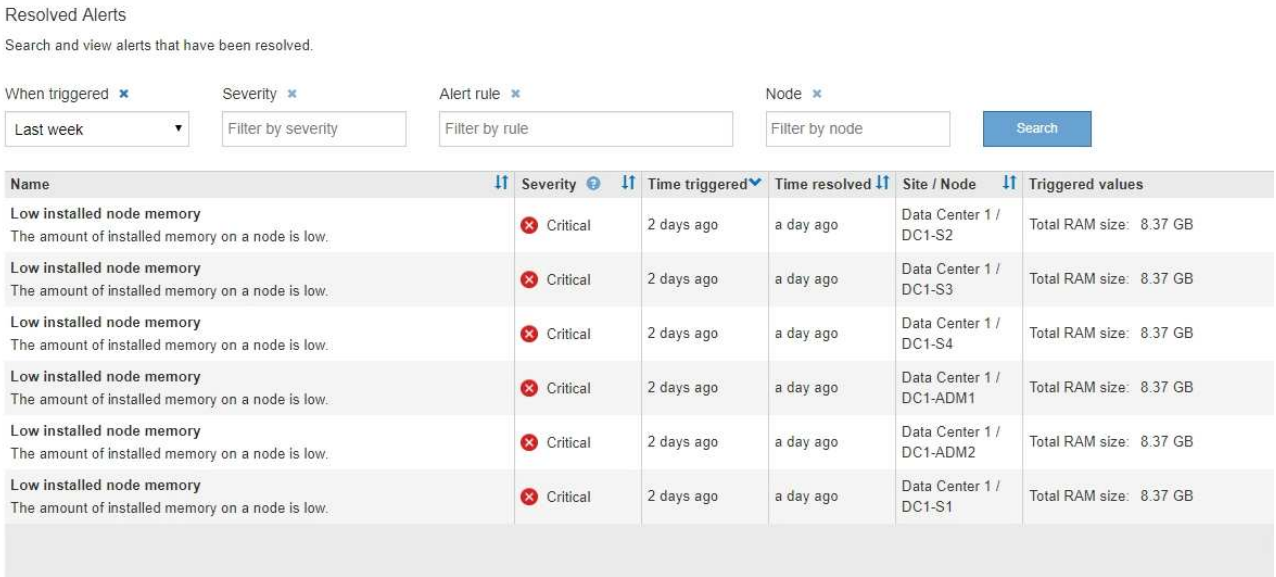
- È necessario accedere a Grid Manager utilizzando un browser web supportato.

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.

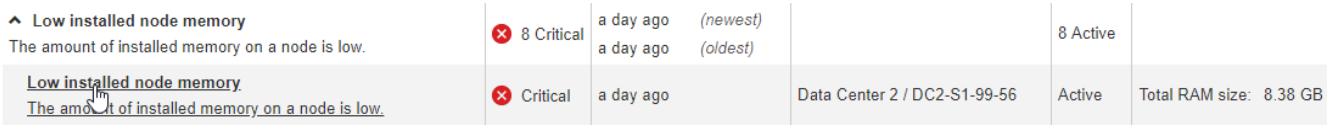
Fasi

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

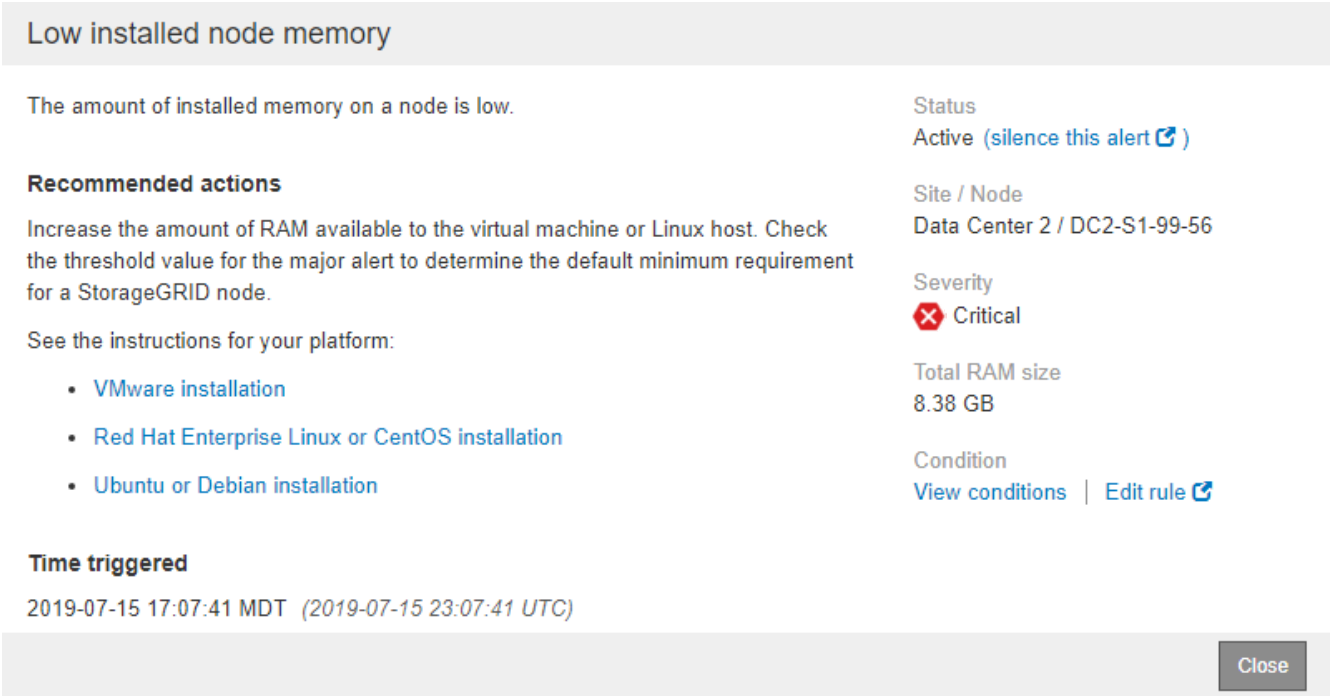
Intestazione di colonna	Descrizione
Avviso corrente	• Dal pannello Health (Salute) della dashboard, fare clic sul collegamento **Current alerts** (Avvisi correnti). Questo collegamento viene visualizzato solo se è attivo almeno un avviso. Questo collegamento è nascosto se non sono presenti avvisi correnti 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.

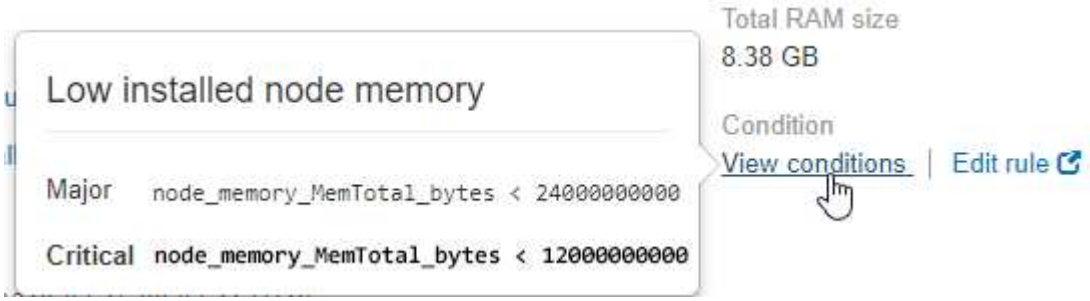
Per tacitare una regola di avviso, è necessario disporre dell'autorizzazione di accesso Gestisci avvisi o root.

> 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

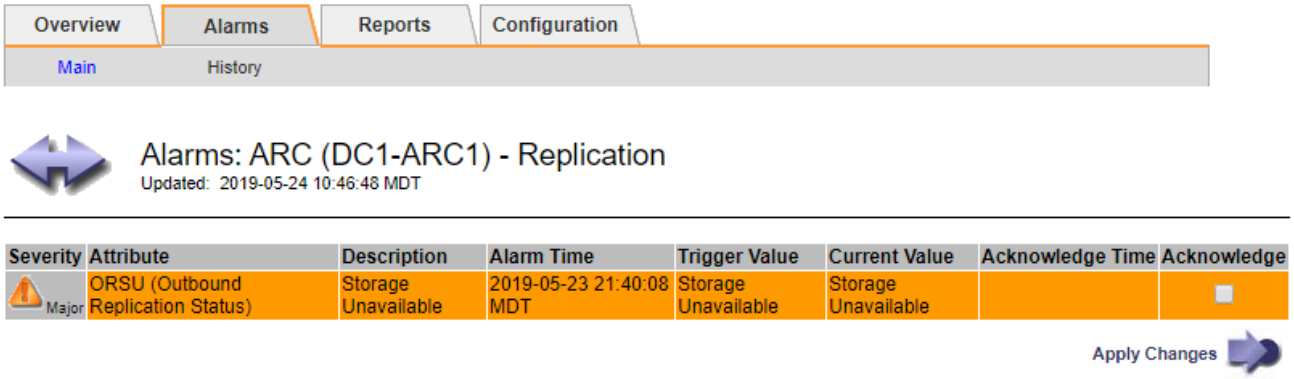
1. Selezionare **SUPPORTO Allarmi (legacy) Allarmi correnti**.

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.

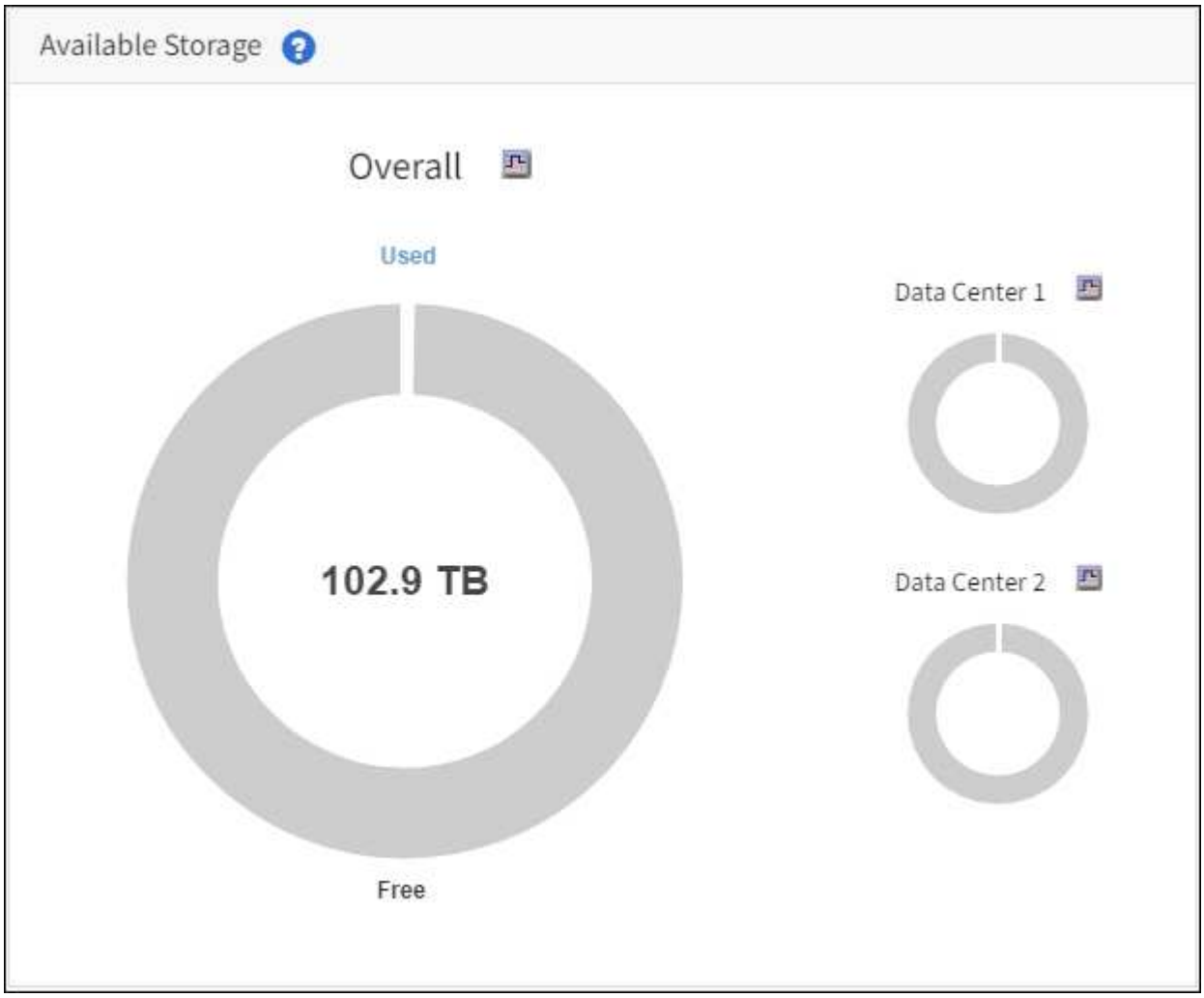
Fasi

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

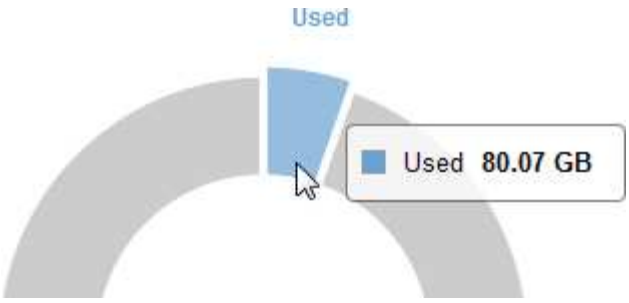
   a. Selezionare **Dashboard**.

   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

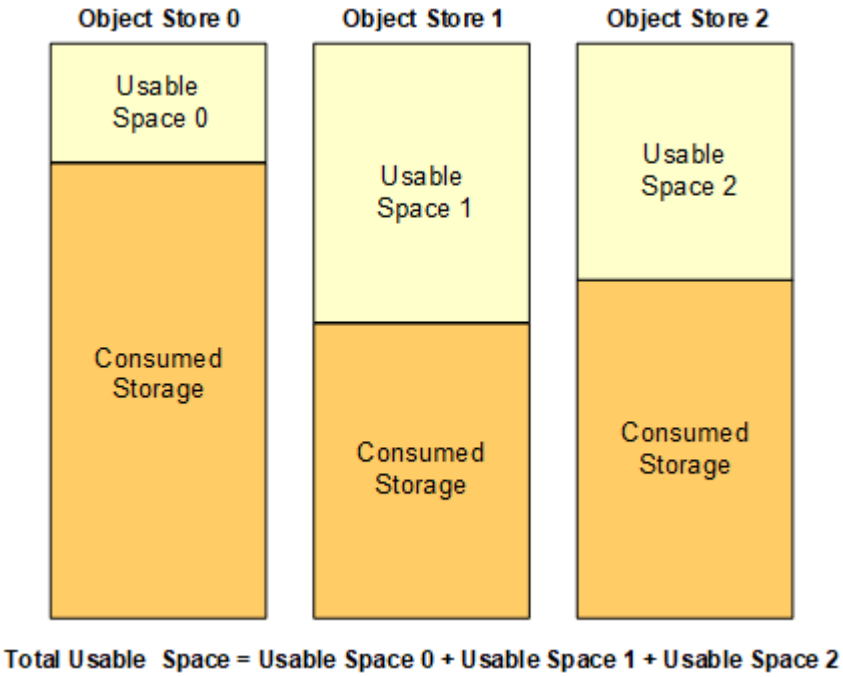
Monitorare lo spazio totale utilizzabile per ciascun nodo di storage per garantire che il nodo disponga di spazio sufficiente per i nuovi dati dell'oggetto.

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**.

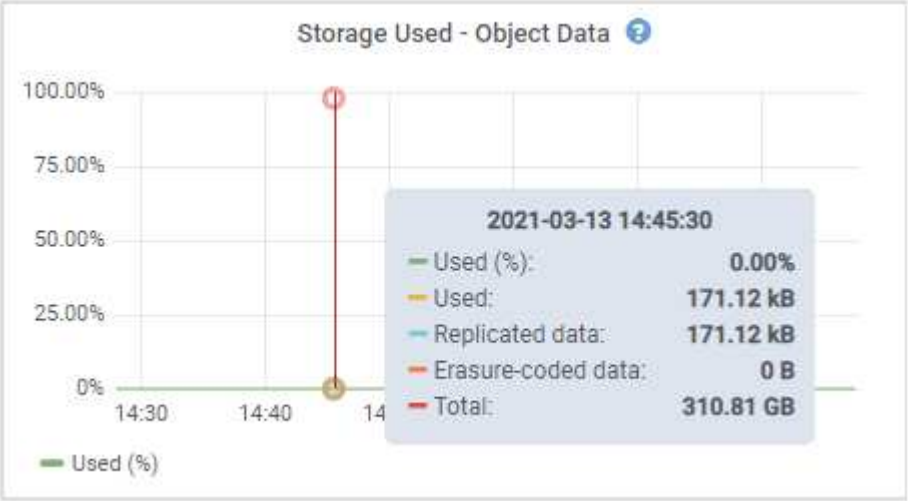
   Vengono visualizzati i grafici e le tabelle del nodo.

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

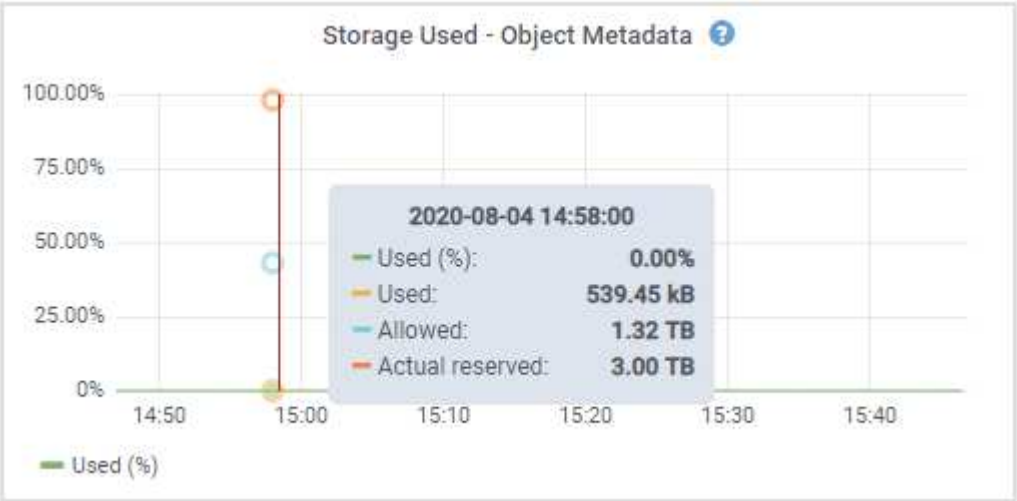
StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di storage di ogni sito utilizzando lo spazio riservato ai metadati sul volume di storage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

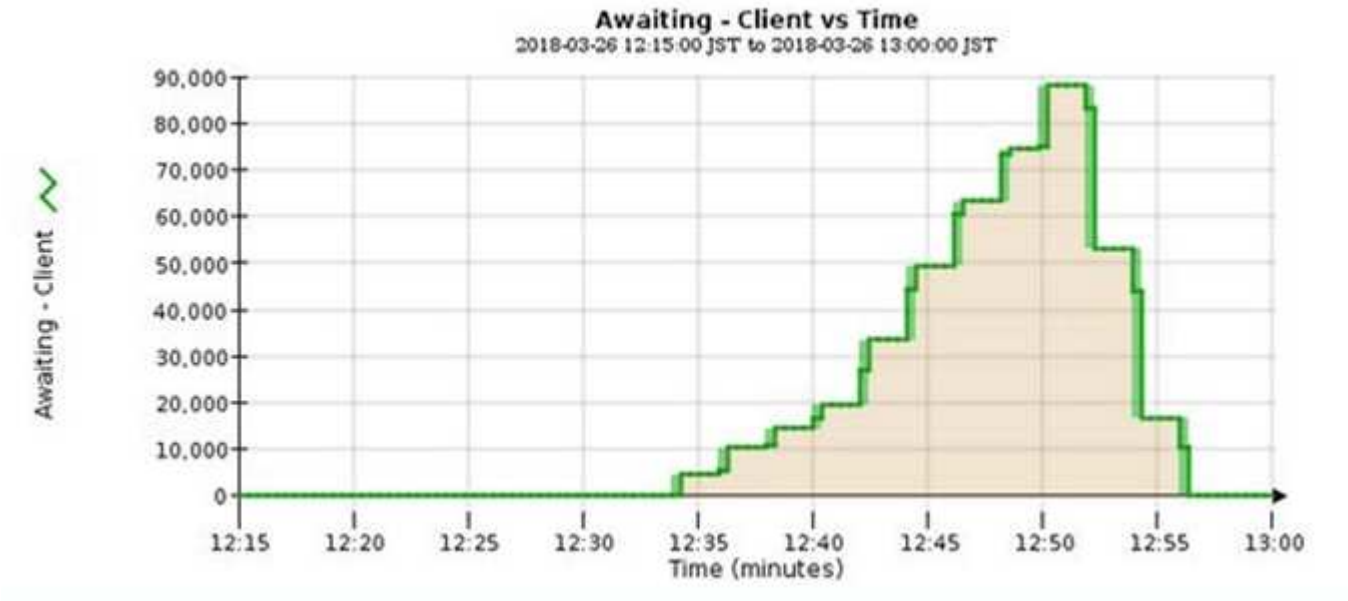
conservazione di ciascuna copia.

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.

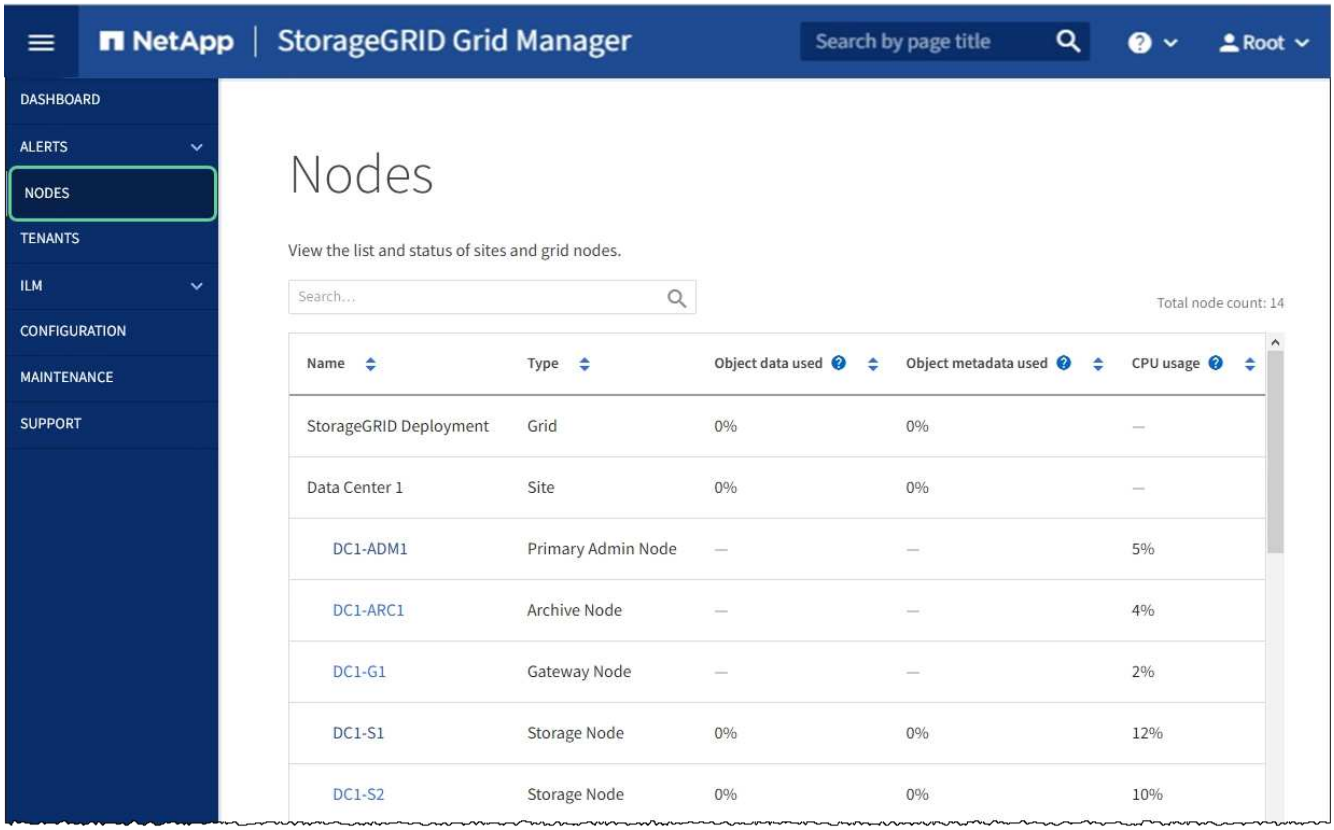
È possibile utilizzare Grid Manager per monitorare la connettività e le performance di rete, in modo da poter risolvere tempestivamente qualsiasi problema.

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

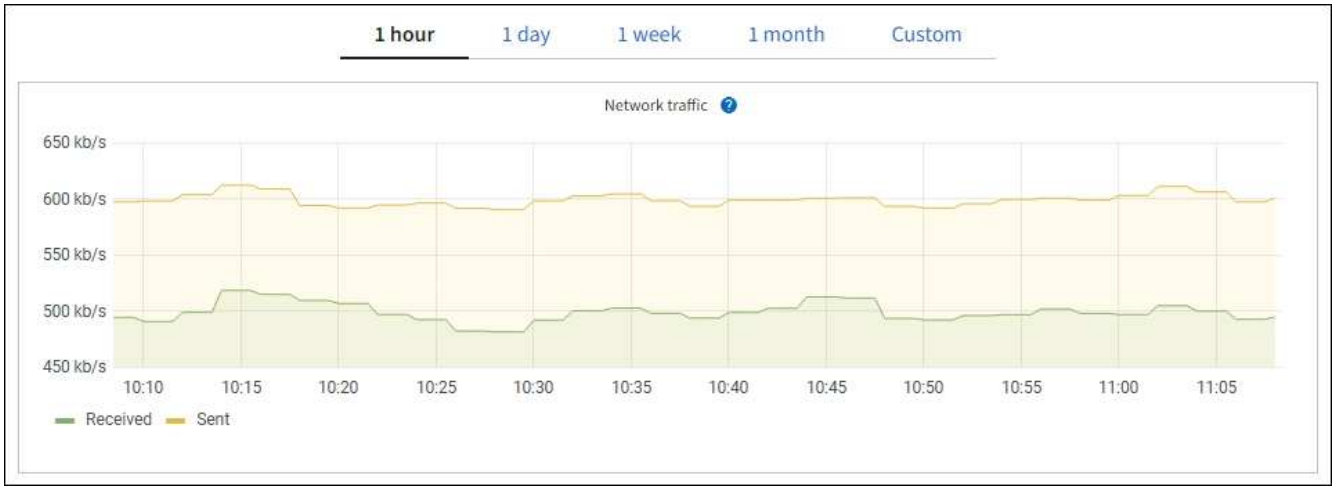
1. Selezionare **NODI**.

   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

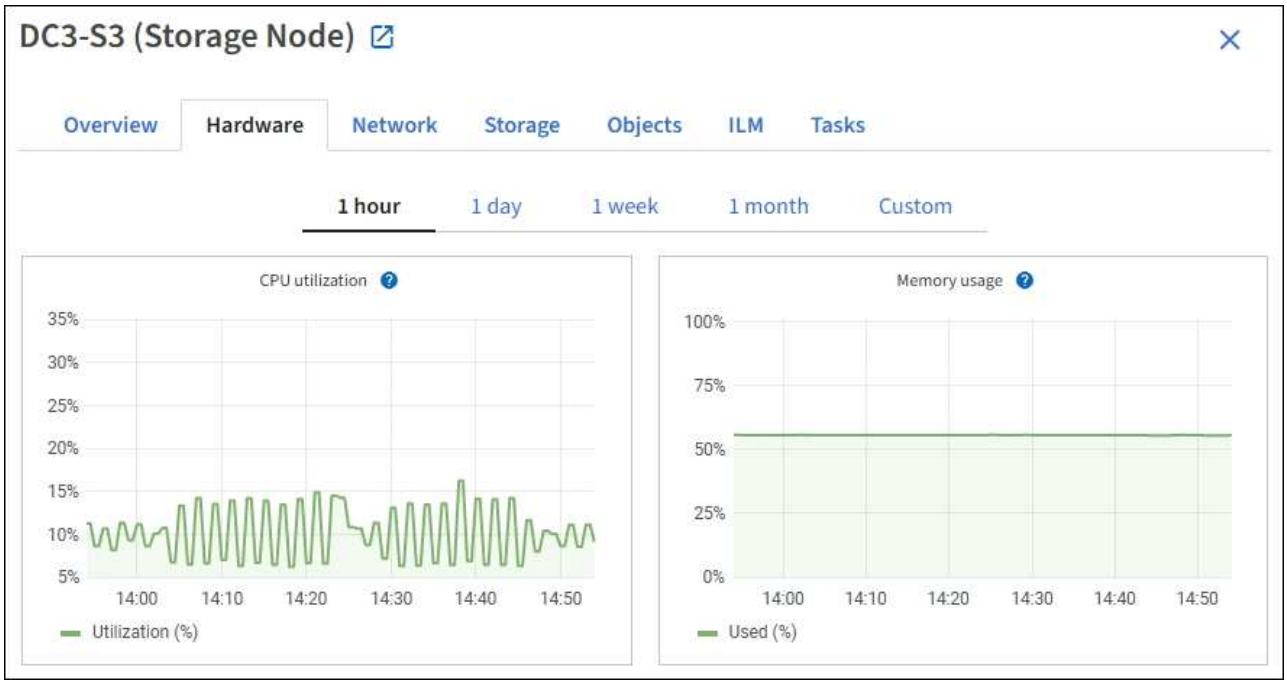
- È necessario accedere a Grid Manager utilizzando un browser web supportato.

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.

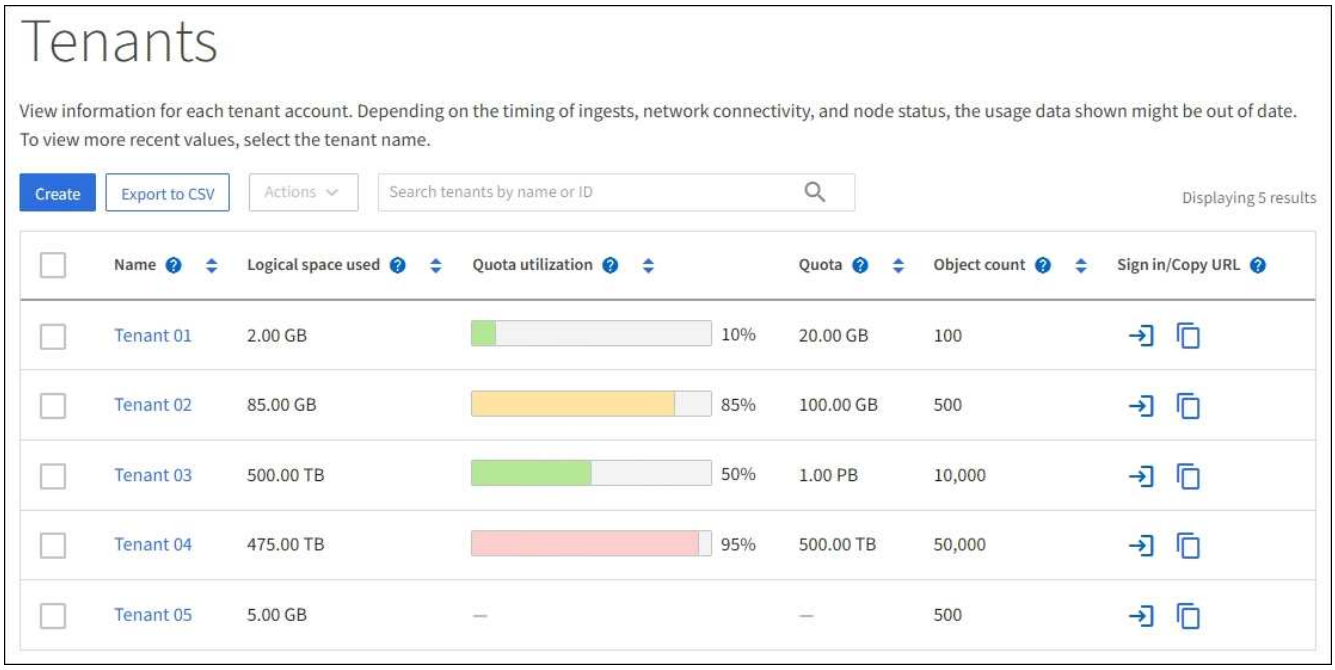
A proposito di questa attività

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.

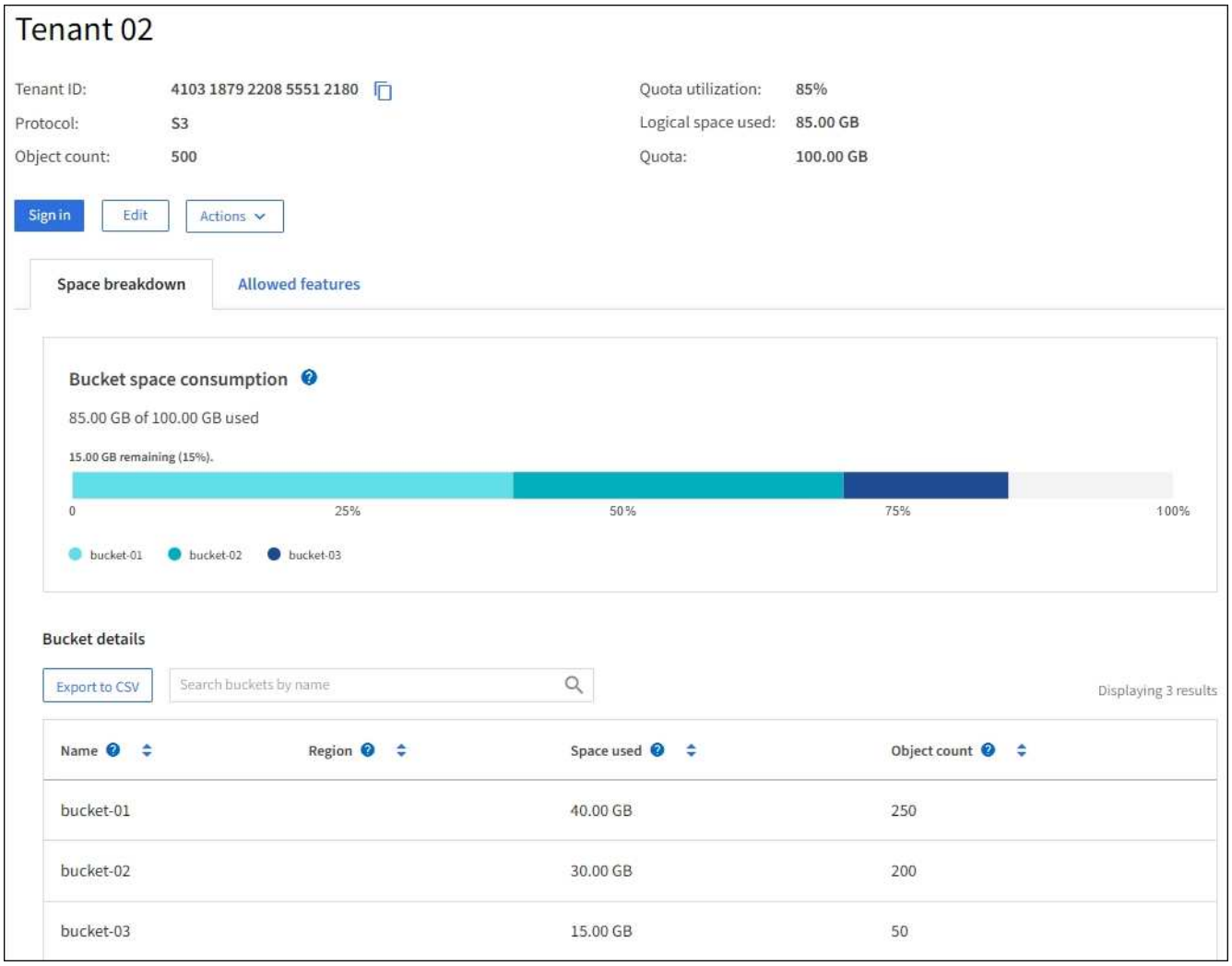
   Viene richiesto di aprire o salvare `.csv` file.

   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**

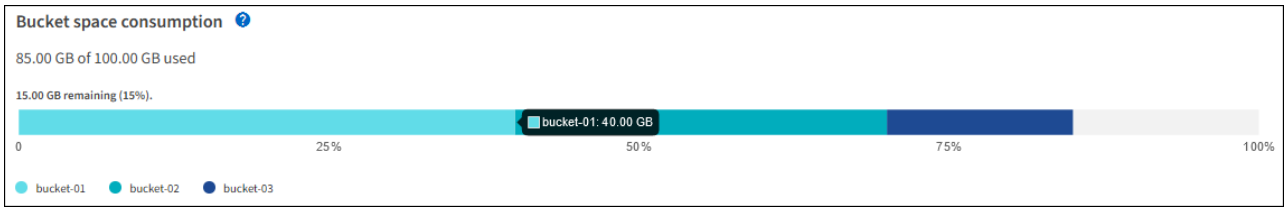
  L'area panoramica del tenant contiene i valori per il conteggio degli oggetti, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.

- **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

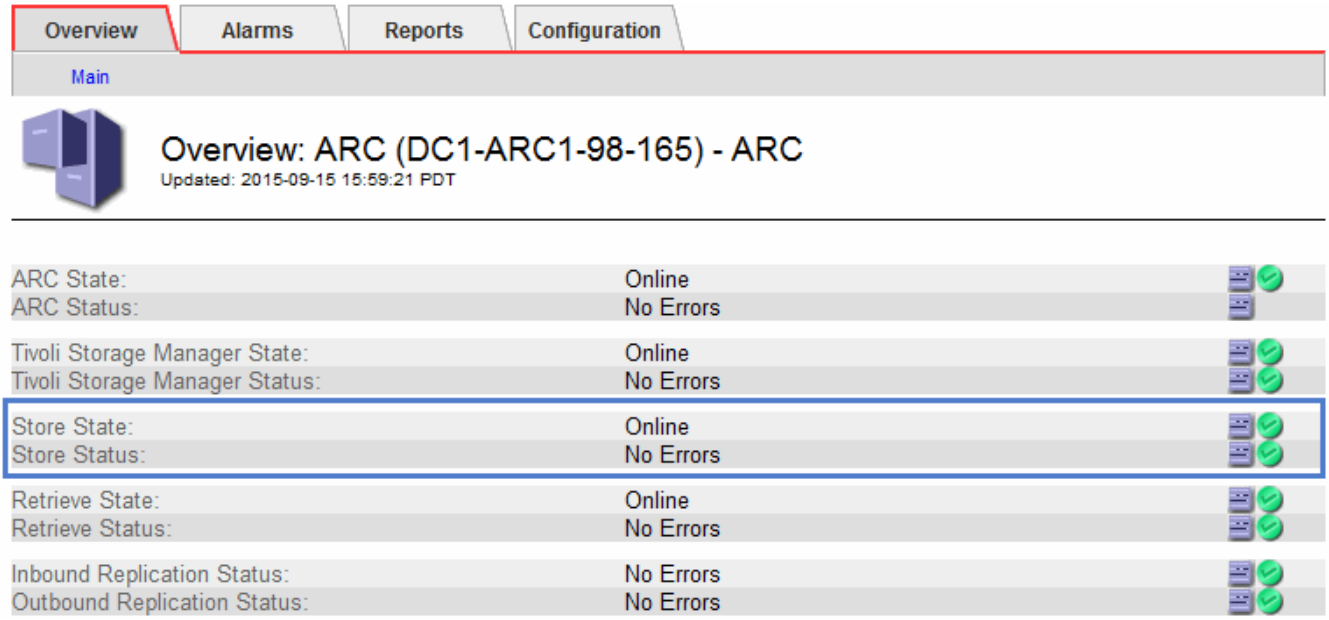
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

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.

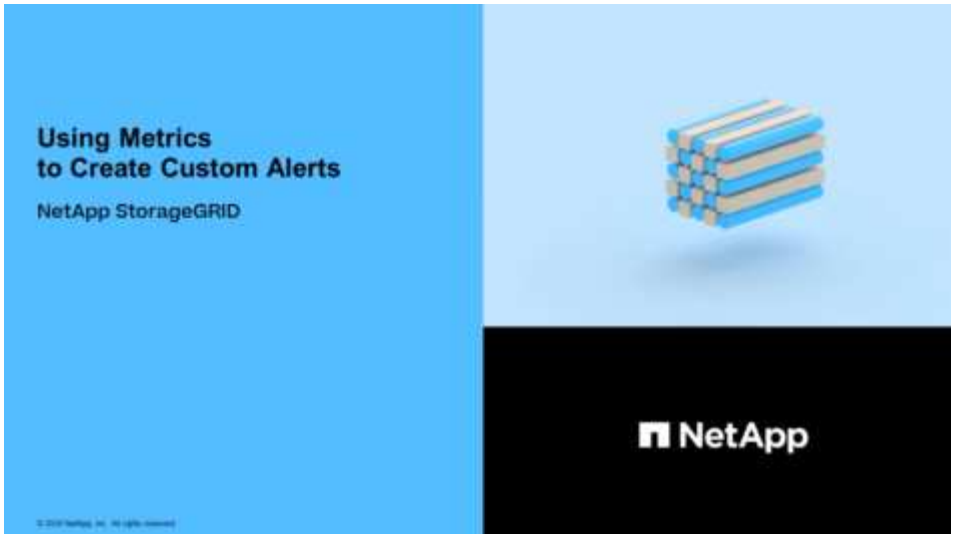
- Più avvisi dello stesso tipo sono raggruppati in un'e-mail per ridurre il numero di notifiche. Inoltre, nella pagina Avvisi vengono visualizzati più avvisi dello stesso tipo come gruppo. È possibile espandere e comprimere i gruppi di avvisi per mostrare o nascondere i singoli avvisi. Ad esempio, se 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"



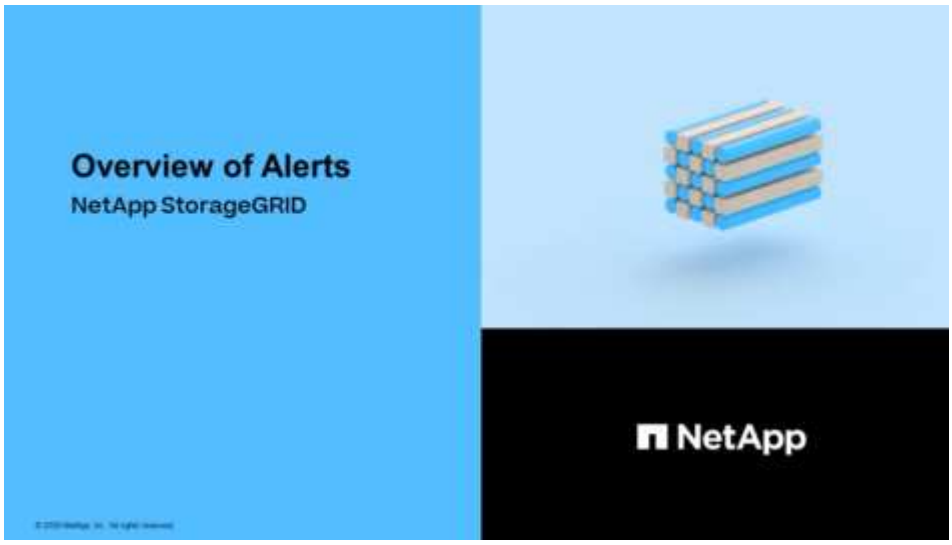
Visualizzare le regole degli avvisi

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.

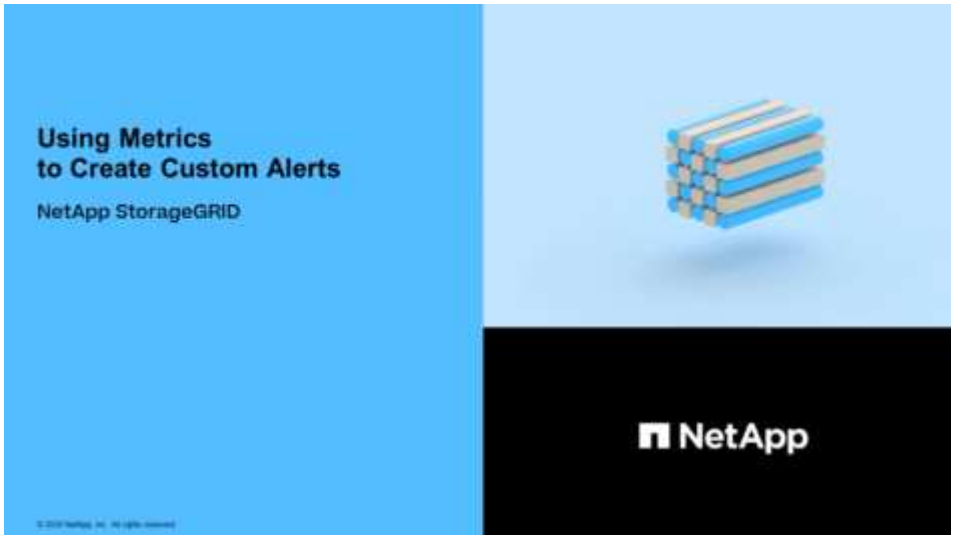
Intestazione di colonna	Descrizione
Tipo	Il tipo di regola di avviso: • **Default**: Una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificare le condizioni e la durata di una regola di avviso predefinita. Non è possibile rimuovere una regola di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

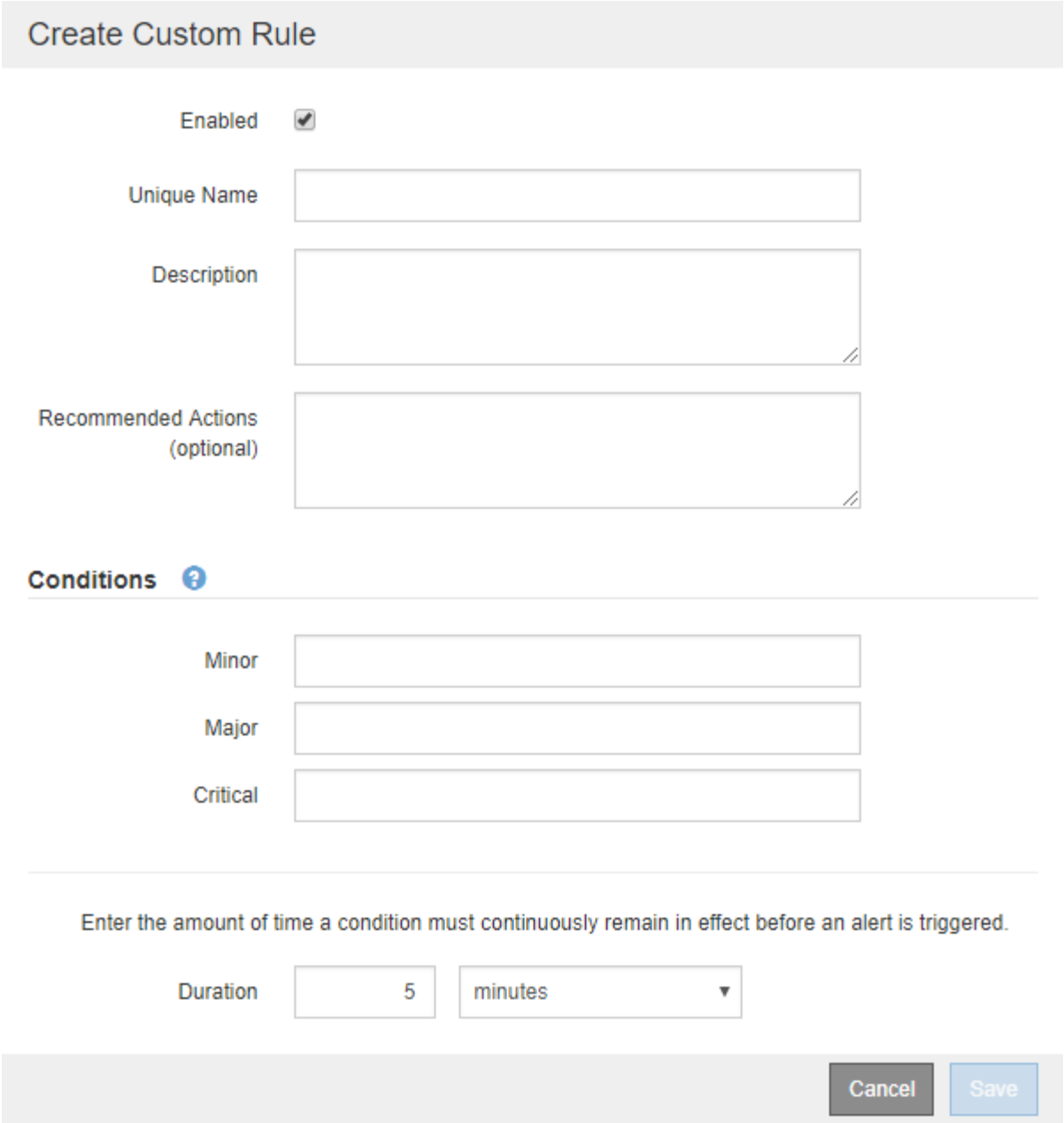
Fasi

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.

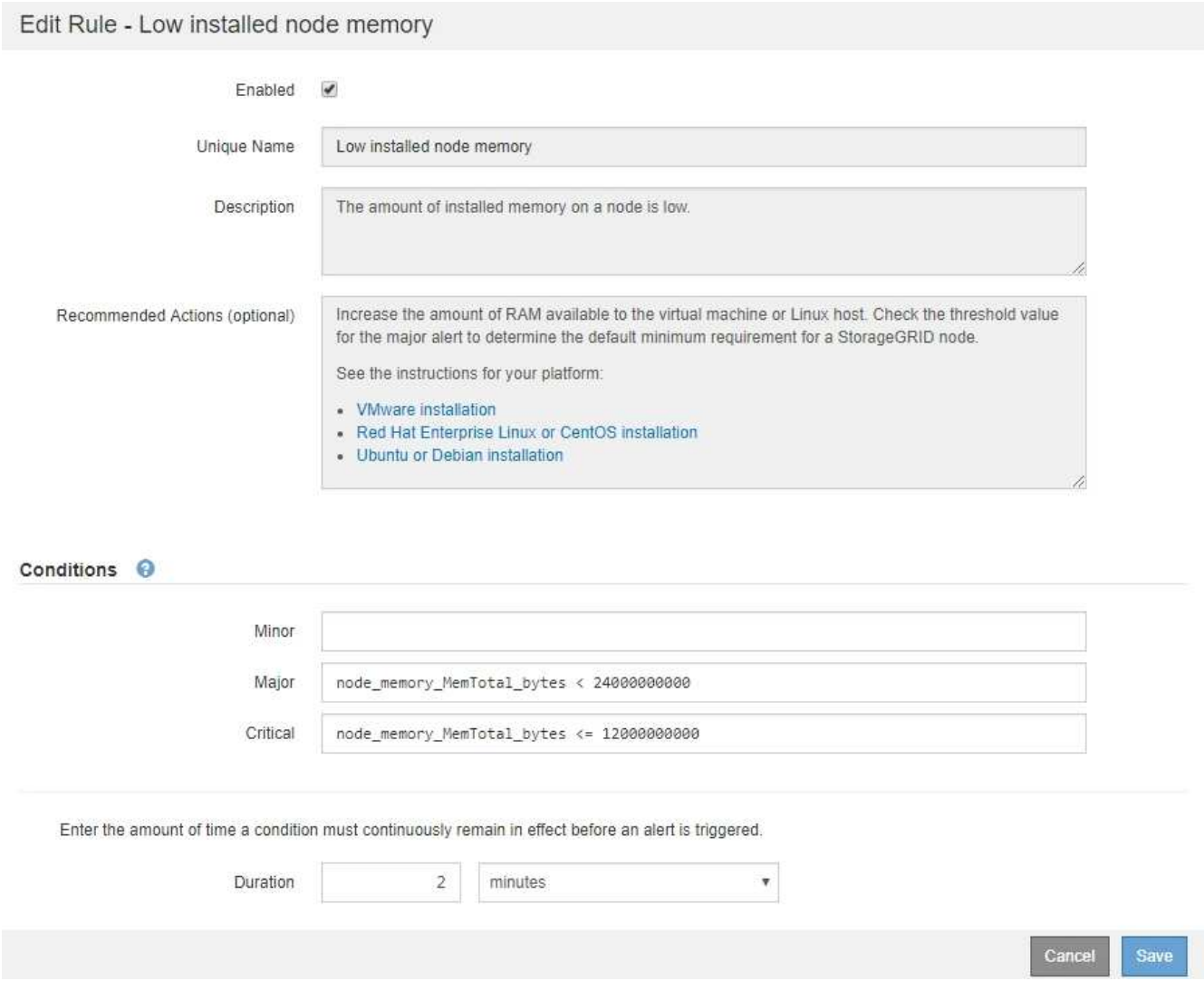
Fasi

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.

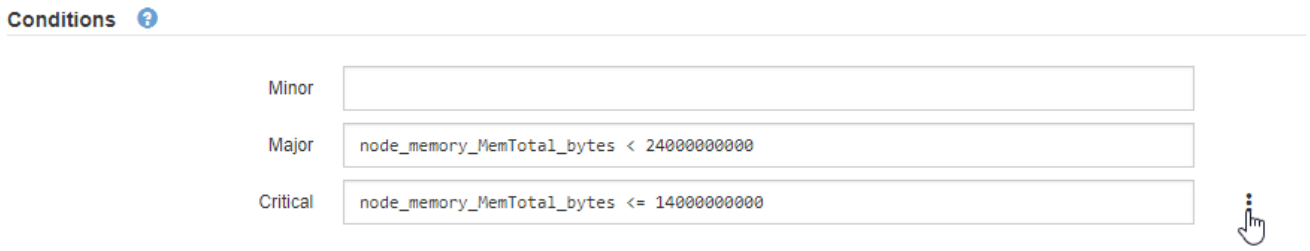
5. Per le regole di avviso personalizzate, aggiornare le seguenti informazioni secondo necessità.

   > 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

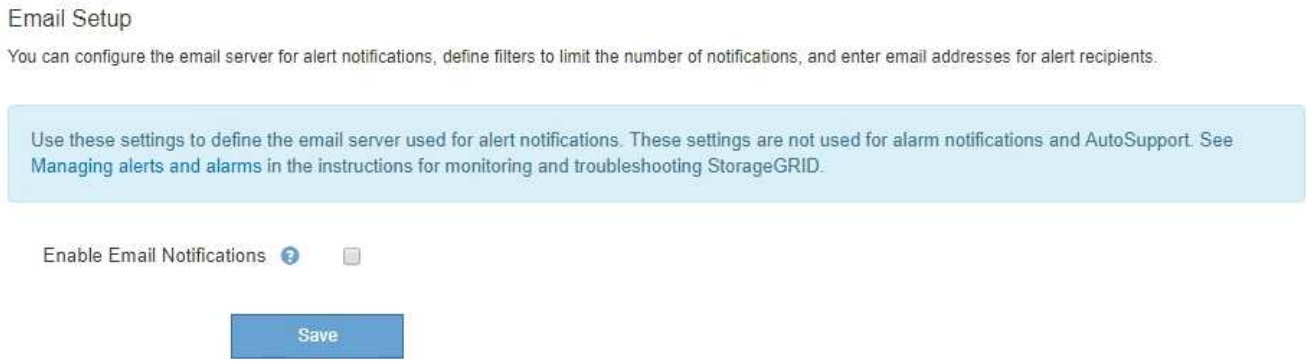
Poiché gli allarmi e gli avvisi sono sistemi indipendenti, la configurazione dell'e-mail utilizzata per le notifiche di avviso non viene utilizzata per le notifiche di allarme e i messaggi AutoSupport. Tuttavia, è possibile utilizzare lo stesso server di posta elettronica per tutte le notifiche.

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.

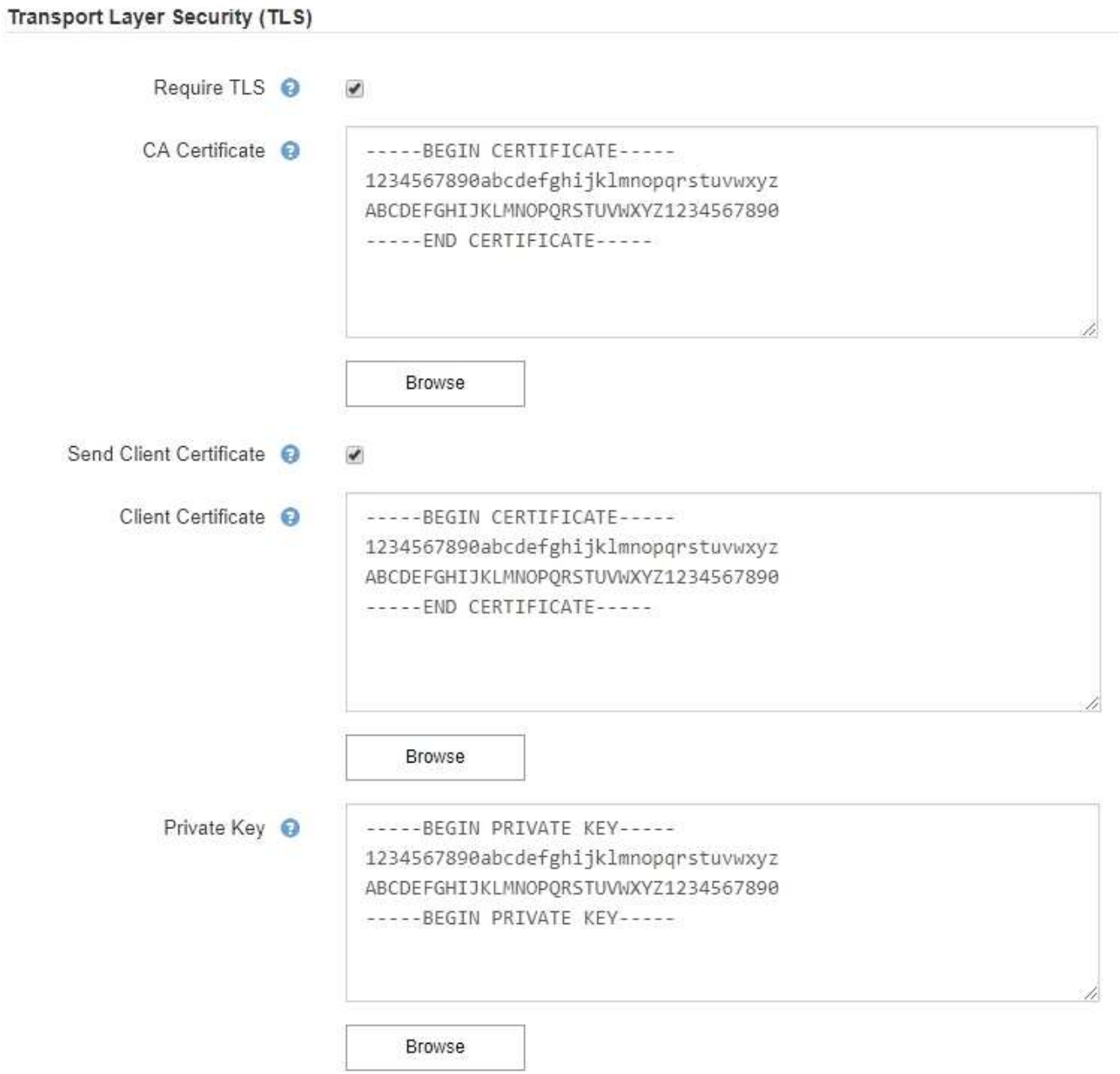
c. Nel campo **certificato client**, fornire il certificato client con codifica PEM da inviare al server SMTP.

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**.

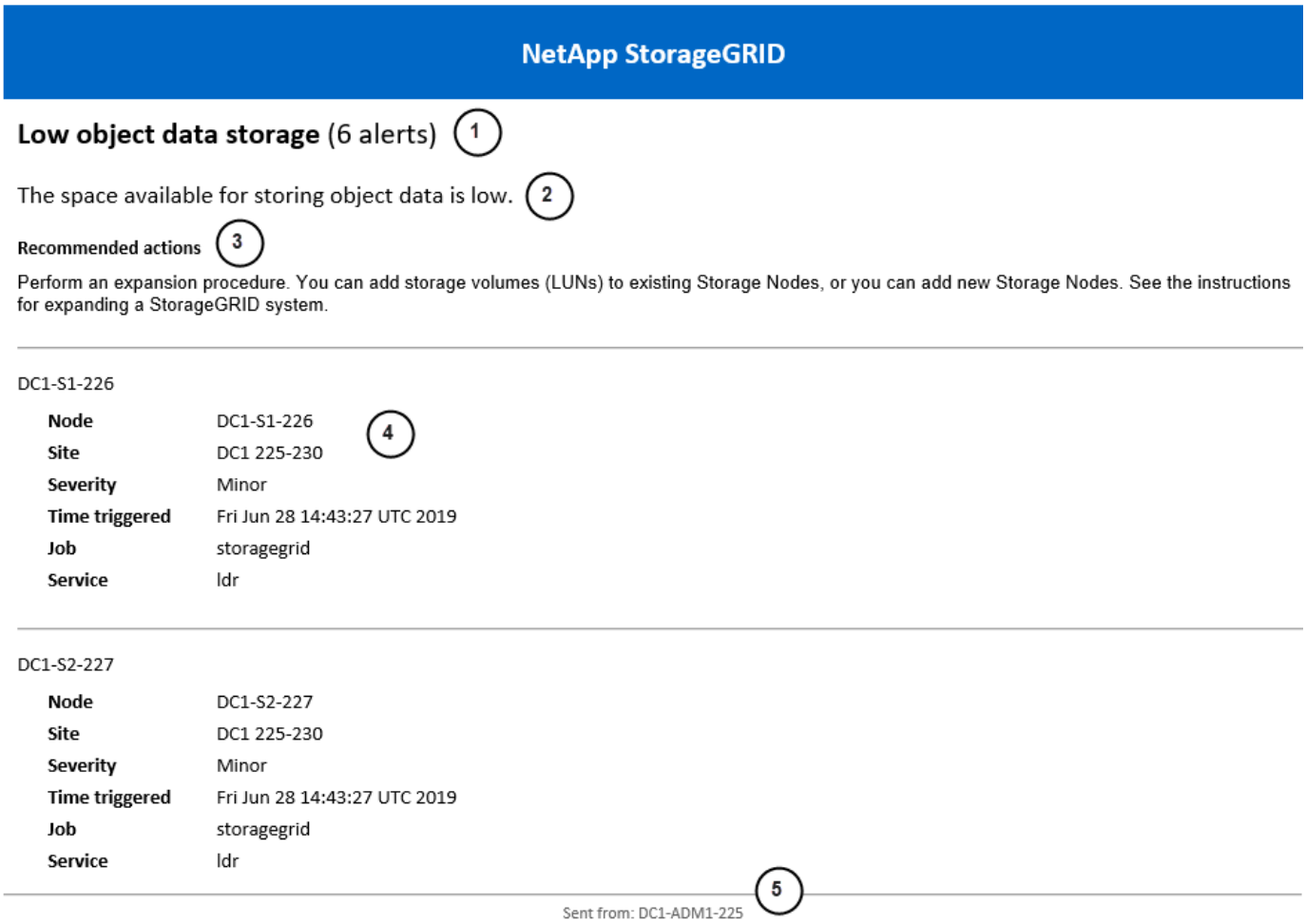
   L'invio di un'e-mail di prova non salva le impostazioni. Selezionare **Salva**.

   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.

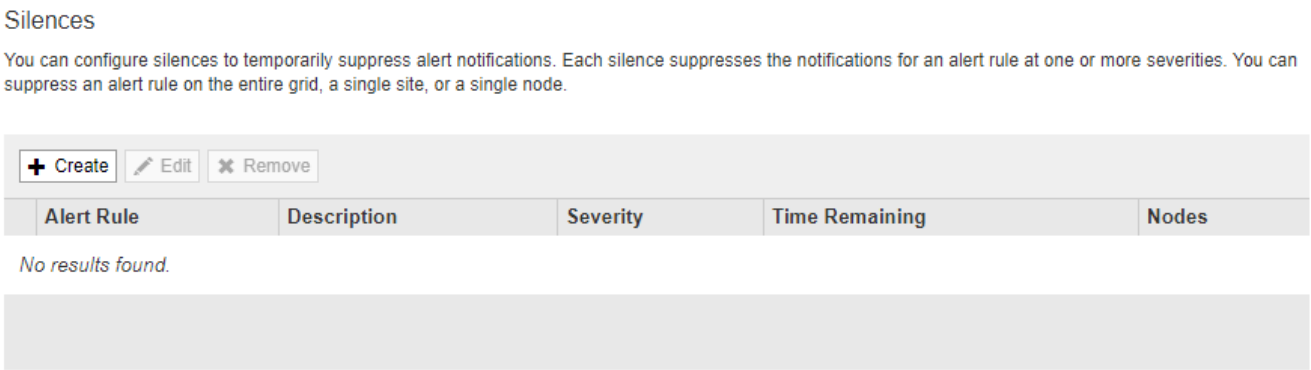
> Prestare attenzione quando si decide di tacitare una regola di avviso. Se si tacita un avviso, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

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

Fasi

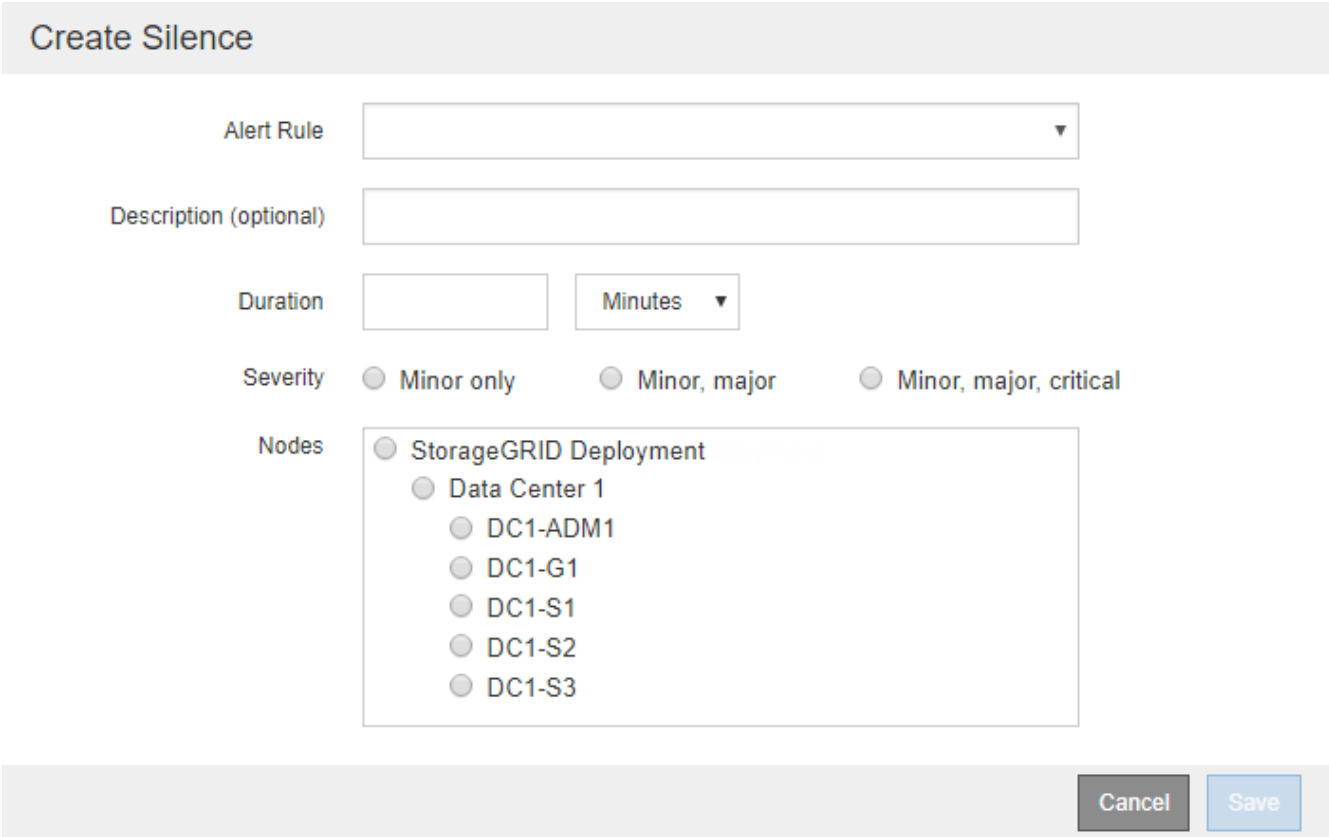
1. Selezionare **ALERTS silences**.

   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.

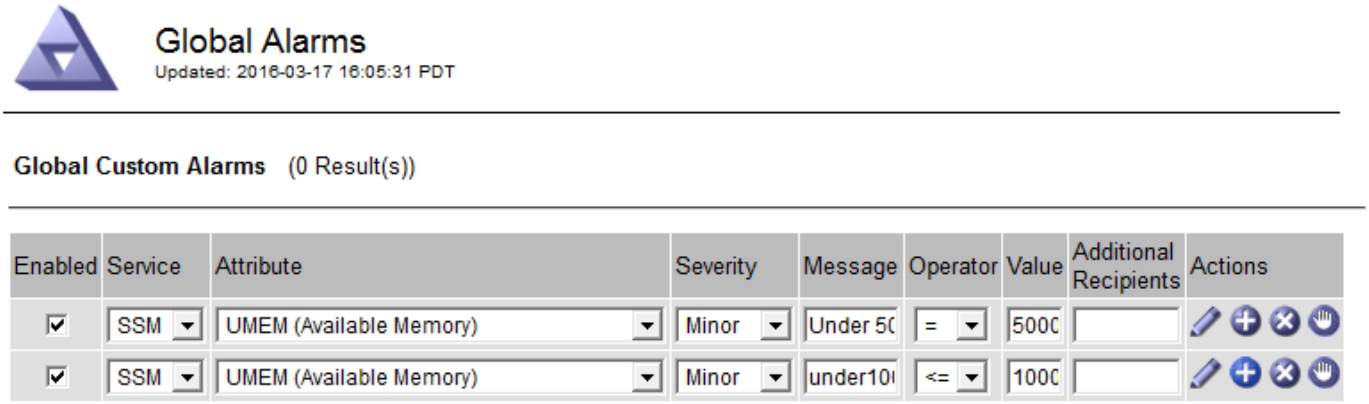
Dopo lo scenario precedente, se l'allarme Global Custom è disattivato, non cambia nulla. Il valore dell'attributo deve essere rivalutato prima che venga attivato un nuovo livello di allarme.

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.

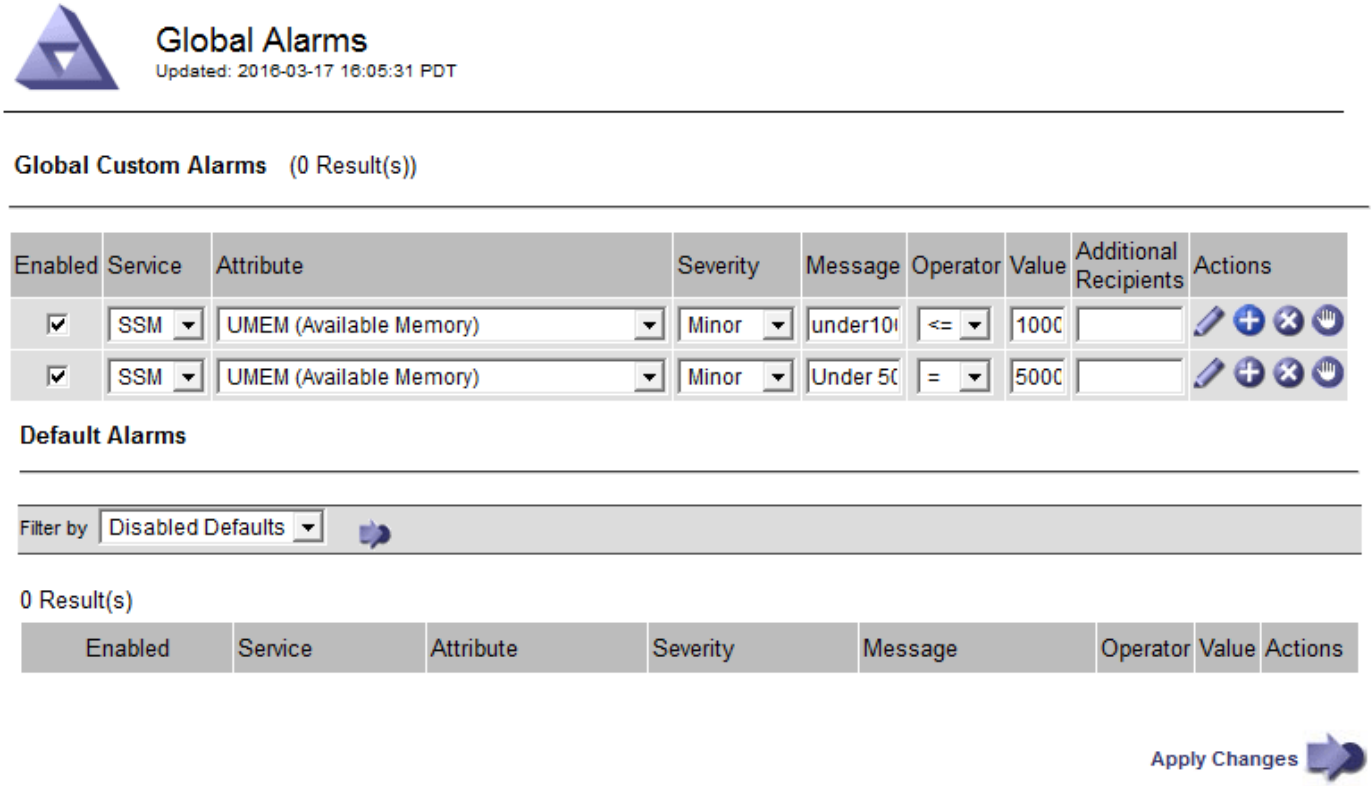
Allarmi della stessa severità

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

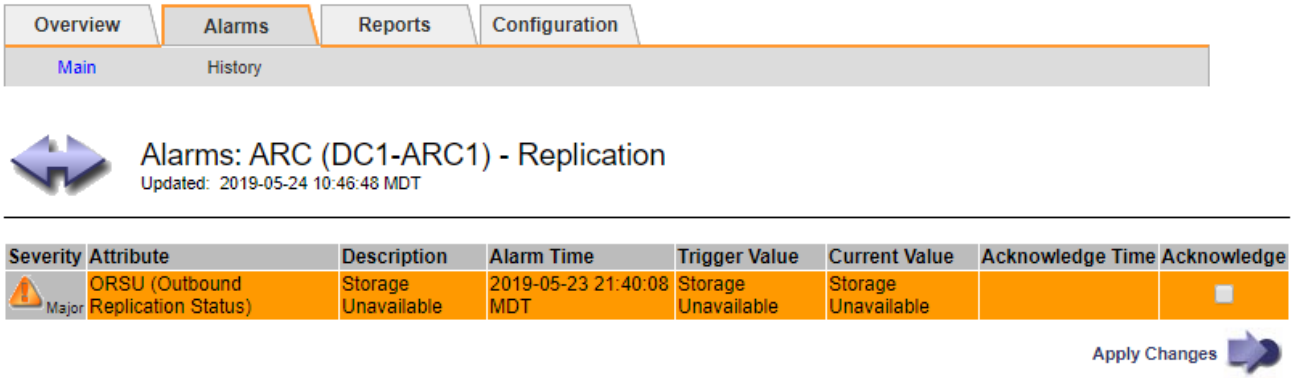
Show Acknowledged Alarms (1 - 1 of 1)

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.

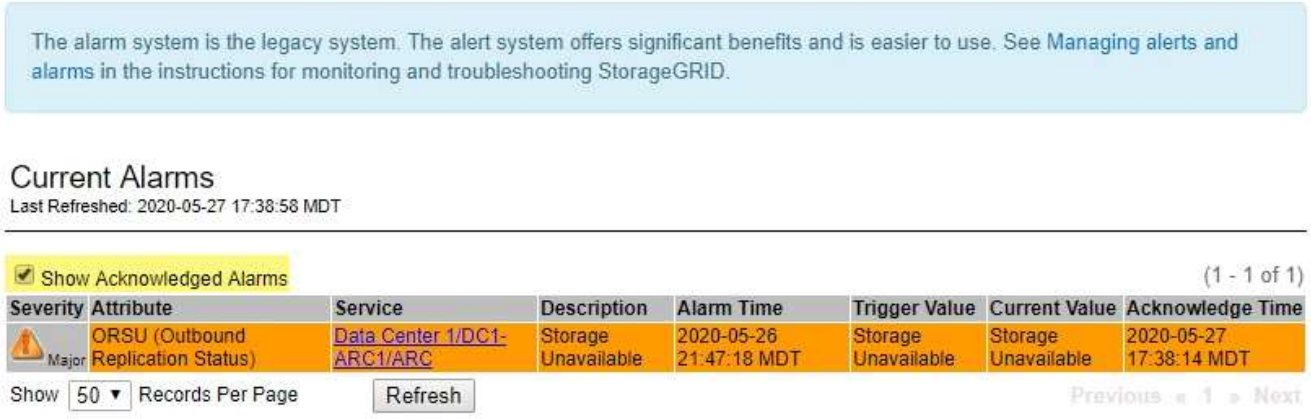
   > Quando si riconosce un allarme, la conferma non viene copiata in altri nodi di amministrazione. Per questo motivo, se si visualizza la dashboard da un altro nodo amministrativo, è possibile continuare a visualizzare l'allarme attivo.

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

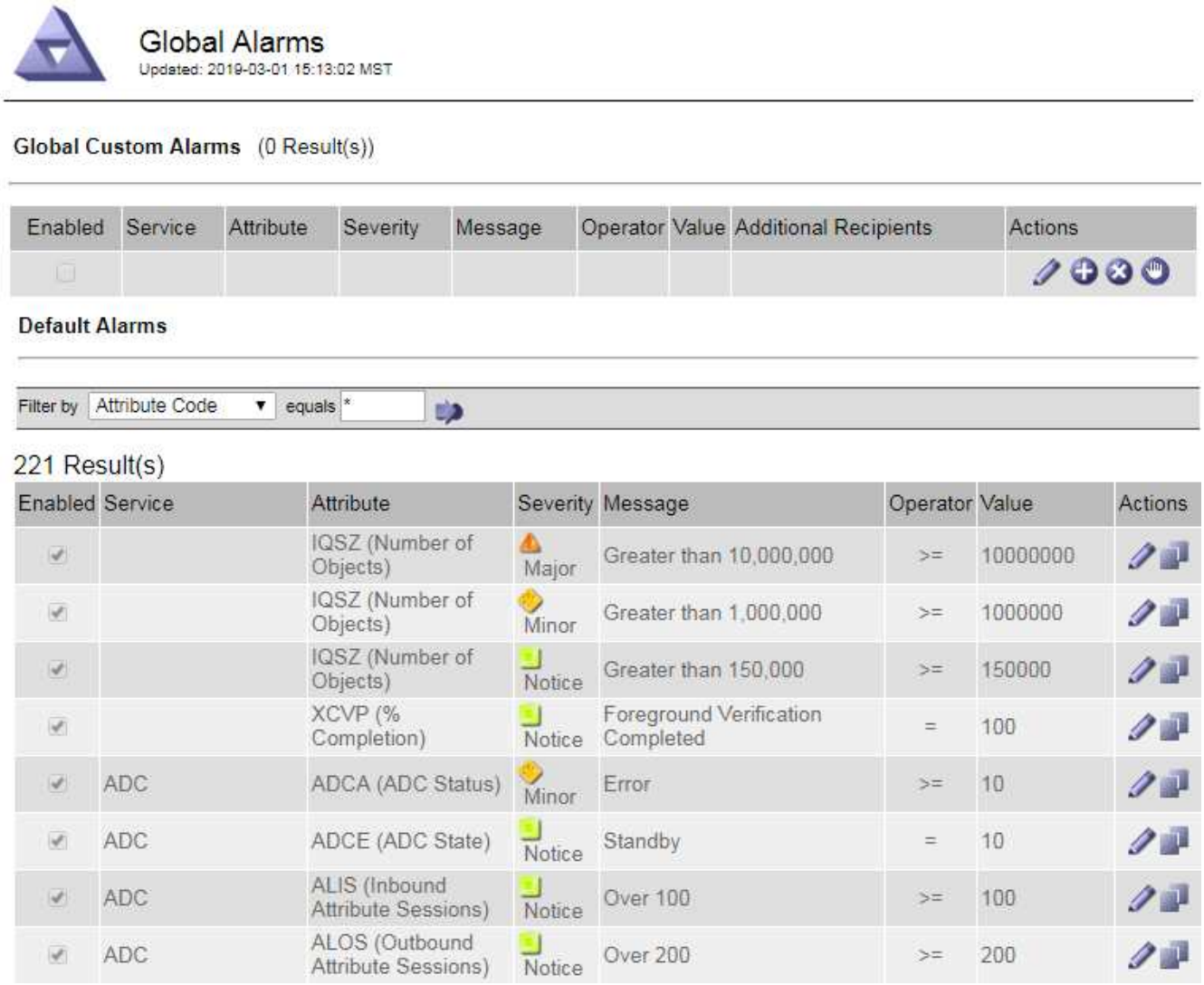
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

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.

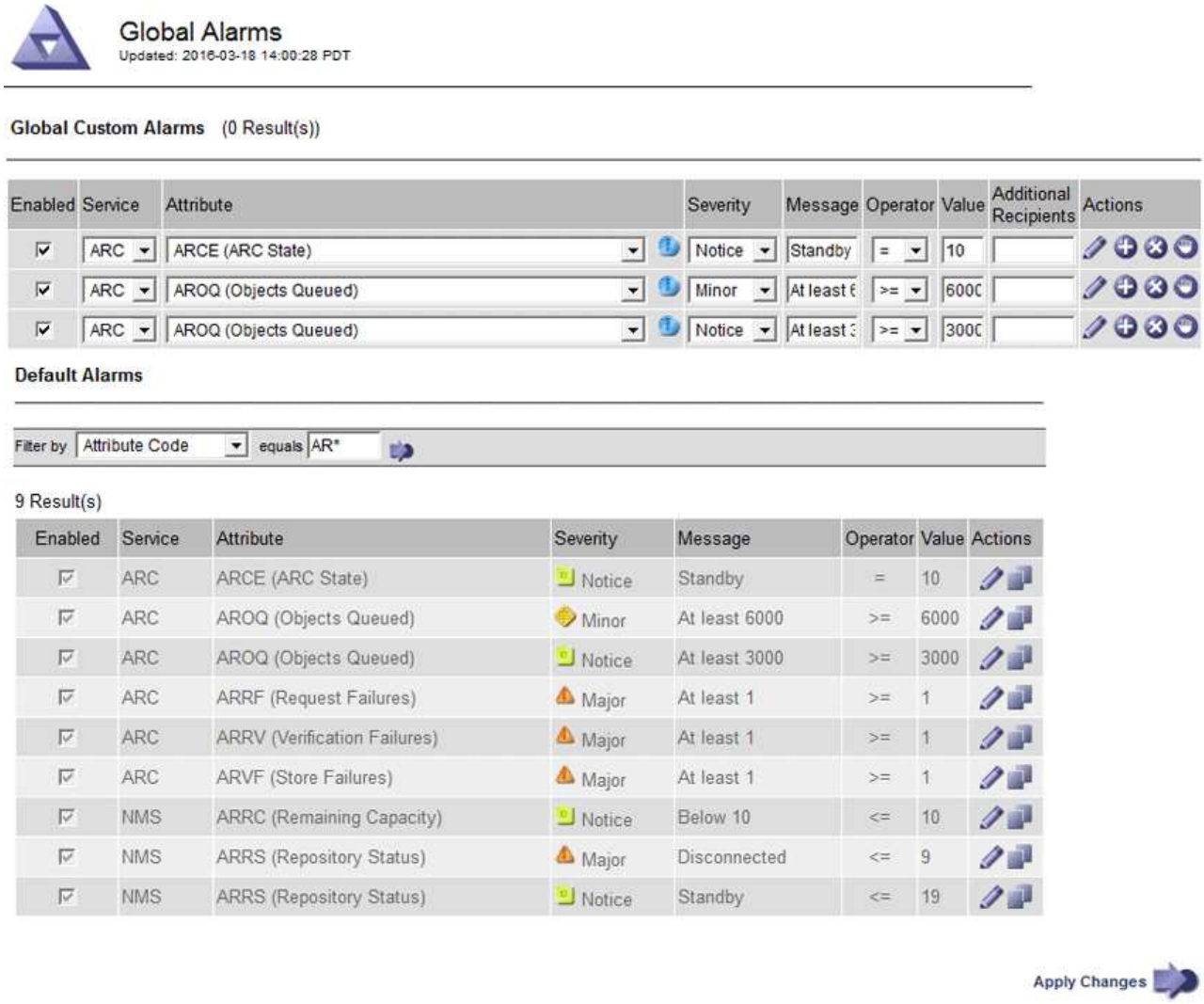
> Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

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.
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

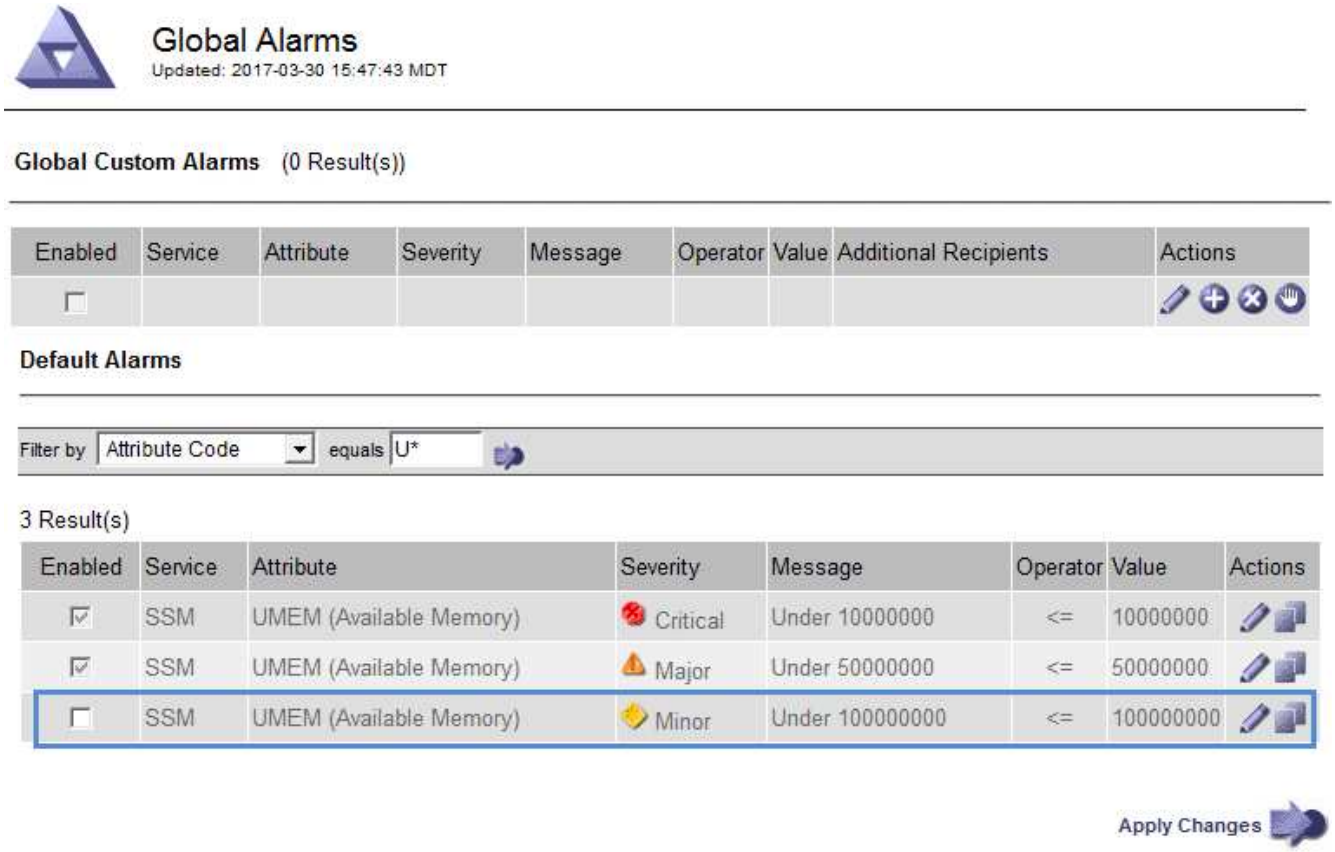
1. Selezionare **SUPPORTO Allarmi (legacy) Allarmi globali**.
2. Cercare l'allarme predefinito da disattivare.
   a. Nella sezione Allarmi predefiniti, selezionare **Filtra per Codice attributo** o **Nome attributo**.
   b. Digitare una stringa di ricerca.

      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

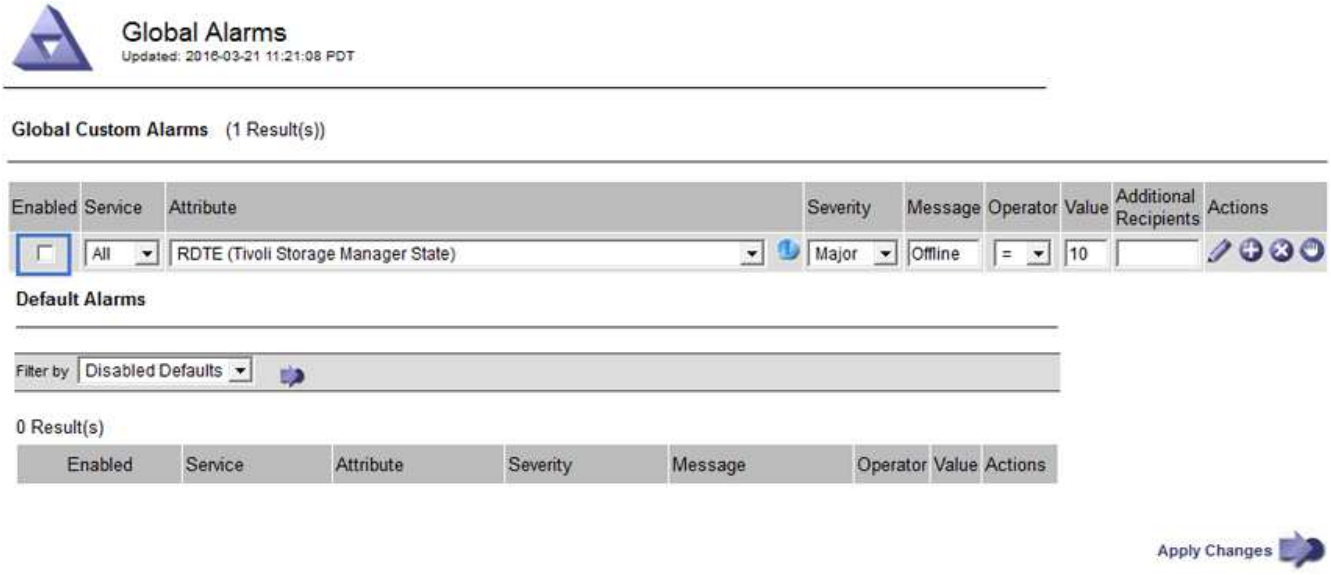
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

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.

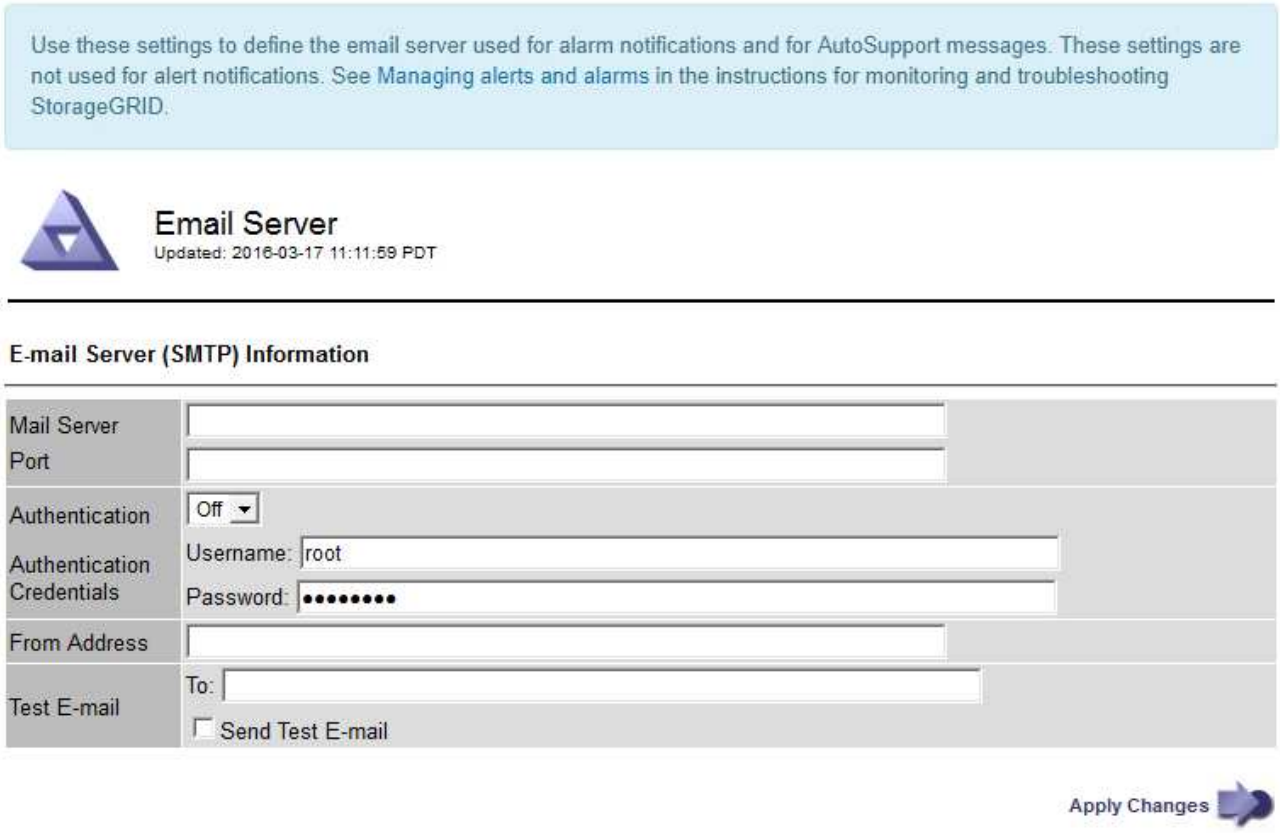
Se si utilizza SMTP come protocollo per i messaggi AutoSupport, potrebbe essere già stato configurato un server di posta SMTP. Lo stesso server SMTP viene utilizzato per le notifiche e-mail di allarme, pertanto è possibile saltare questa procedura. Vedere Istruzioni per l'amministrazione di StorageGRID.

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.
Porta	Numero di porta per accedere al server di posta SMTP.
Autenticazione	Consente l'autenticazione del server di posta SMTP. Per impostazione predefinita, l'autenticazione è disattivata.

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

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

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

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

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

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

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

Di cosa hai bisogno

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

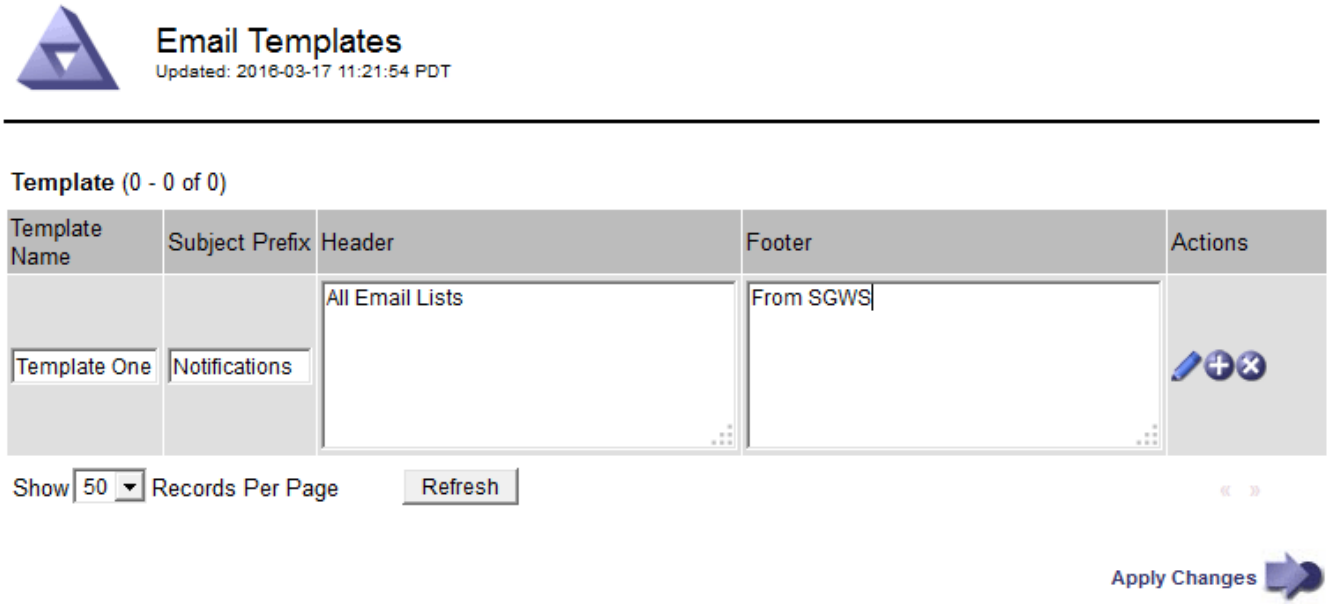
A proposito di questa attività

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

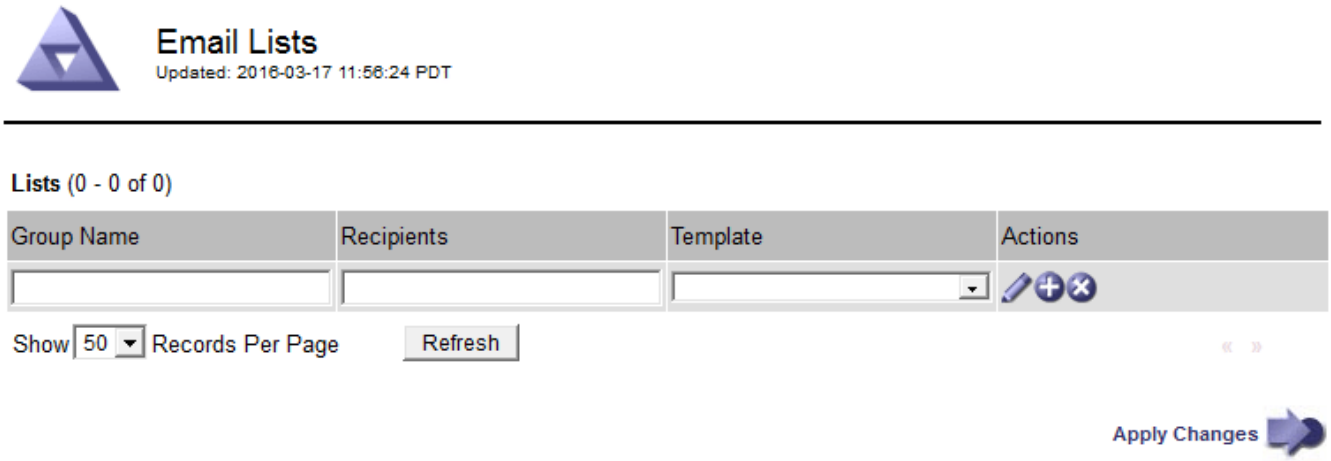
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si desidera specificare un modello e-mail per la mailing list (intestazione personalizzata, piè di pagina e oggetto), è necessario aver già creato il modello.

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.
Destinatari	Singolo indirizzo e-mail, una mailing list precedentemente configurata o un elenco di indirizzi e-mail e mailing list delimitati da virgole a cui verranno inviate le notifiche. **Nota:** se un indirizzo e-mail appartiene a più mailing list, viene inviata solo una notifica e-mail quando si verifica un evento di attivazione della notifica.

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

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

   Viene creata una nuova mailing list.

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

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

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.

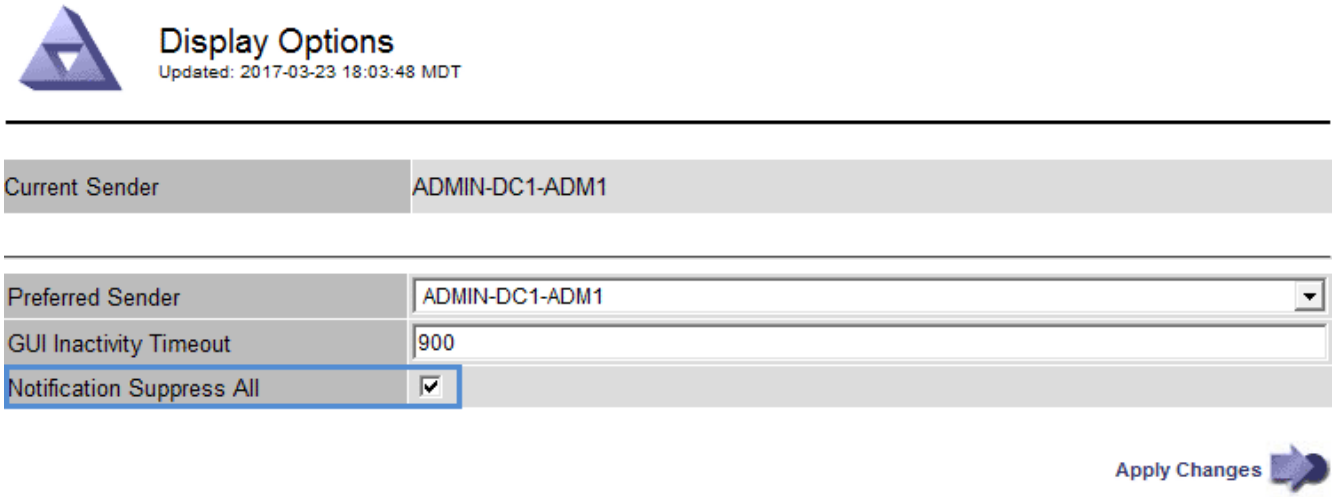
A proposito di questa attività

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.

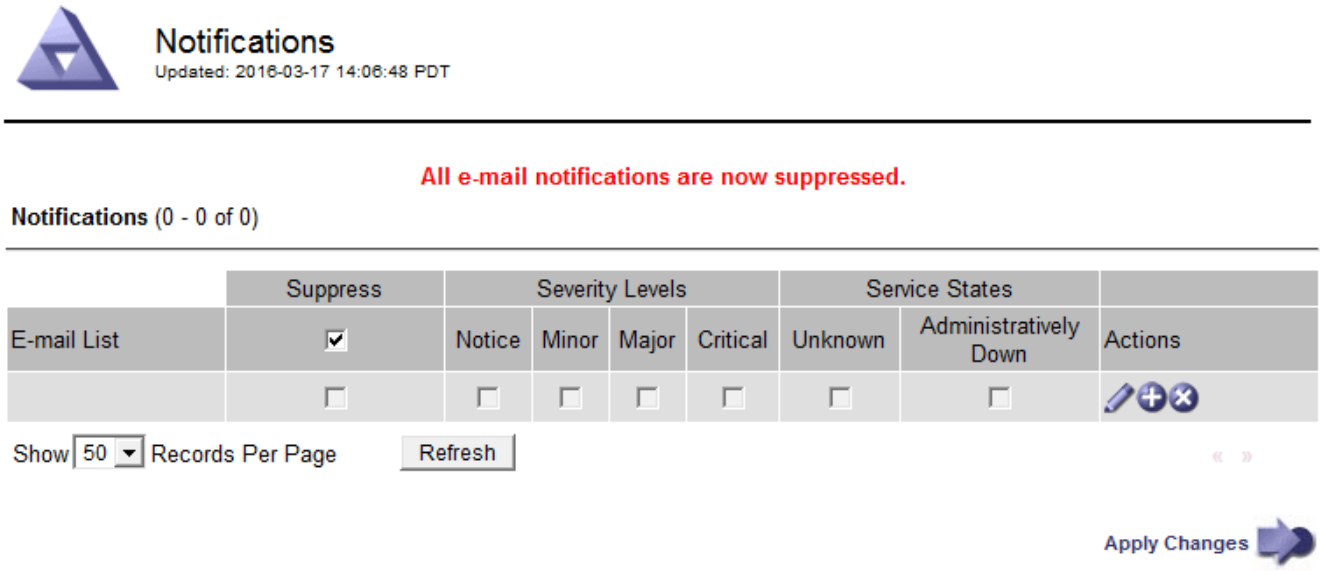
Fasi

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:

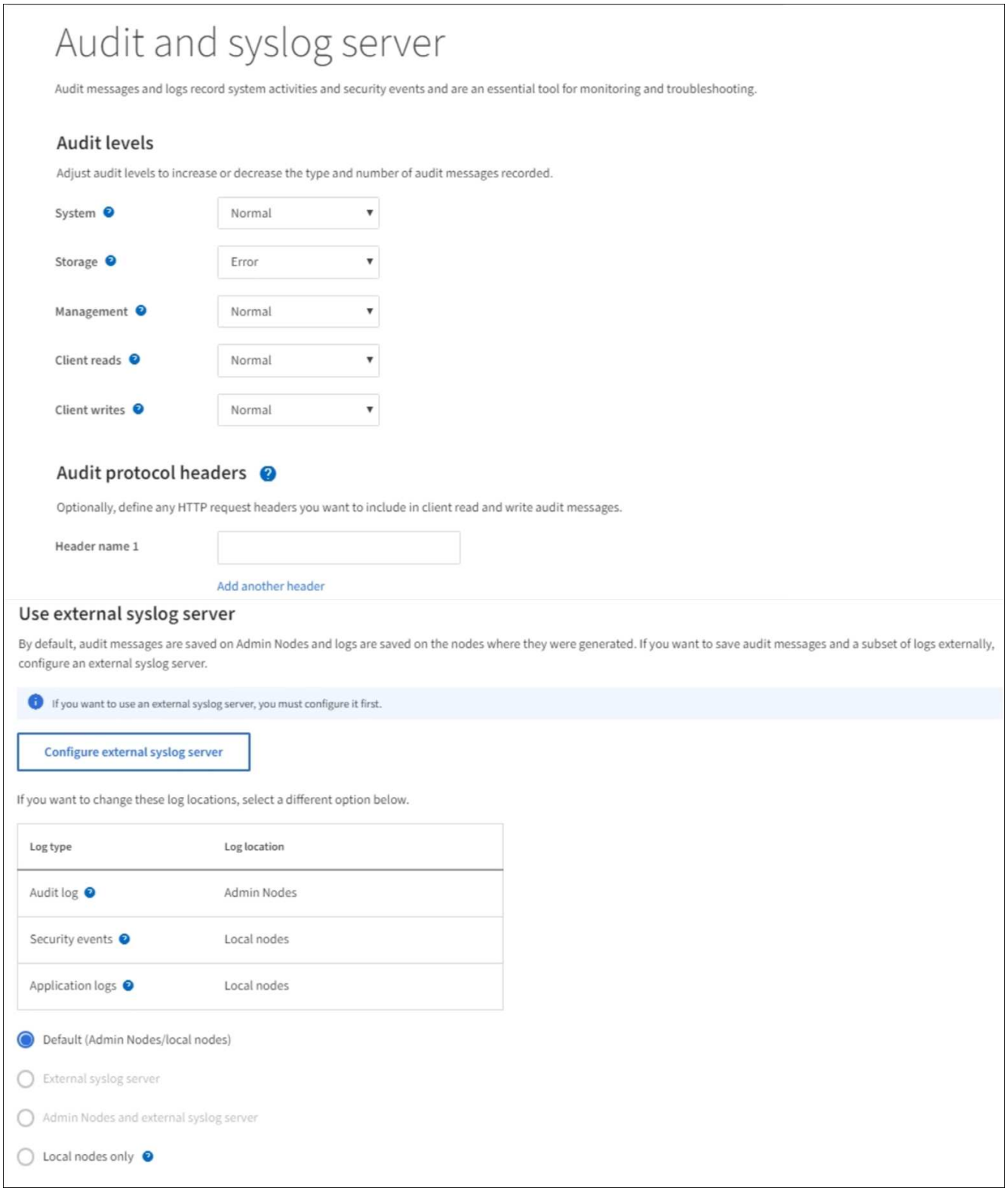
Categoria di audit	Descrizione
Sistema	Per impostazione predefinita, questo livello è impostato su normale. Vedere Messaggi di audit del sistema.
Storage	Per impostazione predefinita, questo livello è impostato su Error (errore). Vedere Messaggi di audit dello storage a oggetti.
Gestione	Per impostazione 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 $0 \leq P \leq 1$ (quindi per un carico di lavoro PUT del 100%, P = 1 e per un carico DI lavoro GET del 100%, P = 0).

Sia K la dimensione media della somma dei nomi 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.

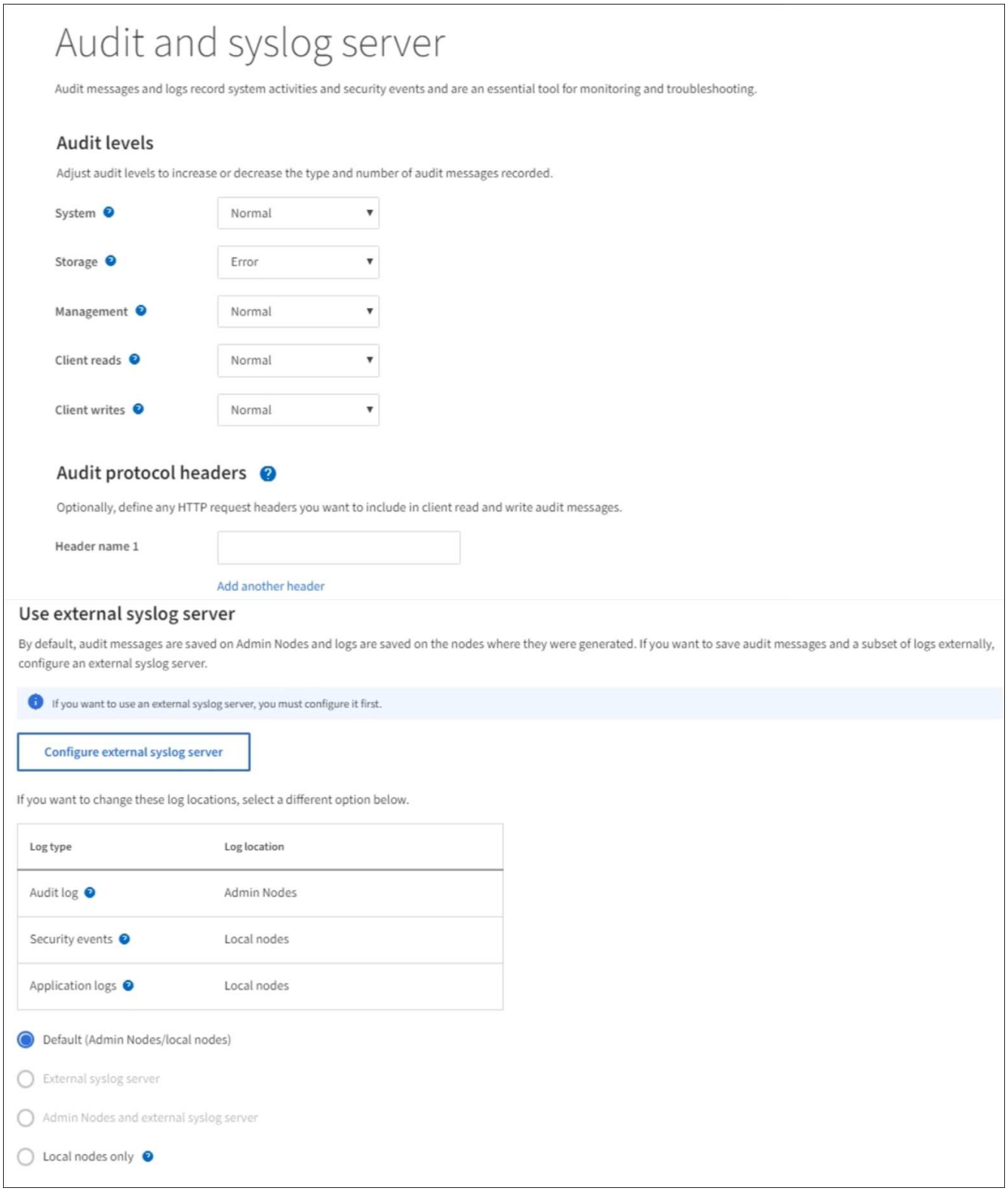
> Per massimizzare le opzioni per il ripristino completo dei dati in caso di guasto del server syslog esterno, su ciascun nodo vengono mantenuti fino a 20 GB di registri locali dei record di controllo (localaudit.log).

> 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

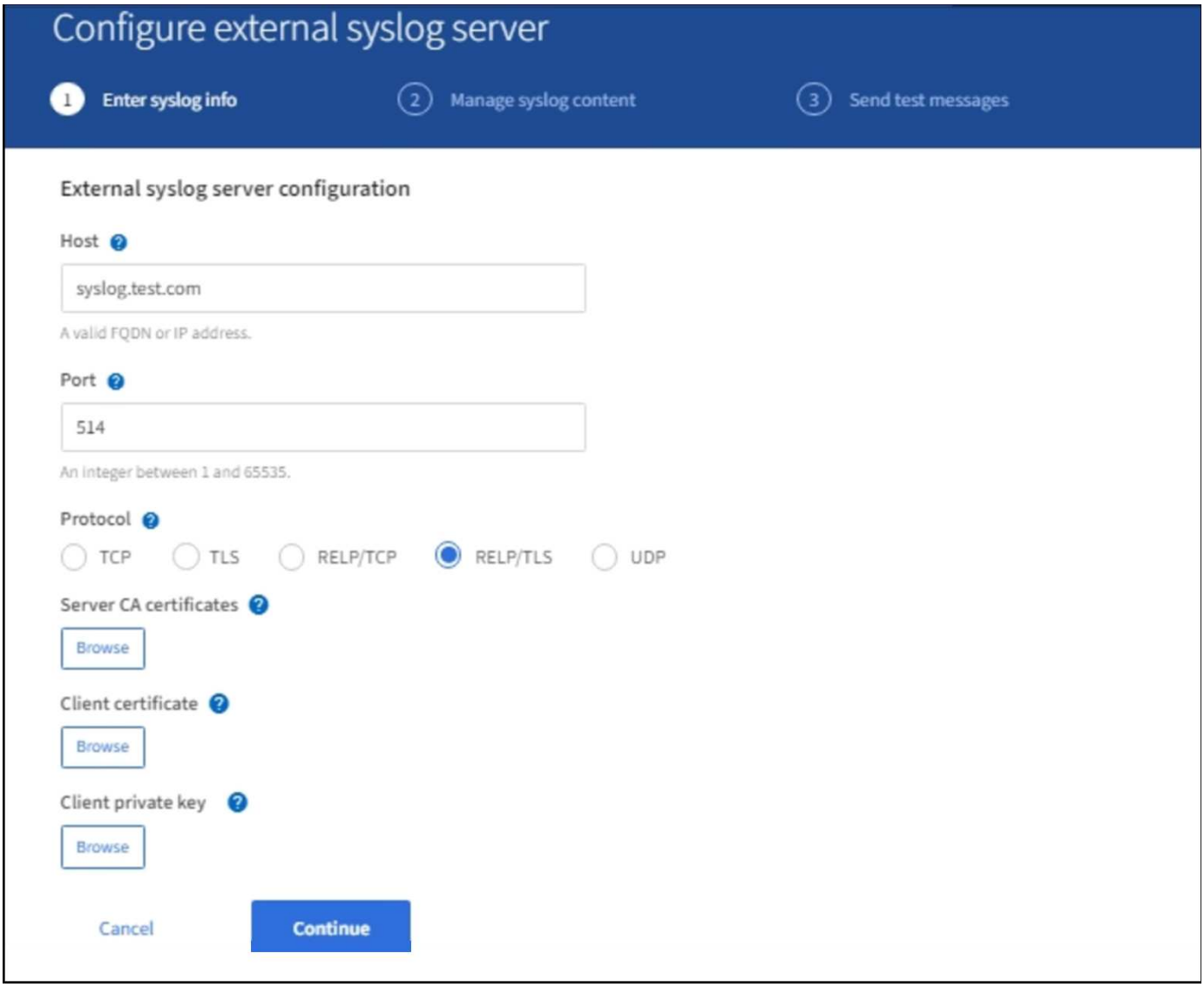
Fasi

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.

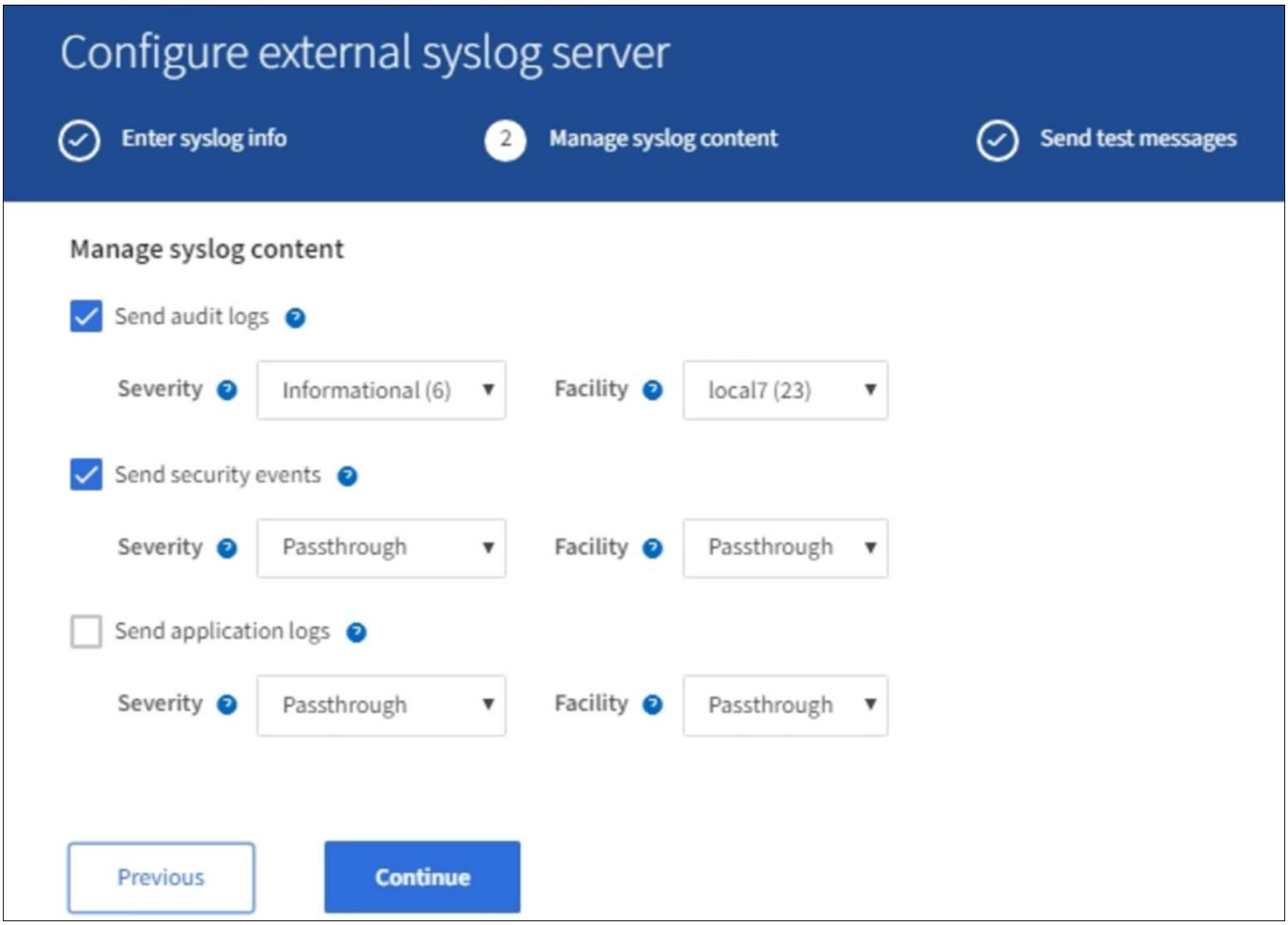
4. Selezionare **continua**.
5. se si seleziona **TLS** o **RELP/TLS**, caricare i seguenti certificati:
   - **Certificati CA del server**: Uno o più certificati CA attendibili per la verifica del server syslog esterno (con codifica PEM). Se omesso, verrà utilizzato il certificato Grid CA predefinito. 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.

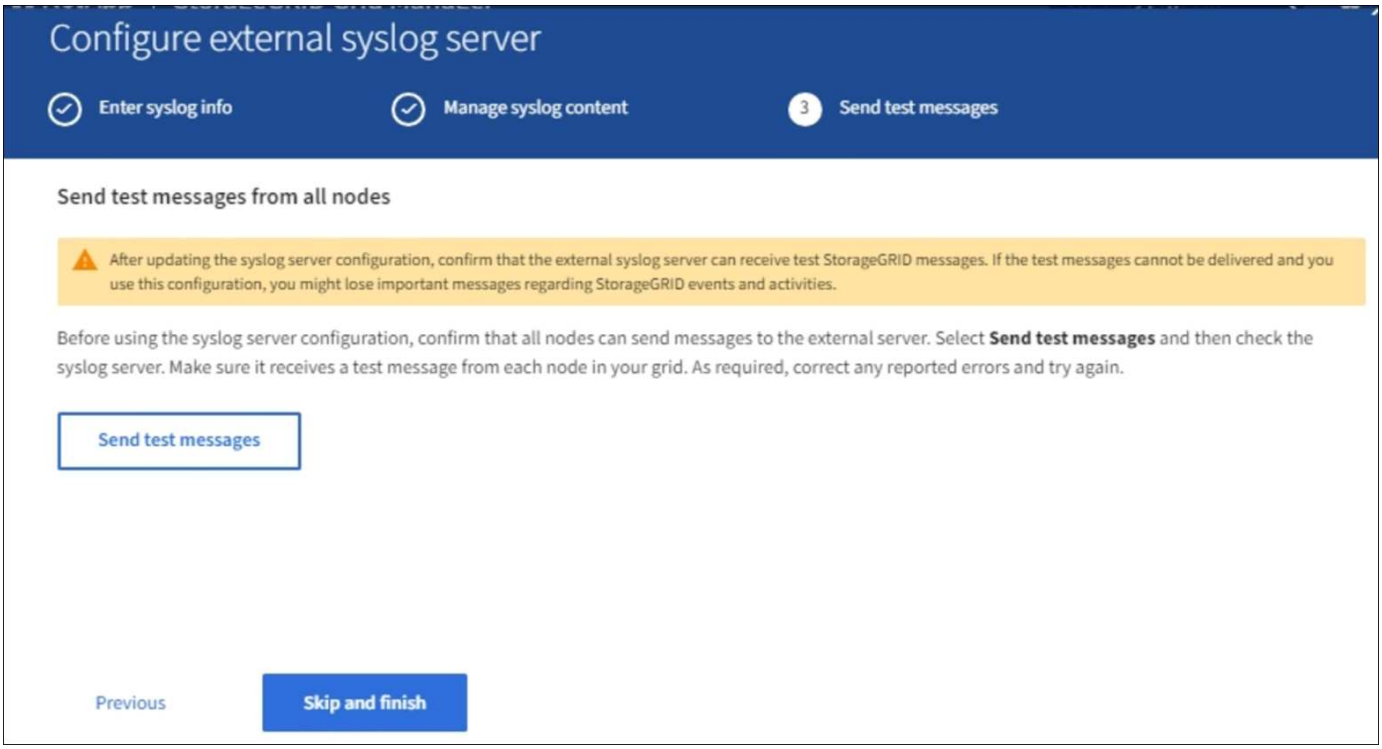
   Il valore selezionato verrà applicato a tutti i messaggi di questo tipo. Le informazioni relative alle diverse strutture andranno perse quando si sceglie di eseguire l'override della struttura con un valore fisso.

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.

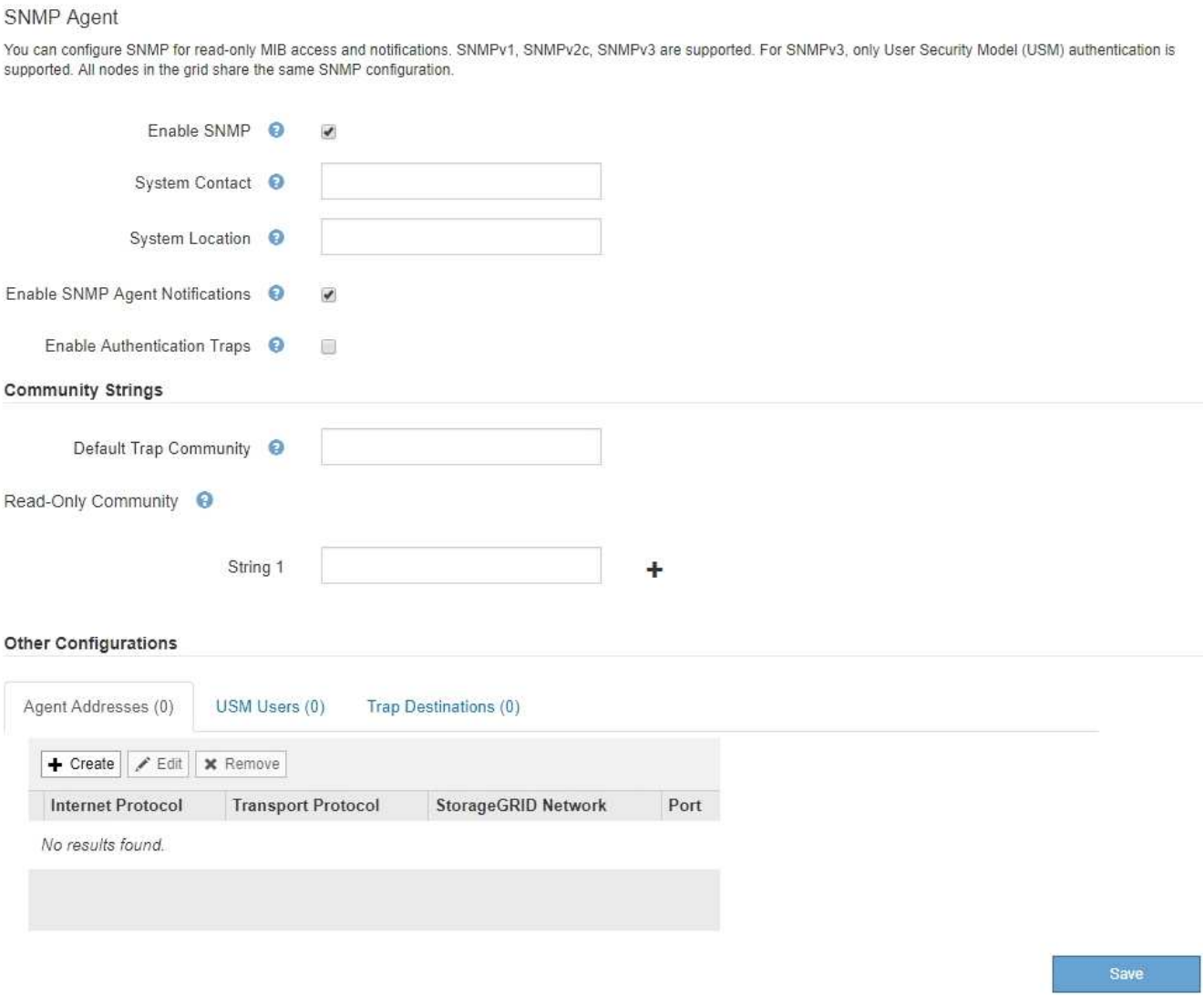
Fasi

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.

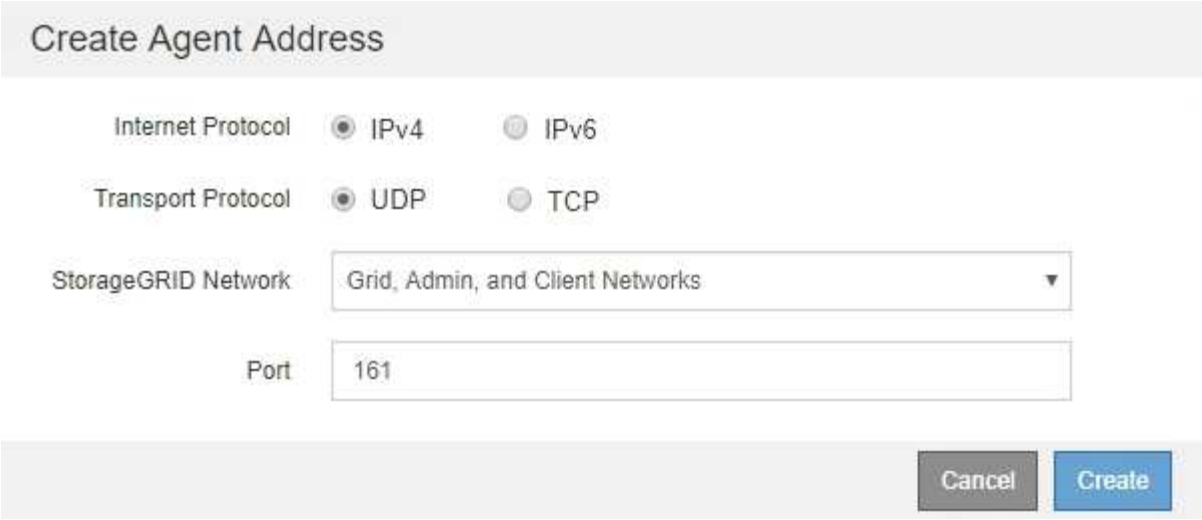
8. Facoltativamente, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

   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.

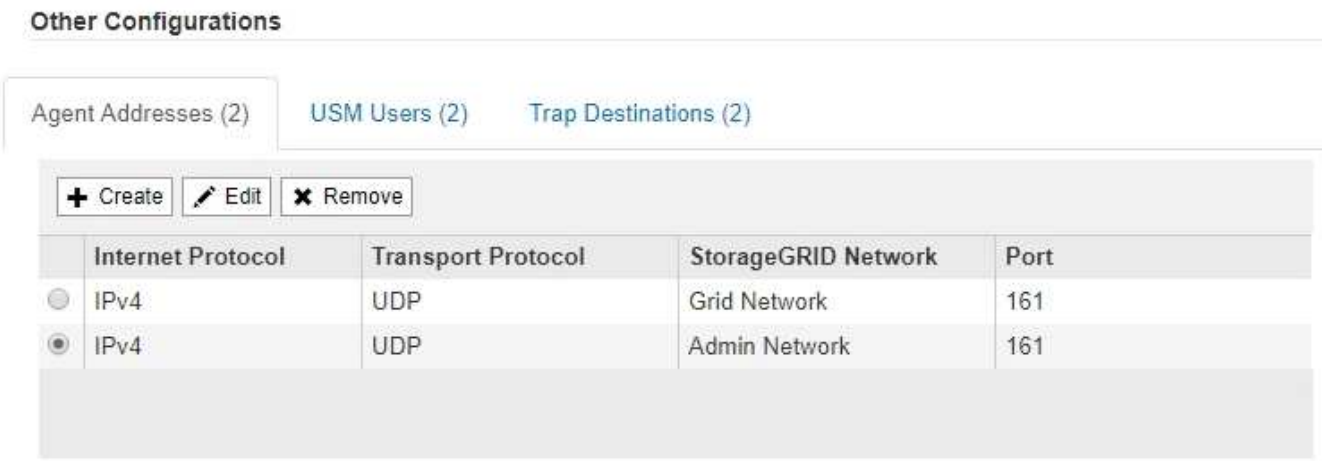
e. Nel campo **Port** (porta), immettere il numero di porta su cui l'agente SNMP deve rimanere in attesa.

   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.



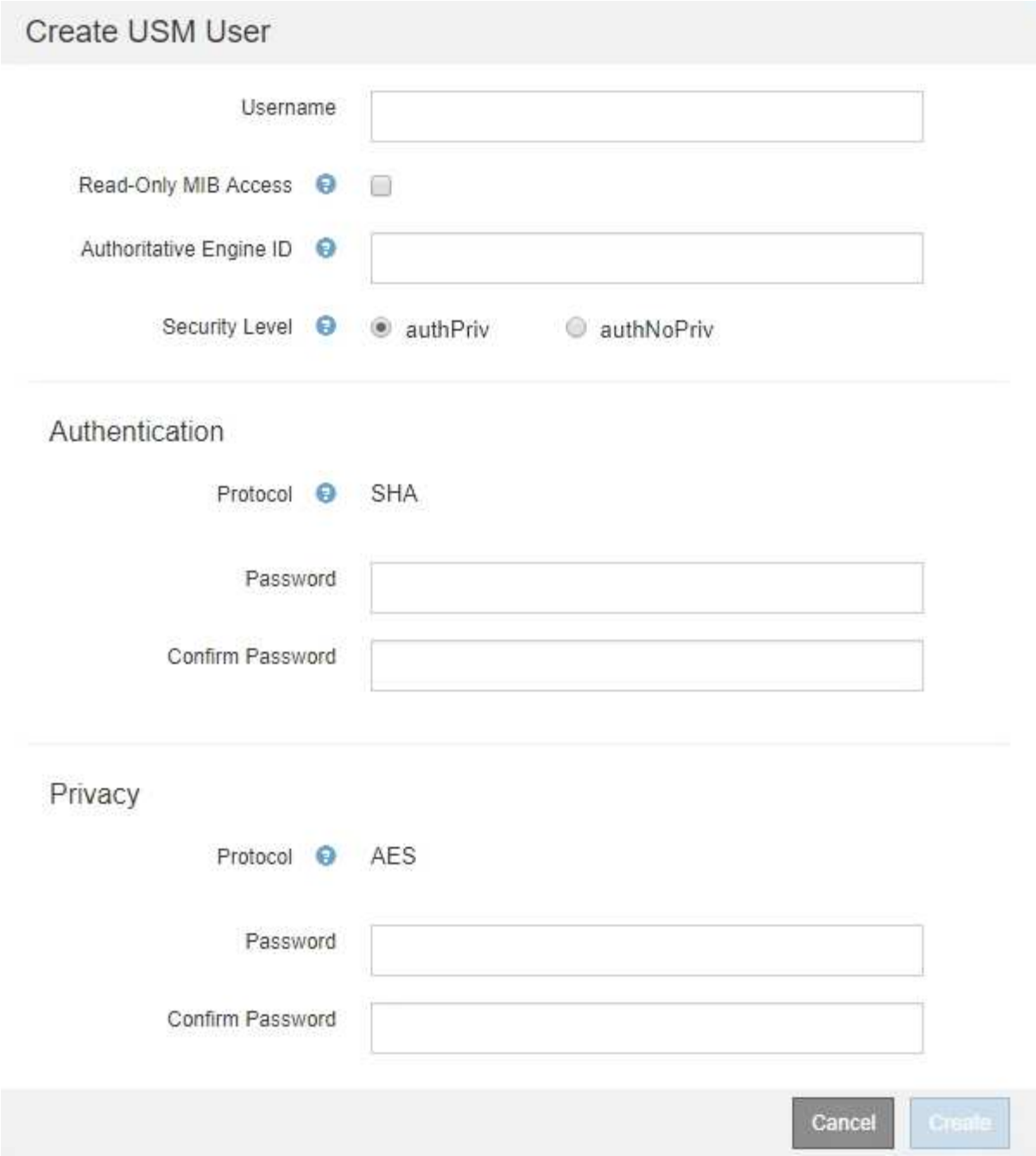
9. Se si utilizza SNMPv3, selezionare la scheda utenti USM nella sezione altre configurazioni.

   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.

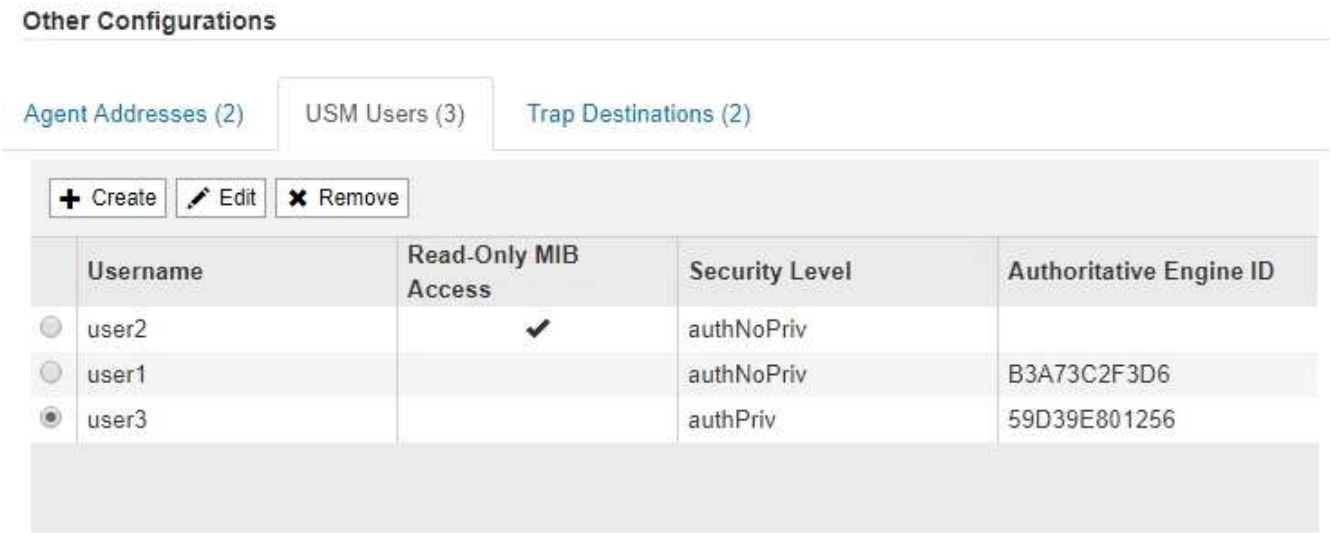
> L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).

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.

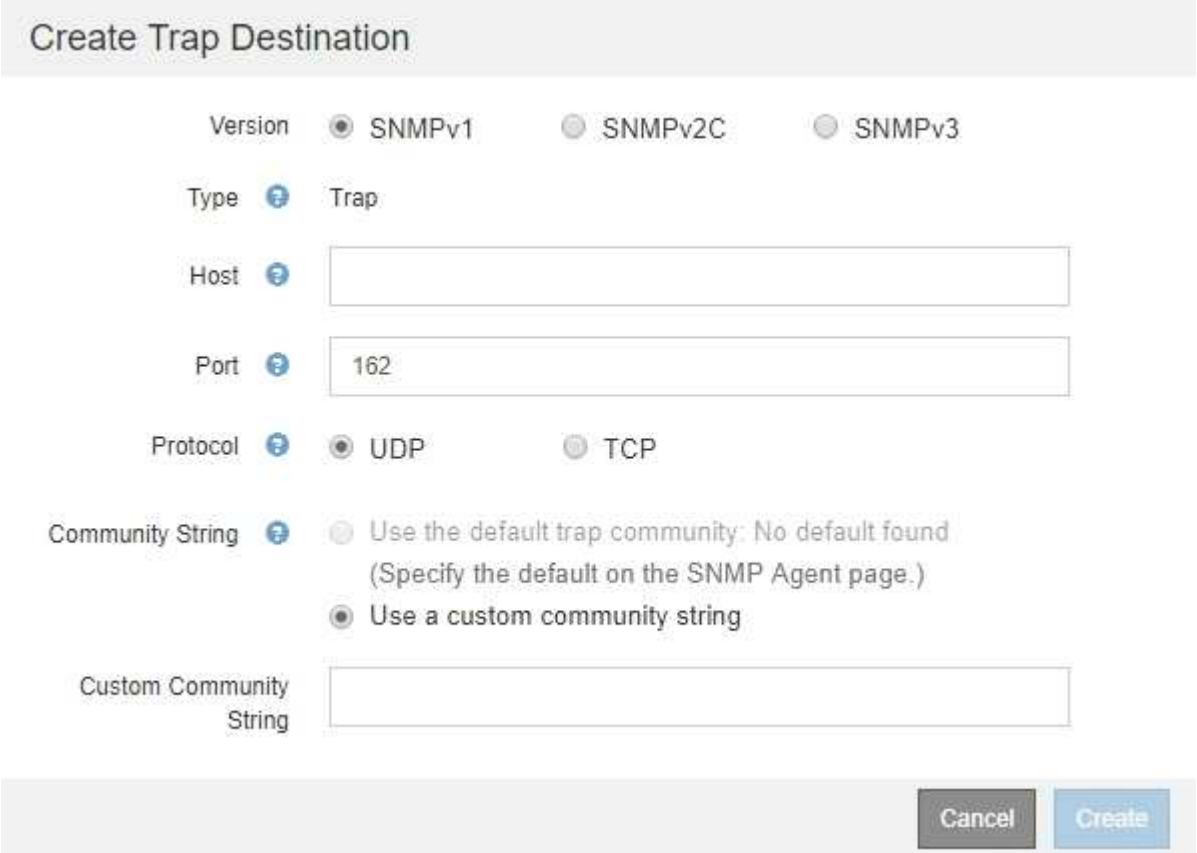


10. nella sezione Other Configurations (altre configurazioni), selezionare la scheda Trap Destinations (Destinazioni trap).

    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.

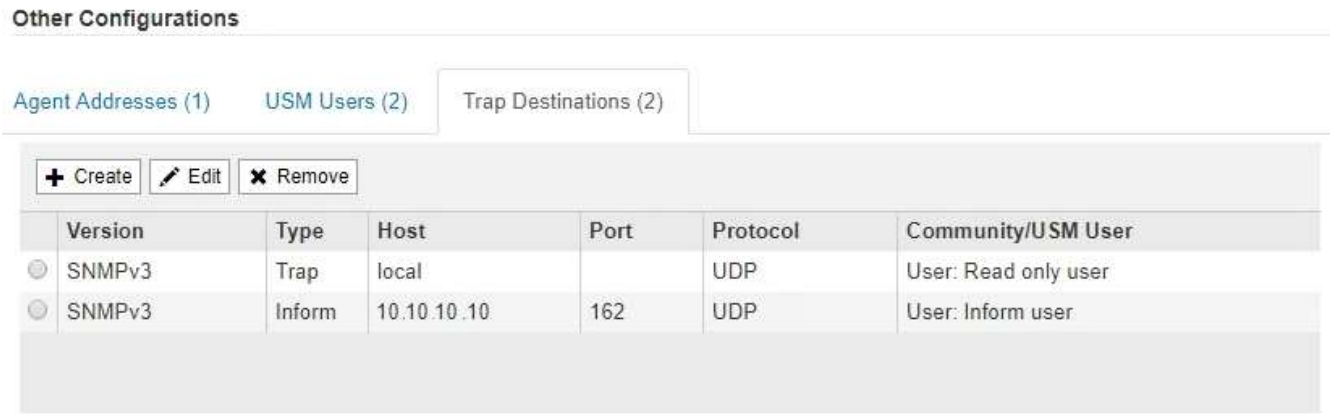
c. Completare il modulo in base alla versione selezionata

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.

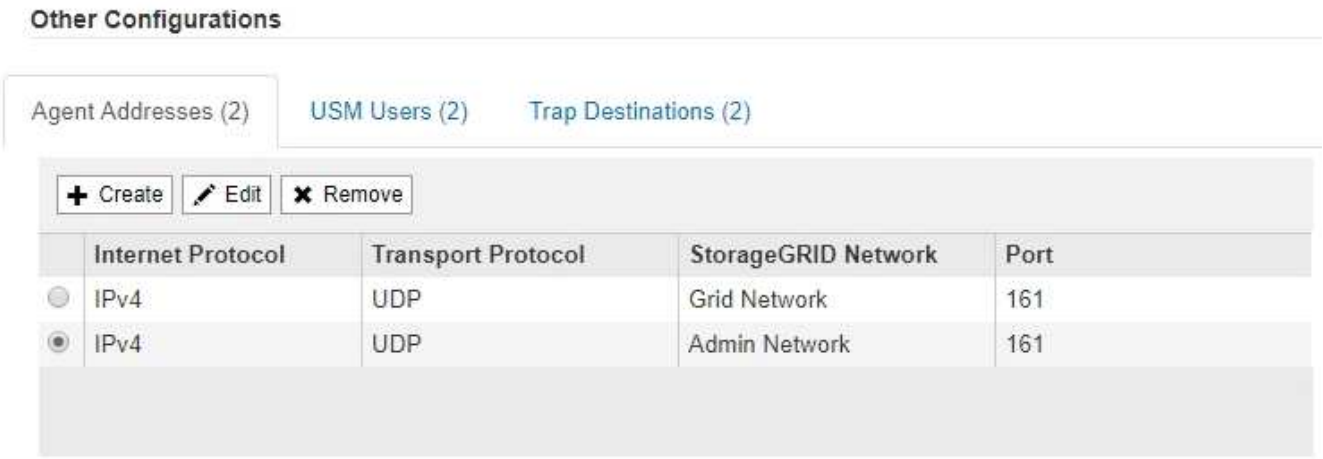
   Se questa casella di controllo non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.

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.

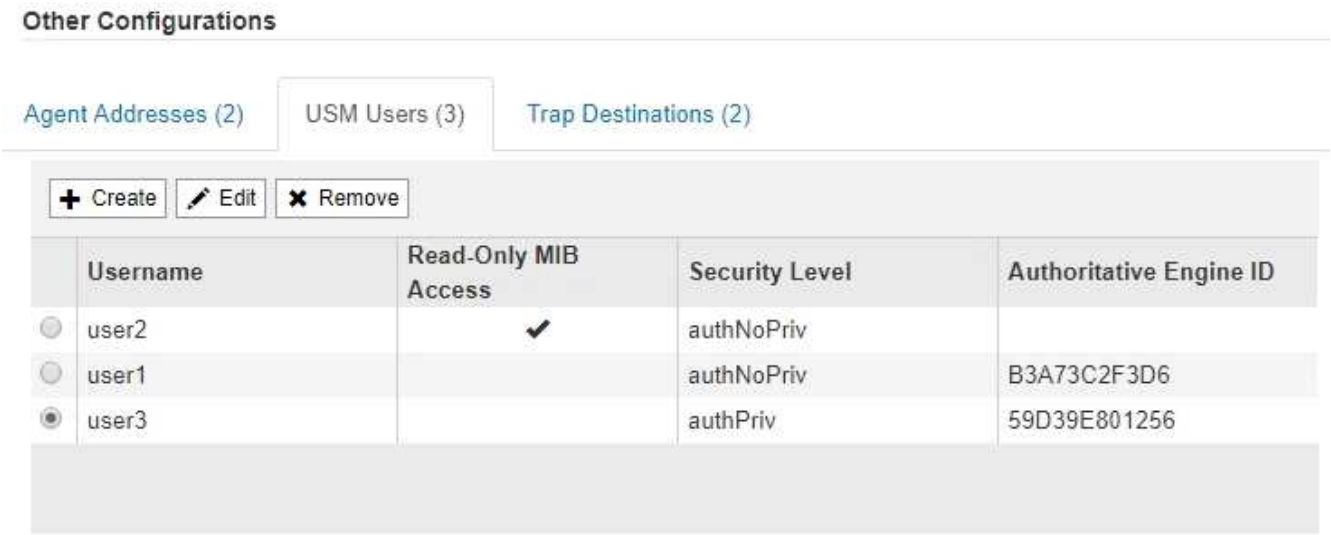
7. Se si desidera aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agenti nella sezione altre configurazioni.



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.

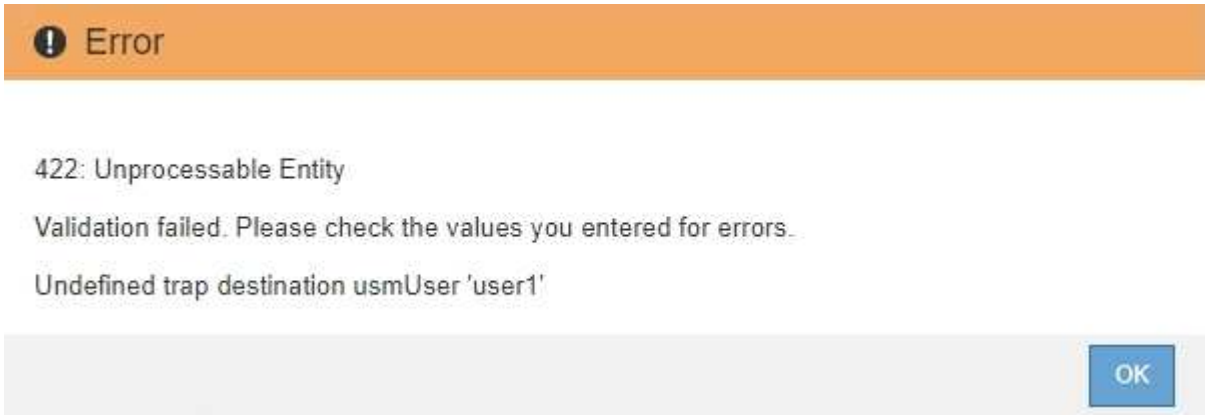
b. Per modificare un utente USM, selezionare il pulsante di opzione dell'utente e fare clic su **Edit** (Modifica). Quindi, fare riferimento alla fase per gli utenti USM nelle istruzioni per la configurazione dell'agente SNMP.

   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.

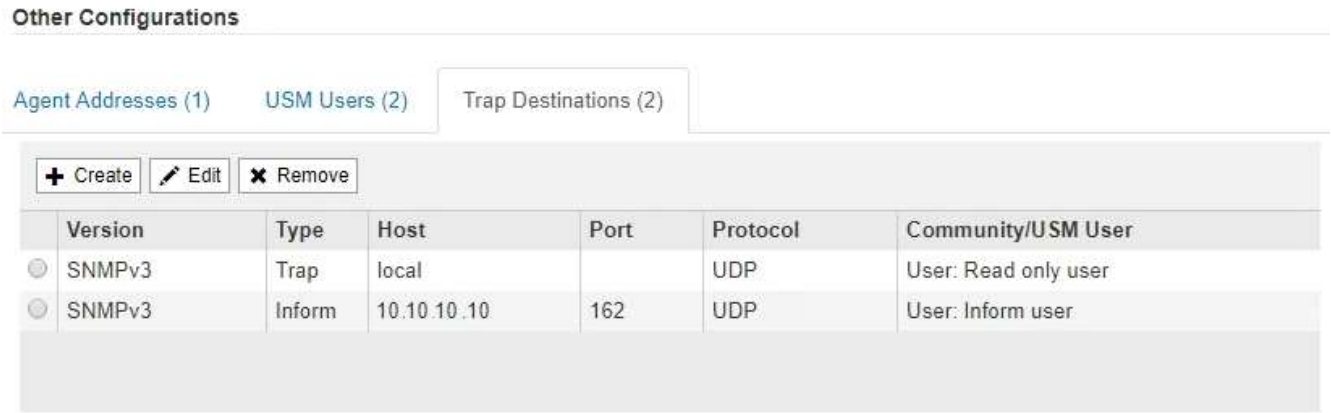
c. Per rimuovere un utente USM, selezionare il pulsante di opzione dell'utente e fare clic su **Remove** (Rimuovi). Quindi, fare clic su **OK** per confermare che si desidera rimuovere l'utente.

   > 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

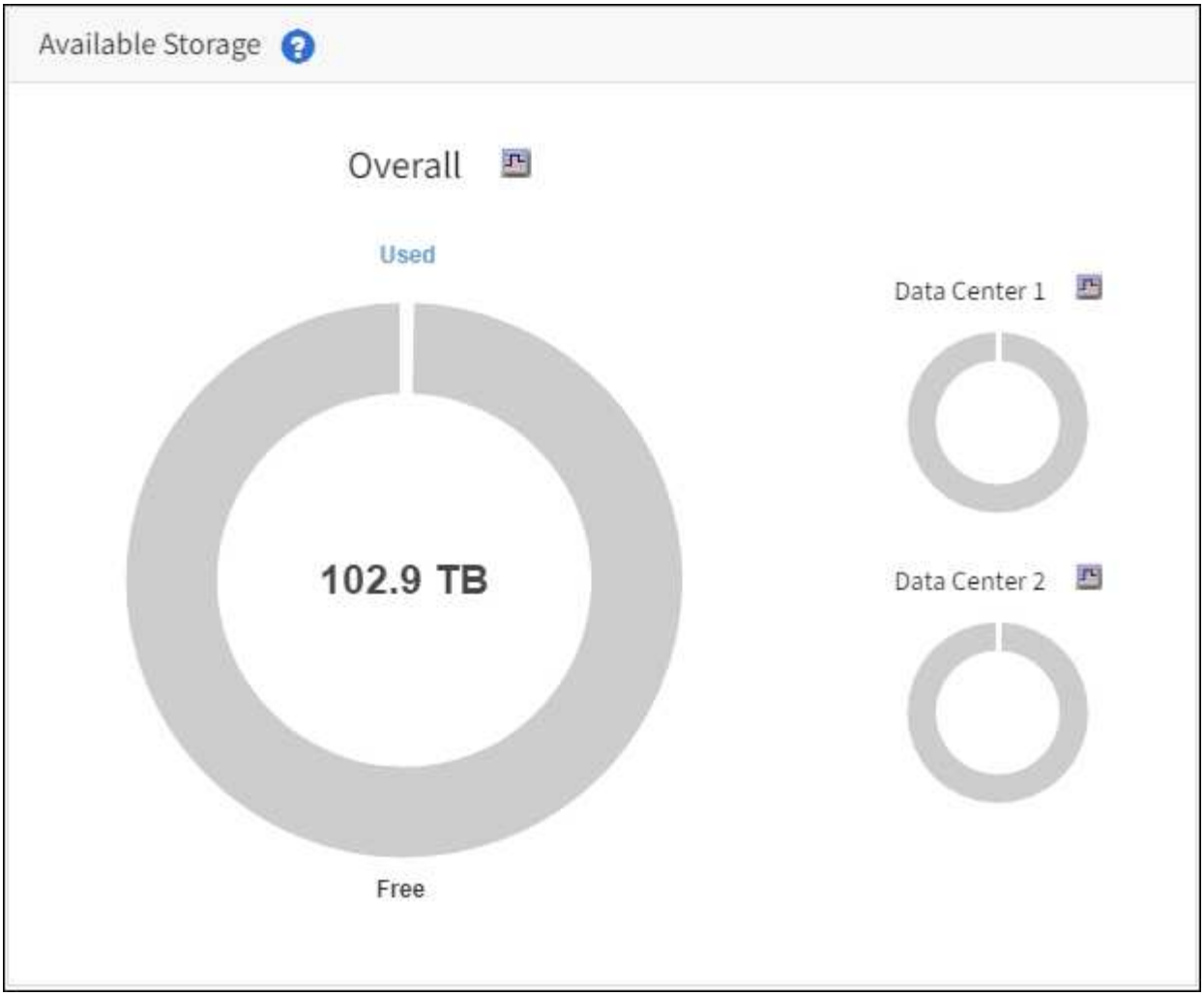
Utilizzare grafici e grafici

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

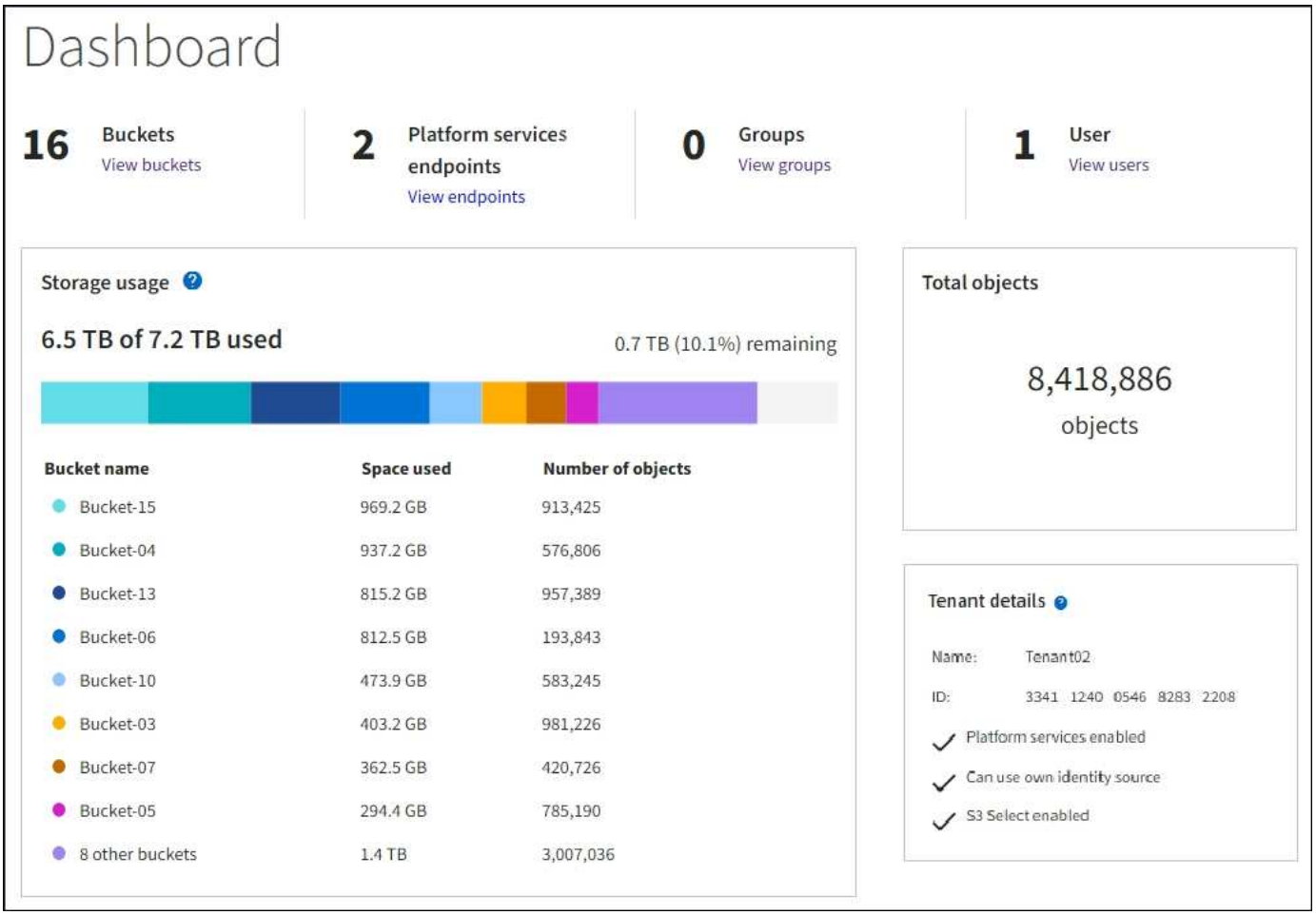
I grafici e i grafici riassumono i valori delle metriche e degli attributi specifici di StorageGRID.

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:

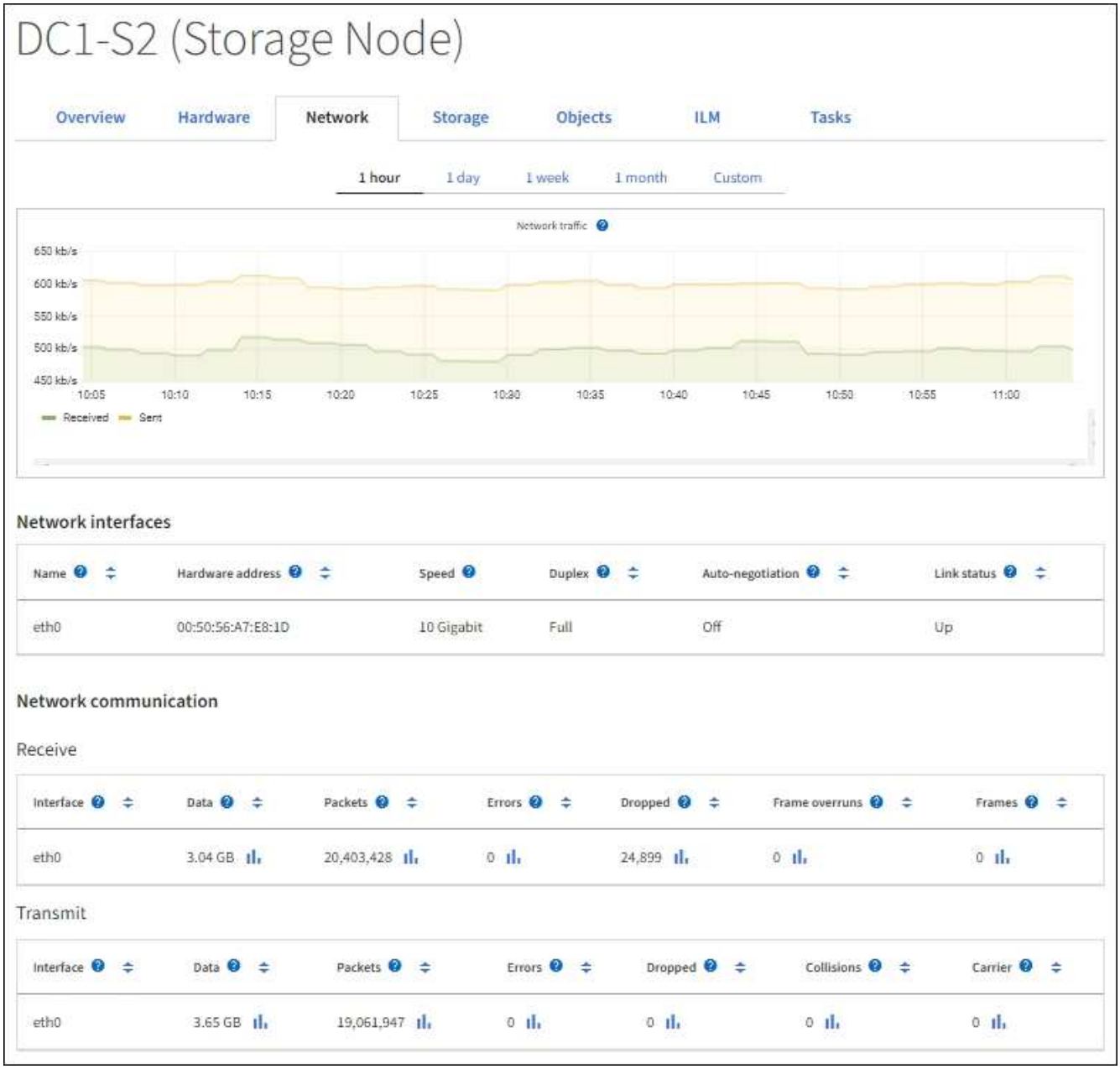
- Un elenco dei bucket più grandi (S3) o container (Swift) per il tenant
- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi
- La quantità totale di spazio utilizzato e, se viene impostata una quota, la quantità e la percentuale di spazio rimanente



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**.

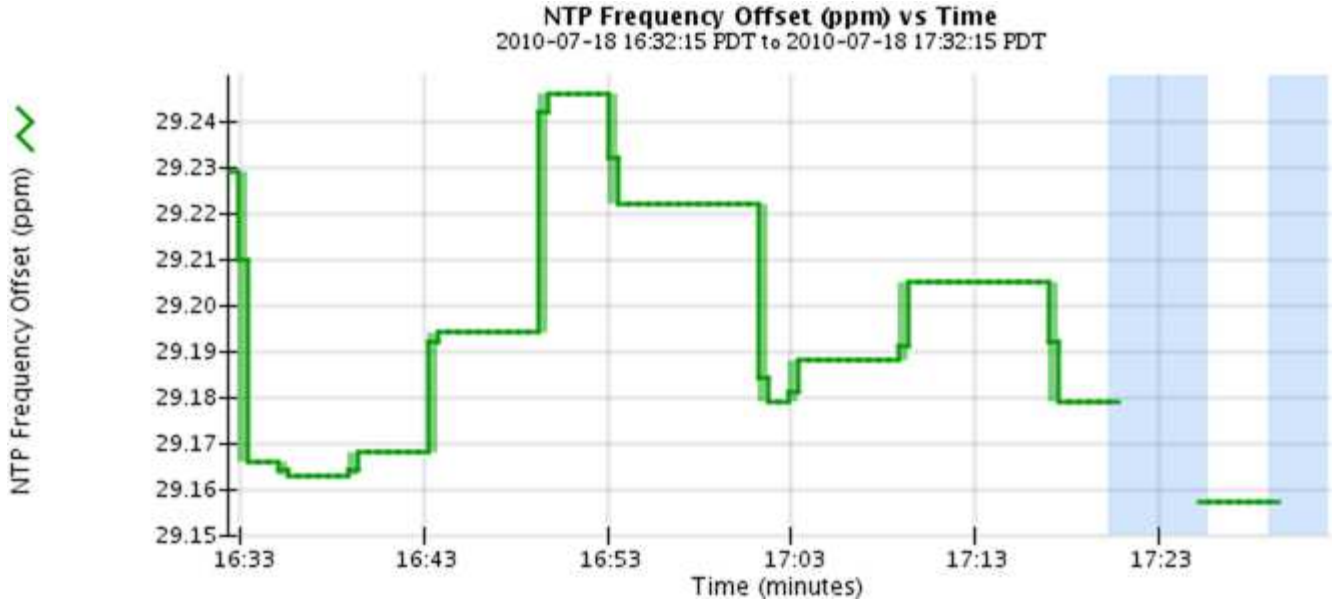
Esistono quattro tipi di grafici:

- **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.

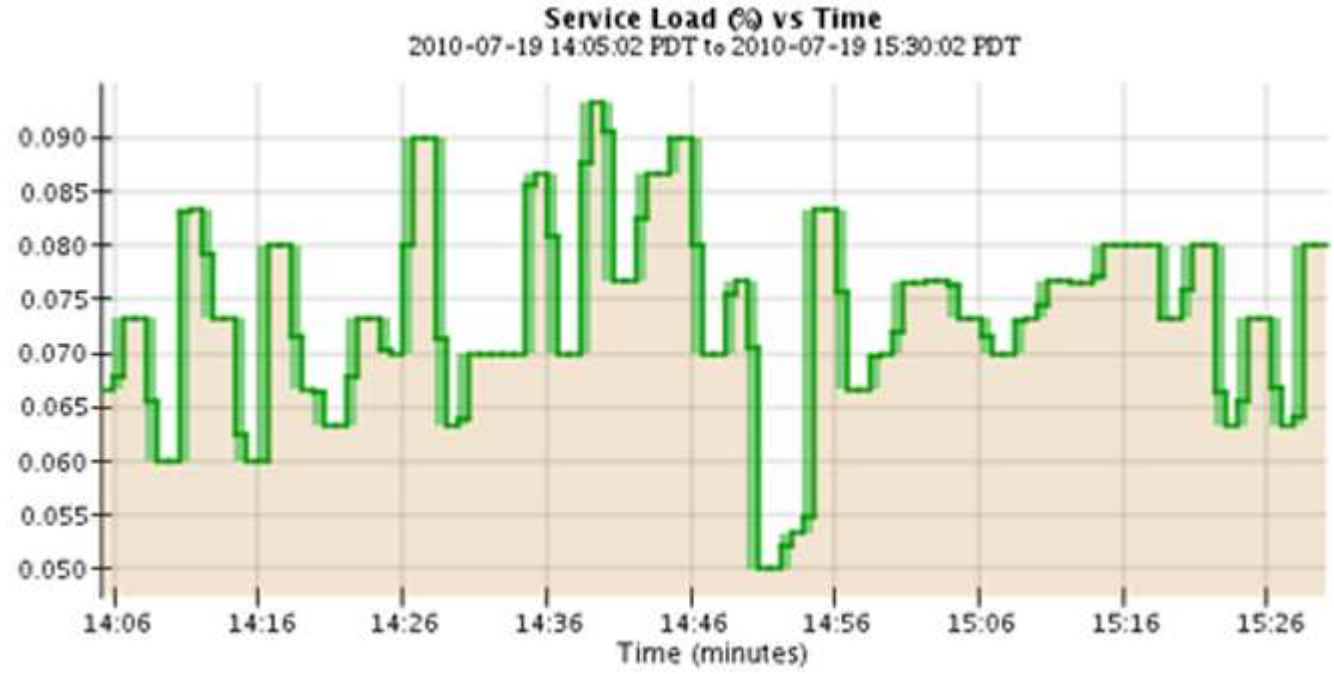


I grafici Grafana sono inclusi anche nelle dashboard predefinite disponibili nella pagina **SUPPORT Tools Metrics**.

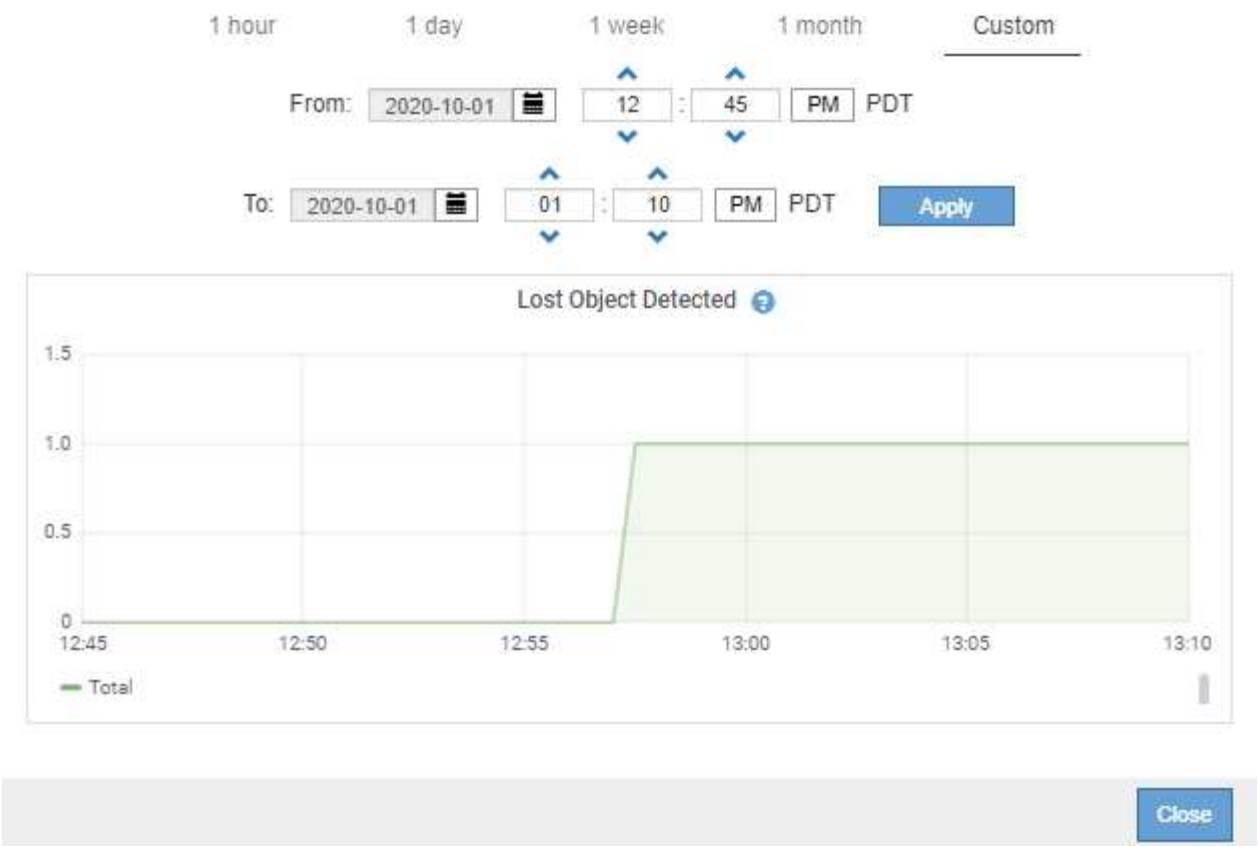
- **Grafici di linea**: Disponibili dalla pagina nodi e dalla pagina **SUPPORTO Strumenti topologia di griglia** (selezionare l'icona del grafico Dopo un valore di dati), i grafici a linee vengono utilizzati per rappresentare graficamente i valori degli attributi StorageGRID che hanno un valore unitario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



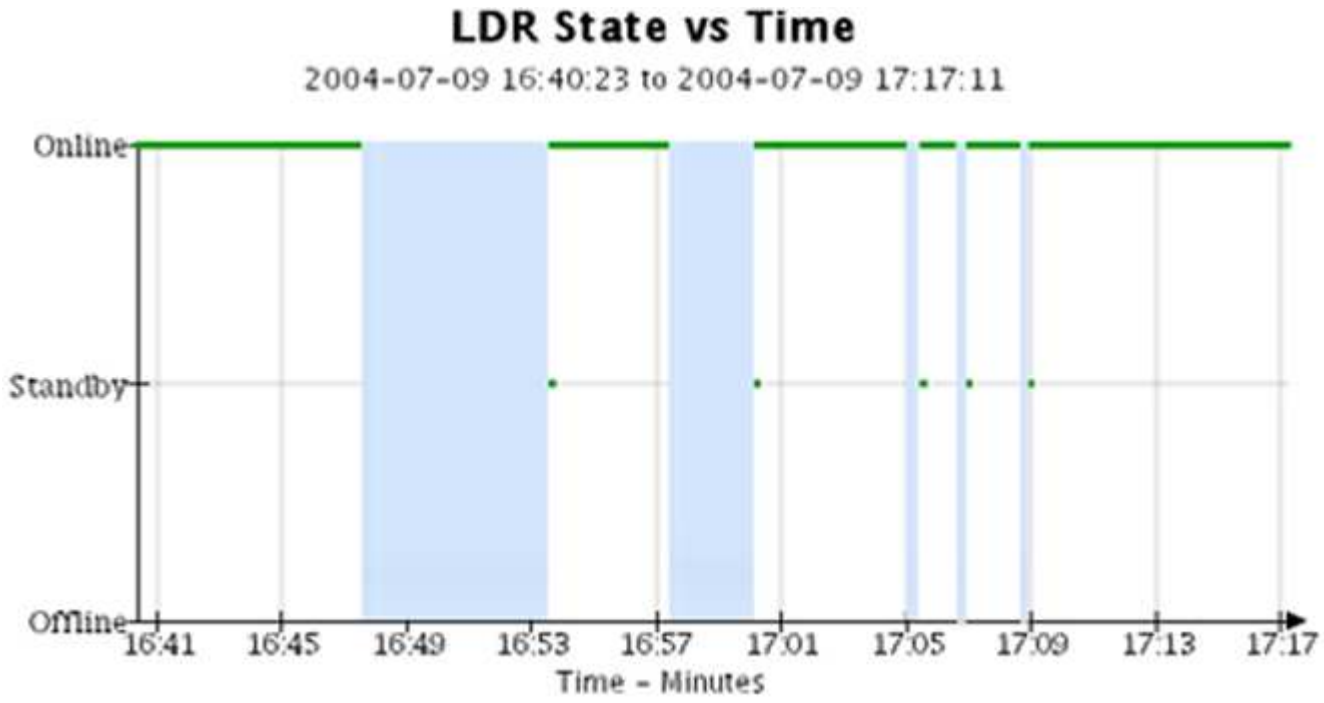
- **Area Graphs**: Disponibile dalla pagina Nodes e dalla pagina **SUPPORT Tools Grid topology** (selezionare l'icona del grafico) dopo un valore di dati), i grafici di area vengono utilizzati per rappresentare graficamente le quantità di attributi volumetrici, come i conteggi di oggetti o i valori di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

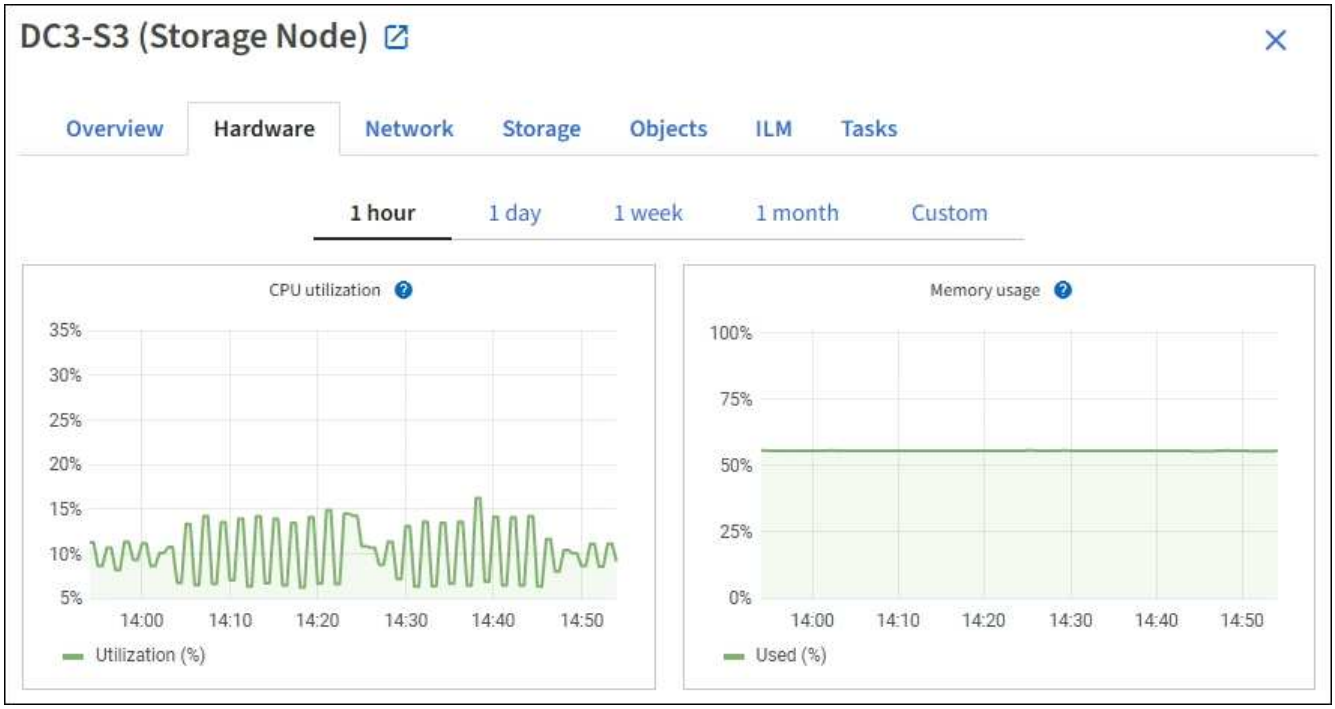
Di cosa hai bisogno

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

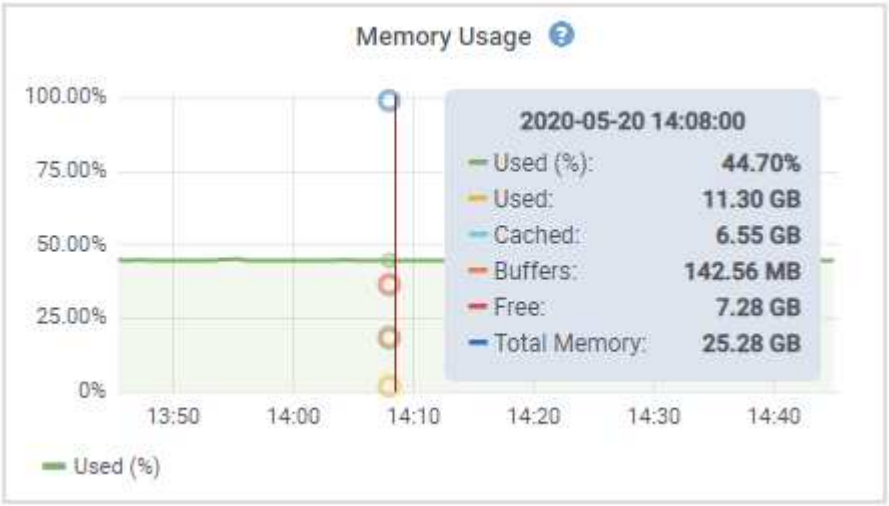
Fasi

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.

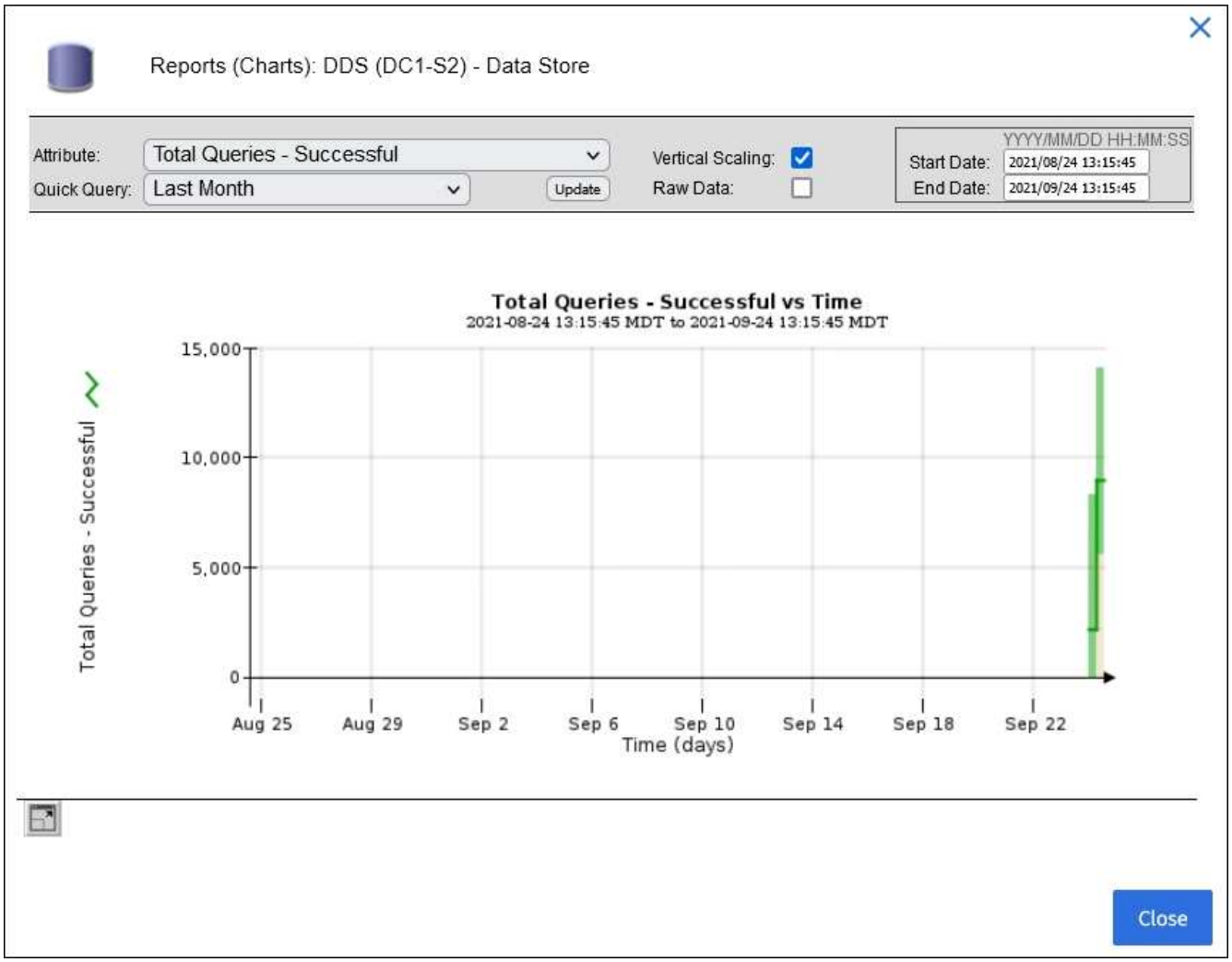


4. In base alle esigenze, spesso è possibile visualizzare un grafico per un attributo o una metrica specifici. Nella tabella della pagina nodi, selezionare l'icona del grafico a destra del nome dell'attributo.

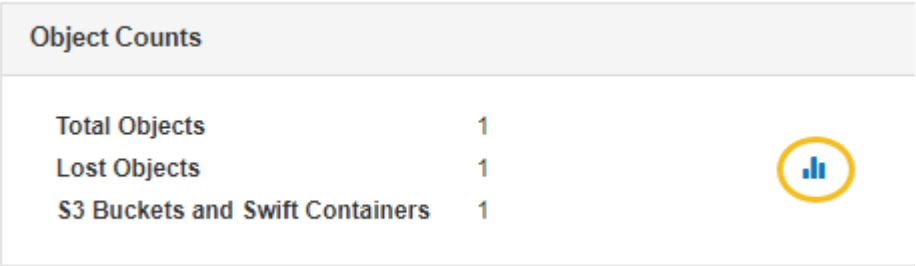
> I grafici non sono disponibili per tutte le metriche e gli attributi.

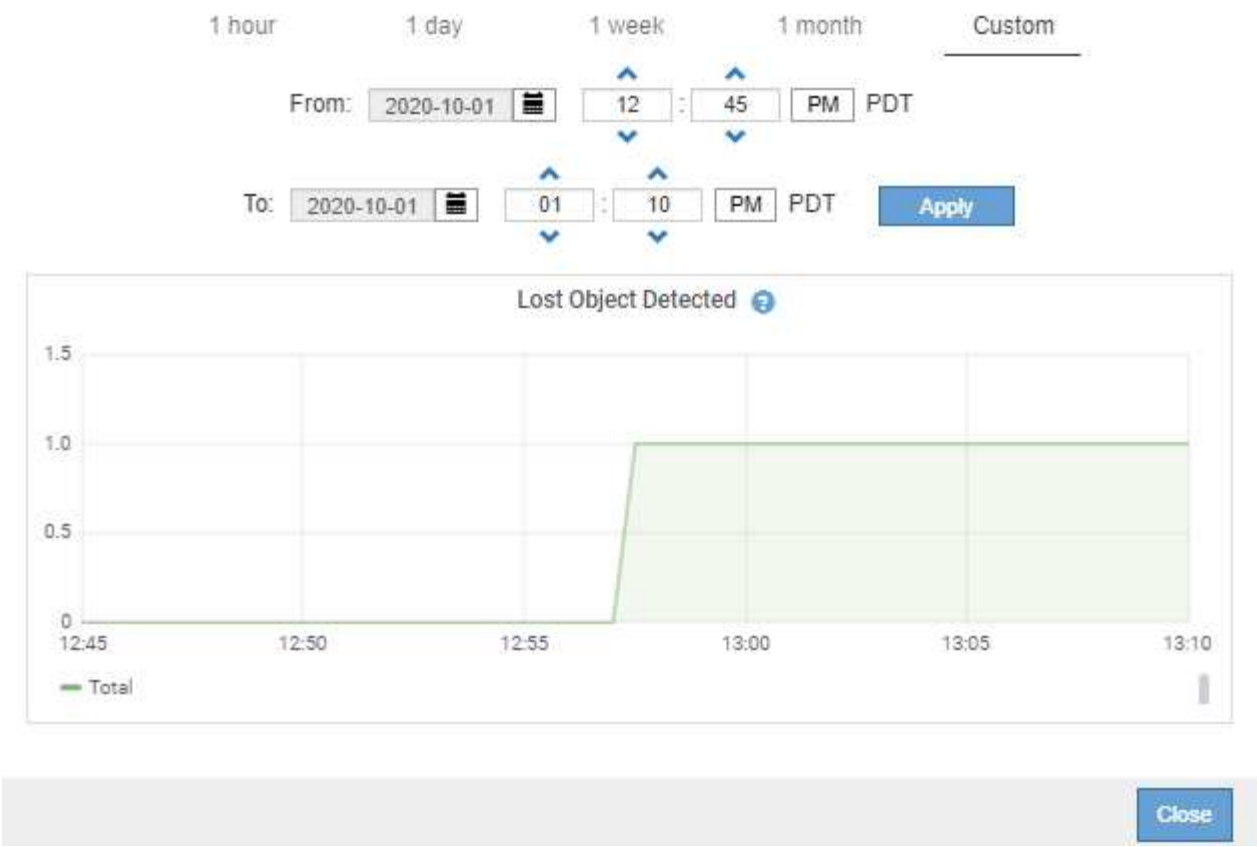
Esempio 1: Dalla scheda oggetti di un nodo di storage, è possibile selezionare l'icona del grafico Per visualizzare il numero totale di query di archiviazione dei metadati riuscite per il nodo di storage.

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

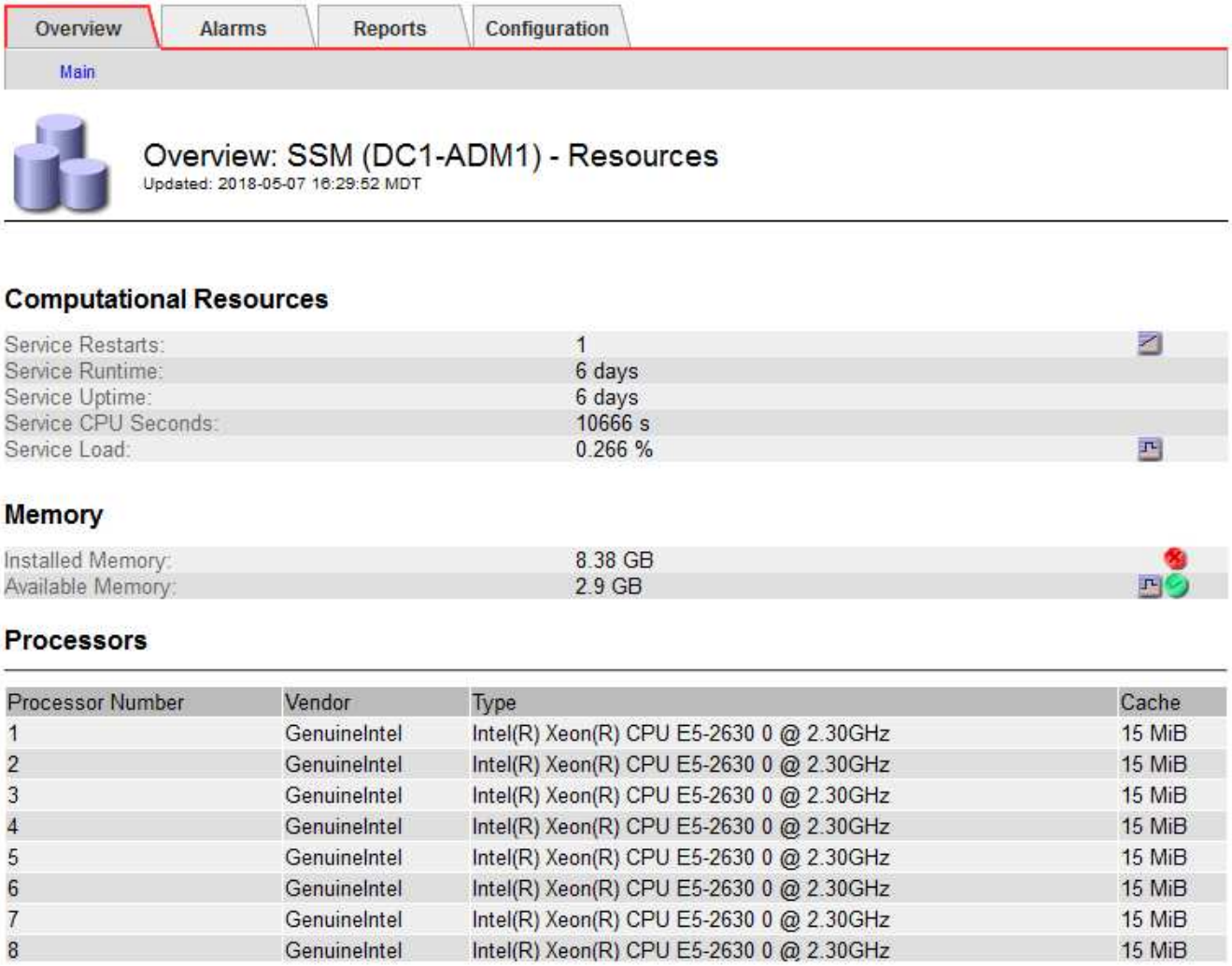


Esempio 2: Dalla scheda oggetti di un nodo di storage, è possibile selezionare l'icona del grafico Per visualizzare il grafico Grafana del numero di oggetti persi rilevati nel tempo.





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

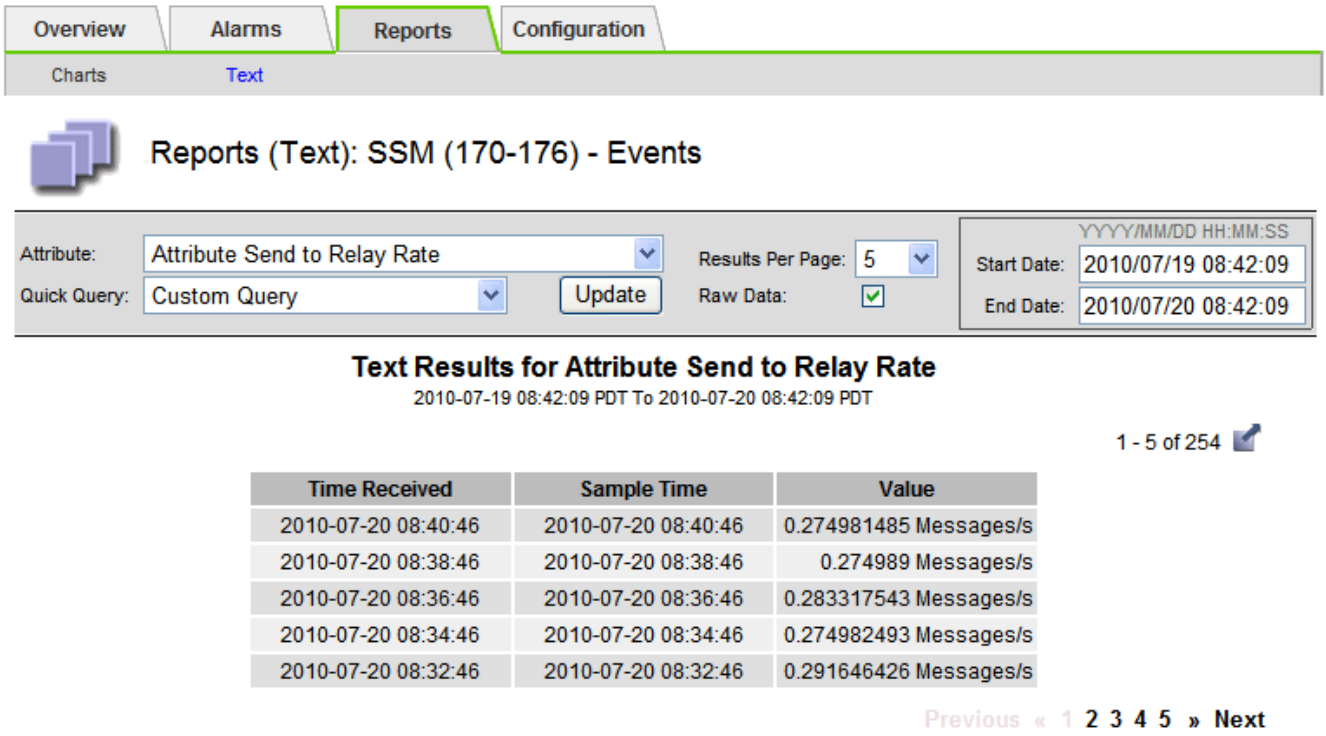
I report di testo esportati aprono una nuova scheda del browser che consente di selezionare e copiare i dati.

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.

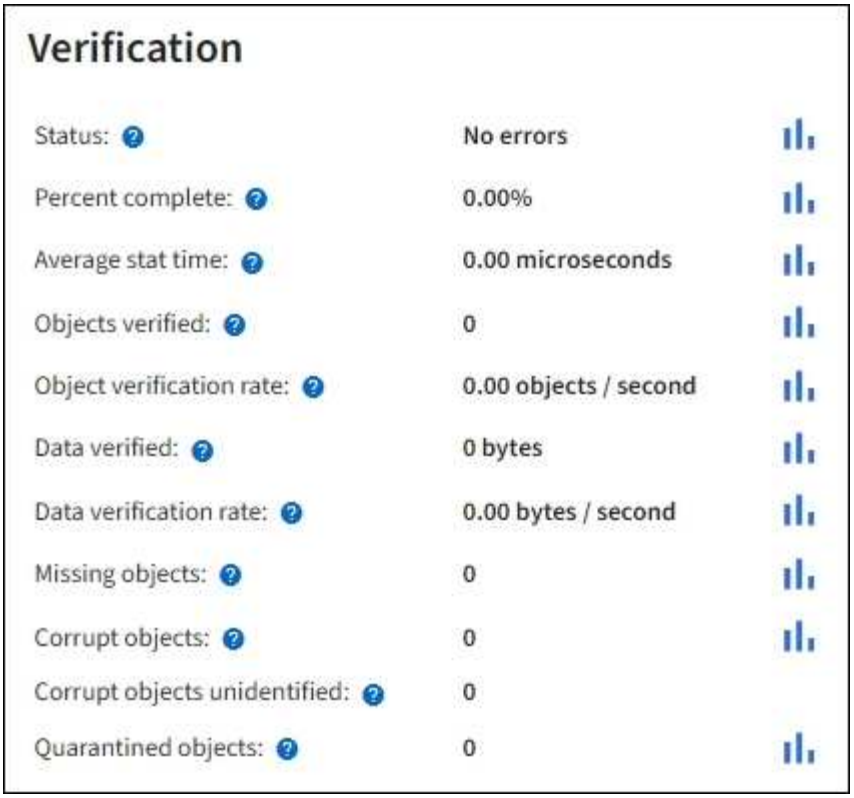
Fasi

1. Esaminare i risultati delle verifiche in background:

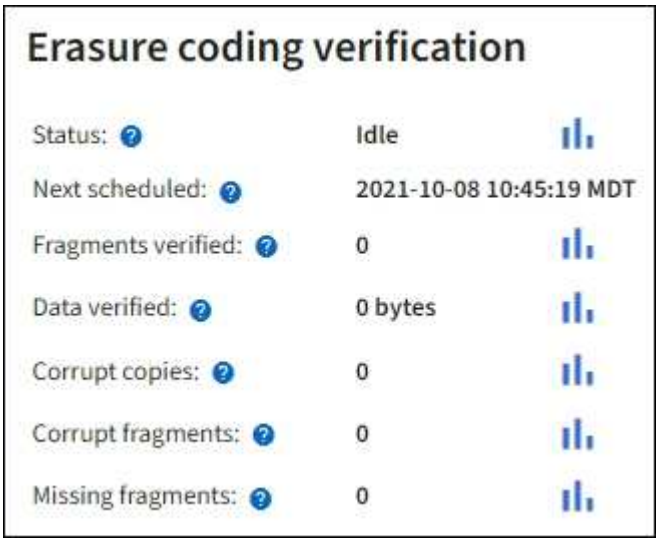
   a. Selezionare **NODI *nodo di storage* oggetti**.

   b. Verificare i risultati della verifica:

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

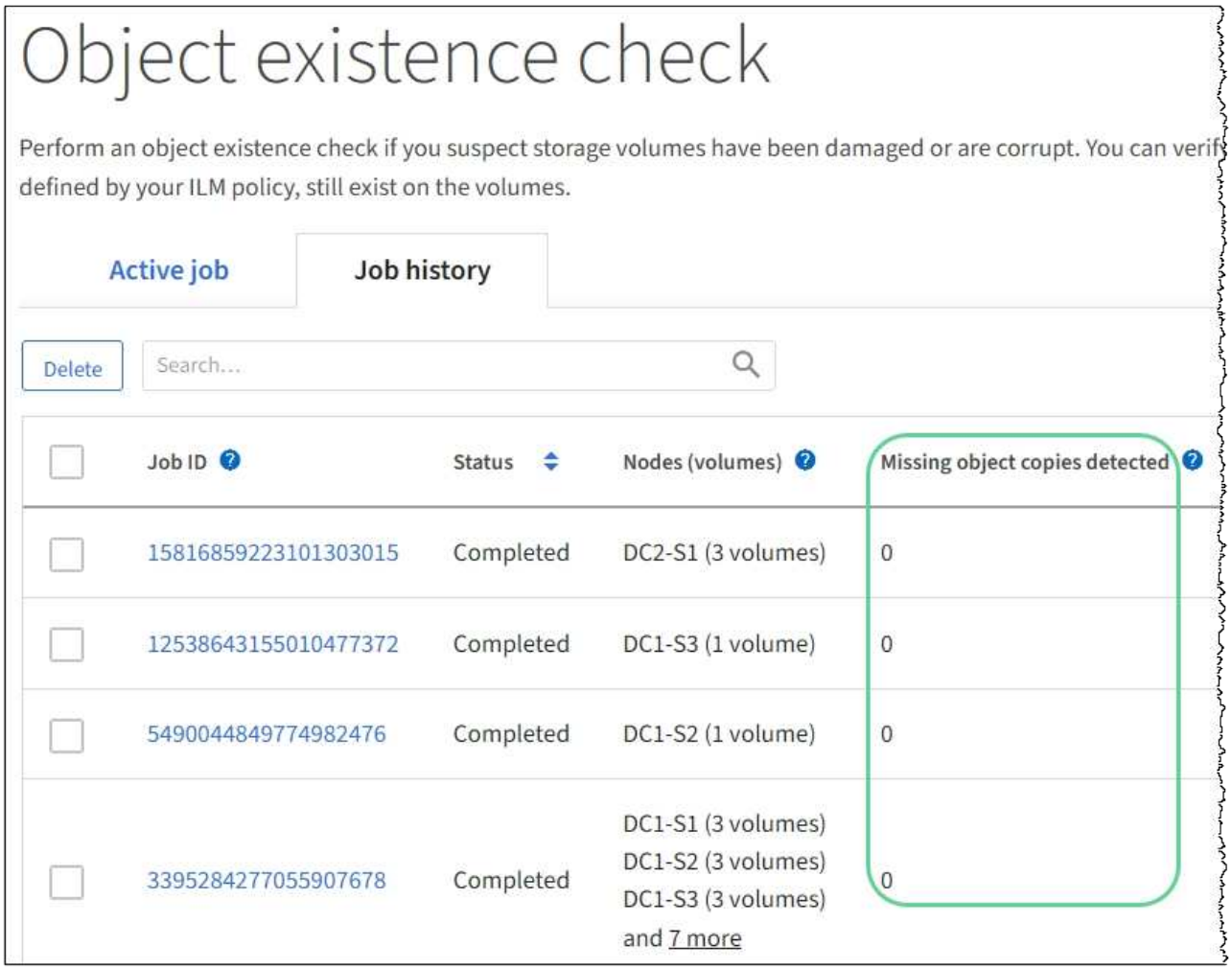


- Per controllare la verifica dei frammenti con codifica di cancellazione, selezionare ***Storage Node* ILM** e controllare gli attributi nella sezione Erasure coding verifcation.



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**.

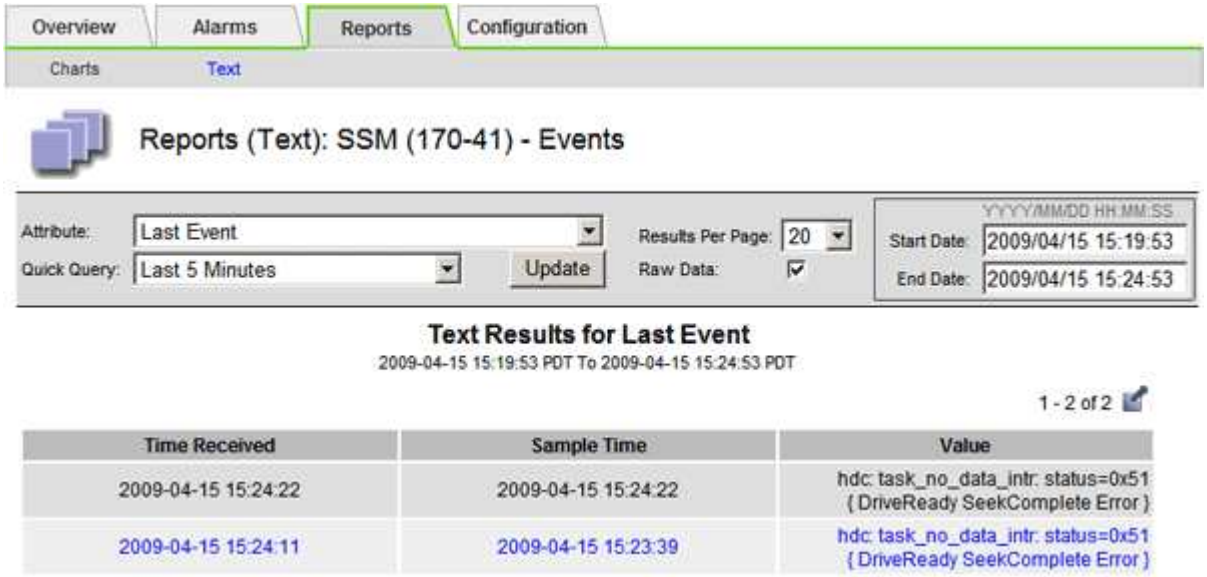
c. Selezionare **testo**.

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.

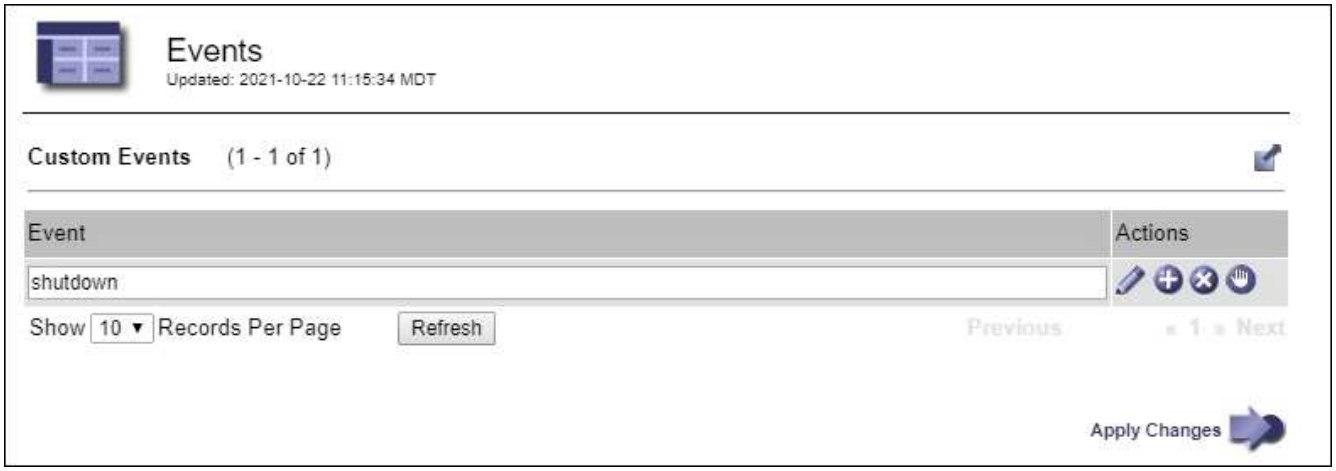
- Dopo la creazione di un evento personalizzato, viene monitorata ogni occorrenza.
- Per creare un evento personalizzato in base alle parole chiave in `/var/local/log/messages` i log in questi file devono essere:
  - Generato dal kernel
  - Generato da daemon o programma utente a livello di errore o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

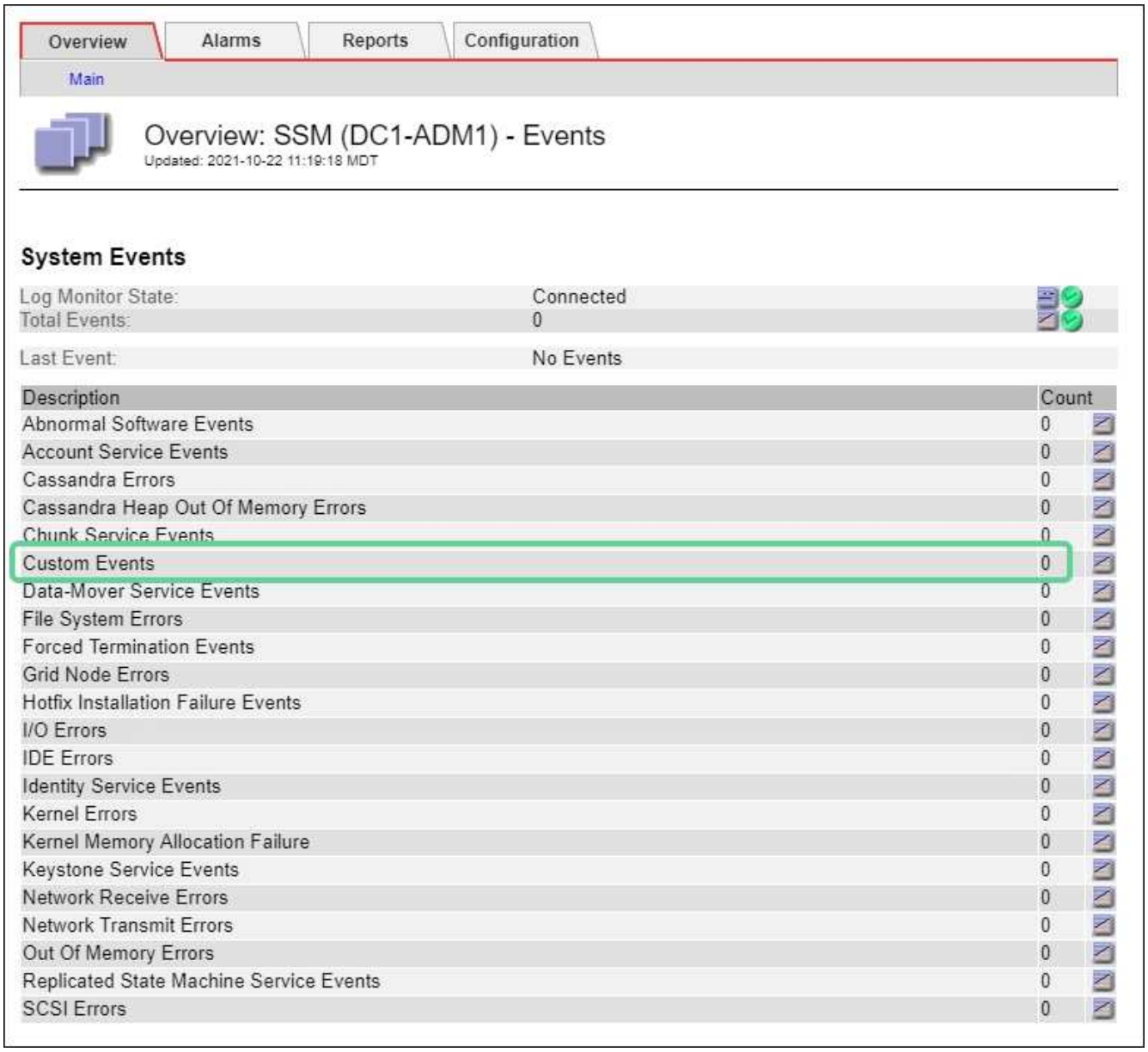
1. Selezionare **SUPPORT Alarms (legacy) Custom events**.
2. Fare clic su **Edit** (Modifica) (O **Inserisci** se questo non è il primo evento).

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.



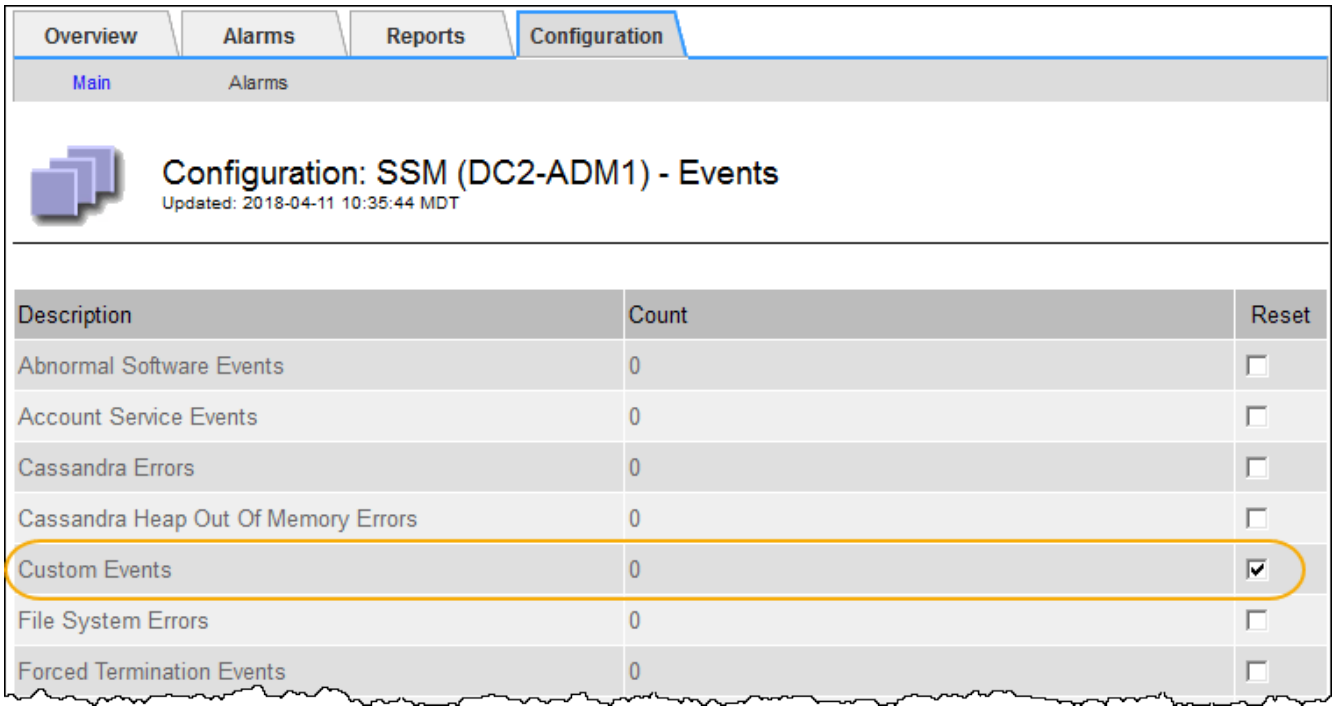
Azzerare il numero di eventi personalizzati

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.

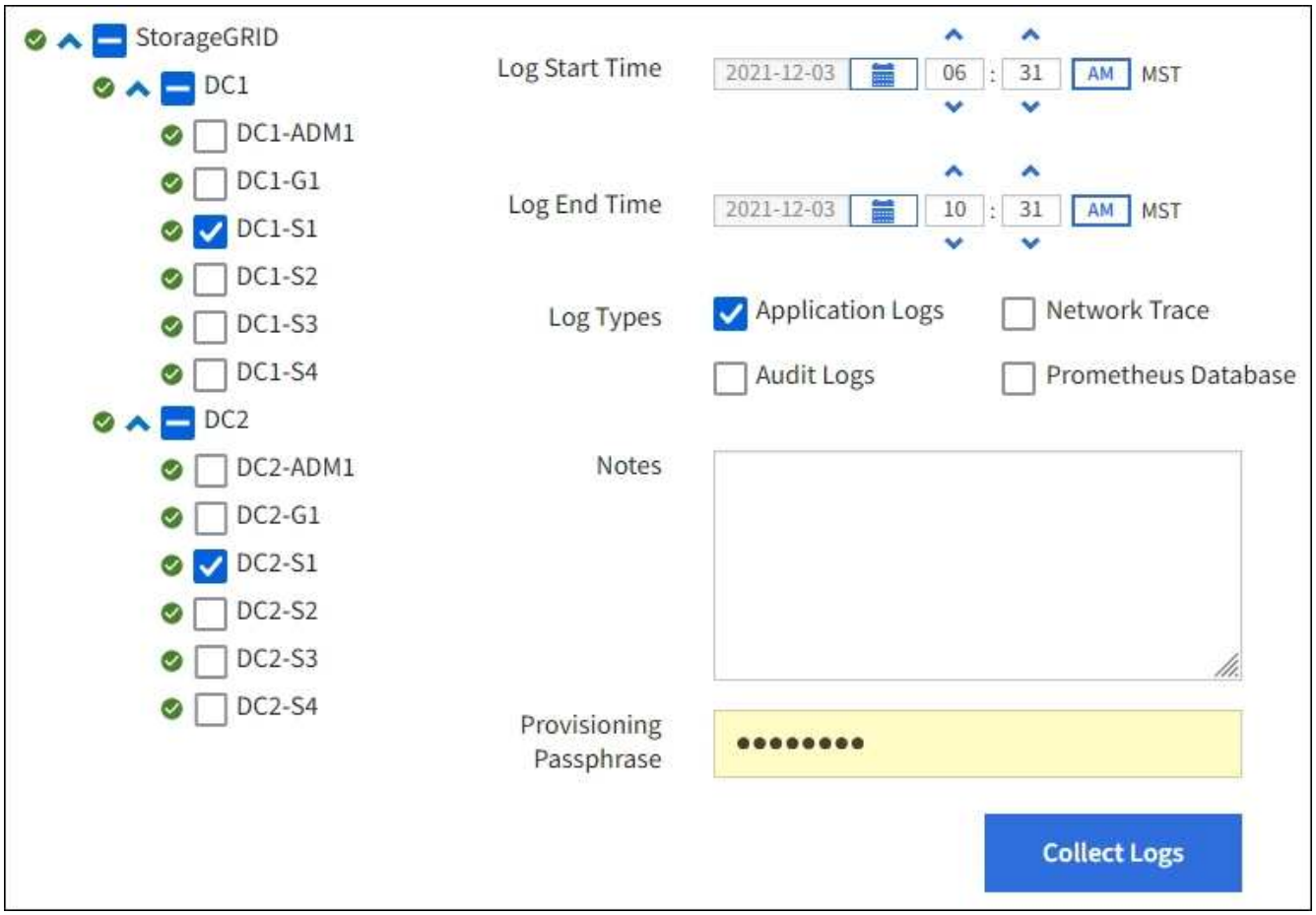
A proposito di questa attività

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.

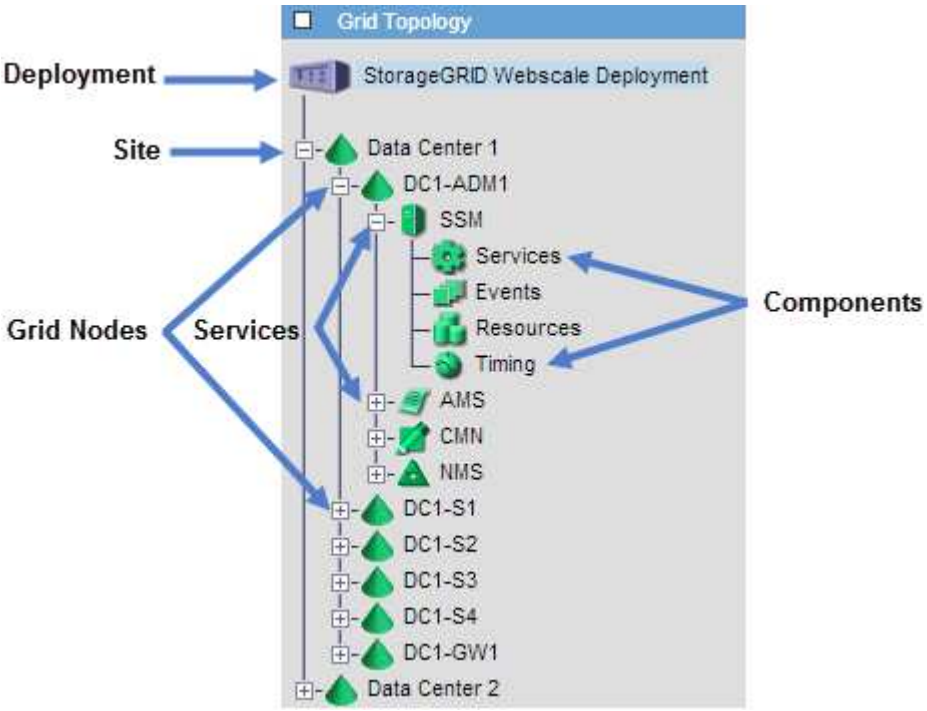
Informazioni correlate

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

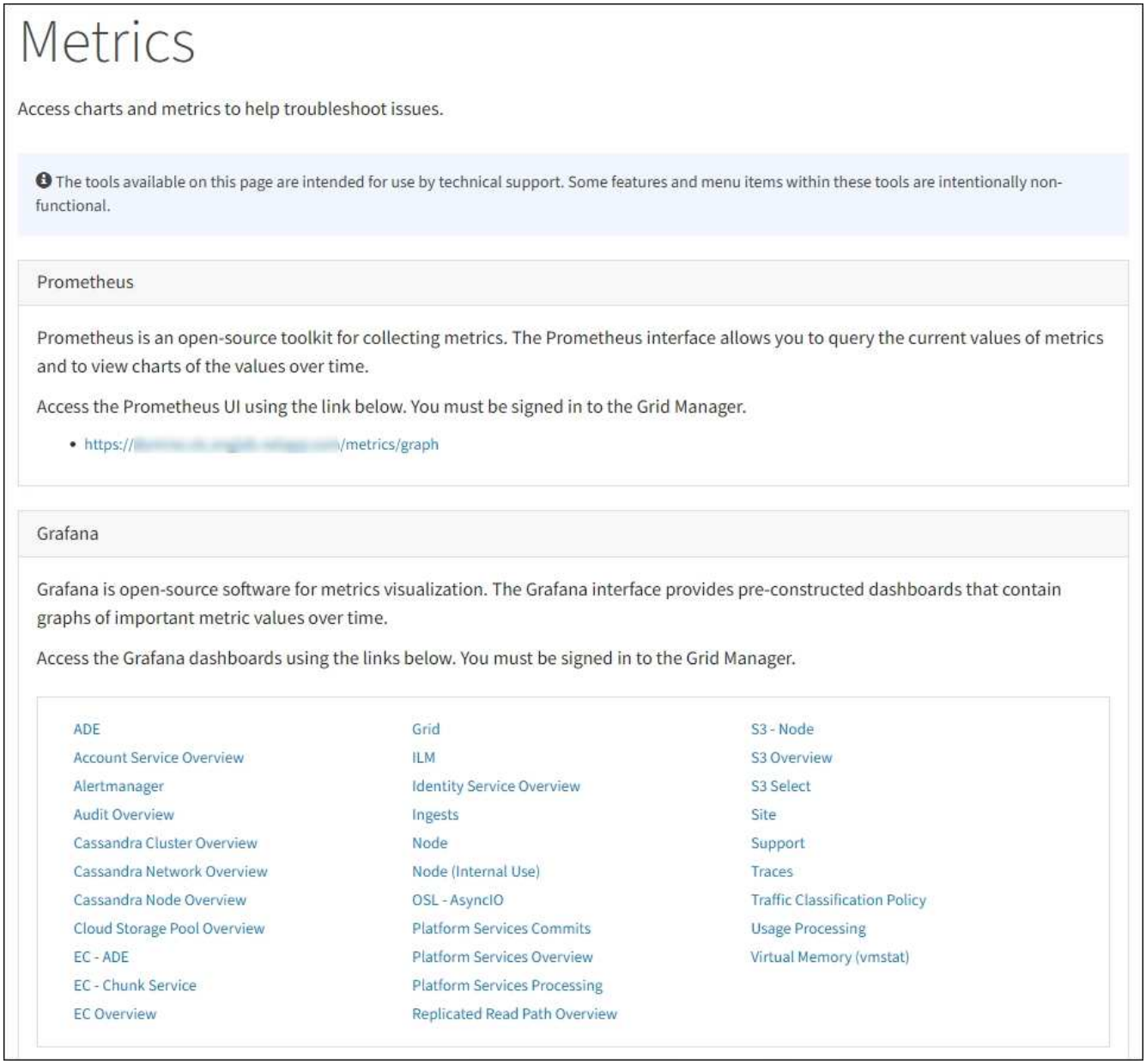
software open-source per la raccolta di metriche. Grafana è un software open-source per la visualizzazione delle metriche.

> 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**.

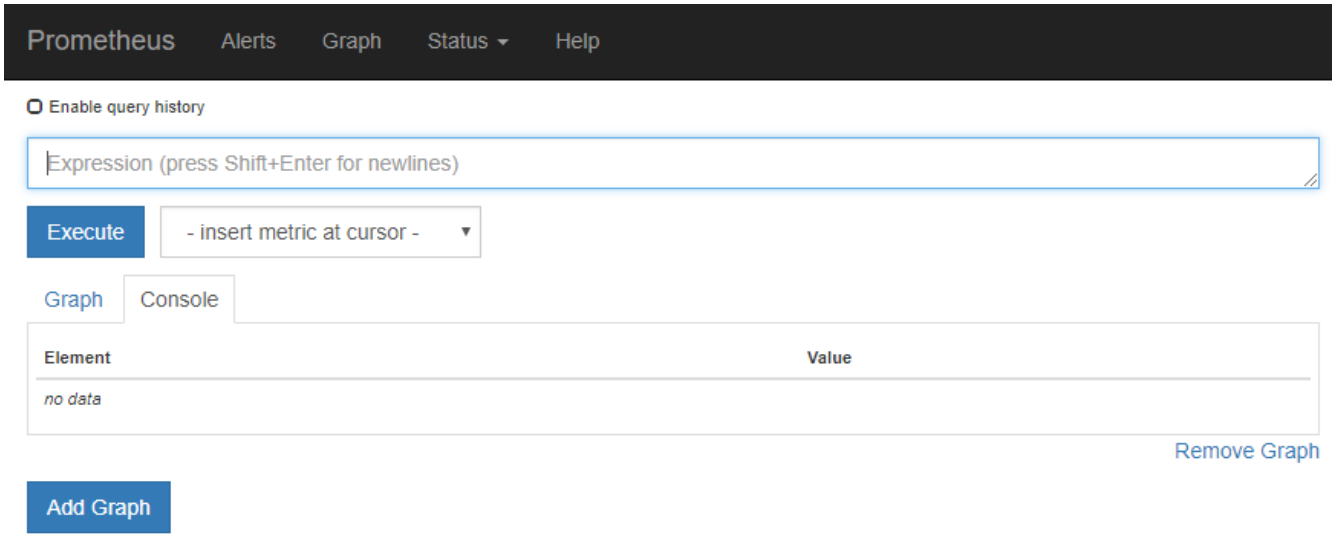
   Di seguito è riportato un esempio della pagina Metrics (metriche):



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.

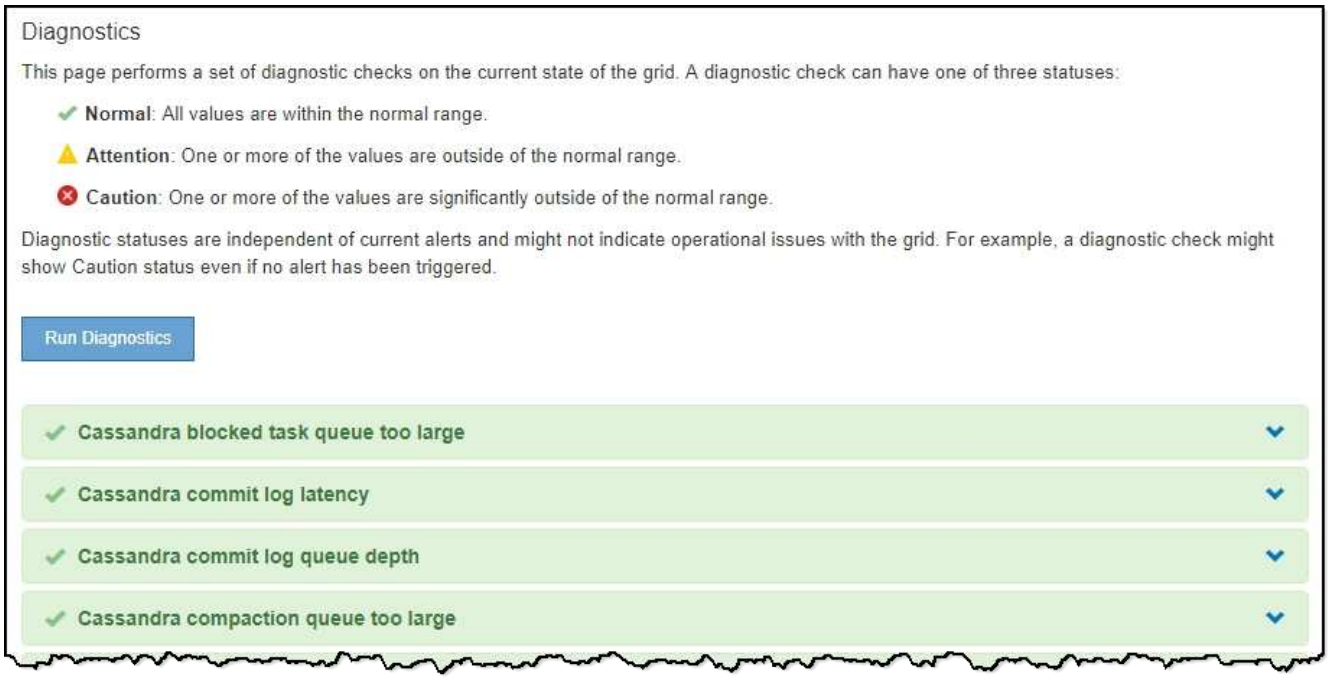
Gli stati di diagnostica sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la griglia. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato di attenzione anche se non è stato attivato alcun allarme.

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.



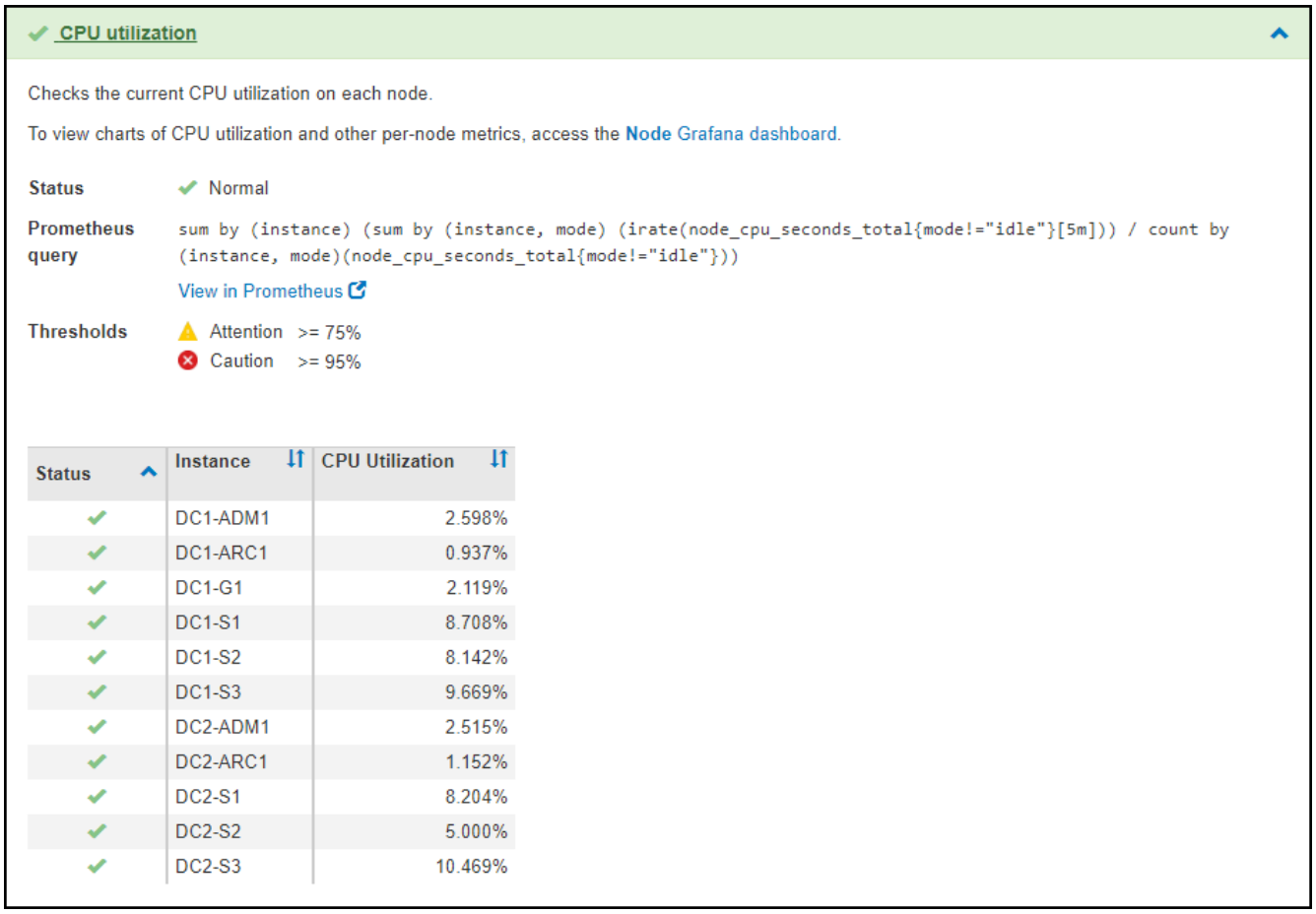
2. Per ulteriori informazioni su una diagnostica specifica, fare clic in un punto qualsiasi della riga.

   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**.

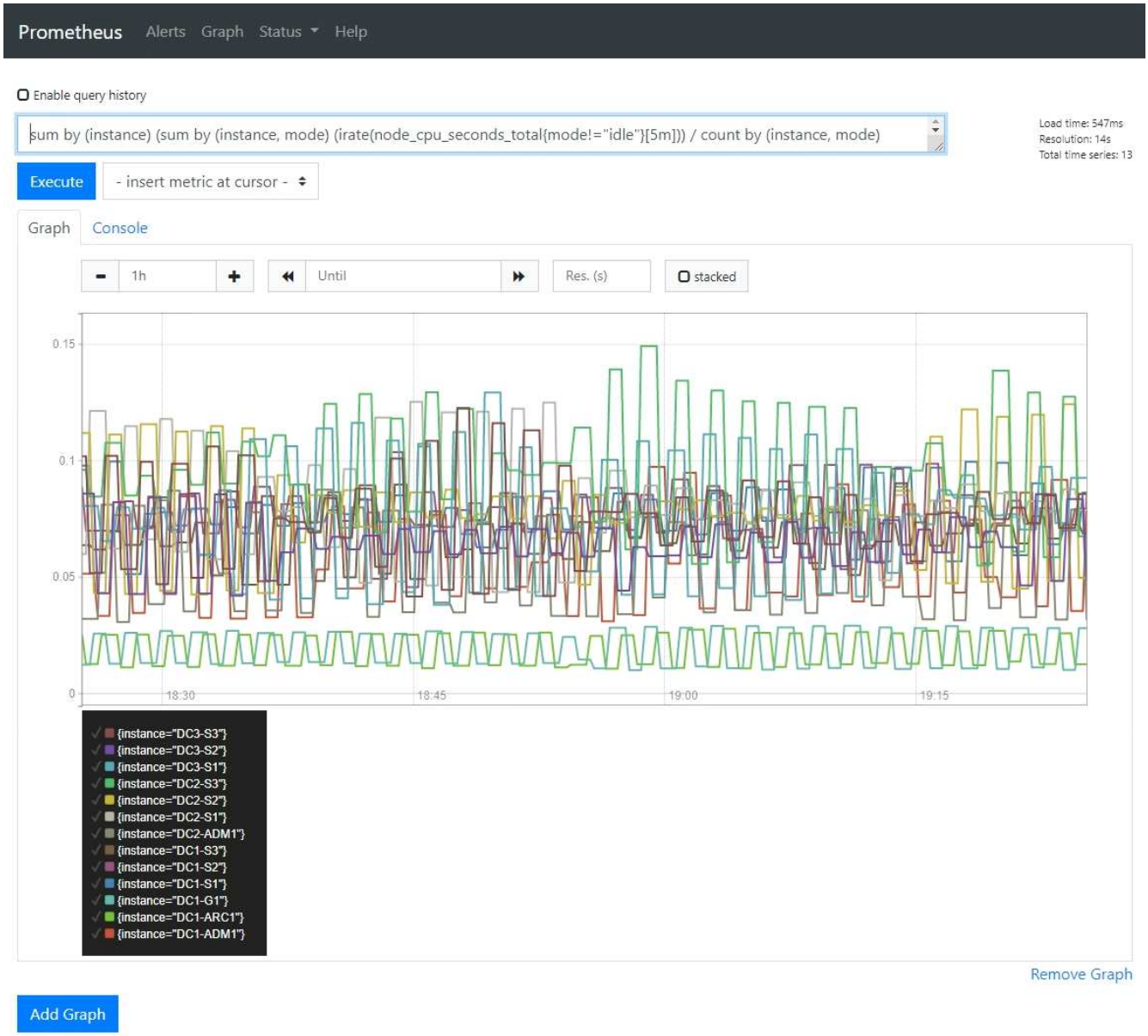
   Questo collegamento non viene visualizzato per tutte le diagnostiche.

   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.

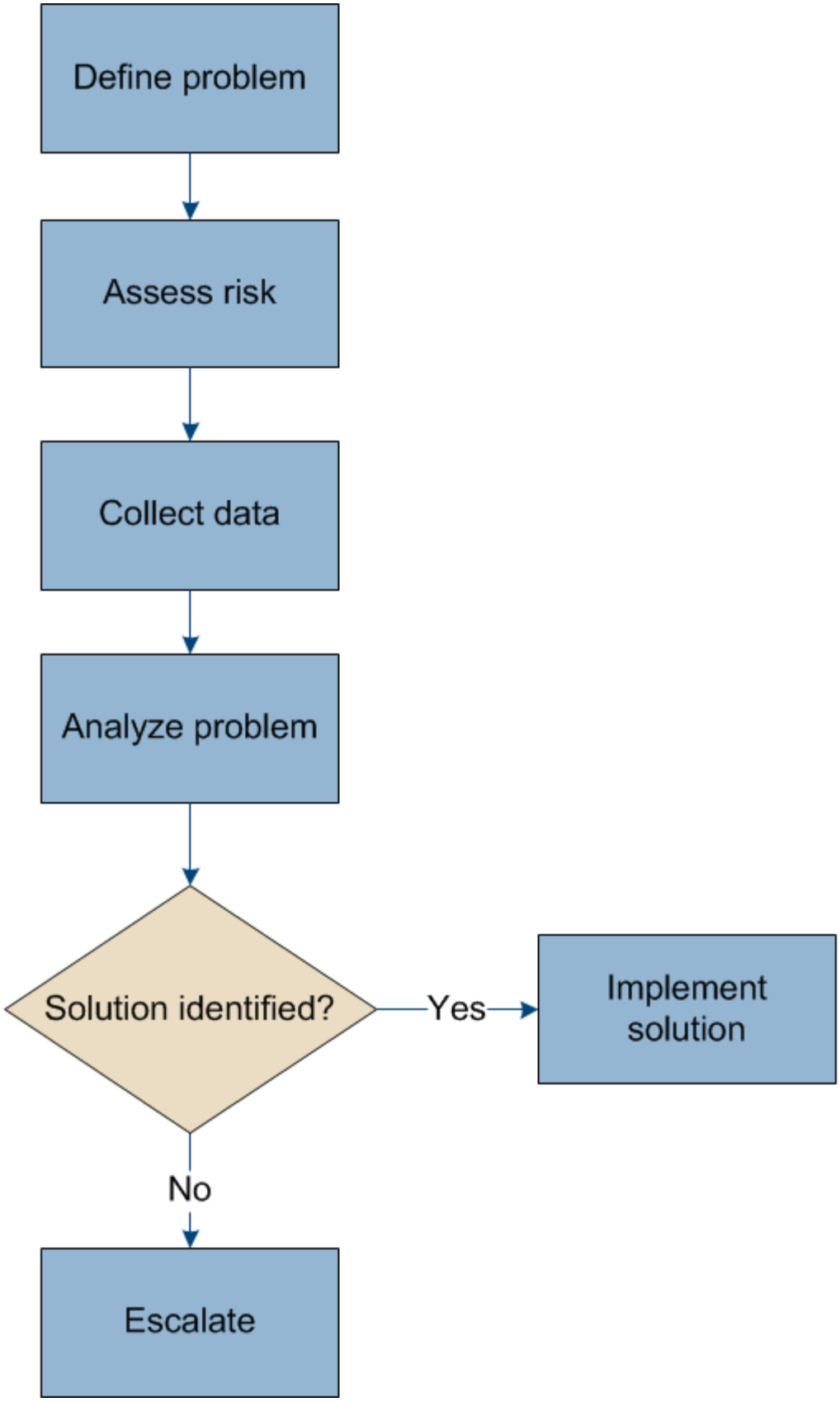
Risolvere i problemi di un sistema StorageGRID

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

Tipo di dati da raccogliere	Perché raccogliere questo dat	Istruzioni
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
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

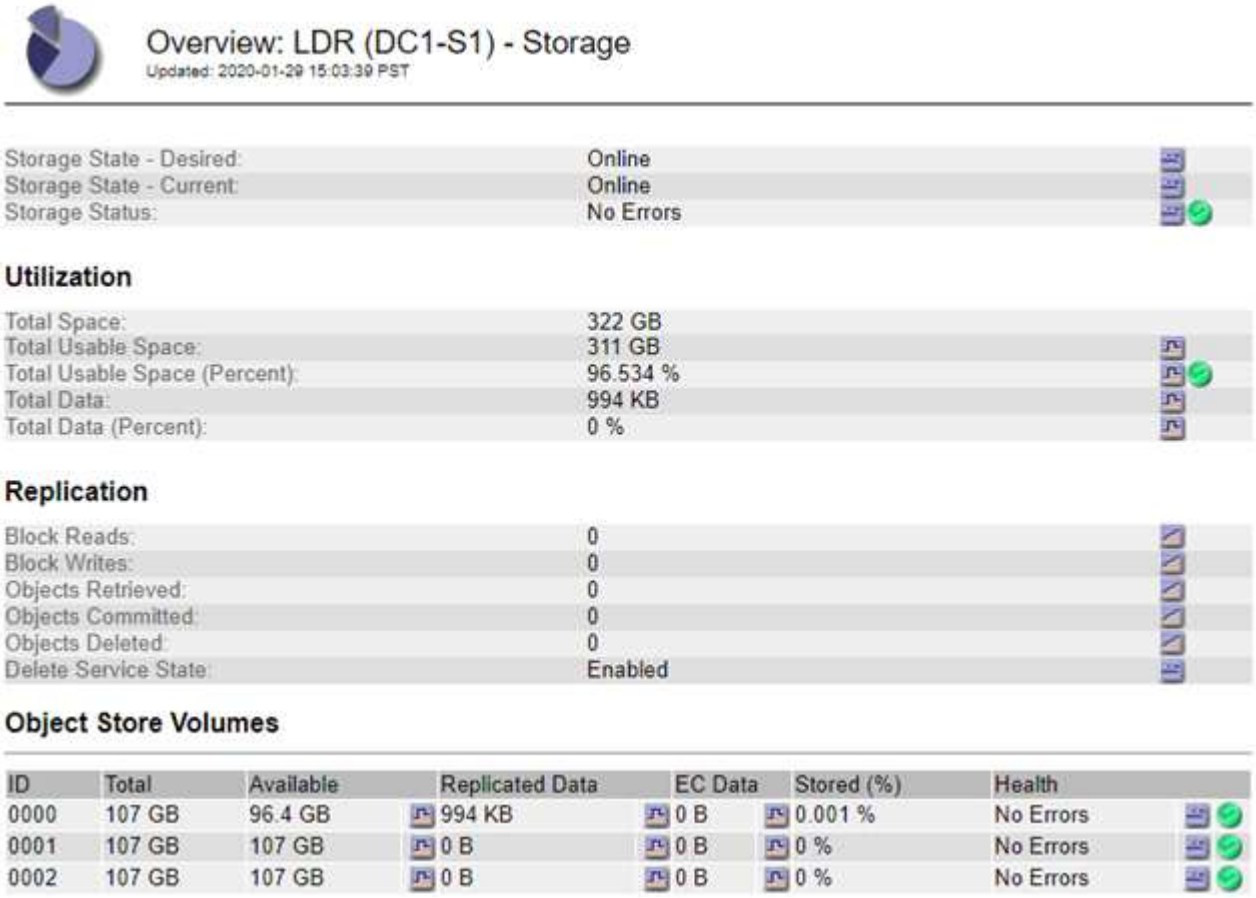
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online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

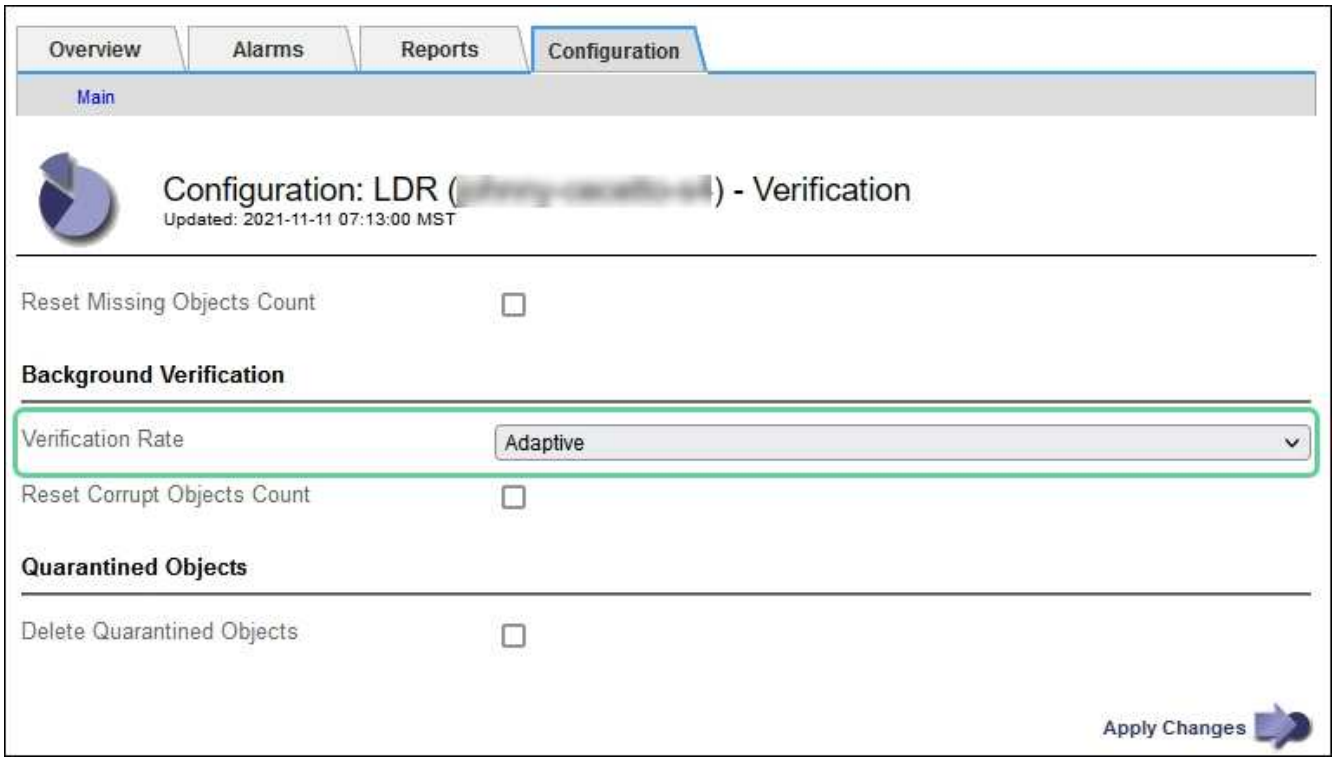
È possibile modificare il tasso di verifica per la verifica in background su un nodo di storage:

- 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:

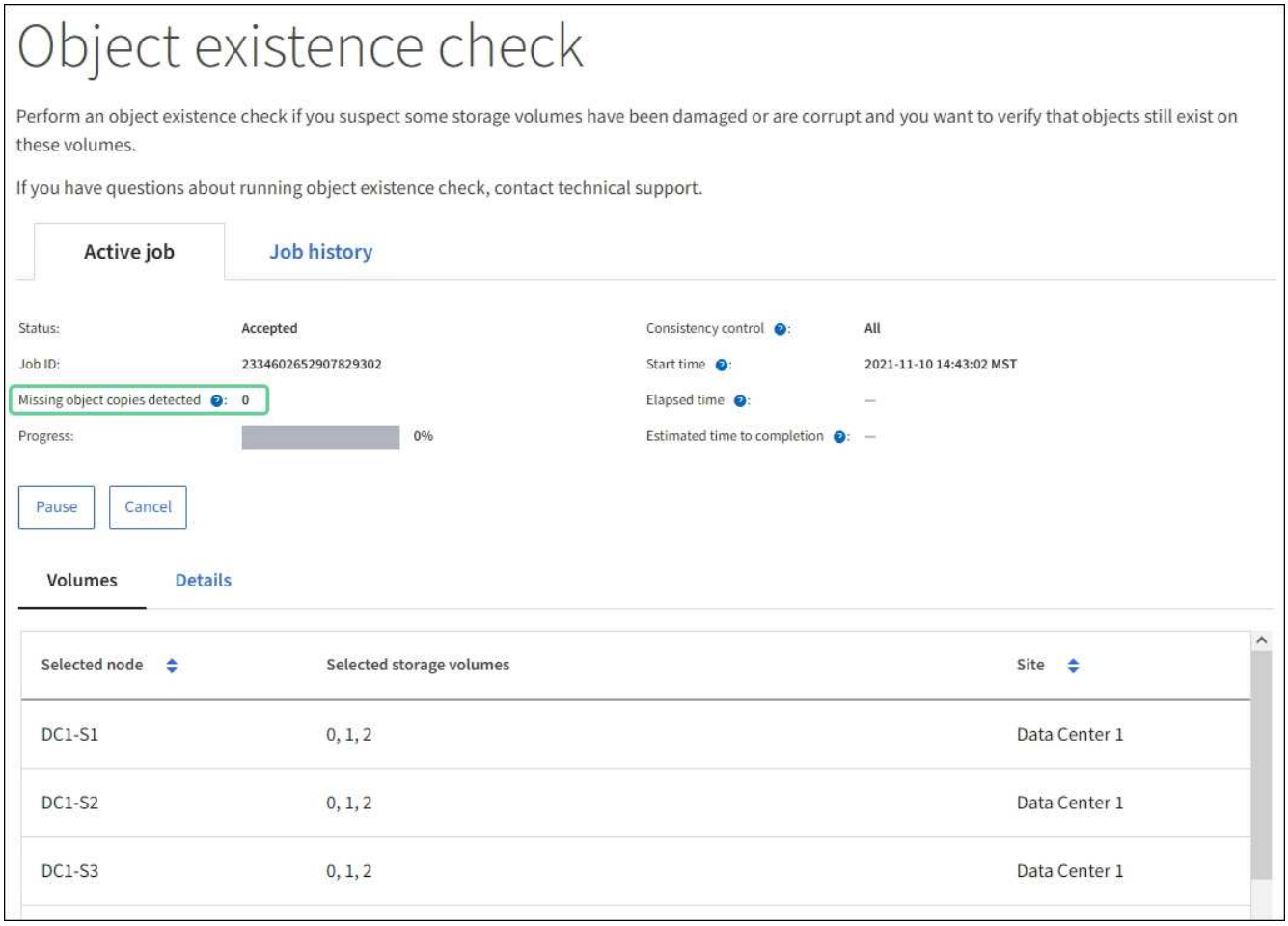
   - Il lavoro viene completato.
   - Il processo viene sospeso o annullato. È possibile riprendere un lavoro che è stato messo in pausa, ma non è possibile riprendere un lavoro che è stato annullato.
   - Il lavoro si blocca. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto bloccato**. Seguire 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.

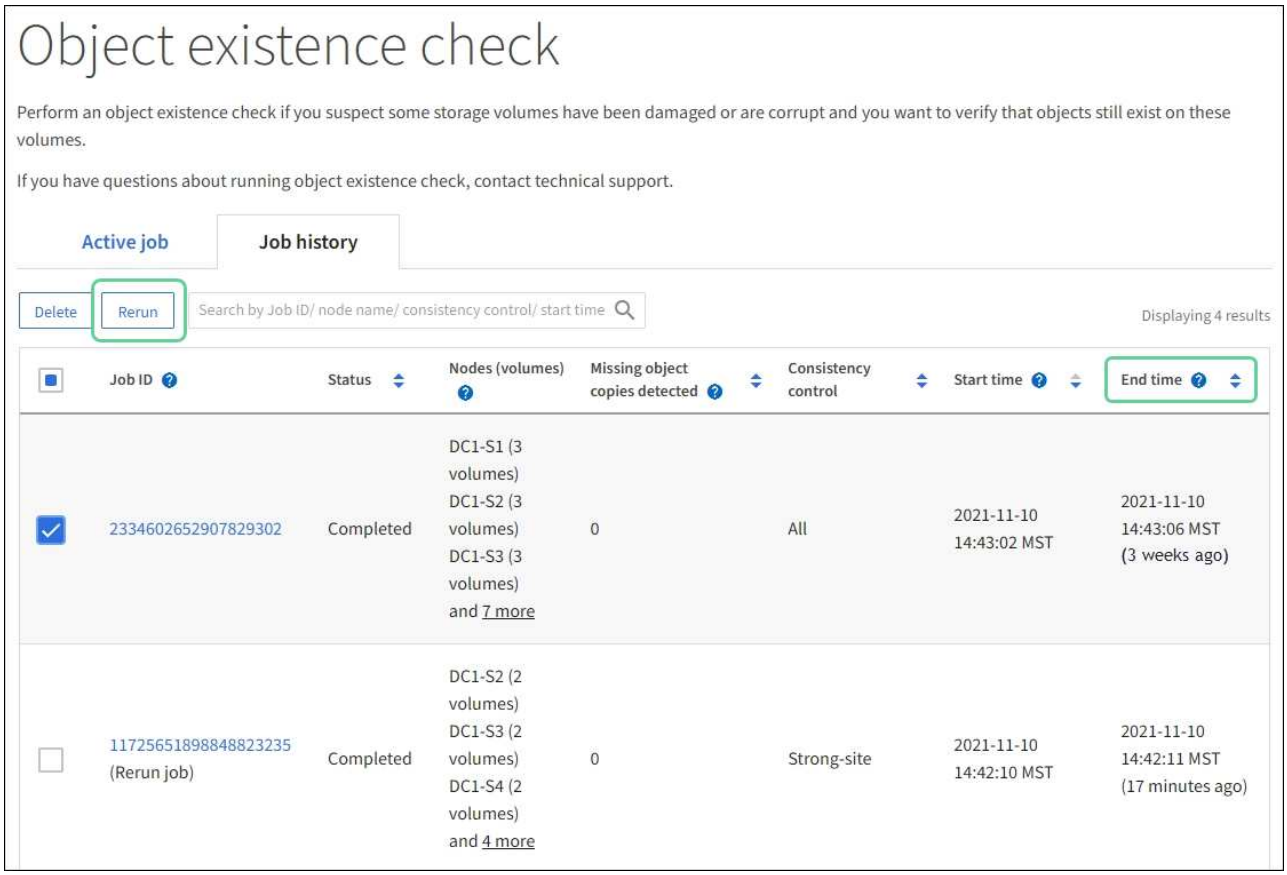
    Quando StorageGRID ha avuto il tempo di ottenere la coerenza dei metadati per i nodi e i volumi inclusi nel processo, la riesecuzione del processo potrebbe eliminare le copie degli oggetti mancanti segnalate erroneamente o causare il controllo di altre copie degli oggetti in caso di mancata esecuzione.

    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.

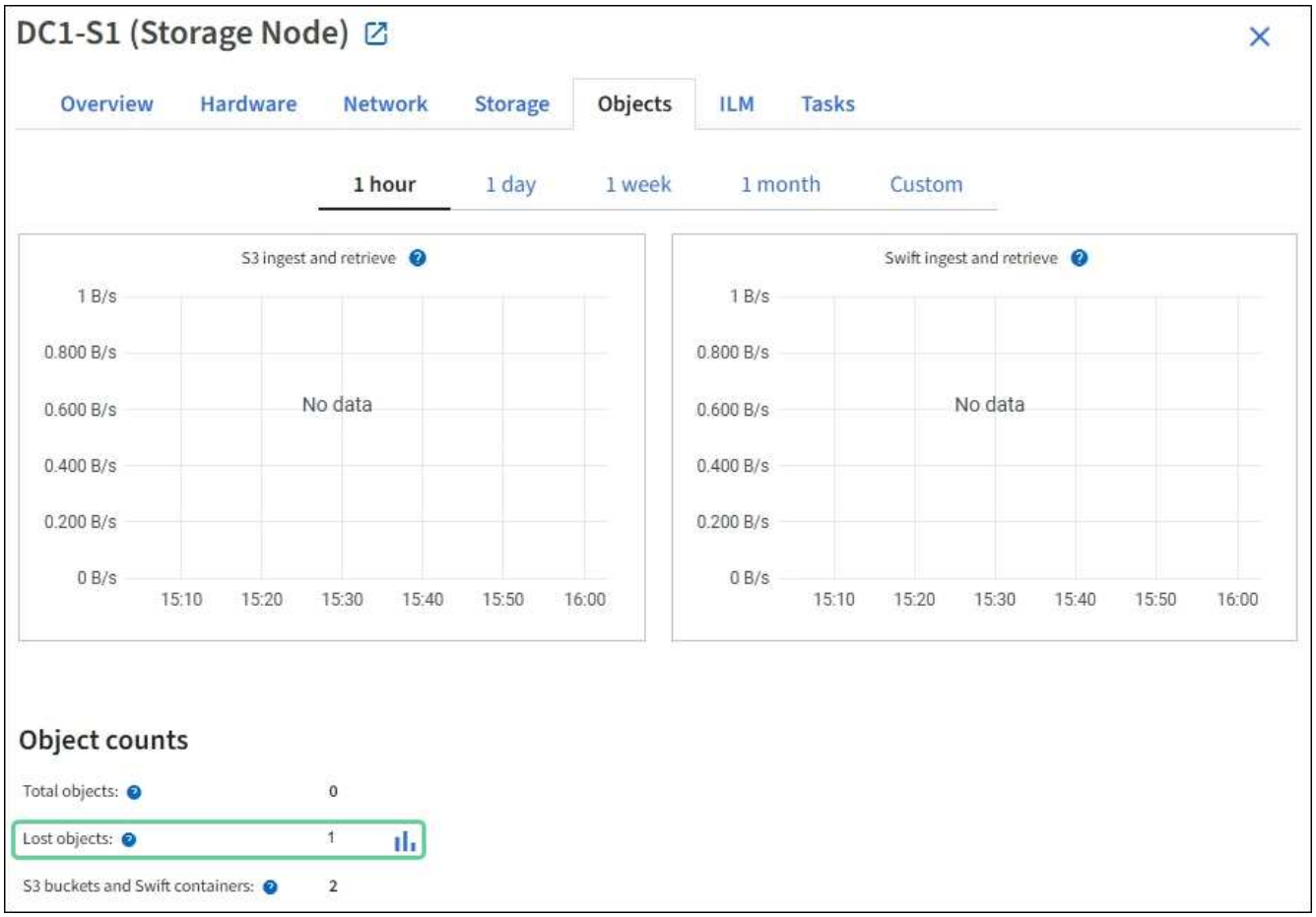
Esaminare immediatamente gli avvisi di oggetti smarriti. Potrebbe essere necessario intervenire per evitare ulteriori perdite di dati. In alcuni casi, potrebbe essere possibile ripristinare un oggetto perso se si esegue un'azione rapida.

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

Ripristinare i conteggi degli oggetti persi e mancanti

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

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

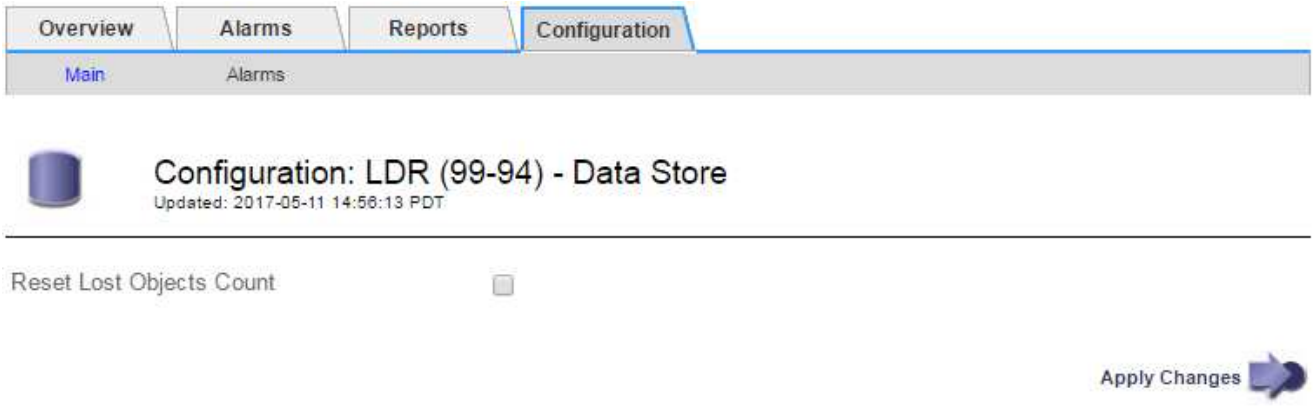
È possibile reimpostare il contatore Lost Objects da una delle seguenti pagine:

- **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.

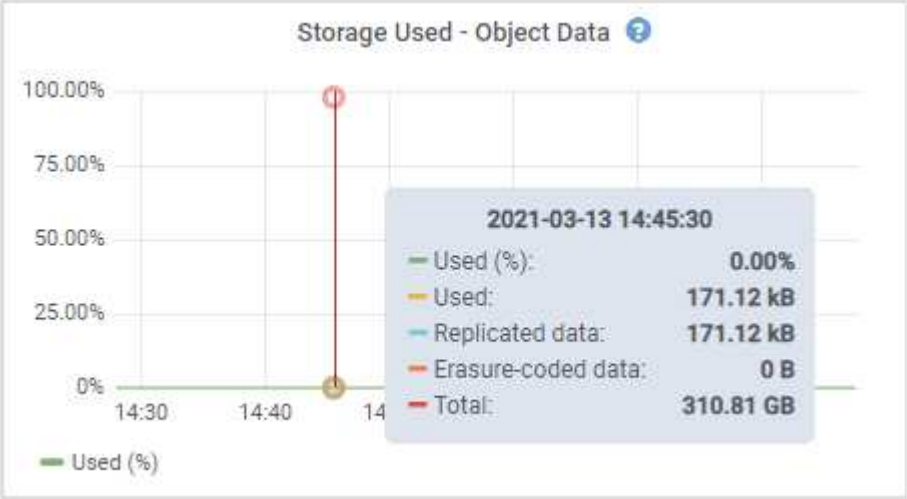
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low Object Data Storage**, se necessario, e selezionare l'avviso che si desidera visualizzare.

   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

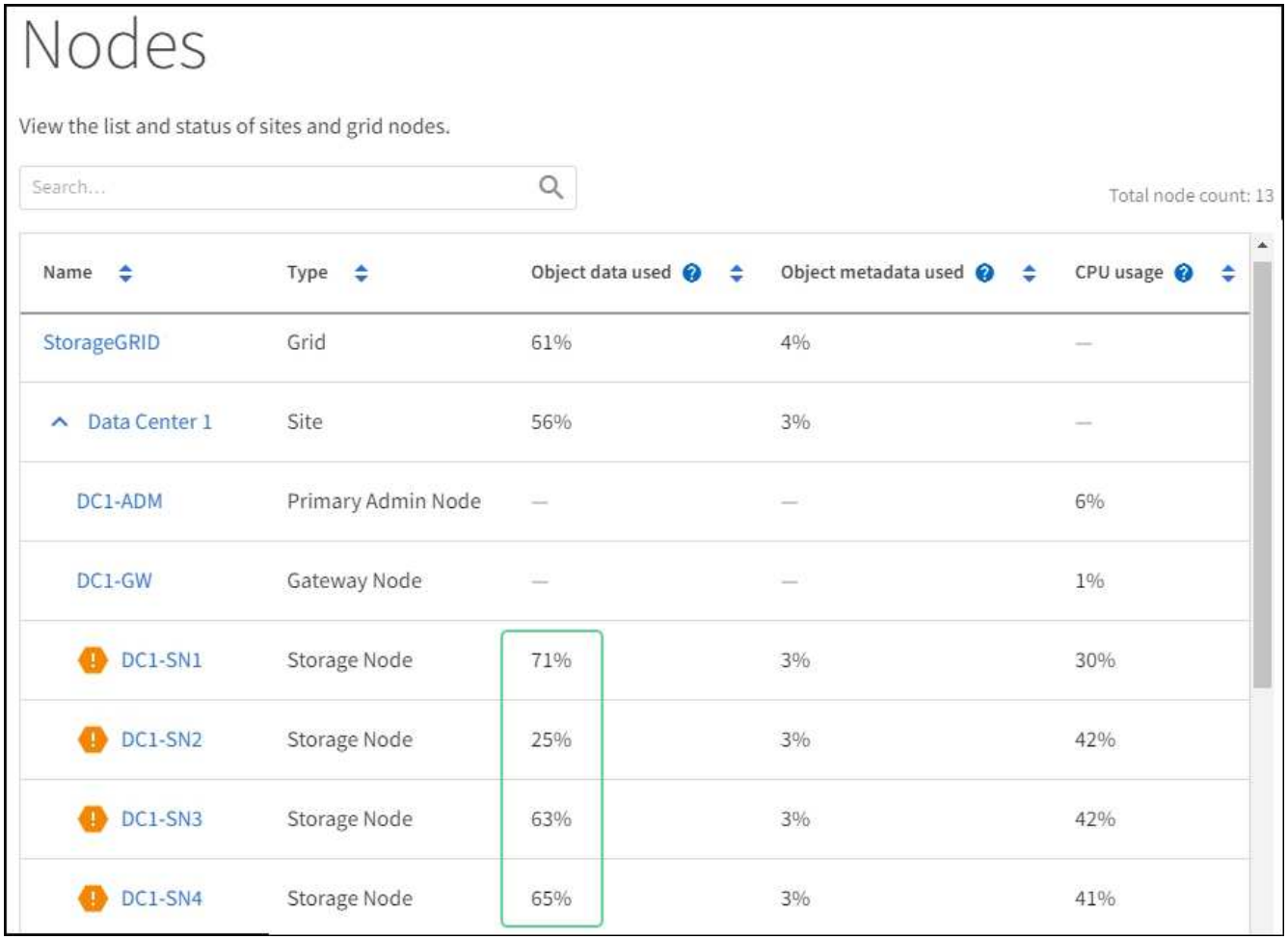
- L'aggiornamento a StorageGRID 11.6 è stato completato.
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root.

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.

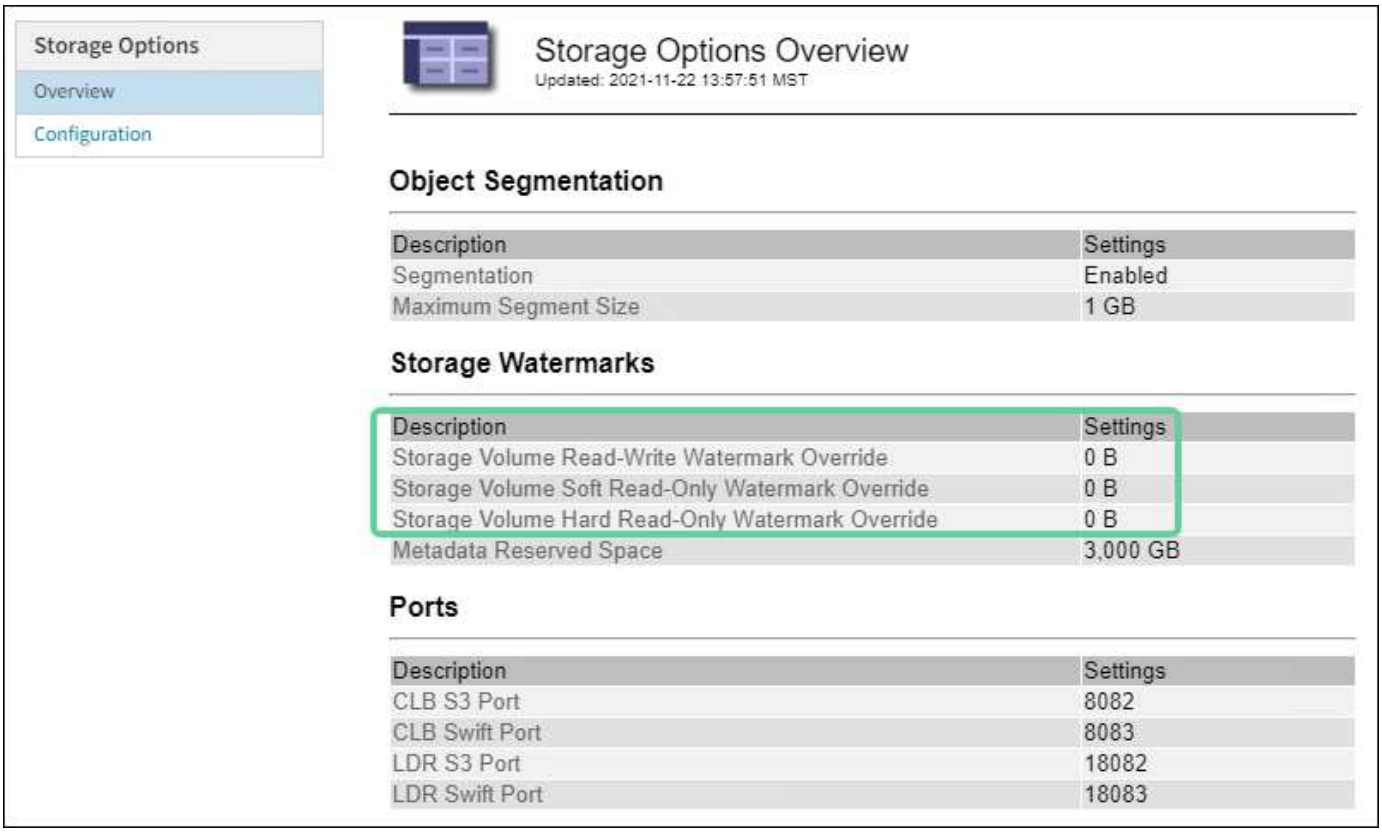
4. Se è necessario continuare a utilizzare valori personalizzati per le filigrane del volume di storage, silenzio oppure disattiva L'avviso **deroga filigrana di sola lettura bassa**.

   > 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

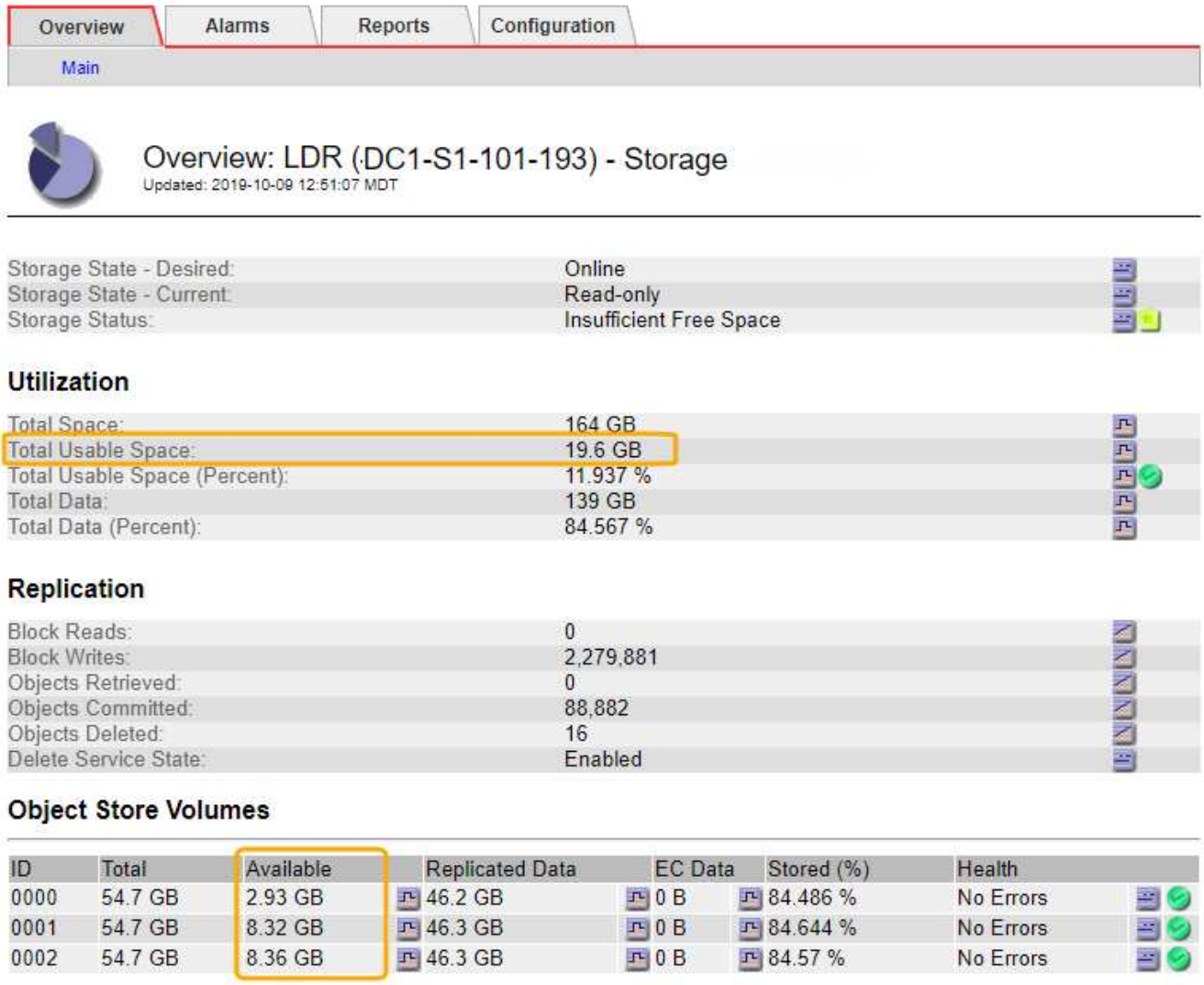
Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT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

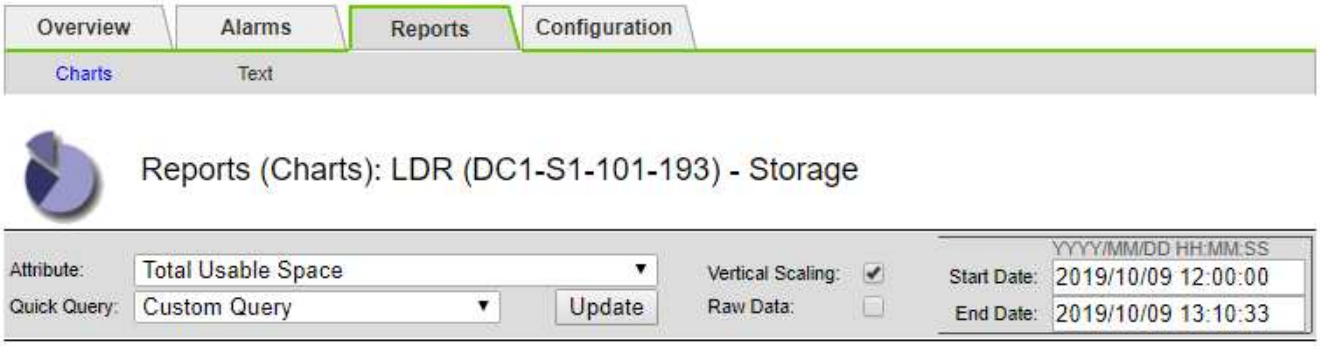
3. Per determinare la quantità di spazio utilizzabile effettivamente disponibile, selezionare **LDR Storage Overview** e individuare l'attributo Total Usable Space (STAS).

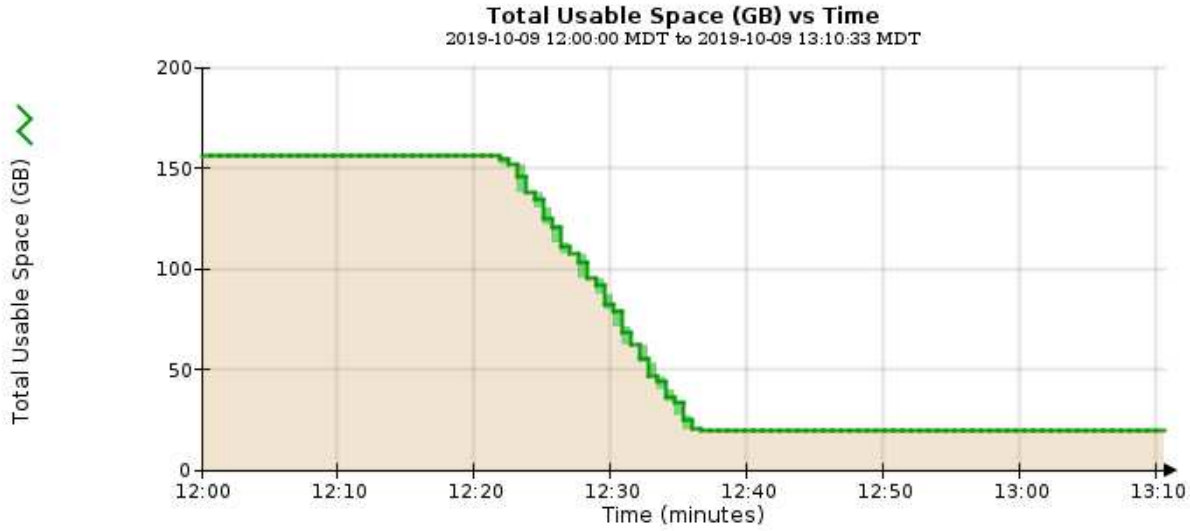


In questo esempio, rimangono disponibili solo 19.6 GB dei 164 GB di spazio su questo nodo di storage. Si noti che il valore totale è la somma dei valori **Available** per i tre volumi dell'archivio di oggetti. L'allarme SSTS è stato attivato perché ciascuno dei tre volumi di storage aveva meno di 10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

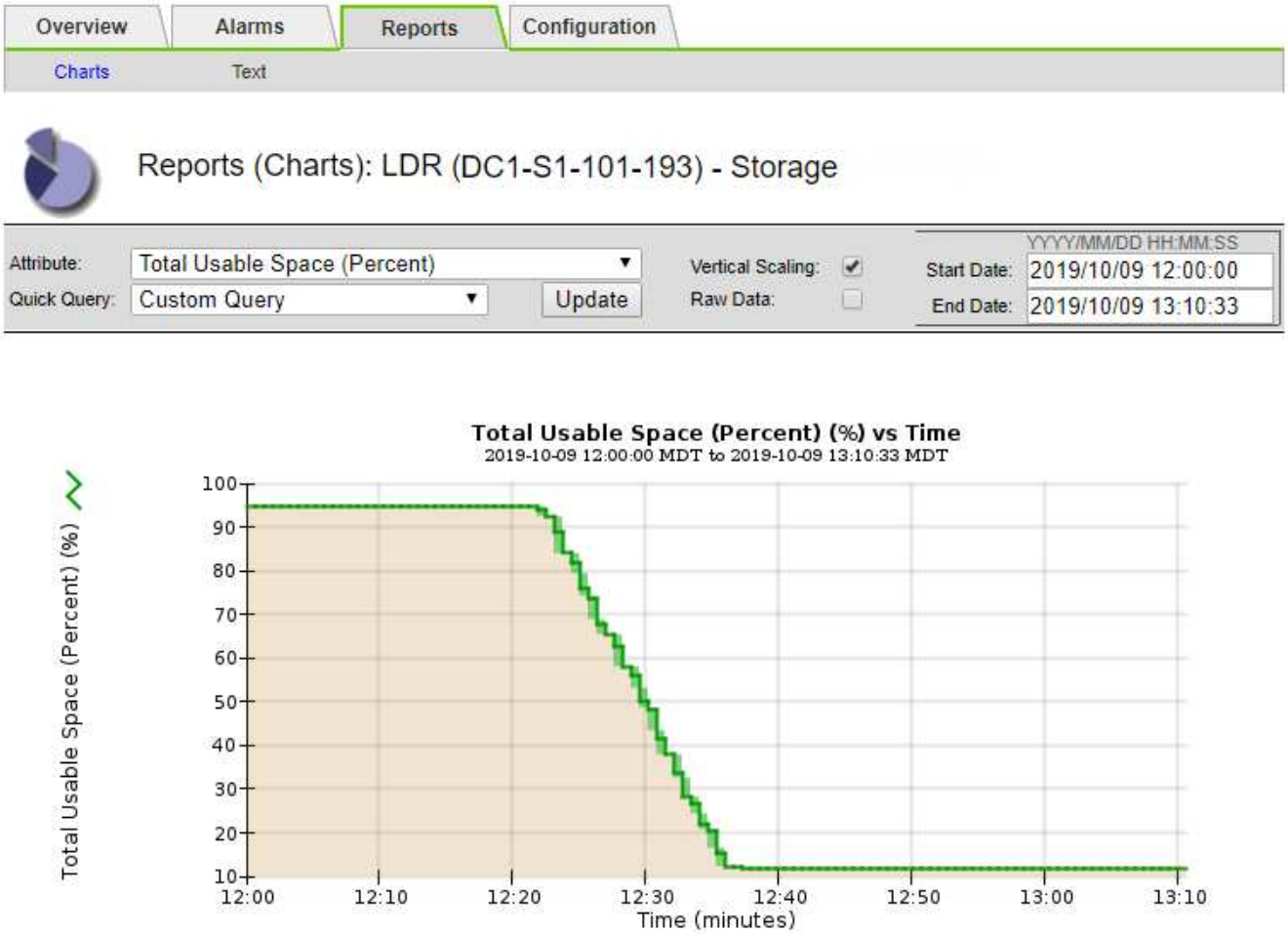
   In questo esempio, lo spazio utilizzabile totale è sceso da circa 155 GB a 12:00 a 20 GB a 12:35, il che corrisponde al momento in cui è stato attivato l'allarme SSTS.





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

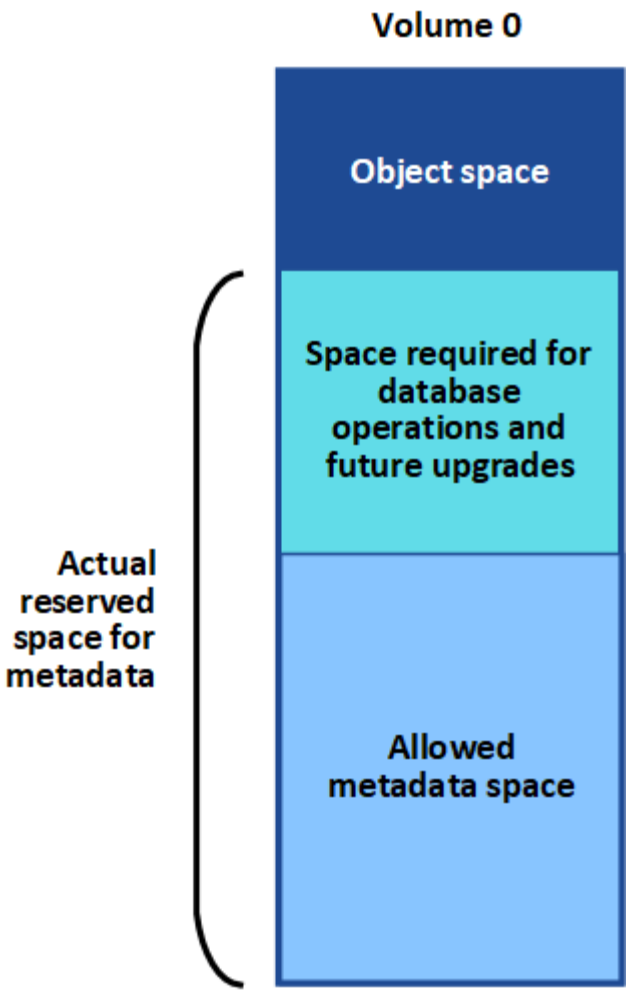
Se viene attivato l'avviso **Low metadata storage**, è necessario aggiungere nuovi nodi di storage.

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.

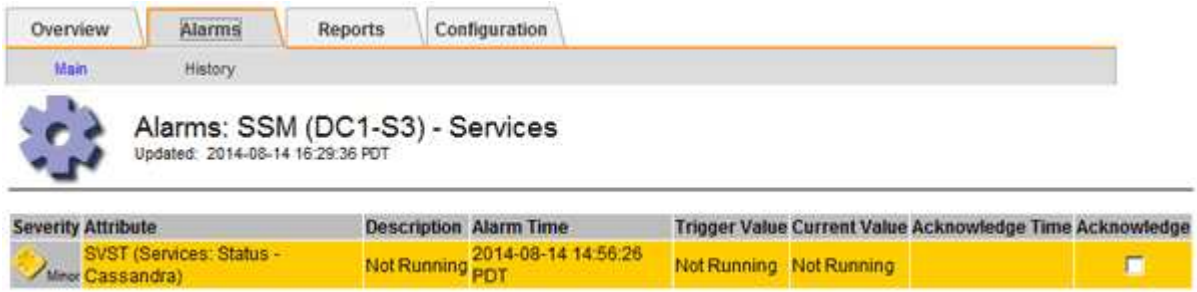
È possibile eseguire la diagnostica per ottenere ulteriori informazioni sullo stato corrente della griglia.

> 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.

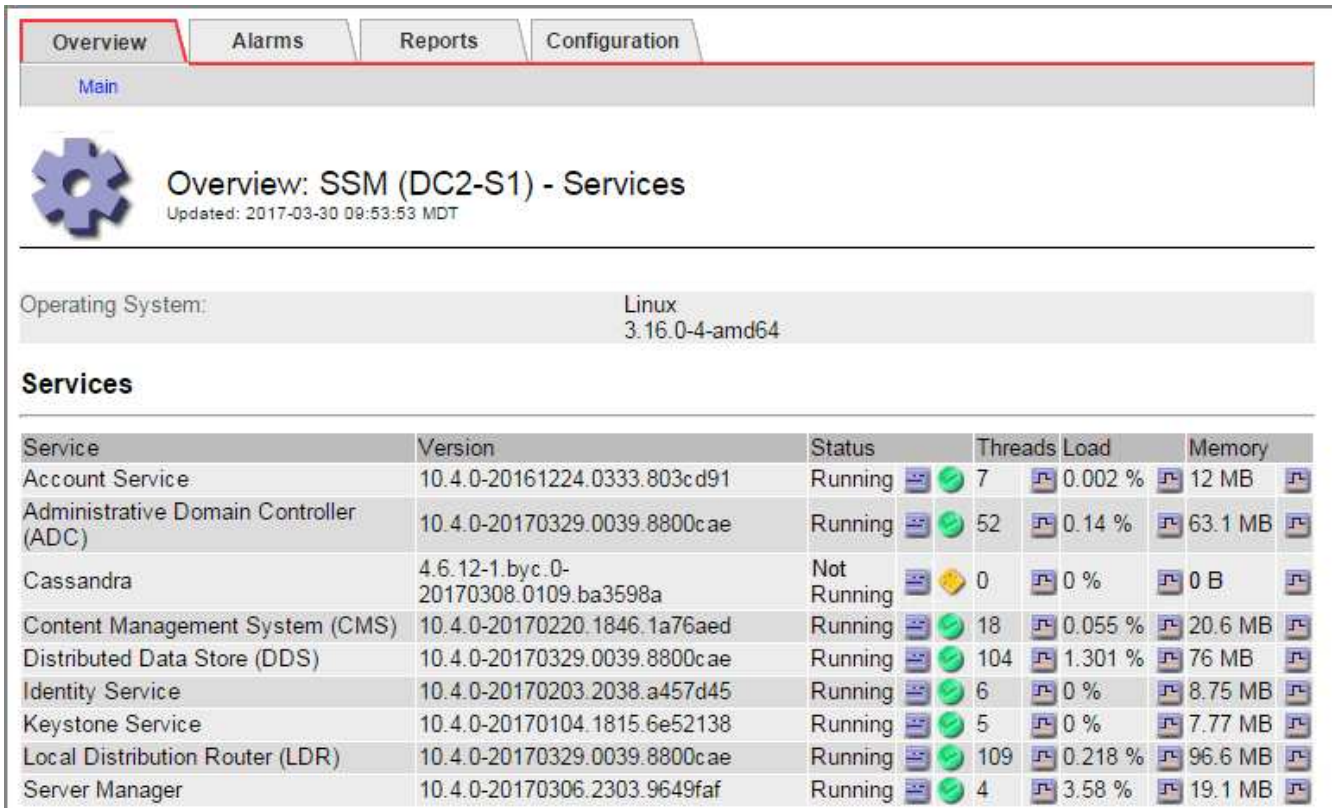
Fasi

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.



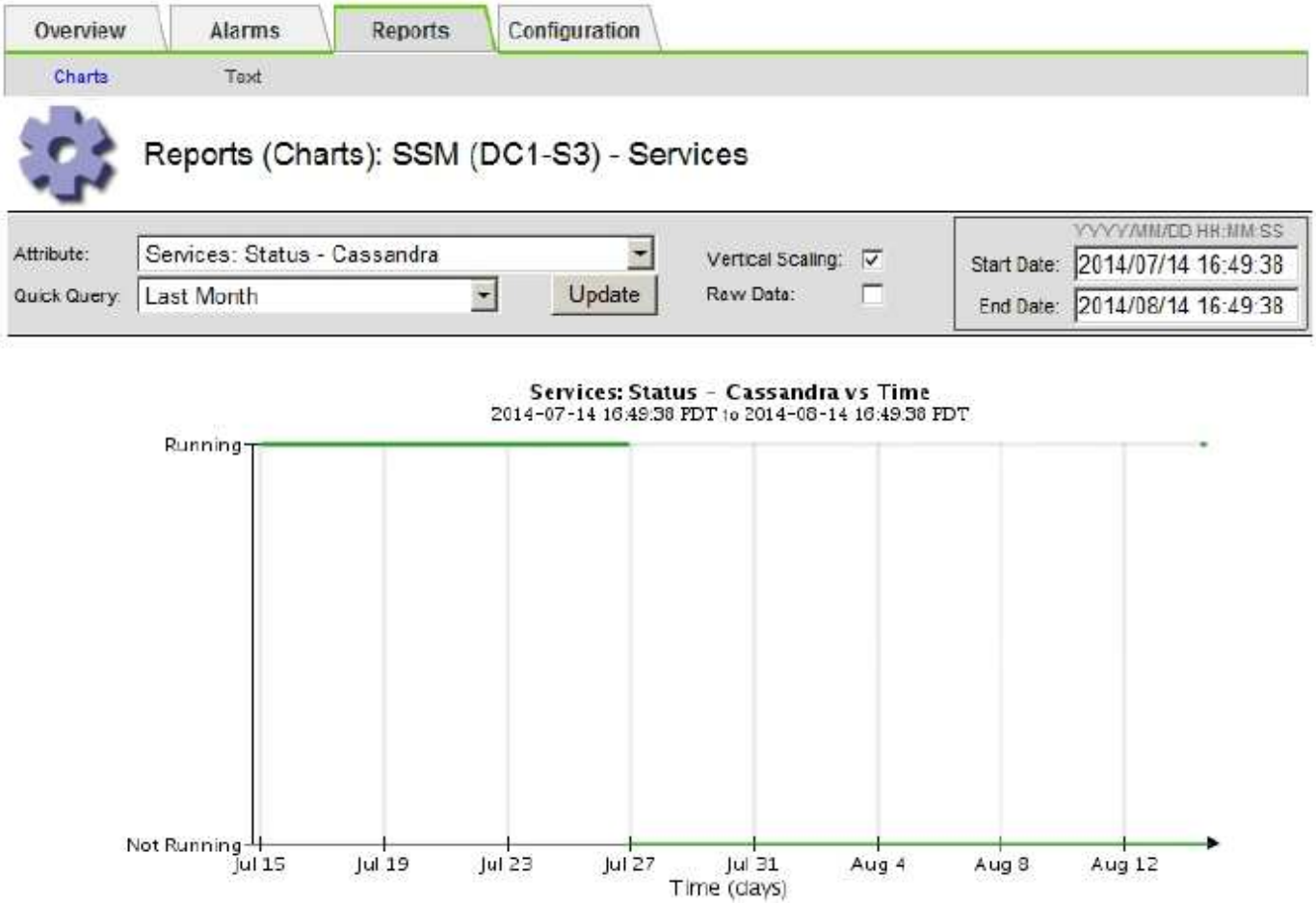
3. prova a riavviare Cassandra dal nodo di storage:
   a. Accedere al nodo Grid:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la 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.

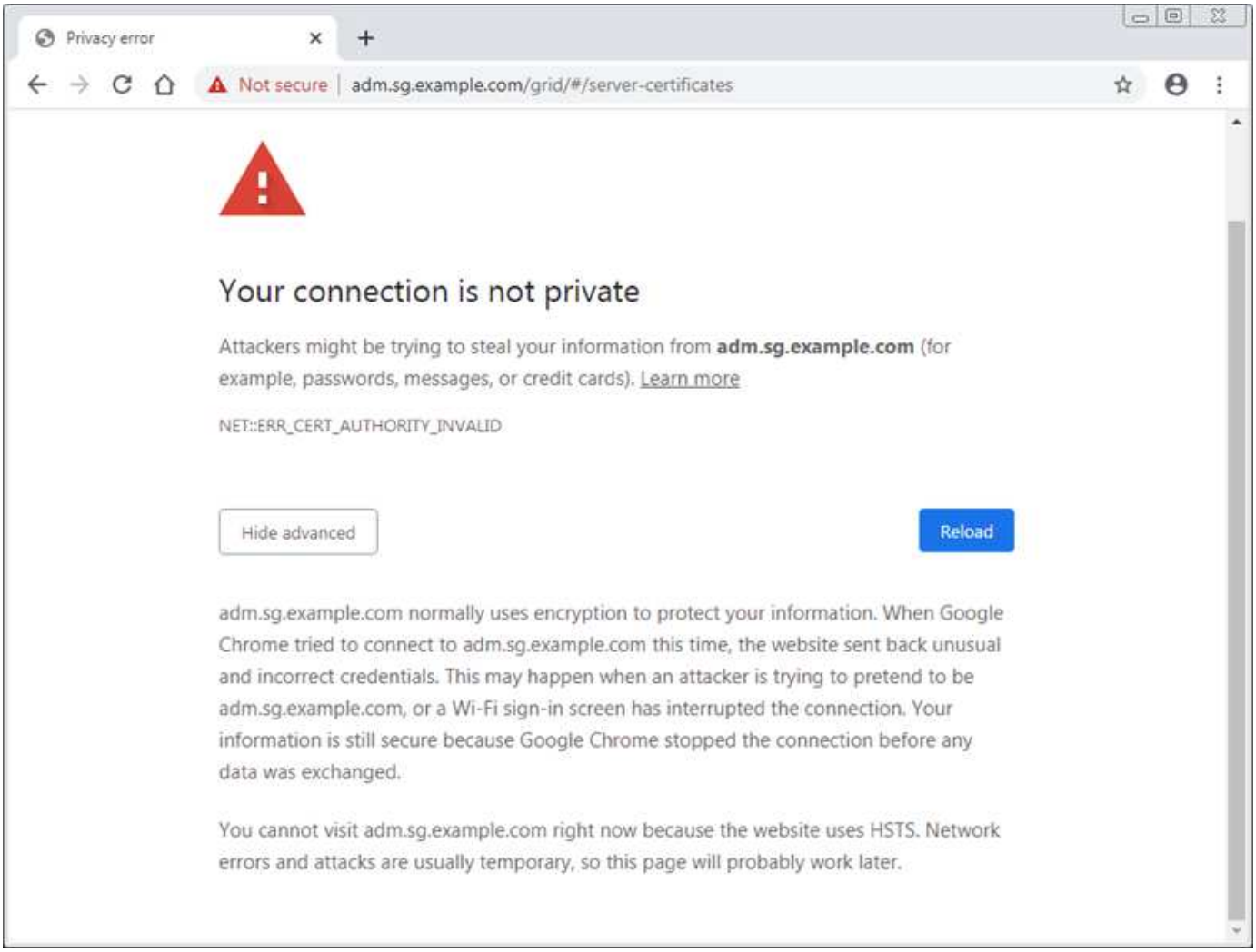
A proposito di questa attività

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

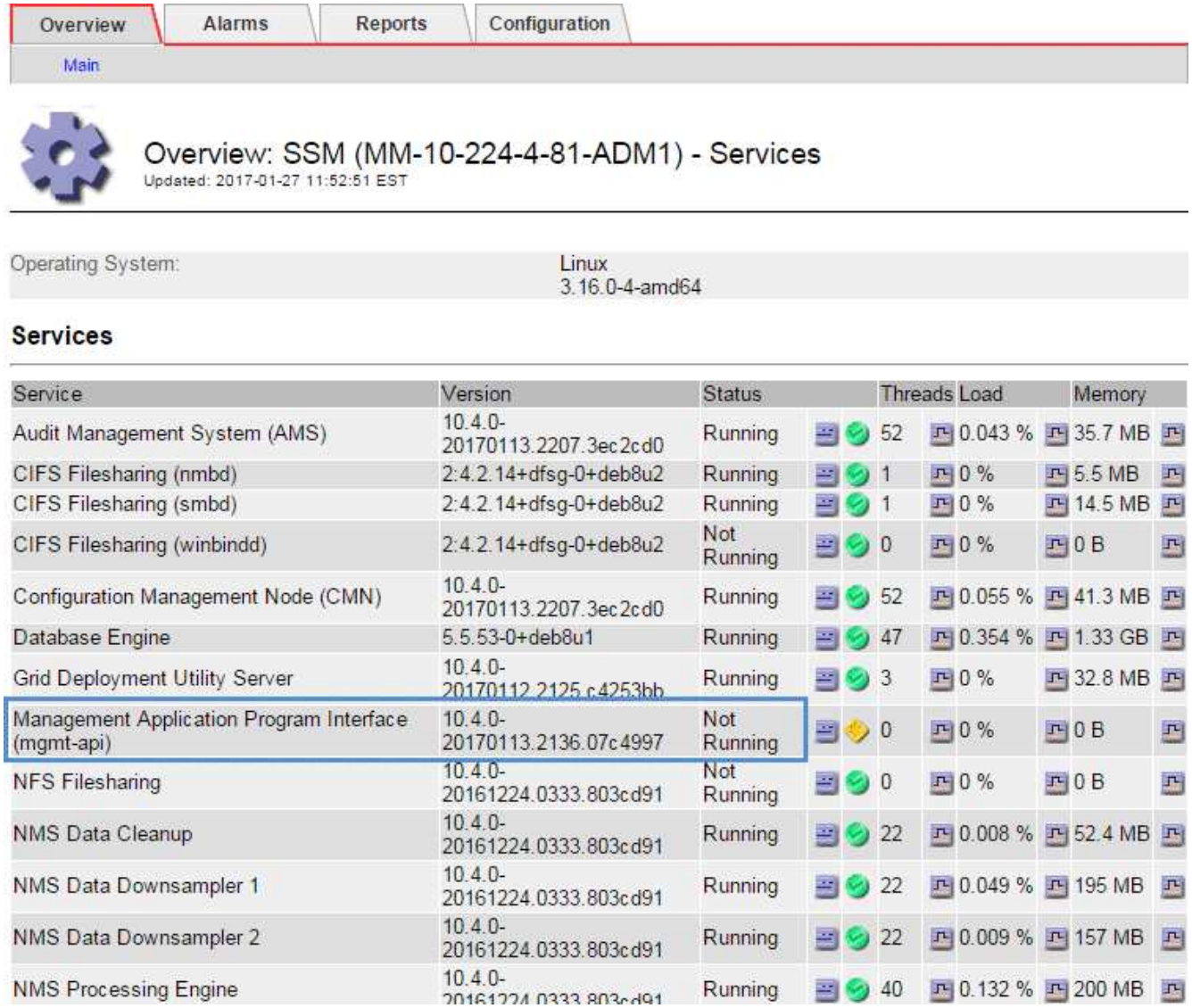
Se il sistema StorageGRID include più nodi di amministrazione, è possibile utilizzare un altro nodo di amministrazione per controllare lo stato di un nodo di amministrazione non disponibile.

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
   ```

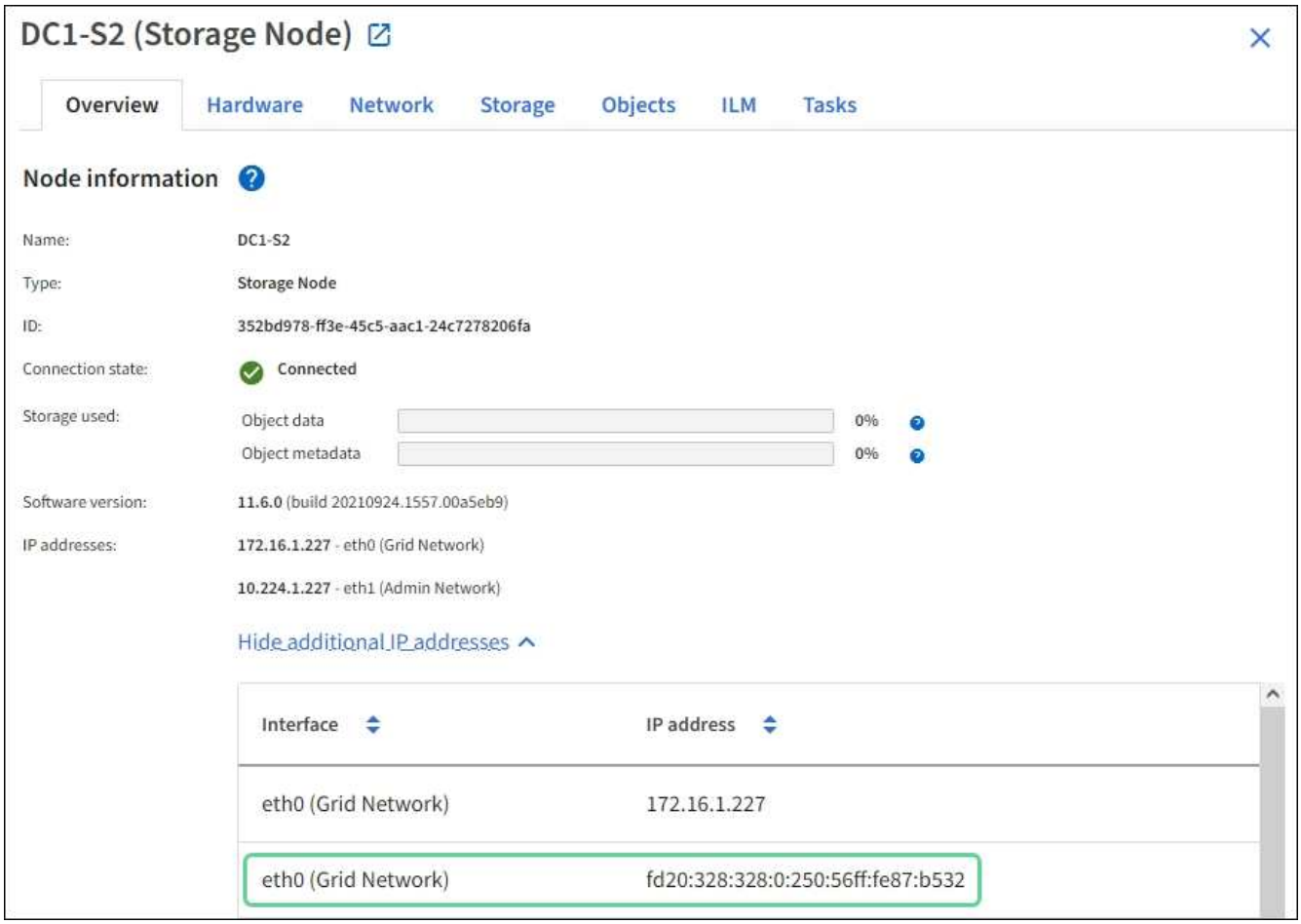
Linux: Risoluzione dei problemi relativi al supporto IPv6

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.
lumberjack.log	Messaggi di debug relativi alla raccolta dei log.

Percorso di archiviazione	Descrizione
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
`/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

Nome del file	Note	Trovato in
`/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

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

Severità dei messaggi nel bycast.log

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

Ad esempio:

- **NOTA** — si è verificato un evento da registrare. La maggior parte dei messaggi di log è a questo livello.
- **ATTENZIONE** — si è verificata una condizione imprevista.
- **ERRORE** — si è verificato un errore grave che ha un impatto sulle operazioni.
- **CRITICO** — si è verificata una condizione anomala che ha interrotto le normali operazioni. È necessario risolvere immediatamente la condizione sottostante. I messaggi critici vengono visualizzati anche in Grid Manager. Selezionare **SUPPORT Tools Grid topology**. Quindi selezionare **Sito nodo SSM Eventi**.

Codici di errore in `bycast.log`

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

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

Codice di errore	Significato
SUC	Nessun errore
GERR	Sconosciuto
CANC	Annullato
ABRT	Interrotto

Codice di errore	Significato
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
010	ECHILD	Nessun processo figlio

Numero di errore	Codice di errore	Significato
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
031	EMSINK	Troppi collegamenti

Numero di errore	Codice di errore	Significato
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
052	EBADE	Scambio non valido

Numero di errore	Codice di errore	Significato
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
073	EDOTDOT	Errore specifico RFS

Numero di errore	Codice di errore	Significato
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
093	EPROTONOSUPPORT	Protocollo non supportato

Numero di errore	Codice di errore	Significato
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
114	EALREADY	Operazione già in corso

Numero di errore	Codice di errore	Significato
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

Espandi il tuo grid

Espandi la tua griglia: Panoramica

Utilizzare queste istruzioni per espandere la capacità o le funzionalità del sistema StorageGRID senza interrompere le operazioni del sistema.

A proposito di queste istruzioni

Queste istruzioni descrivono come eseguire un'espansione StorageGRID per aggiungere volumi di storage a nodi di storage, nuovi nodi grid a un sito esistente o a un intero nuovo sito.

Queste istruzioni sono destinate al personale tecnico responsabile della configurazione e del supporto del sistema StorageGRID dopo l'installazione.

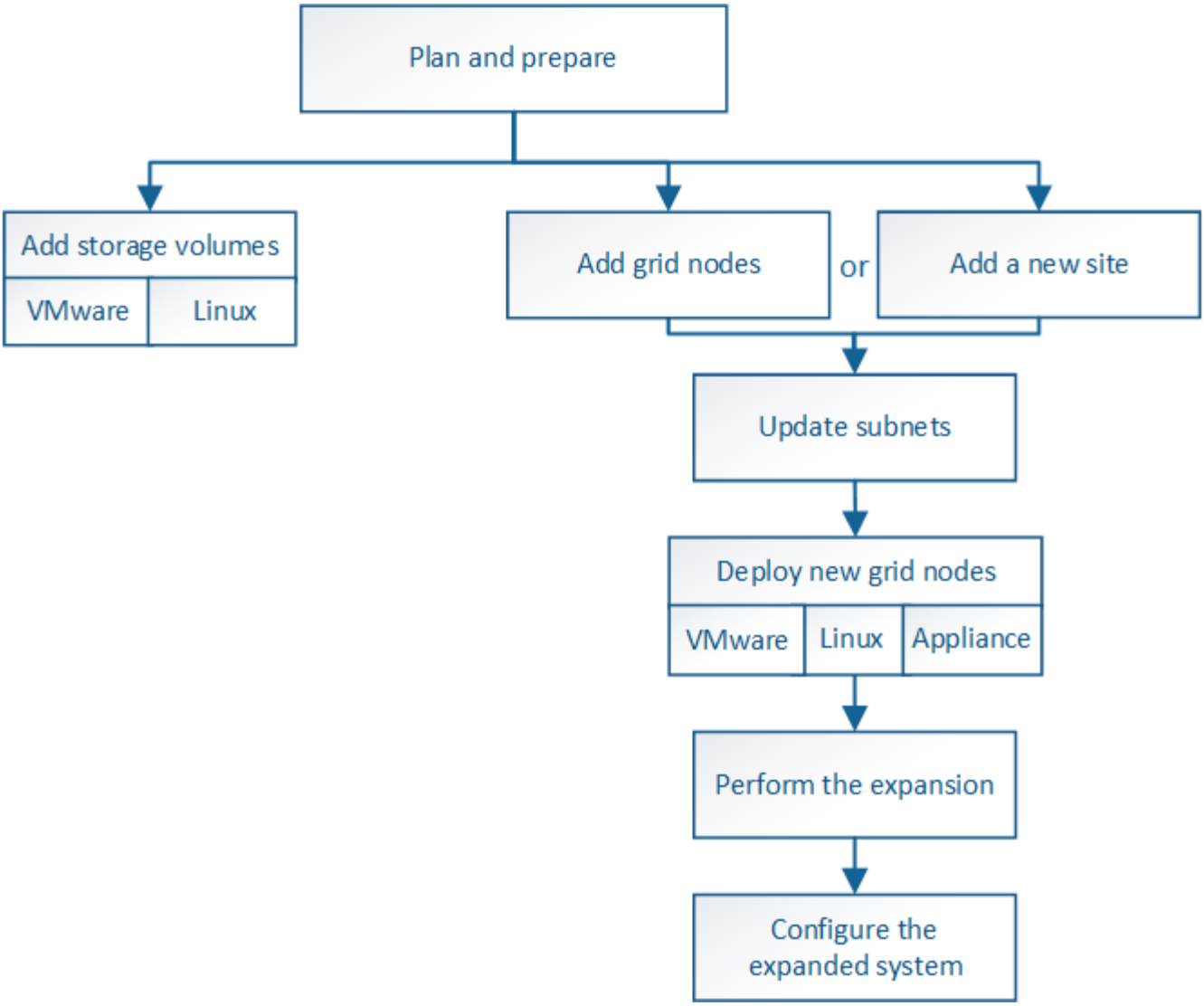
Panoramica della procedura di espansione

Il motivo dell'espansione determina il numero di nuovi nodi di ciascun tipo da aggiungere e la posizione dei nuovi nodi. Ad esempio, se si esegue un'espansione per aumentare la capacità dello storage, aggiungere la capacità dei metadati o aggiungere ridondanza o nuove funzionalità, esistono diversi requisiti dei nodi.

Come mostrato nel diagramma del flusso di lavoro, le fasi per eseguire un'espansione dipendono dall'aggiunta di volumi di storage a un nodo di storage, dall'aggiunta di nuovi nodi a un sito esistente o dall'aggiunta di un nuovo sito. In tutti i casi, è possibile eseguire l'espansione senza interrompere il funzionamento del sistema corrente.

La procedura per l'aggiunta di nodi dipende anche dall'aggiunta di appliance StorageGRID o di host che eseguono VMware o Linux.

> "Linux" si riferisce a una distribuzione Red Hat® Enterprise Linux®, Ubuntu®, CentOS o Debian®. Utilizzare "Tool di matrice di interoperabilità NetApp (IMT)" per ottenere un elenco delle versioni supportate.



Pianificare l'espansione di StorageGRID

Aggiungere capacità di storage

Linee guida per l'aggiunta della capacità degli oggetti

È possibile espandere la capacità dello storage a oggetti del sistema StorageGRID aggiungendo volumi di storage ai nodi di storage esistenti o aggiungendo nuovi nodi di storage ai siti esistenti. È necessario aggiungere capacità di storage in modo che soddisfi i requisiti della policy ILM (Information Lifecycle Management).

Linee guida per l'aggiunta di volumi di storage

Prima di aggiungere volumi di storage ai nodi di storage esistenti, consultare le seguenti linee guida e limitazioni:

- È necessario esaminare le regole ILM correnti per determinare dove e quando aggiungere volumi di storage per aumentare lo storage disponibile per gli oggetti replicati o con codifica di cancellazione. Consultare le istruzioni per gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

- Non è possibile aumentare la capacità dei metadati del sistema aggiungendo volumi di storage perché i metadati degli oggetti vengono memorizzati solo sul volume 0.
- Ogni nodo di storage basato su software può supportare un massimo di 16 volumi di storage. Se è necessario aggiungere capacità oltre tale limite, è necessario aggiungere nuovi nodi di storage.
- È possibile aggiungere uno o due shelf di espansione a ciascuna appliance SG6060 o SG6060X. Ogni shelf di espansione aggiunge 16 volumi di storage. Con entrambi gli shelf di espansione installati, SG6060 e SG6060X possono supportare ciascuno un totale di 48 volumi di storage.
- Non è possibile aggiungere volumi di storage ad altre appliance di storage.
- Non è possibile aumentare le dimensioni di un volume di storage esistente.
- Non è possibile aggiungere volumi di storage a un nodo di storage contemporaneamente all'aggiornamento del sistema, all'operazione di recovery o a un'altra espansione.

Dopo aver deciso di aggiungere volumi di storage e aver determinato i nodi di storage da espandere per soddisfare la policy ILM, seguire le istruzioni relative al tipo di nodo di storage:

- Per aggiungere uno o due shelf di espansione a un'appliance di storage SG6060 o SG6060X, visitare il sito Web all'indirizzo Aggiungere shelf di espansione a SG6060 o SG6060X implementati.
- Per un nodo basato su software, seguire le istruzioni perAggiunta di volumi di storage ai nodi di storage.

Linee guida per l'aggiunta di nodi di storage

Prima di aggiungere nodi di storage ai siti esistenti, consultare le seguenti linee guida e limitazioni:

- È necessario esaminare le regole ILM correnti per determinare dove e quando aggiungere nodi di storage per aumentare lo storage disponibile per gli oggetti replicati o con codifica di cancellazione. Consultare le istruzioni per gestione degli oggetti con la gestione del ciclo di vita delle informazioni.
- Non aggiungere più di 10 nodi di storage in una singola procedura di espansione.
- È possibile aggiungere nodi di storage a più siti in una singola procedura di espansione.
- È possibile aggiungere nodi di storage e altri tipi di nodi in una singola procedura di espansione.
- Prima di avviare la procedura di espansione, è necessario confermare che tutte le operazioni di riparazione dei dati eseguite nell'ambito di un ripristino sono state completate. Vedere Controllare i lavori di riparazione dei dati.
- Se è necessario rimuovere i nodi di storage prima o dopo l'esecuzione di un'espansione, non è necessario decommissionare più di 10 nodi di storage in una singola procedura Decommission Node.

Linee guida per il servizio ADC sui nodi di storage

Quando si configura l'espansione, è necessario scegliere se includere il servizio ADC (Administrative Domain Controller) in ogni nuovo nodo di storage. Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi grid.

- Il sistema StorageGRID richiede un Quorum dei servizi ADC essere disponibile in ogni sito e in qualsiasi momento.
- Almeno tre nodi di storage in ogni sito devono includere il servizio ADC.
- Si sconsiglia di aggiungere il servizio ADC a ogni nodo di storage. L'inclusione di un numero eccessivo di servizi ADC può causare rallentamenti dovuti all'aumento della comunicazione tra i nodi.
- Un singolo grid non deve avere più di 48 nodi di storage con il servizio ADC. Ciò equivale a 16 siti con tre servizi ADC in ogni sito.

- In generale, quando si seleziona l'impostazione **Servizio ADC** per un nuovo nodo, selezionare **automatico**. Selezionare **Sì** solo se il nuovo nodo sostituirà un altro nodo di storage che include il servizio ADC. Poiché non è possibile decommissionare un nodo di storage se rimangono pochi servizi ADC, ciò garantisce che un nuovo servizio ADC sia disponibile prima che il vecchio servizio venga rimosso.
- Non è possibile aggiungere il servizio ADC a un nodo dopo averlo implementato.

Aggiungere capacità di storage per gli oggetti replicati

Se il criterio ILM (Information Lifecycle Management) per l'implementazione include una regola che crea copie replicate di oggetti, è necessario considerare la quantità di storage da aggiungere e la posizione in cui aggiungere i nuovi volumi di storage o i nuovi nodi di storage.

Per informazioni su dove aggiungere storage aggiuntivo, esaminare le regole ILM che creano copie replicate. Se le regole ILM creano due o più copie di oggetti, pianificare di aggiungere storage in ogni posizione in cui vengono eseguite le copie di oggetti. Ad esempio, se si dispone di un grid a due siti e di una regola ILM che crea una copia dell'oggetto in ciascun sito, è necessario aggiungere storage a ciascun sito per aumentare la capacità complessiva dell'oggetto del grid. Consultare le istruzioni per gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Per motivi di performance, dovresti cercare di mantenere la capacità dello storage e la potenza di calcolo bilanciati tra i siti. Pertanto, per questo esempio, è necessario aggiungere lo stesso numero di nodi di storage a ciascun sito o volumi di storage aggiuntivi in ciascun sito.

Se si dispone di una policy ILM più complessa che include regole che posizionano oggetti in posizioni diverse in base a criteri come il nome del bucket o regole che cambiano le posizioni degli oggetti nel tempo, l'analisi dei punti in cui è richiesto lo storage per l'espansione sarà simile, ma più complessa.

La creazione di grafici sulla velocità di consumo della capacità di storage complessiva può aiutare a comprendere la quantità di storage da aggiungere all'espansione e quando sarà necessario lo spazio di storage aggiuntivo. È possibile utilizzare Grid Manager per monitorare e memorizzare la capacità di storage come descritto nelle istruzioni per Monitoraggio e risoluzione dei problemi di StorageGRID.

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

Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione

Se il criterio ILM include una regola che crea copie con codifica di cancellazione, è necessario pianificare dove aggiungere nuovo storage e quando aggiungere nuovo storage. La quantità di storage aggiunta e la tempistica dell'aggiunta possono influire sulla capacità di storage utilizzabile del grid.

Il primo passo nella pianificazione di un'espansione dello storage consiste nell'esaminare le regole dei criteri ILM che creano oggetti con codifica in cancellazione. Poiché StorageGRID crea *k+m* frammenti per ogni oggetto con codifica di cancellazione e memorizza ciascun frammento su un nodo di storage diverso, è necessario assicurarsi che almeno *k+m* nodi di storage abbiano spazio per i nuovi dati con codifica di cancellazione dopo l'espansione. Se il profilo di erasure coding fornisce la protezione dalla perdita di sito, è necessario aggiungere storage a ciascun sito. Vedere Gestire gli oggetti con ILM.

Il numero di nodi da aggiungere dipende anche dal livello di riempimento dei nodi esistenti quando si esegue l'espansione.

Raccomandazioni generali per l'aggiunta di capacità di storage per gli oggetti con codifica di cancellazione

Se si desidera evitare calcoli dettagliati, è possibile aggiungere due nodi di storage per sito quando i nodi di storage esistenti raggiungono il 70% della capacità.

Questa raccomandazione generale fornisce risultati ragionevoli in un'ampia gamma di schemi di erasure coding sia per le griglie a sito singolo che per le griglie in cui la codifica erasure fornisce protezione dalle perdite di sito.

Per comprendere meglio i fattori che portano a questo suggerimento o per sviluppare un piano più preciso per il tuo sito, consulta la sezione successiva. Per un consiglio personalizzato e ottimizzato per la tua situazione, contatta il tuo rappresentante commerciale NetApp.

Calcola il numero di nodi storage di espansione da aggiungere per gli oggetti con codifica in cancellazione

Per ottimizzare il modo in cui si espande un'implementazione che memorizza oggetti con codifica in cancellazione, è necessario prendere in considerazione molti fattori:

- Schema di erasure coding in uso
- Caratteristiche del pool di storage utilizzato per l'erasure coding, incluso il numero di nodi in ogni sito e la quantità di spazio libero in ogni nodo
- Se la griglia è stata precedentemente espansa (perché la quantità di spazio libero per nodo di storage potrebbe non essere approssimativamente la stessa su tutti i nodi)
- Natura esatta del criterio ILM, ad esempio se le regole ILM rendono oggetti replicati e codificati in cancellazione

Gli esempi seguenti possono aiutare a comprendere l'impatto dello schema di erasure coding, il numero di nodi nel pool di storage e la quantità di spazio libero su ciascun nodo.

Considerazioni simili influiscono sui calcoli di una policy ILM che memorizza dati replicati e codificati in cancellazione e sui calcoli di una griglia precedentemente espansa.

> Gli esempi di questa sezione rappresentano le Best practice per l'aggiunta di capacità di storage a un sistema StorageGRID. Se non si riesce ad aggiungere il numero di nodi consigliato, potrebbe essere necessario eseguire la procedura di ribilanciamento EC per consentire la memorizzazione di ulteriori oggetti con codifica di cancellazione. Vedere Ribilanciare i dati codificati in cancellazione.

Esempio 1: Espandere la griglia di un sito che utilizza la codifica di cancellazione 2+1

Questo esempio mostra come espandere un semplice grid che include solo tre nodi di storage.

> Questo esempio utilizza solo tre nodi di storage per semplicità. Tuttavia, si sconsiglia di utilizzare solo tre nodi di storage: Un vero e proprio grid di produzione dovrebbe utilizzare un minimo di $k+m+1$ nodi di storage per la ridondanza, che equivale a quattro nodi di storage (2+1+1) per questo esempio.

Si supponga quanto segue:

- Tutti i dati vengono memorizzati utilizzando lo schema di erasure coding 2+1. Con lo schema di erasure coding 2+1, ogni oggetto viene memorizzato come tre frammenti e ogni frammento viene salvato su un

nodo di storage diverso.

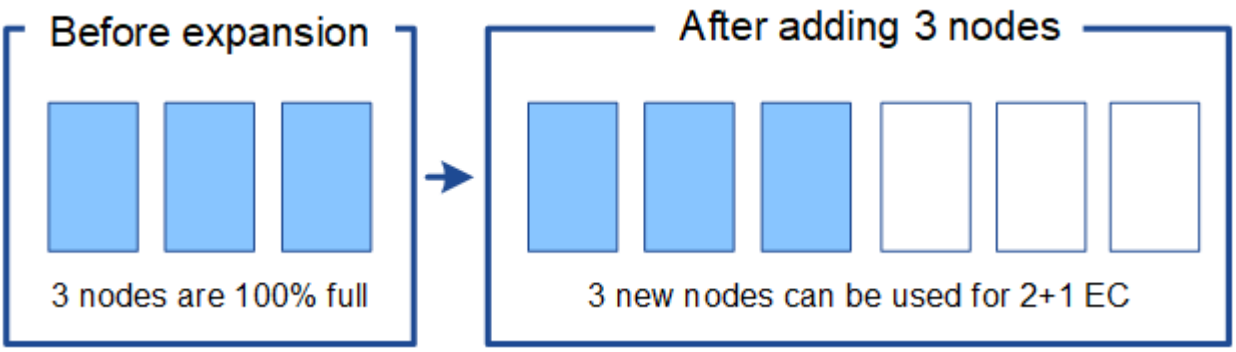
- Hai un sito con tre nodi di storage. Ogni nodo di storage ha una capacità totale di 100 TB.
- Si desidera espandere aggiungendo nuovi nodi di storage da 100 TB.
- Si desidera bilanciare i dati con codifica erasure tra il vecchio e il nuovo nodo.

Sono disponibili diverse opzioni, in base alla quantità di memoria dei nodi di storage quando si esegue l'espansione.

- **Aggiungere tre nodi di storage da 100 TB quando i nodi esistenti sono pieni al 100%**

  In questo esempio, i nodi esistenti sono pieni al 100%. Poiché non esiste capacità libera, è necessario aggiungere immediatamente tre nodi per continuare la cancellazione della codifica 2+1.

  Una volta completata l'espansione, quando gli oggetti vengono codificati in modo cancellabile, tutti i frammenti verranno posizionati sui nuovi nodi.

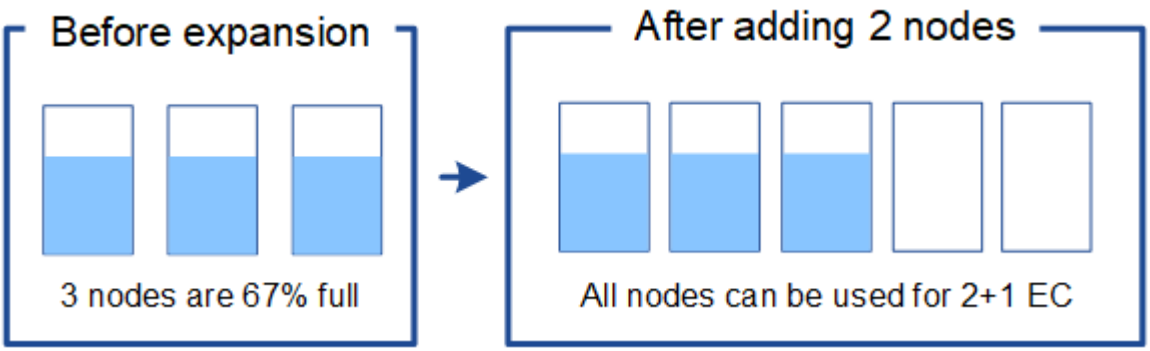


> Questa espansione aggiunge *k+m* nodi. Si consiglia di aggiungere quattro nodi per la ridondanza. Se si aggiungono solo nodi storage di espansione *k+m* quando i nodi esistenti sono pieni al 100%, tutti i nuovi oggetti vengono memorizzati nei nodi di espansione. Se uno dei nuovi nodi diventa non disponibile, anche temporaneamente, StorageGRID non può soddisfare i requisiti ILM.

- **Aggiungere due nodi di storage da 100 TB, quando i nodi di storage esistenti sono pieni al 67%**

  In questo esempio, i nodi esistenti sono pieni al 67%. Poiché i nodi esistenti (33 TB per nodo) offrono 100 TB di capacità libera, è necessario aggiungere due nodi solo se si esegue l'espansione ora.

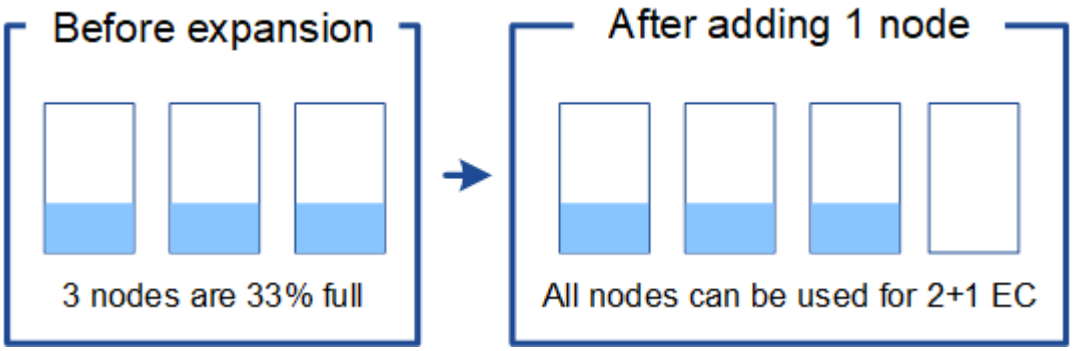
  L'aggiunta di 200 TB di capacità aggiuntiva consente di continuare la cancellazione 2+1 della codifica e di bilanciare i dati con codifica erasure in tutti i nodi.



- **Aggiungere un nodo di storage da 100 TB quando i nodi di storage esistenti sono pieni al 33%**

  In questo esempio, i nodi esistenti sono pieni al 33%. Poiché i nodi esistenti (67 TB per nodo) offrono 200 TB di capacità libera, è necessario aggiungere un solo nodo se si esegue l'espansione ora.

  L'aggiunta di 100 TB di capacità aggiuntiva consente di continuare la cancellazione 2+1 della codifica e di bilanciare i dati con codifica erasure in tutti i nodi.



Esempio 2: Espandere la griglia a tre siti che utilizza la codifica di cancellazione 6+3

Questo esempio mostra come sviluppare un piano di espansione per un grid multi-sito con uno schema di erasure coding con un numero maggiore di frammenti. Nonostante le differenze tra questi esempi, il piano di espansione consigliato è molto simile.

Si supponga quanto segue:

- Tutti i dati vengono memorizzati utilizzando lo schema di erasure coding 6+3. Con lo schema di erasure coding 6+3, ogni oggetto viene memorizzato come 9 frammenti e ogni frammento viene salvato in un nodo di storage diverso.
- Si dispone di tre siti e ciascun sito dispone di quattro nodi di storage (12 nodi in totale). Ogni nodo ha una capacità totale di 100 TB.
- Si desidera espandere aggiungendo nuovi nodi di storage da 100 TB.
- Si desidera bilanciare i dati con codifica erasure tra il vecchio e il nuovo nodo.

Sono disponibili diverse opzioni, in base alla quantità di memoria dei nodi di storage quando si esegue l'espansione.

- **Aggiungere nove nodi di storage da 100 TB (tre per sito), quando i nodi esistenti sono pieni al 100%**

  In questo esempio, i 12 nodi esistenti sono pieni al 100%. Poiché non esiste capacità libera, è necessario aggiungere immediatamente nove nodi (900 TB di capacità aggiuntiva) per continuare la cancellazione dei codici 6+3.

  Una volta completata l'espansione, quando gli oggetti vengono codificati in modo cancellabile, tutti i frammenti verranno posizionati sui nuovi nodi.

  > Questa espansione aggiunge *k+m* nodi. Si consiglia di aggiungere 12 nodi (quattro per sito) per la ridondanza. Se si aggiungono solo nodi storage di espansione *k+m* quando i nodi esistenti sono pieni al 100%, tutti i nuovi oggetti vengono memorizzati nei nodi di espansione. Se uno dei nuovi nodi diventa non disponibile, anche temporaneamente, StorageGRID non può soddisfare i requisiti ILM.

- **Aggiungere sei nodi di storage da 100 TB (due per sito), quando i nodi esistenti sono pieni al 75%**

  In questo esempio, i 12 nodi esistenti sono pieni al 75%. Poiché esistono 300 TB di capacità libera (25 TB per nodo), è necessario aggiungere sei nodi solo se si esegue l'espansione ora. Aggiungere due nodi a ciascuno dei tre siti.

  L'aggiunta di 600 TB di capacità di storage consente di continuare la cancellazione di codici 6+3 e di bilanciare i dati con codifica erasure in tutti i nodi.

- **Aggiungere tre nodi di storage da 100 TB (uno per sito), quando i nodi esistenti sono pieni al 50%**

  In questo esempio, i 12 nodi esistenti sono pieni al 50%. Poiché esistono 600 TB di capacità libera (50 TB per nodo), è sufficiente aggiungere tre nodi se si esegue l'espansione ora. Aggiungere un nodo a ciascuno dei tre siti.

  L'aggiunta di 300 TB di capacità di storage consente di continuare la cancellazione di codici 6+3 e di bilanciare i dati con codifica erasure in tutti i nodi.

Considerazioni per il ribilanciamento dei dati con codifica erasure

Se si sta eseguendo un'espansione per aggiungere nodi di storage e il criterio ILM include una o più regole ILM per la cancellazione dei dati del codice, potrebbe essere necessario eseguire la procedura di ribilanciamento EC al termine dell'espansione.

Ad esempio, se non è possibile aggiungere il numero consigliato di nodi di storage per lo schema di erasure coding in uso, potrebbe essere necessario eseguire la procedura di ribilanciamento EC per consentire la memorizzazione di ulteriori oggetti con codifica di erasure.

Dopo aver esaminato queste considerazioni, eseguire l'espansione, quindi passare a. Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage per eseguire la procedura.

Cos'è il ribilanciamento EC?

Il ribilanciamento EC è una procedura StorageGRID che potrebbe essere necessaria dopo l'espansione di un nodo di storage. La procedura viene eseguita come script della riga di comando dal nodo di amministrazione primario. Quando si esegue la procedura di ribilanciamento EC, StorageGRID ridistribuisce i frammenti con codifica erasure tra i nodi di storage esistenti e quelli appena espansi in un sito.

Procedura di ribilanciamento CE:

- Sposta solo i dati degli oggetti con codifica erasure. Non sposta i dati degli oggetti replicati.
- Ridistribuisce i dati all'interno di un sito. Non sposta i dati tra siti.
- Ridistribuisce i dati tra tutti i nodi di storage di un sito. Non ridistribuisce i dati all'interno dei volumi di storage.
- Non prende in considerazione l'utilizzo dei dati replicati su ciascun nodo di storage quando determina dove spostare i dati con codifica di cancellazione

Al termine della procedura di ribilanciamento EC:

- I dati con codifica erasure vengono spostati dai nodi di storage con meno spazio disponibile ai nodi di storage con più spazio disponibile.
- I valori utilizzati (%) potrebbero rimanere diversi tra i nodi di storage perché la procedura di ribilanciamento

EC non sposta le copie replicate degli oggetti.

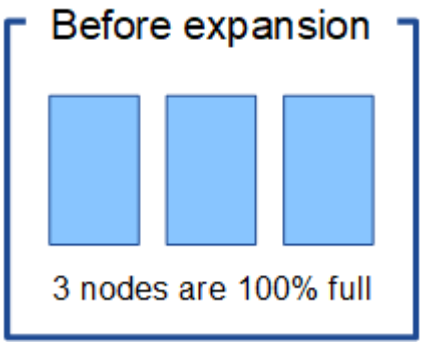
- La protezione dei dati degli oggetti con codifica erasure rimane invariata.

Quando la procedura di ribilanciamento EC è in esecuzione, è probabile che le prestazioni delle operazioni ILM e delle operazioni dei client S3 e Swift ne risentano. Per questo motivo, questa procedura deve essere eseguita solo in casi limitati.

Quando non eseguire il ribilanciamento EC

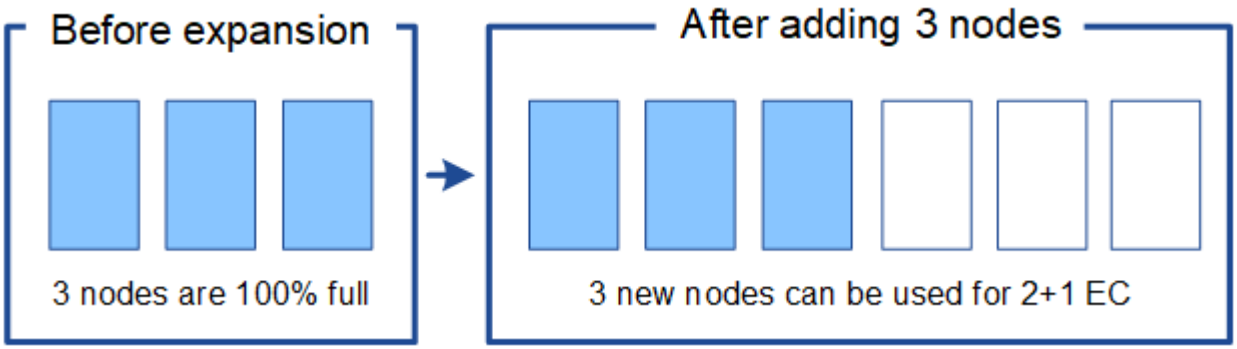
Come esempio di quando non è necessario eseguire un ribilanciamento EC, considerare quanto segue:

- StorageGRID viene eseguito in un singolo sito, che contiene tre nodi di storage.
- Il criterio ILM utilizza una regola di erasure coding 2+1 per tutti gli oggetti più grandi di 1.0 MB e una regola di replica a 2 copie per gli oggetti più piccoli.
- Tutti i nodi di storage sono completamente pieni e l'avviso **Low Object Storage** è stato attivato al livello di severità maggiore. Si consiglia di eseguire una procedura di espansione per aggiungere nodi di storage.



Per espandere il sito in questo esempio, si consiglia di aggiungere tre o più nuovi nodi di storage. StorageGRID richiede tre nodi di storage per la erasure coding 2+1, in modo da poter posizionare i due frammenti di dati e un frammento di parità su nodi diversi.

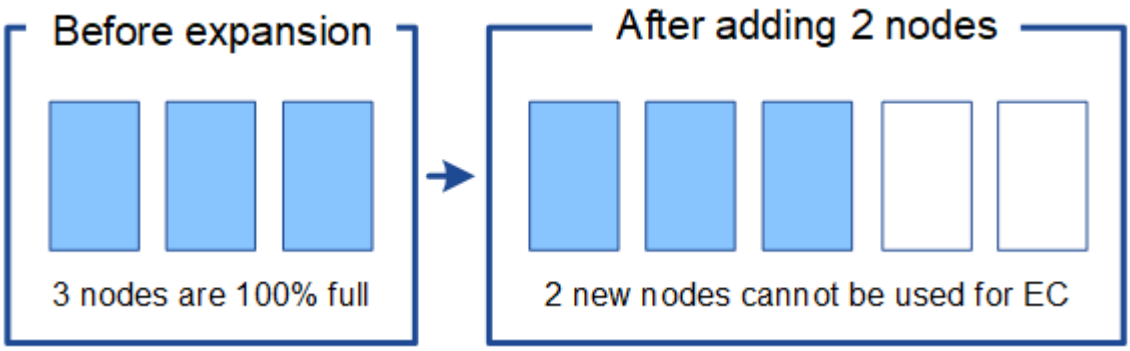
Dopo aver aggiunto i tre nodi di storage, i nodi di storage originali rimangono pieni, ma gli oggetti possono continuare ad essere acquisiti nello schema di erasure coding 2+1 sui nuovi nodi. L'esecuzione della procedura di ribilanciamento EC non è consigliata in questo caso: L'esecuzione della procedura ridurrà temporaneamente le prestazioni, con un impatto sulle operazioni del client.



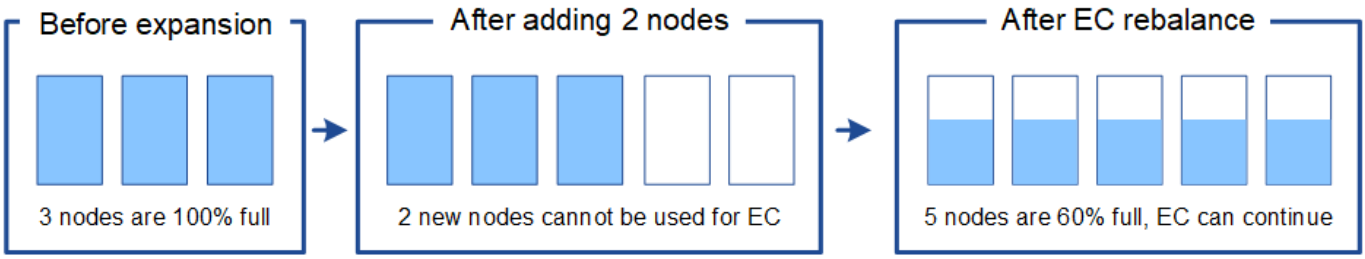
Quando eseguire il ribilanciamento EC

Come esempio di quando si deve eseguire la procedura di ribilanciamento EC, considerare lo stesso esempio, ma si presume che sia possibile aggiungere solo due nodi di storage. Poiché la codifica di cancellazione 2+1

richiede almeno tre nodi di storage, i nuovi nodi non possono essere utilizzati per i dati con codifica di cancellazione.



Per risolvere questo problema e utilizzare i nuovi nodi di storage, è possibile eseguire la procedura di ribilanciamento EC. Quando viene eseguita questa procedura, StorageGRID ridistribuisce i dati con codifica erasure e i frammenti di parità tra tutti i nodi di storage del sito. In questo esempio, quando la procedura di ribilanciamento EC è completa, tutti e cinque i nodi sono ora pieni solo al 60% e gli oggetti possono continuare ad essere acquisiti nello schema di codifica di cancellazione 2+1 su tutti i nodi di storage.



Requisiti per il ribilanciamento CE

In generale, è necessario eseguire la procedura di ribilanciamento EC solo in casi limitati. In particolare, è necessario eseguire il ribilanciamento EC solo se tutte le seguenti affermazioni sono vere:

- Si utilizza la codifica di cancellazione per i dati dell'oggetto.
- L'avviso **Low Object Storage** è stato attivato per uno o più nodi di storage in un sito, a indicare che i nodi sono pieni al 80% o più.
- Non è possibile aggiungere il numero consigliato di nuovi nodi di storage per lo schema di erasure coding in uso. Vedere Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione.
- I client S3 e Swift possono tollerare prestazioni inferiori per le operazioni di scrittura e lettura durante l'esecuzione della procedura di ribilanciamento EC.

Come la procedura di ribilanciamento EC interagisce con altre attività di manutenzione

Non è possibile eseguire alcune procedure di manutenzione contemporaneamente all'esecuzione della procedura di ribilanciamento EC.

Procedura	Consentito durante la procedura di ribilanciamento EC?
Ulteriori procedure di ribilanciamento EC	No È possibile eseguire una sola procedura di ribilanciamento EC alla volta.

Procedura	Consentito durante la procedura di ribilanciamento EC?
Procedura di decommissionamento Lavoro di riparazione dei dati EC	No • Non è possibile avviare una procedura di decommissionamento o una riparazione dei dati EC mentre è in esecuzione la procedura di ribilanciamento EC. • Non è possibile avviare la procedura di ribilanciamento EC mentre è in esecuzione una procedura di decommissionamento del nodo di storage o una riparazione dei dati EC.
Procedura di espansione	No Se è necessario aggiungere nuovi nodi di storage in un'espansione, è necessario attendere l'esecuzione della procedura di ribilanciamento EC fino a quando non sono stati aggiunti tutti i nuovi nodi. Se è in corso una procedura di ribilanciamento EC quando si aggiungono nuovi nodi di storage, i dati non verranno spostati in tali nodi.
Procedura di aggiornamento	No Se è necessario aggiornare il software StorageGRID, eseguire la procedura di aggiornamento prima o dopo l'esecuzione della procedura di ribilanciamento EC. Se necessario, è possibile terminare la procedura di ribilanciamento EC per eseguire un aggiornamento del software.
Procedura di clone del nodo dell'appliance	No Se è necessario clonare un nodo di storage dell'appliance, è necessario attendere l'esecuzione della procedura di ribilanciamento EC fino a quando non viene aggiunto il nuovo nodo. Se è in corso una procedura di ribilanciamento EC quando si aggiungono nuovi nodi di storage, i dati non verranno spostati in tali nodi.
Procedura di hotfix	Sì. È possibile applicare una correzione rapida StorageGRID mentre è in esecuzione la procedura di ribilanciamento EC.
Altre procedure di manutenzione	No È necessario terminare la procedura di ribilanciamento EC prima di eseguire altre procedure di manutenzione.

Come la procedura di ribilanciamento EC interagisce con ILM

Durante l'esecuzione della procedura di ribilanciamento EC, evitare di apportare modifiche ILM che potrebbero modificare la posizione degli oggetti con codifica di cancellazione esistenti. Ad esempio, non iniziare a utilizzare una regola ILM con un profilo di codifica Erasure diverso. Se è necessario apportare tali modifiche ILM, interrompere la procedura di ribilanciamento EC.

Aggiungere capacità di metadati

Per garantire che sia disponibile spazio adeguato per i metadati degli oggetti, potrebbe essere necessario eseguire una procedura di espansione per aggiungere nuovi nodi di storage in ogni sito.

StorageGRID riserva spazio per i metadati degli oggetti sul volume 0 di ciascun nodo di storage. In ogni sito vengono conservate tre copie di tutti i metadati degli oggetti, distribuite uniformemente in tutti i nodi di storage.

È possibile utilizzare Grid Manager per monitorare la capacità dei metadati dei nodi di storage e stimare la velocità di utilizzo della capacità dei metadati. Inoltre, l'avviso **Low metadata storage** viene attivato per un nodo di storage quando lo spazio di metadati utilizzato raggiunge determinate soglie.

Si noti che la capacità dei metadati degli oggetti di una griglia potrebbe essere consumata più rapidamente rispetto alla capacità dello storage a oggetti, a seconda di come si utilizza la griglia. Ad esempio, se in genere si acquisiscono grandi quantità di oggetti di piccole dimensioni o si aggiungono grandi quantità di metadati o tag utente agli oggetti, potrebbe essere necessario aggiungere nodi di storage per aumentare la capacità dei metadati anche se rimane sufficiente capacità di storage a oggetti.

Per ulteriori informazioni, vedere quanto segue:

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

Linee guida per aumentare la capacità dei metadati

Prima di aggiungere nodi di storage per aumentare la capacità dei metadati, consultare le seguenti linee guida e limitazioni:

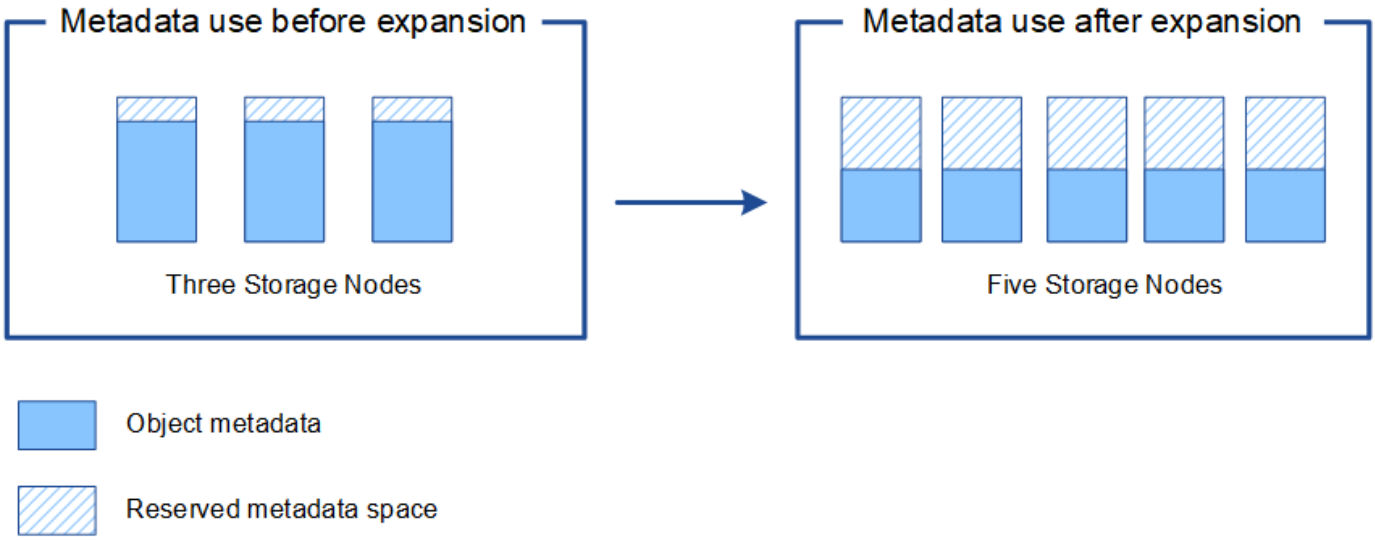
- Supponendo che sia disponibile una capacità di storage a oggetti sufficiente, avere più spazio disponibile per i metadati a oggetti aumenta il numero di oggetti che è possibile memorizzare nel sistema StorageGRID.
- È possibile aumentare la capacità dei metadati di un grid aggiungendo uno o più nodi di storage a ciascun sito.
- Lo spazio effettivo riservato ai metadati dell'oggetto su qualsiasi nodo di storage specifico dipende dall'opzione di storage Metadata Reserved Space (impostazione a livello di sistema), dalla quantità di RAM allocata al nodo e dalla dimensione del volume 0 del nodo. Consultare le istruzioni per Amministrazione di StorageGRID.
- Non è possibile aumentare la capacità dei metadati aggiungendo volumi di storage ai nodi di storage esistenti, perché i metadati vengono memorizzati solo sul volume 0.
- Non è possibile aumentare la capacità dei metadati aggiungendo un nuovo sito.
- StorageGRID conserva tre copie di tutti i metadati degli oggetti in ogni sito. Per questo motivo, la capacità dei metadati del sistema è limitata dalla capacità dei metadati del sito più piccolo.
- Quando si aggiunge la capacità dei metadati, è necessario aggiungere lo stesso numero di nodi di storage a ciascun sito.

Come vengono ridistribuiti i metadati quando si aggiungono nodi di storage

Quando si aggiungono nodi di storage in un'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti nei nuovi nodi di ciascun sito, aumentando così la capacità complessiva dei metadati del grid. Non è richiesta alcuna azione da parte dell'utente.

La figura seguente mostra come StorageGRID ridistribuisce i metadati degli oggetti quando si aggiungono nodi di storage in un'espansione. Il lato sinistro della figura rappresenta il volume 0 di tre nodi di storage prima di un'espansione. I metadati consumano una porzione relativamente grande dello spazio di metadati disponibile di ciascun nodo ed è stato attivato l'avviso **Low metadata storage**.

Il lato destro della figura mostra come vengono ridistribuiti i metadati esistenti dopo l'aggiunta di due nodi di storage al sito. La quantità di metadati su ciascun nodo è diminuita, l'avviso **Low metadata storage** non viene più attivato e lo spazio disponibile per i metadati è aumentato.



Aggiungi nodi grid per aggiungere funzionalità al tuo sistema

È possibile aggiungere ridondanza o funzionalità aggiuntive a un sistema StorageGRID aggiungendo nuovi nodi grid ai siti esistenti.

Ad esempio, è possibile scegliere di aggiungere altri nodi gateway per supportare la creazione di gruppi ad alta disponibilità di nodi gateway oppure aggiungere un nodo amministratore in un sito remoto per consentire il monitoraggio utilizzando un nodo locale.

È possibile aggiungere uno o più dei seguenti tipi di nodi a uno o più siti esistenti in una singola operazione di espansione:

- Nodi amministrativi non primari
- Nodi di storage
- Nodi gateway
- Nodi di archiviazione

Durante la preparazione all'aggiunta di nodi di rete, tenere presente le seguenti limitazioni:

- Il nodo di amministrazione primario viene implementato durante l'installazione iniziale. Non è possibile aggiungere un nodo amministratore primario durante un'espansione.
- È possibile aggiungere nodi di storage e altri tipi di nodi nella stessa espansione.
- Quando si aggiungono nodi di storage, è necessario pianificare attentamente il numero e la posizione dei nuovi nodi. Vedere Linee guida per l'aggiunta della capacità degli oggetti.
- Se si aggiungono nodi di archiviazione, tenere presente che ciascun nodo di archiviazione supporta solo il

nastro tramite il middleware Tivoli Storage Manager (TSM).

- Se l'opzione **New Node Client Network Default** è impostata su **Untrusted** nella pagina Untrusted Client Networks, le applicazioni client che si connettono ai nodi di espansione utilizzando la rete client devono connettersi utilizzando una porta endpoint del bilanciamento del carico (**CONFIGURAZIONE** > **rete** > **reti client non attendibili**). Consultare le istruzioni per Amministrazione di StorageGRID per modificare l'impostazione del nuovo nodo e configurare gli endpoint del bilanciamento del carico.

Aggiungere un nuovo sito

È possibile espandere il sistema StorageGRID aggiungendo un nuovo sito.

Linee guida per l'aggiunta di un sito

Prima di aggiungere un sito, esaminare i seguenti requisiti e limitazioni:

- È possibile aggiungere un solo sito per ciascuna operazione di espansione.
- Non è possibile aggiungere nodi griglia a un sito esistente come parte della stessa espansione.
- Tutti i siti devono includere almeno tre nodi di storage.
- L'aggiunta di un nuovo sito non aumenta automaticamente il numero di oggetti che è possibile memorizzare. La capacità totale degli oggetti di un grid dipende dalla quantità di storage disponibile, dal criterio ILM e dalla capacità dei metadati di ciascun sito.
- Quando si ridimensiona un nuovo sito, è necessario assicurarsi che includa una capacità di metadati sufficiente.

  StorageGRID conserva una copia di tutti i metadati degli oggetti in ogni sito. Quando si aggiunge un nuovo sito, è necessario assicurarsi che includa una capacità di metadati sufficiente per i metadati degli oggetti esistenti e una capacità di metadati sufficiente per la crescita.

  Per ulteriori informazioni, vedere quanto segue:

  - Gestire lo storage dei metadati degli oggetti
  - Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage
- È necessario considerare la larghezza di banda della rete disponibile tra i siti e il livello di latenza della rete. Gli aggiornamenti dei metadati vengono continuamente replicati tra i siti anche se tutti gli oggetti vengono memorizzati solo nel sito in cui vengono acquisiti.
- Poiché il sistema StorageGRID rimane operativo durante l'espansione, è necessario rivedere le regole ILM prima di avviare la procedura di espansione. Assicurarsi che le copie a oggetti non vengano memorizzate nel nuovo sito fino al completamento della procedura di espansione.

  Ad esempio, prima di iniziare l'espansione, determinare se alcune regole utilizzano il pool di storage predefinito (tutti i nodi di storage). In tal caso, è necessario creare un nuovo pool di storage contenente i nodi di storage esistenti e aggiornare le regole ILM per utilizzare il nuovo pool di storage. In caso contrario, gli oggetti verranno copiati nel nuovo sito non appena il primo nodo del sito diventa attivo.

  Per ulteriori informazioni sulla modifica di ILM durante l'aggiunta di un nuovo sito, vedere l'esempio relativo alla modifica di un criterio ILM nelle istruzioni per Gestione degli oggetti con ILM.

Raccogliere il materiale necessario

Prima di eseguire un'operazione di espansione, raccogliere i materiali e installare e

configurare eventuali nuovi hardware e reti.

Elemento	Note
Archivio di installazione di StorageGRID	Se si aggiungono nuovi nodi di griglia o un nuovo sito, è necessario scaricare ed estrarre l'archivio di installazione di StorageGRID. È necessario utilizzare la stessa versione attualmente in esecuzione sulla griglia. Per ulteriori informazioni, consultare le istruzioni di Download ed estrazione dei file di installazione di StorageGRID. **Nota:** non è necessario scaricare i file se si aggiungono nuovi volumi di storage ai nodi di storage esistenti o si installa una nuova appliance StorageGRID.
Laptop di assistenza	Il laptop di assistenza dispone di quanto segue: • Porta di rete • Client SSH (ad esempio, putty) • Browser Web supportato
`Passwords.txt` file	Contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando. Incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.

Documentazione StorageGRID	• Amministrare StorageGRID
	• Note di rilascio
	• Istruzioni per l'installazione della piattaforma
	  ◦ Installare Red Hat Enterprise Linux o CentOS
	  ◦ Installare Ubuntu o Debian
	  ◦ Installare VMware

Documentazione aggiornata per la piattaforma	Per le versioni supportate, vedere "Matrice di interoperabilità".

Scaricare ed estrarre i file di installazione di StorageGRID

Prima di poter aggiungere nuovi nodi grid o un nuovo sito, è necessario scaricare l'archivio di installazione StorageGRID appropriato ed estrarre i file.

A proposito di questa attività

È necessario eseguire operazioni di espansione utilizzando la versione di StorageGRID attualmente in esecuzione sulla griglia.

Fasi

1. Vai alla pagina dei download NetApp per StorageGRID.

   "Download NetApp: StorageGRID"

2. Selezionare la versione di StorageGRID attualmente in esecuzione nella griglia.
3. Accedi con il nome utente e la password del tuo account NetApp.
4. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
5. Nella colonna **Installa StorageGRID** della pagina di download, selezionare `.tgz` oppure `.zip` file per la tua piattaforma.

   La versione mostrata nel file di archivio dell'installazione deve corrispondere alla versione del software attualmente installato.

   Utilizzare `.zip` File se si esegue Windows sul laptop di assistenza.

Piattaforma	Archivio di installazione

Red Hat Enterprise Linux o CentOS	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Ubuntu o Debian o appliance	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

OpenStack/Altro hypervisor	Per espandere una distribuzione esistente su OpenStack, è necessario implementare una macchina virtuale che esegue una delle distribuzioni Linux supportate elencate sopra e seguire le istruzioni appropriate per Linux.

6. Scaricare ed estrarre il file di archivio.
7. Seguire la fase appropriata per la piattaforma per scegliere i file necessari, in base alla piattaforma, alla topologia della griglia pianificata e al modo in cui si espanderà il sistema StorageGRID.

   I percorsi elencati nella fase per ciascuna piattaforma sono relativi alla directory di primo livello installata dal file di archivio.

8. Se stai espandendo un sistema Red Hat Enterprise Linux o CentOS, seleziona i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.

Percorso e nome del file	Descrizione
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	PACCHETTO RPM per l'installazione delle immagini dei nodi StorageGRID sugli host RHEL o CentOS.
	PACCHETTO RPM per l'installazione del servizio host StorageGRID sugli host RHEL o CentOS.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di manuale e ruolo Ansible per la configurazione degli host RHEL o CentOS per l'implementazione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema Ubuntu o Debian, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	Checksum MD5 per il file `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PACCHETTO DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.

Percorso e nome del file	Descrizione
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema VMware, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file di modello Open Virtualization Format (`.ovf`) e il file manifest (`.mf`) Per l'implementazione del nodo di amministrazione primario.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi amministrativi non primari.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi di archiviazione.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi gateway.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi di storage basati su macchine virtuali.
Tool di scripting per la distribuzione	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.

Percorso e nome del file	Descrizione
	Un file di configurazione di esempio da utilizzare con `deploy-vsphere-ovftool.sh` script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema basato su appliance StorageGRID, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	PACCHETTO DEB per l'installazione delle immagini del nodo StorageGRID sulle appliance.
	Checksum del pacchetto di installazione DEB utilizzato dal programma di installazione dell'appliance StorageGRID per verificare che il pacchetto sia intatto dopo il caricamento.

> Per l'installazione dell'appliance, questi file sono necessari solo se è necessario evitare il traffico di rete. L'appliance può scaricare i file richiesti dal nodo di amministrazione principale.

Verificare l'hardware e il collegamento in rete

Prima di iniziare l'espansione del sistema StorageGRID, verificare quanto segue:

- L'hardware necessario per supportare i nuovi nodi di rete o il nuovo sito è stato installato e configurato.
- Tutti i nuovi nodi dispongono di percorsi di comunicazione bidirezionali per tutti i nodi esistenti e nuovi (un requisito per la Grid Network).
- Il nodo di amministrazione primario può comunicare con tutti i server di espansione destinati a ospitare il sistema StorageGRID.
- Se uno dei nuovi nodi ha un indirizzo IP Grid Network su una subnet non utilizzata in precedenza, l'operazione è già stata effettuata aggiunta della nuova subnet Nell'elenco Grid Network Subnet (subnet rete griglia). In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e avviare nuovamente la procedura.
- Non si utilizza la conversione degli indirizzi di rete (NAT) sulla rete di rete tra nodi di rete o tra siti StorageGRID. Quando si utilizzano indirizzi IPv4 privati per Grid Network, tali indirizzi devono essere direttamente instradabili da ogni nodo di griglia in ogni sito. L'utilizzo di NAT per il bridge della rete Grid attraverso un segmento di rete pubblica è supportato solo se si utilizza un'applicazione di tunneling trasparente per tutti i nodi della griglia, il che significa che i nodi della griglia non richiedono alcuna conoscenza degli indirizzi IP pubblici.

  Questa restrizione NAT è specifica per i nodi di griglia e la rete di griglia. Se necessario, è possibile utilizzare NAT tra client esterni e nodi di rete, ad esempio per fornire un indirizzo IP pubblico per un nodo gateway.

Aggiungere volumi di storage

Aggiungere volumi di storage ai nodi di storage

È possibile espandere la capacità di storage dei nodi di storage con un numero di volumi di storage inferiore o uguale a 16 aggiungendo ulteriori volumi di storage. Potrebbe essere necessario aggiungere volumi di storage a più di un nodo di storage per soddisfare i requisiti ILM per le copie replicate o con codifica di cancellazione.

Di cosa hai bisogno

Prima di aggiungere volumi di storage, consultare linee guida per l'aggiunta della capacità degli oggetti Per assicurarsi di sapere dove aggiungere volumi per soddisfare i requisiti della policy ILM.

> Queste istruzioni sono valide solo per i nodi storage basati su software. Vedere Aggiungere shelf di espansione a SG6060 o SG6060X implementati Per scoprire come aggiungere volumi di storage a SG6060 o SG6060X installando shelf di espansione. Non è possibile espandere altri nodi storage dell'appliance.

A proposito di questa attività

Lo storage sottostante di un nodo di storage è diviso in diversi volumi di storage. I volumi di storage sono dispositivi di storage basati su blocchi formattati dal sistema StorageGRID e montati per memorizzare oggetti. Ciascun nodo di storage può supportare fino a 16 volumi di storage, denominati *archivi di oggetti* in Grid Manager.

> I metadati degli oggetti sono sempre memorizzati nell'archivio di oggetti 0.

Ogni archivio di oggetti viene montato su un volume che corrisponde al relativo ID. Ad esempio, l'archivio di oggetti con un ID di 0000 corrisponde a. `/var/local/rangedb/0` punto di montaggio.

Prima di aggiungere nuovi volumi di storage, utilizzare Grid Manager per visualizzare gli archivi di oggetti correnti per ciascun nodo di storage e i punti di montaggio corrispondenti. È possibile utilizzare queste informazioni quando si aggiungono volumi di storage.

Fasi

1. Selezionare **NODES** > ***Site*** > ***Storage Node*** > **Storage**.
2. Scorrere verso il basso per visualizzare le quantità di storage disponibili per ciascun volume e archivio di oggetti.

   Per i nodi di storage dell'appliance, il nome globale di ciascun disco corrisponde all'identificativo mondiale del volume (WWID) visualizzato quando si visualizzano le proprietà dei volumi standard 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
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

3. Seguire le istruzioni della piattaforma per aggiungere nuovi volumi di storage al nodo di storage.
    - VMware: Aggiunta di volumi di storage a Storage Node
    - Linux: Aggiunta di volumi direct-attached o SAN al nodo di storage

VMware: Aggiunta di volumi di storage a Storage Node

Se un nodo di storage include meno di 16 volumi di storage, è possibile aumentarne la capacità utilizzando VMware vSphere per aggiungere volumi.

Di cosa hai bisogno

- È possibile accedere alle istruzioni per l'installazione di StorageGRID per le implementazioni VMware.
    - Installare VMware
- Hai il `Passwords.txt` file.
- Si dispone di autorizzazioni di accesso specifiche.

> Non tentare di aggiungere volumi di storage a un nodo di storage mentre è attiva una procedura di aggiornamento del software, di ripristino o un'altra procedura di espansione.

A proposito di questa attività

Il nodo di storage non è disponibile per un breve periodo di tempo quando si aggiungono volumi di storage. È necessario eseguire questa procedura su un nodo di storage alla volta per evitare impatti sui servizi grid rivolti al client.

Fasi

1. Se necessario, installare nuovo hardware per lo storage e creare nuovi datastore VMware.
2. Aggiungere uno o più dischi rigidi alla macchina virtuale per utilizzarli come storage (archivi di oggetti).

    a. Aprire VMware vSphere Client.

    b. Modificare le impostazioni della macchina virtuale per aggiungere uno o più dischi rigidi aggiuntivi.

    I dischi rigidi sono in genere configurati come Virtual Machine Disk (VMDK). I VMDK sono più comunemente utilizzati e sono più facili da gestire, mentre i RDM possono fornire performance migliori per i carichi di lavoro che utilizzano oggetti di dimensioni maggiori (ad esempio, superiori a 100 MB). Per ulteriori informazioni sull'aggiunta di dischi rigidi alle macchine virtuali, consultare la documentazione di VMware vSphere.

3. Riavviare la macchina virtuale utilizzando l'opzione **Restart Guest OS** (Riavvia sistema operativo guest) in VMware vSphere Client o immettendo il seguente comando in una sessione ssh sulla macchina virtuale:`sudo reboot`

    > Non utilizzare **Power Off** o **Reset** per riavviare la macchina virtuale.

4. Configurare il nuovo storage per l'utilizzo da parte del 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. Configurare i nuovi volumi di storage:

```
sudo add_rangedbs.rb
```

Questo script trova i nuovi volumi di storage e richiede di formattarli.

a. Immettere **y** per accettare la formattazione.
b. Se uno dei volumi è stato precedentemente formattato, decidere se si desidera riformattarlo.
   - Immettere **y** per riformattare.
   - Inserire **n** per saltare la riformattazione.
c. Quando richiesto, immettere **y** per interrompere i servizi di storage.

   I servizi di storage vengono arrestati e l' `setup_rangedbs.sh` lo script viene eseguito automaticamente. Una volta che i volumi sono pronti per l'uso come rangedb, i servizi vengono riavviati.

5. Verificare che i servizi vengano avviati correttamente:

   a. Visualizzare un elenco dello stato di tutti i servizi sul server:

   ```
   sudo storagegrid-status
   ```

   Lo stato viene aggiornato automaticamente.

   a. Attendere che tutti i servizi siano in esecuzione o verificati.
   b. Uscire dalla schermata di stato:

   ```
   Ctrl+C
   ```

6. Verificare che il nodo di storage sia in linea:
   a. Accedere a Grid Manager utilizzando un browser web supportato.
   b. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
   c. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Storage**.
   d. Selezionare la scheda **Configurazione**, quindi la scheda **principale**.
   e. Se l'elenco a discesa **Storage state - Desired** (Stato di storage - desiderato) è impostato su Read-only (sola lettura) o Offline (non in linea), selezionare **Online**.
   f. Selezionare **Applica modifiche**.
7. Per visualizzare i nuovi archivi di oggetti:
   a. Selezionare **NODES** > ***Site*** > ***Storage Node*** > **Storage**.
   b. Visualizzare i dettagli nella tabella **Object Stores**.

Risultato

È possibile utilizzare la capacità estesa dei nodi di storage per salvare i dati degli oggetti.

Linux: Aggiunta di volumi direct-attached o SAN al nodo di storage

Se un nodo di storage include meno di 16 volumi di storage, è possibile aumentarne la capacità aggiungendo nuovi dispositivi di storage a blocchi, rendendoli visibili agli host Linux e aggiungendo i nuovi mapping dei dispositivi a blocchi al file di configurazione StorageGRID utilizzato per il nodo di storage.

Di cosa hai bisogno

- Hai accesso alle istruzioni per l'installazione di StorageGRID per la tua piattaforma Linux.
  - Installare Red Hat Enterprise Linux o CentOS
  - Installare Ubuntu o Debian
- Hai il `Passwords.txt` file.
- Si dispone di autorizzazioni di accesso specifiche.

> Non tentare di aggiungere volumi di storage a un nodo di storage mentre è attiva una procedura di aggiornamento del software, di ripristino o un'altra procedura di espansione.

A proposito di questa attività

Il nodo di storage non è disponibile per un breve periodo di tempo quando si aggiungono volumi di storage. È necessario eseguire questa procedura su un nodo di storage alla volta per evitare impatti sui servizi grid rivolti al client.

Fasi

1. Installare il nuovo hardware di storage.

   Per ulteriori informazioni, consultare la documentazione fornita dal fornitore dell'hardware.

2. Creare nuovi volumi di storage a blocchi delle dimensioni desiderate.
   - Collegare le nuove unità disco e aggiornare la configurazione del controller RAID secondo necessità oppure allocare le nuove LUN SAN sugli array di storage condivisi e consentire all'host Linux di accedervi.
   - Utilizzare lo stesso schema di denominazione persistente utilizzato per i volumi di storage sul nodo di storage esistente.
   - Se si utilizza la funzionalità di migrazione dei nodi StorageGRID, rendere visibili i nuovi volumi agli altri host Linux che sono destinazioni di migrazione per questo nodo di storage. Per ulteriori informazioni, consulta le istruzioni per l'installazione di StorageGRID per la tua piattaforma Linux.
3. Accedere all'host Linux che supporta il nodo di storage come root o con un account che dispone dell'autorizzazione sudo.
4. Verificare che i nuovi volumi di storage siano visibili sull'host Linux.

   Potrebbe essere necessario eseguire una nuova scansione per le periferiche.

5. Eseguire il seguente comando per disattivare temporaneamente il nodo di storage:

   ```
   sudo storagegrid node stop <node-name>
   ```

6. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo per il nodo di storage, disponibile all'indirizzo `/etc/storagegrid/nodes/<node-name>.conf`.

7. Individuare la sezione del file di configurazione del nodo che contiene le mappature dei dispositivi di blocco dello storage a oggetti esistenti.

   Nell'esempio, `BLOCK_DEVICE_RANGEDB_00` a. `BLOCK_DEVICE_RANGEDB_03` sono le mappature esistenti dei dispositivi a blocchi di storage a oggetti.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Aggiungere nuove mappature dei dispositivi a blocchi di storage a oggetti corrispondenti ai volumi di storage a blocchi aggiunti per questo nodo di storage.

   Assicurarsi di iniziare dal successivo `BLOCK_DEVICE_RANGEDB_nn`. Non lasciare spazio.

   - In base all'esempio precedente, iniziare da `BLOCK_DEVICE_RANGEDB_04`.
   - Nell'esempio riportato di seguito, sono stati aggiunti quattro nuovi volumi di storage a blocchi al nodo: `BLOCK_DEVICE_RANGEDB_04` a. `BLOCK_DEVICE_RANGEDB_07`.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo per il nodo di storage:

   ```
   sudo storagegrid node validate <node-name>
   ```

   Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

   > Se si osserva un errore simile a quanto segue, significa che il file di configurazione del nodo sta tentando di mappare il dispositivo a blocchi utilizzato da `<node-name>` per `<PURPOSE>` al dato `<path-name>` Nel file system Linux, ma non esiste un file speciale valido per il dispositivo a blocchi (o un softlink a un file speciale per il dispositivo a blocchi) in tale posizione.
   >
   > ```
   > Checking configuration file for node <node-name>…
   > ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
   > <path-name> is not a valid block device
   > ```
   >
   > Verificare di aver inserito il corretto `<path-name>`.

10. Eseguire il seguente comando per riavviare il nodo con le nuove mappature del dispositivo a blocchi in posizione:

    ```
    sudo storagegrid node start <node-name>
    ```

11. Accedere al nodo di storage come amministratore utilizzando la password elencata in `Passwords.txt` file.
12. Verificare che i servizi vengano avviati correttamente:
    a. Visualizzare un elenco dello stato di tutti i servizi sul server:

```
sudo storagegrid-status
```

Lo stato viene aggiornato automaticamente.

b. Attendere che tutti i servizi siano in esecuzione o verificati.
c. Uscire dalla schermata di stato:

```
Ctrl+C
```

13. Configurare il nuovo storage per l'utilizzo da parte del nodo di storage:

a. Configurare i nuovi volumi di storage:

```
sudo add_rangedbs.rb
```

Questo script trova i nuovi volumi di storage e richiede di formattarli.

a. Inserire **y** per formattare i volumi di storage.
b. Se uno dei volumi è stato precedentemente formattato, decidere se si desidera riformattarlo.
   - Immettere **y** per riformattare.
   - Inserire **n** per saltare la riformattazione.
c. Quando richiesto, immettere **y** per interrompere i servizi di storage.

I servizi di storage vengono arrestati e l' `setup_rangedbs.sh` lo script viene eseguito automaticamente. Una volta che i volumi sono pronti per l'uso come rangedb, i servizi vengono riavviati.

14. Verificare che i servizi vengano avviati correttamente:

a. Visualizzare un elenco dello stato di tutti i servizi sul server:

```
sudo storagegrid-status
```

Lo stato viene aggiornato automaticamente.

a. Attendere che tutti i servizi siano in esecuzione o verificati.
b. Uscire dalla schermata di stato:

```
Ctrl+C
```

15. Verificare che il nodo di storage sia in linea:

a. Accedere a Grid Manager utilizzando un browser web supportato.
b. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
c. Selezionare ***Site*** > ***Storage Node*** > **LDR** > **Storage**.
d. Selezionare la scheda **Configurazione**, quindi la scheda **principale**.
e. Se l'elenco a discesa **Storage state - Desired** (Stato di storage - desiderato) è impostato su Read-only (sola lettura) o Offline (non in linea), selezionare **Online**.
f. Fare clic su **Applica modifiche**.

16. Per visualizzare i nuovi archivi di oggetti:
    a. Selezionare **NODES** > ***Site*** > ***Storage Node*** > **Storage**.
    b. Visualizzare i dettagli nella tabella **Object Stores**.

Risultato

È ora possibile utilizzare la capacità estesa dei nodi di storage per salvare i dati degli oggetti.

Aggiunta di nodi o siti grid

Aggiunta di nodi di griglia al sito esistente o aggiunta di un nuovo sito

È possibile seguire questa procedura per aggiungere nodi di griglia a siti esistenti o per aggiungere un nuovo sito, ma non è possibile eseguire entrambi i tipi di espansione contemporaneamente.

Di cosa hai bisogno

- Si dispone dell'autorizzazione di accesso root o di manutenzione.
- Tutti i nodi esistenti nel grid sono attivi e in esecuzione in tutti i siti.
- Tutte le precedenti procedure di espansione, aggiornamento, disattivazione o ripristino sono state completate.

> Non è possibile avviare un'espansione mentre è in corso un'altra procedura di espansione, aggiornamento, ripristino o decommissionamento attivo. Tuttavia, se necessario, è possibile sospendere una procedura di decommissionamento per avviare un'espansione.

Fasi

1. Aggiornare le subnet per Grid Network.
2. Implementare nuovi nodi grid.
3. Eseguire l'espansione.

Aggiornare le subnet per Grid Network

Quando si aggiungono nodi griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere sottoreti alla rete Grid.

StorageGRID mantiene un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete (eth0). Queste voci includono le subnet utilizzate per la rete griglia da ciascun sito nel sistema StorageGRID, nonché le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della rete griglia.

Di cosa hai bisogno

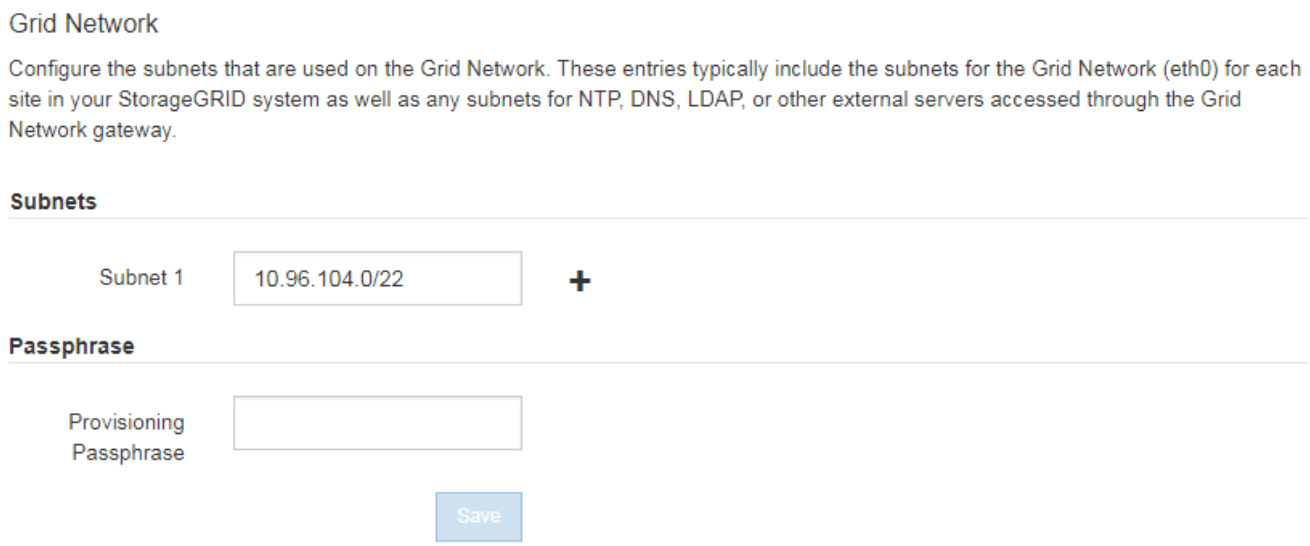
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso Maintenance o Root.
- Si dispone della passphrase di provisioning.
- Si dispone degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

A proposito di questa attività

Se uno dei nuovi nodi ha un indirizzo IP Grid Network su una subnet non utilizzata in precedenza, è necessario aggiungere la nuova subnet all'elenco Grid Network subnet prima di avviare l'espansione. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e avviare nuovamente la procedura.

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **rete griglia**.



2. Nell'elenco delle subnet, selezionare il segno più per aggiungere una nuova subnet nella notazione CIDR.

   Ad esempio, inserire 10.96.104.0/22.

3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).

   Le subnet specificate vengono configurate automaticamente per il sistema StorageGRID.

Implementare nuovi nodi grid

I passaggi per l'implementazione di nuovi nodi grid in un'espansione sono gli stessi utilizzati al momento dell'installazione della griglia. Prima di eseguire l'espansione, è necessario implementare tutti i nuovi nodi grid.

Quando si espande la griglia, i nodi aggiunti non devono corrispondere ai tipi di nodo esistenti. È possibile aggiungere nodi VMware, nodi Linux basati su container o nodi appliance.

VMware: Implementazione di nodi grid

È necessario implementare una macchina virtuale in VMware vSphere per ciascun nodo VMware che si desidera aggiungere all'espansione.

Fasi

1. Implementare il nuovo nodo come macchina virtuale E connetterlo a una o più reti StorageGRID.

   Quando si implementa il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.

2. Dopo aver implementato tutti i nuovi nodi VMware, eseguire la procedura di espansione.

Linux: Implementazione di nodi grid

È possibile implementare nodi grid su nuovi host Linux o su host Linux esistenti. Se sono necessari altri host Linux per supportare i requisiti di CPU, RAM e storage dei nodi StorageGRID che si desidera aggiungere al grid, è necessario prepararli nello stesso modo in cui sono stati preparati gli host al momento dell'installazione. Quindi, i nodi di espansione vengono implementati nello stesso modo in cui vengono implementati i nodi di rete durante l'installazione.

Di cosa hai bisogno

- Sono disponibili le istruzioni per l'installazione di StorageGRID per la versione di Linux in uso e i requisiti hardware e storage.
  - Installare Red Hat Enterprise Linux o CentOS
  - Installare Ubuntu o Debian
- Se si prevede di implementare nuovi nodi grid su host esistenti, è stato confermato che gli host esistenti dispongono di CPU, RAM e capacità di storage sufficienti per i nodi aggiuntivi.
- Hai un piano per ridurre al minimo i domini di guasto. Ad esempio, non è necessario implementare tutti i nodi gateway su un singolo host fisico.

> In un'implementazione in produzione, non eseguire più di un nodo di storage su un singolo host fisico o virtuale. L'utilizzo di un host dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

- Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verificare che il volume non disponga di un criterio di tiering FabricPool attivato. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

Fasi

1. Se si aggiungono nuovi host, accedere alle istruzioni di installazione per l'implementazione dei nodi StorageGRID.
2. Per implementare i nuovi host, seguire le istruzioni per la preparazione degli host.
3. Per creare file di configurazione del nodo e convalidare la configurazione StorageGRID, seguire le istruzioni per l'implementazione dei nodi Grid.
4. Se si aggiungono nodi a un nuovo host Linux, avviare il servizio host StorageGRID.
5. Se si aggiungono nodi a un host Linux esistente, avviare i nuovi nodi utilizzando la CLI del servizio host StorageGRID:`sudo storagegrid node start [<node name\>]`

Al termine

Dopo aver implementato tutti i nuovi nodi grid, è possibile eseguire l'espansione.

Appliance: Implementazione di storage, gateway o nodi di amministrazione non primari

Per installare il software StorageGRID su un nodo appliance, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance. In un'espansione, ogni appliance di storage funziona come un singolo nodo di storage e ogni appliance di servizi funziona come un singolo nodo di gateway o un nodo di amministrazione non primario. Qualsiasi appliance può connettersi a Grid Network, Admin Network e Client Network.

Di cosa hai bisogno

- L'apparecchio è stato installato in un rack o in un cabinet, collegato alla rete e acceso.
- Il programma di installazione dell'appliance StorageGRID è stato utilizzato per completare tutte le fasi di "configurazione dell'hardware" nelle istruzioni di installazione e manutenzione dell'appliance.
  - Appliance di servizi SG100 e SG1000
  - Configurare l'hardware (SG5600)
  - Configurare l'hardware (SG5700)
  - Configurare l'hardware (SG6000)

  La configurazione dell'hardware dell'appliance include i passaggi necessari per la configurazione delle connessioni StorageGRID (collegamenti di rete e indirizzi IP), nonché i passaggi facoltativi per abilitare la crittografia dei nodi, modificare la modalità RAID e rimappare le porte di rete.
- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete griglia nel nodo di amministrazione principale.
- Il firmware del programma di installazione dell'appliance StorageGRID sull'appliance sostitutiva è compatibile con la versione del software StorageGRID attualmente in esecuzione sulla griglia. Ad esempio, la versione 3.6 del programma di installazione dell'appliance StorageGRID è compatibile con la versione 11.6 di StorageGRID. (Se le versioni non sono compatibili, è necessario aggiornare il firmware del programma di installazione dell'appliance StorageGRID).
- Si dispone di un laptop di assistenza con un browser web supportato.
- Conosci uno degli indirizzi IP assegnati al controller di calcolo dell'appliance. È possibile utilizzare l'indirizzo IP per qualsiasi rete StorageGRID collegata.

A proposito di questa attività

Il processo di installazione di StorageGRID su un nodo appliance prevede le seguenti fasi:

- Specificare o confermare l'indirizzo IP del nodo Admin primario e il nome del nodo appliance.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.

  Durante le attività di installazione dell'appliance, l'installazione viene interrotta. Per riprendere l'installazione, accedi a Grid Manager, approva tutti i nodi della griglia e completa il processo di installazione di StorageGRID.

> Se è necessario implementare più nodi appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando `configure-sga.py` Script di installazione dell'appliance.

Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di elaborazione dell'appliance.

   `https://Controller_IP:8443`

   Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Nella sezione connessione **Primary Admin Node**, determinare se è necessario specificare l'indirizzo IP per il nodo di amministrazione primario.

   Se in precedenza sono stati installati altri nodi in questo data center, il programma di installazione

dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, supponendo che il nodo di amministrazione primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente sulla stessa sottorete.

3. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Immissione manuale dell'IP	a. Deselezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Fare clic su **Save** (Salva). d. Attendere che lo stato di connessione del nuovo indirizzo IP diventi pronto.
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Attendere che venga visualizzato l'elenco degli indirizzi IP rilevati. c. Selezionare il nodo di amministrazione principale per la griglia in cui verrà implementato il nodo di storage dell'appliance. d. Fare clic su **Save** (Salva). e. Attendere che lo stato di connessione del nuovo indirizzo IP diventi pronto.

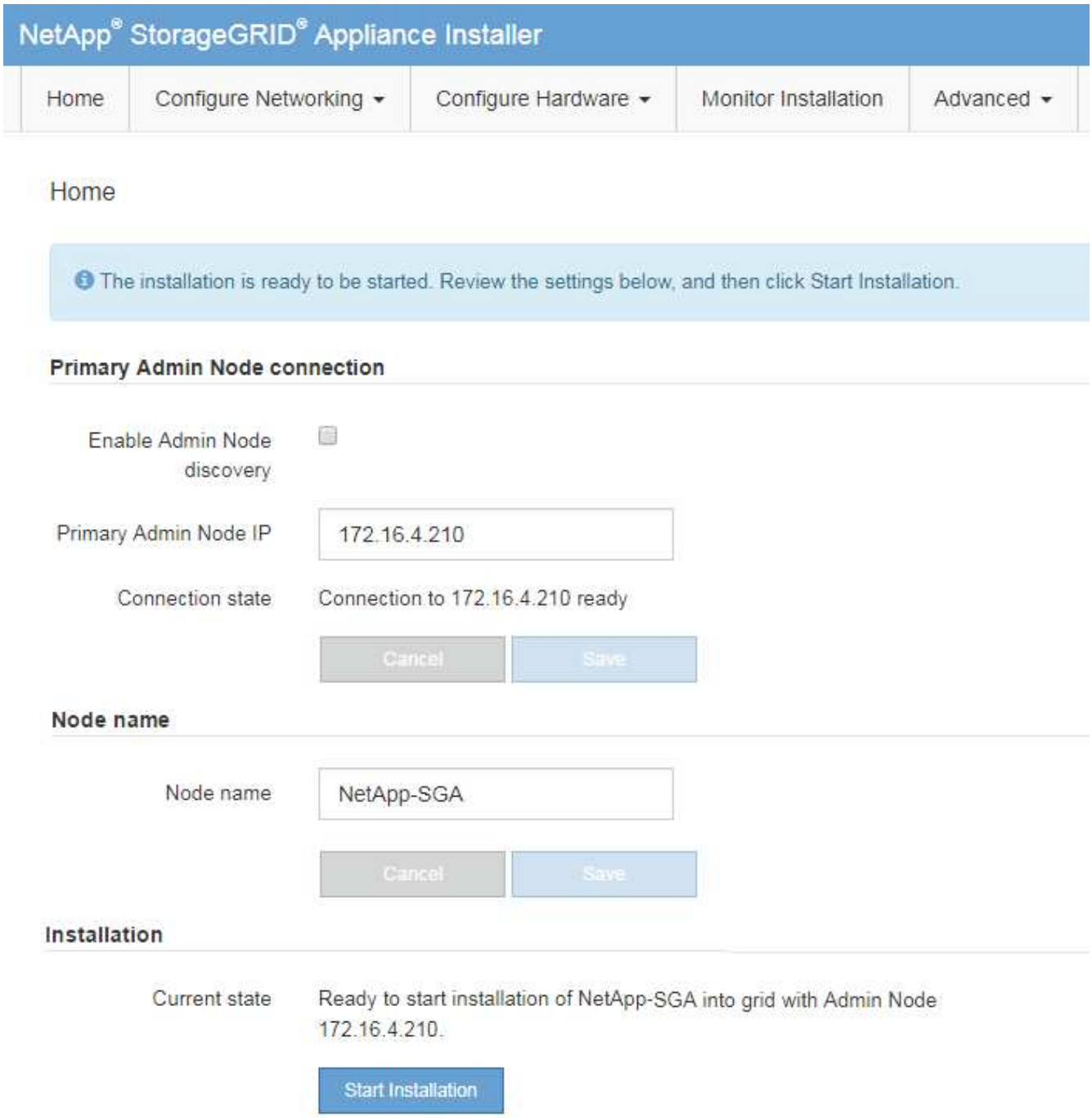
4. Nel campo **Node name** (Nome nodo), immettere il nome che si desidera utilizzare per il nodo dell'appliance e selezionare **Save** (Salva).

   Il nome del nodo viene assegnato al nodo dell'appliance nel sistema StorageGRID. Viene visualizzato nella pagina nodi (scheda Panoramica) di Grid Manager. Se necessario, è possibile modificare il nome quando si approva il nodo.

5. Nella sezione **Installazione**, verificare che lo stato corrente sia "Ready to start installation of *node name* into grid with primary Admin Node *admin_ip*" e che il pulsante **Start Installation** sia attivato.

   Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di installazione e manutenzione dell'apparecchio.

6. Dalla home page del programma di installazione dell'appliance StorageGRID, selezionare **Avvia installazione**.



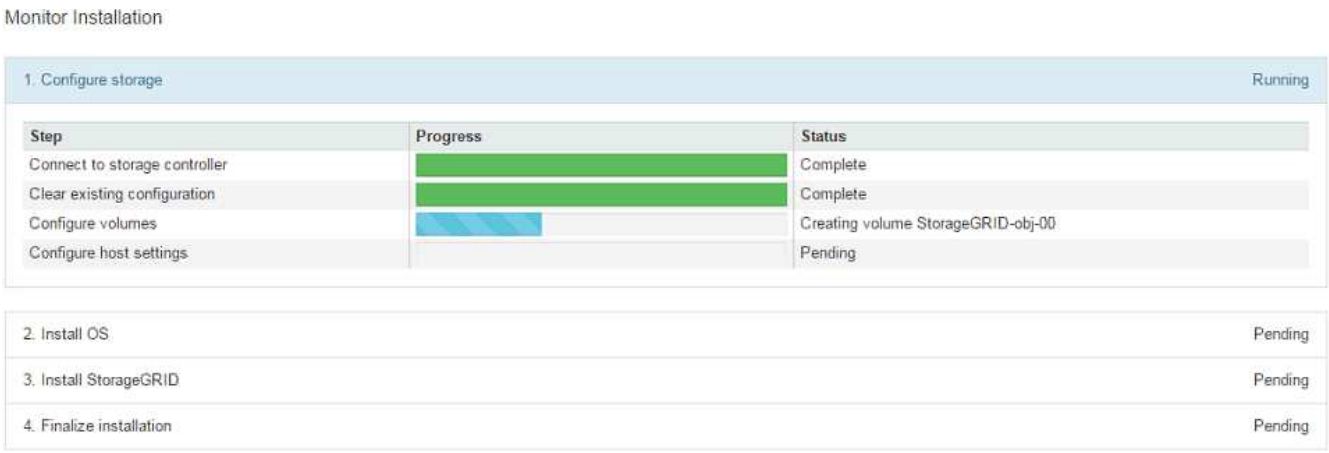
Lo stato corrente cambia in “Installation is in Progress” (Installazione in corso) e viene visualizzata la pagina Monitor Installation (Installazione monitor).

7. Se l’espansione include più nodi appliance, ripetere i passaggi precedenti per ogni appliance.

> Se è necessario implementare più nodi storage dell’appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando lo script di installazione dell’appliance configure-sga.py.

8. Per accedere manualmente alla pagina Installazione monitor, selezionare **Installazione monitor** dalla barra dei menu.

   La pagina Monitor Installation (Installazione monitor) mostra lo stato di avanzamento dell’installazione.



La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.

> Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si esegue nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "Skipped".

9. Esaminare i progressi delle prime due fasi dell'installazione.

   1. Configurare l'appliance

   In questa fase, si verifica uno dei seguenti processi:

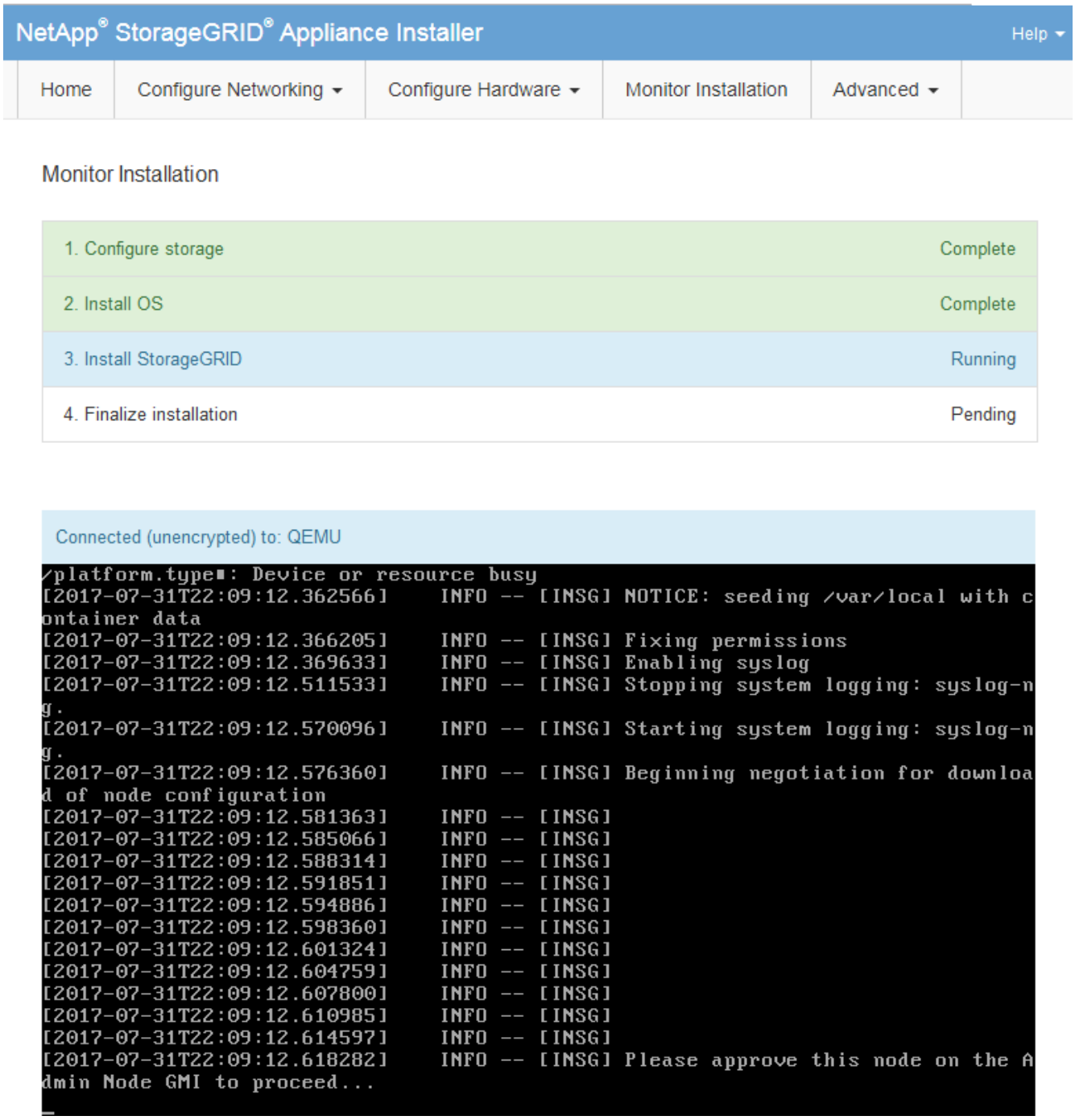
   - Per un'appliance di storage, il programma di installazione si connette al controller di storage, cancella qualsiasi configurazione esistente, comunica con il software SANtricity per configurare i volumi e configura le impostazioni dell'host.
   - Per un'appliance di servizi, il programma di installazione cancella qualsiasi configurazione esistente dai dischi nel controller di calcolo e configura le impostazioni dell'host.

   2. Installare il sistema operativo

   In questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID nell'appliance.

10. Continuare a monitorare l'avanzamento dell'installazione fino a quando non viene visualizzato un messaggio nella finestra della console, che richiede di utilizzare Grid Manager per approvare il nodo.

> Attendere che tutti i nodi aggiunti a questa espansione siano pronti per l'approvazione prima di passare al Grid Manager per approvare i nodi.



Eseguire l’espansione

Quando si esegue l’espansione, i nuovi nodi grid vengono aggiunti all’implementazione StorageGRID esistente.

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.
- Sono stati implementati tutti i nodi grid che vengono aggiunti in questa espansione.

- Se si aggiungono nodi di storage, si conferma che tutte le operazioni di riparazione dei dati eseguite come parte di un ripristino sono state completate. Vedere Controllare i lavori di riparazione dei dati.
- Se si aggiunge un nuovo sito, è necessario rivedere e aggiornare le regole ILM prima di avviare la procedura di espansione per assicurarsi che le copie degli oggetti non vengano memorizzate nel nuovo sito fino al completamento dell'espansione. Ad esempio, se una regola utilizza il pool di storage predefinito (tutti i nodi di storage), è necessario creare un nuovo pool di storage che contenga solo i nodi di storage esistenti e aggiornare la regola ILM per utilizzare il nuovo pool di storage. In caso contrario, gli oggetti verranno copiati nel nuovo sito non appena il primo nodo del sito diventa attivo. Consultare le istruzioni per Gestione degli oggetti con ILM.

A proposito di questa attività

L'esecuzione dell'espansione comprende le seguenti fasi:

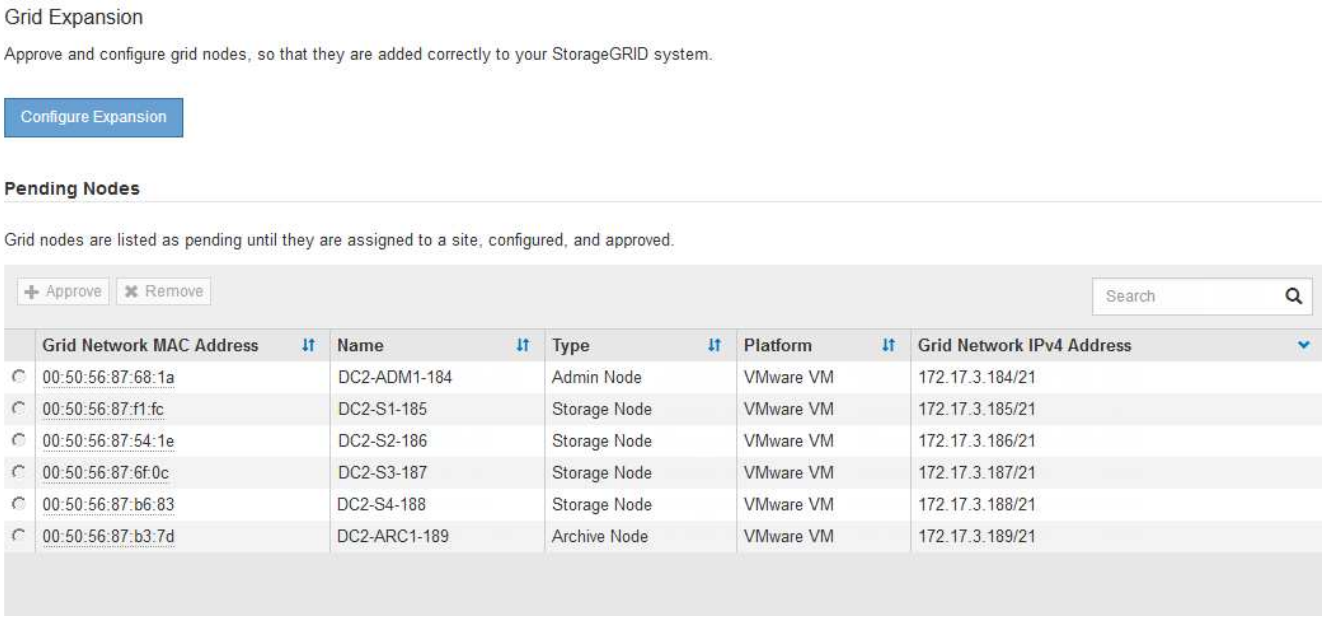
1. Per configurare l'espansione, specificare se si desidera aggiungere nuovi nodi griglia o un nuovo sito e approvare i nodi griglia da aggiungere.
2. Si avvia l'espansione.
3. Durante il processo di espansione, viene scaricato un nuovo file del pacchetto di ripristino.
4. È possibile monitorare lo stato delle fasi di configurazione della griglia, che vengono eseguite automaticamente. L'insieme di fasi dipende dai tipi di nodi di griglia che vengono aggiunti e dall'eventuale aggiunta di un nuovo sito.

> Alcune fasi potrebbero richiedere molto tempo per essere eseguite su una griglia di grandi dimensioni. Ad esempio, lo streaming di Cassandra su un nuovo nodo di storage potrebbe richiedere solo pochi minuti se il database Cassandra è vuoto. Tuttavia, se il database Cassandra include una grande quantità di metadati degli oggetti, questa fase potrebbe richiedere diverse ore o più. Non riavviare i nodi di storage durante le fasi "espansione del cluster Cassandra" o "Avvio di Cassandra e dati in streaming".

Fasi

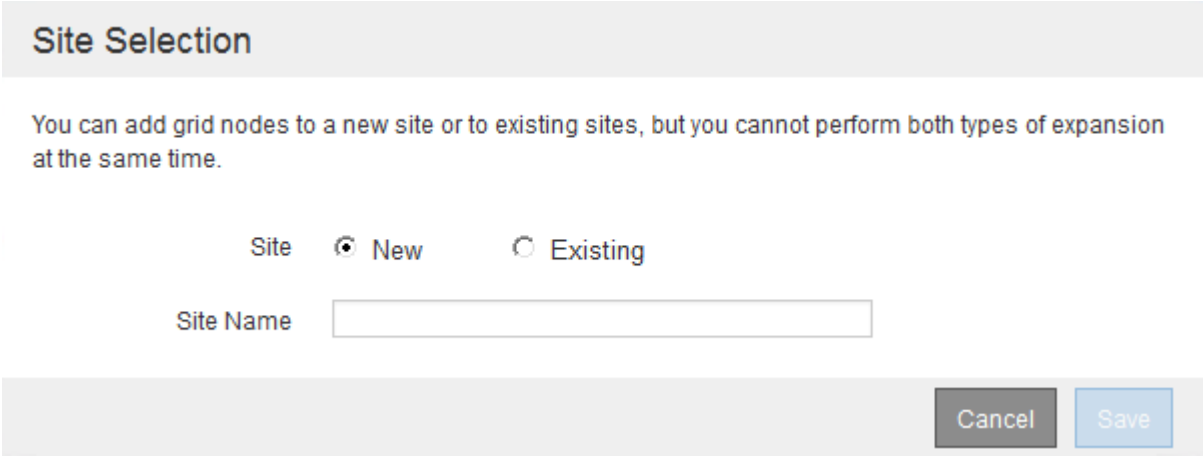
1. Selezionare **MANUTENZIONE** > **attività** > **espansione**.

   Viene visualizzata la pagina Grid Expansion (espansione griglia). La sezione Pending Nodes (nodi in sospeso) elenca tutti i nodi pronti per l'aggiunta.



2. Selezionare **Configure Expansion** (Configura espansione).

   Viene visualizzata la finestra di dialogo Site Selection (selezione sito).



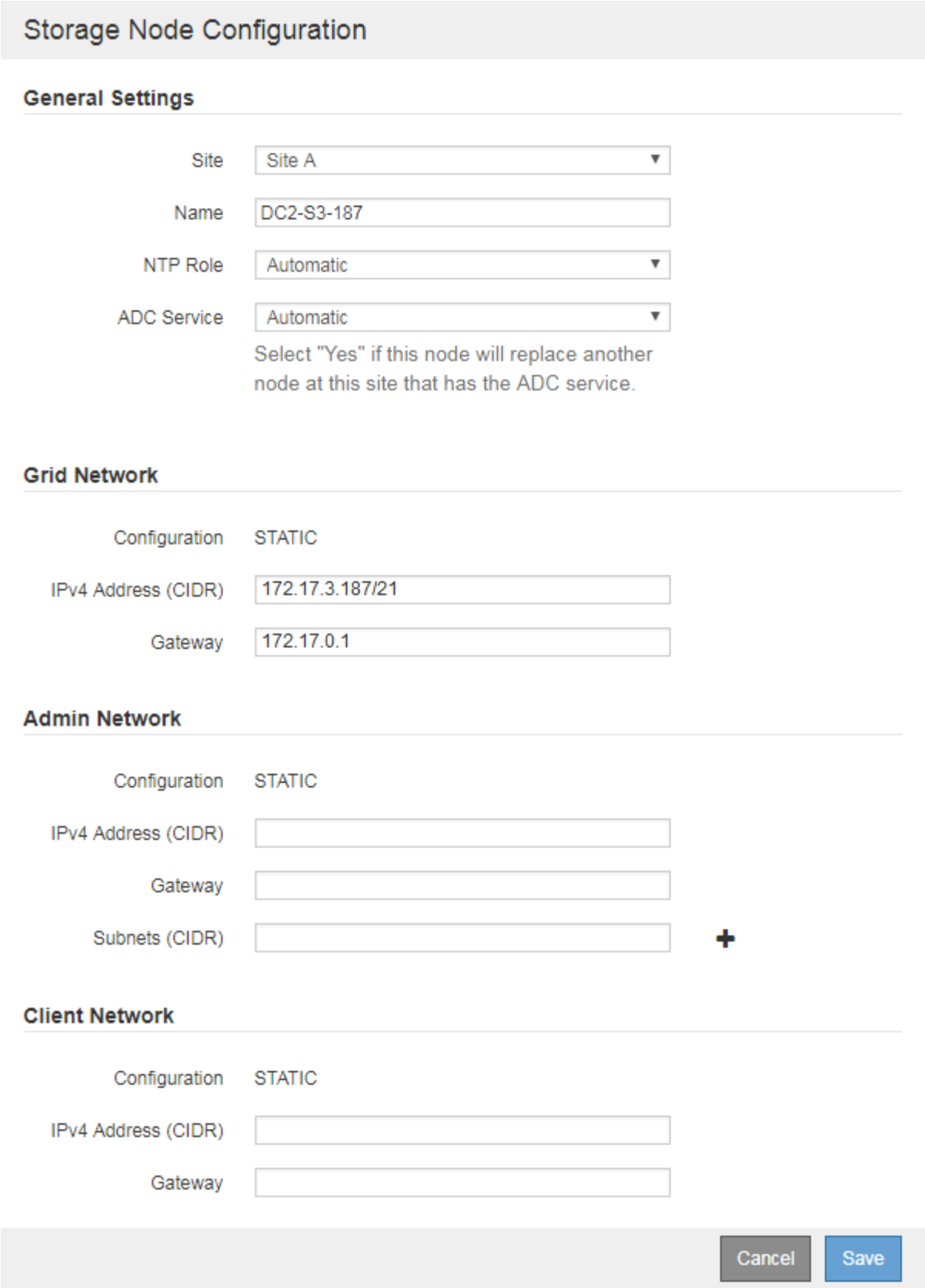
3. Selezionare il tipo di espansione che si desidera avviare:
   - Se si sta aggiungendo un nuovo sito, selezionare **nuovo** e immettere il nome del nuovo sito.
   - Se si aggiungono nodi griglia a un sito esistente, selezionare **esistente**.
4. Selezionare **Salva**.
5. Esaminare l'elenco **Pending Nodes** (nodi in sospeso) e confermare che mostra tutti i nodi della griglia implementati.

   Se necessario, spostare il cursore del mouse sull'indirizzo **Grid Network MAC Address** di un nodo per visualizzare i dettagli relativi a tale nodo.

Se manca un nodo Grid, confermare che è stato implementato correttamente.

6. Dall'elenco dei nodi in sospeso, approvare i nodi della griglia per questa espansione.
   a. Selezionare il pulsante di opzione accanto al primo nodo della griglia in sospeso che si desidera approvare.
   b. Selezionare **approva**.

      Viene visualizzato il modulo di configurazione del nodo della griglia.



c. Se necessario, modificare le impostazioni generali:

- **Sito**: Il nome del sito a cui verrà associato il nodo della griglia. Se si aggiungono più nodi, assicurarsi di selezionare il sito corretto per ciascun nodo. Se si aggiunge un nuovo sito, tutti i nodi vengono aggiunti al nuovo sito.

- **Name**: Il nome host che verrà assegnato al nodo e il nome che verrà visualizzato in Grid Manager.
- **Ruolo NTP**: Ruolo NTP (Network Time Protocol) del nodo Grid. Le opzioni disponibili sono **automatico**, **primario** e **Client**. Selezionando **automatico**, il ruolo primario viene assegnato ai nodi di amministrazione, ai nodi di storage con servizi ADC, ai nodi gateway e a tutti i nodi di griglia che hanno indirizzi IP non statici. A tutti gli altri nodi della griglia viene assegnato il ruolo Client.

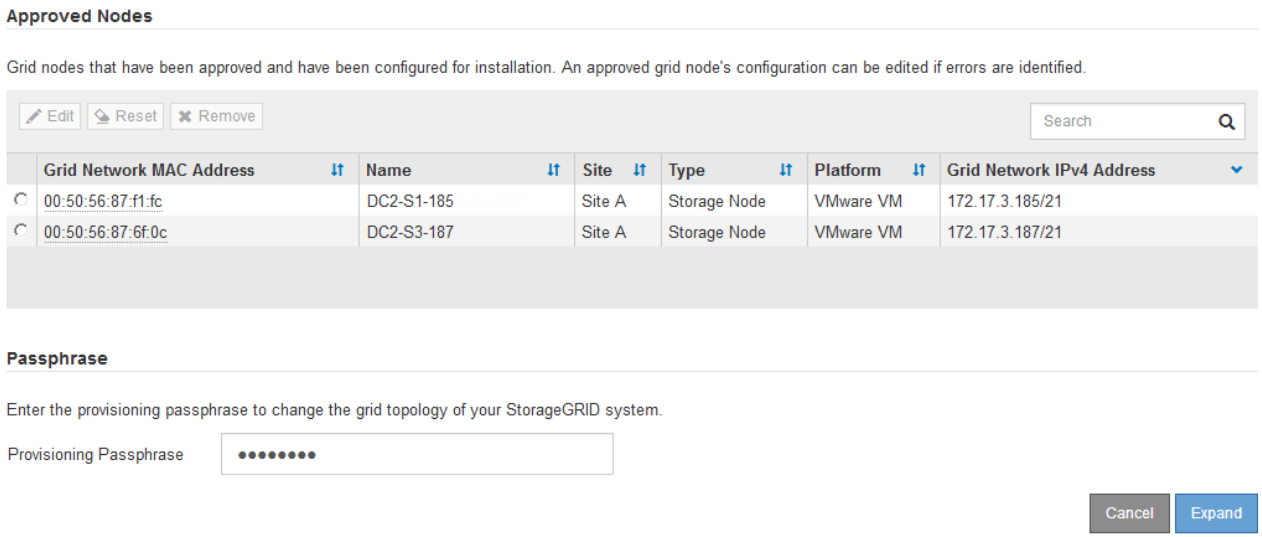
> Assegnare il ruolo NTP primario ad almeno due nodi in ciascun sito. In questo modo, il sistema offre un accesso ridondante a fonti di sincronizzazione esterne.

- **Servizio ADC** (solo nodi di storage): Se questo nodo di storage eseguirà il servizio ADC (Administrative Domain Controller). Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi grid. Almeno tre nodi di storage in ogni sito devono includere il servizio ADC. Non è possibile aggiungere il servizio ADC a un nodo dopo averlo implementato.
  - Se si aggiunge questo nodo per sostituire un nodo di storage, selezionare **Sì** se il nodo da sostituire include il servizio ADC. Poiché non è possibile decommissionare un nodo di storage se rimangono pochi servizi ADC, ciò garantisce che un nuovo servizio ADC sia disponibile prima che il vecchio servizio venga rimosso.
  - In caso contrario, selezionare **automatico** per consentire al sistema di determinare se questo nodo richiede il servizio ADC. Informazioni sul quorum di ADC qui.

d. Se necessario, modificare le impostazioni per Grid Network, Admin Network e Client Network.
   - **IPv4 Address (CIDR)**: Indirizzo di rete CIDR per l'interfaccia di rete. Ad esempio: 172.16.10.100/24
   - **Gateway**: Il gateway predefinito del nodo Grid. Ad esempio: 172.16.10.1
   - **Subnet (CIDR)**: Una o più sottoreti per la rete di amministrazione.

e. Selezionare **Salva**.

   Il nodo della griglia approvata passa all'elenco dei nodi approvati.



   - Per modificare le proprietà di un nodo della griglia approvato, selezionare il relativo pulsante di opzione e selezionare **Modifica**.
   - Per spostare di nuovo un nodo della griglia approvato nell'elenco Pending Nodes (nodi in sospeso), selezionare il relativo pulsante di opzione e selezionare **Reset** (Ripristina).

- Per rimuovere in modo permanente un nodo di rete approvato, spegnere il nodo. Quindi, selezionare il pulsante di opzione corrispondente e selezionare **Rimuovi**.

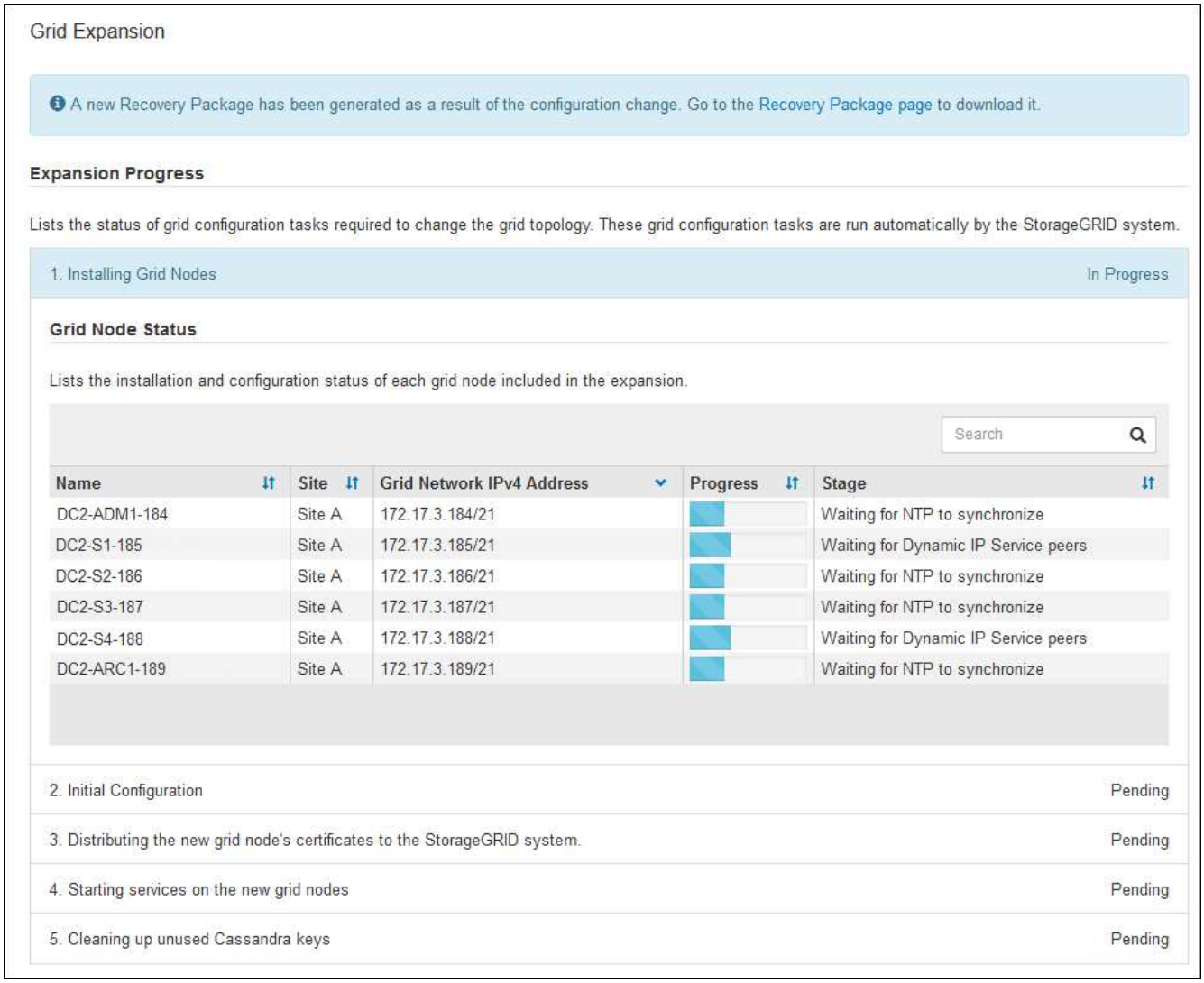
f. Ripetere questi passaggi per ogni nodo griglia in sospeso che si desidera approvare.

> Se possibile, è necessario approvare tutte le note della griglia in sospeso ed eseguire una singola espansione. Se si eseguono più piccole espansioni, sarà necessario più tempo.

7. Una volta approvati tutti i nodi della griglia, immettere la **Provisioning Passphrase** e selezionare **Espandi**.

   Dopo alcuni minuti, questa pagina viene aggiornata per visualizzare lo stato della procedura di espansione. Quando sono in corso attività che influiscono su un singolo nodo della griglia, la sezione Grid Node Status (Stato nodo griglia) elenca lo stato corrente di ciascun nodo della griglia.

> Durante questo processo, il programma di installazione dell'appliance StorageGRID mostra il passaggio dell'installazione dalla fase 3 alla fase 4, finalizzare l'installazione. Al termine della fase 4, il controller viene riavviato.



> Un'espansione del sito include un'attività aggiuntiva per configurare Cassandra per il nuovo sito.

8. Non appena viene visualizzato il collegamento **Download Recovery Package**, scaricare il file Recovery Package.

   È necessario scaricare una copia aggiornata del file del pacchetto di ripristino il prima possibile dopo aver apportato modifiche alla topologia della griglia al sistema StorageGRID. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

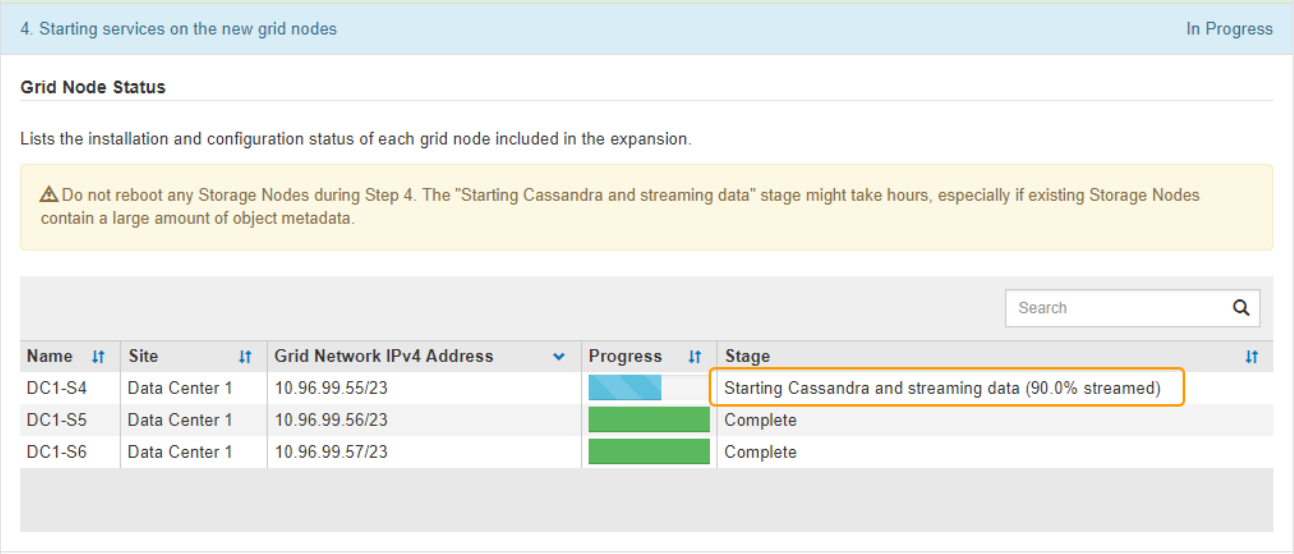
   a. Selezionare il collegamento per il download.
   b. Inserire la passphrase di provisioning e selezionare **Avvia download**.
   c. Al termine del download, aprire `.zip` archiviare e confermare che include un `gpt-backup` directory e a. `_SAID.zip` file. Quindi, estrarre `_SAID.zip` accedere al `/GID*_REV*` e confermare la possibilità di aprire `passwords.txt` file.
   d. Copiare il file del pacchetto di ripristino scaricato (.zip) in due posizioni sicure e separate.

   > Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

9. Seguire le istruzioni per aggiungere un nodo di storage a un sito esistente o aggiungere un nuovo sito.

Aggiungere il nodo di storage al sito esistente

Se si aggiungono uno o più nodi di storage a un sito esistente, monitorare l'avanzamento della fase "Avvio di Cassandra e dati in streaming" esaminando la percentuale indicata nel messaggio di stato.



Questa percentuale stima il completamento dell'operazione di streaming Cassandra in base alla quantità totale di dati Cassandra disponibili e alla quantità già scritta nel nuovo nodo.

> Non riavviare i nodi di storage durante le fasi di "espansione del cluster Cassandra" o "avvio di Cassandra e dati in streaming". Il completamento di queste fasi potrebbe richiedere molte ore per ogni nuovo nodo di storage, soprattutto se i nodi di storage esistenti contengono una grande quantità di metadati degli oggetti.

Aggiungi nuovo sito

Se si aggiunge un nuovo sito, utilizzare `nodetool status` Monitorare i progressi dello streaming Cassandra e verificare quanti metadati sono stati copiati nel nuovo sito durante la fase di "espansione del cluster Cassandra". Il carico totale di dati sul nuovo sito deve essere inferiore a circa il 20% del totale di un sito corrente.

> Non riavviare i nodi di storage durante le fasi di "espansione del cluster Cassandra" o "avvio di Cassandra e dati in streaming". Il completamento di queste fasi potrebbe richiedere molte ore per ogni nuovo nodo di storage, soprattutto se i nodi di storage esistenti contengono una grande quantità di metadati degli oggetti.

1. Continuare a monitorare l'espansione fino al completamento di tutte le attività e alla ricomposizione del pulsante **Configure Expansion** (Configura espansione).

Al termine

A seconda dei tipi di nodi griglia aggiunti, è necessario eseguire ulteriori operazioni di integrazione e configurazione. Vedere Fasi di configurazione dopo l'espansione.

Configurare il sistema esteso

Fasi di configurazione dopo l'espansione

Dopo aver completato un'espansione, è necessario eseguire ulteriori operazioni di integrazione e configurazione.

A proposito di questa attività

È necessario completare le attività di configurazione elencate di seguito per i nodi griglia che si stanno aggiungendo all'espansione. Alcune attività potrebbero essere facoltative, a seconda delle opzioni selezionate durante l'installazione e l'amministrazione del sistema e di come si desidera configurare i nodi della griglia aggiunti durante l'espansione.

Fasi

1. Se è stato aggiunto un nodo di storage, completare le seguenti attività di configurazione:
   a. Esaminare i pool di storage utilizzati nelle regole ILM per assicurarsi che venga utilizzato il nuovo storage. Vedere Gestire gli oggetti con ILM.
      - Se è stato aggiunto un sito, creare un pool di storage per il sito e aggiornare le regole ILM per utilizzare il nuovo pool di storage.
      - Se è stato aggiunto un nodo di storage a un sito esistente, verificare che il nuovo nodo utilizzi il livello di storage corretto.

      > Per impostazione predefinita, un nuovo nodo di storage viene assegnato al livello di storage All Storage Node e aggiunto ai pool di storage che utilizzano tale livello per il sito. Se si desidera che un nuovo nodo utilizzi un livello di storage personalizzato, è necessario assegnarlo manualmente al livello di valutazione personalizzato (**ILM** > **Storage Grades**).

   b. Verificare che il nodo di storage stia acquisendo oggetti. Vedere Verificare che il nodo di storage sia attivo.
   c. Ribilanciare i dati con codifica di cancellazione (solo se non è stato possibile aggiungere il numero consigliato di nodi di storage). VedereRibilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage.
2. Se è stato aggiunto un nodo gateway, completare la seguente attività di configurazione:
   - Se si utilizzano gruppi ad alta disponibilità (ha) per le connessioni client, aggiungere facoltativamente il nodo gateway a un gruppo ha. Selezionare **CONFIGURATION** > **Network** > **High Availability groups** per rivedere l'elenco dei gruppi ha esistenti e aggiungere il nuovo nodo. Vedere Amministrare StorageGRID.
3. Se è stato aggiunto un nodo amministratore, completare le seguenti attività di configurazione:
   a. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, creare un trust per la parte di base per il nuovo nodo di amministrazione. Non è possibile accedere al nodo fino a quando non si crea questo trust per la parte di base. VedereConfigurare il single sign-on.
   b. Se si intende utilizzare il servizio Load Balancer sui nodi Admin, aggiungere facoltativamente il nuovo nodo Admin a un gruppo ha. Selezionare **CONFIGURATION** > **Network** > **High Availability groups** per rivedere l'elenco dei gruppi ha esistenti e aggiungere il nuovo nodo. Vedere Amministrare StorageGRID.
   c. Facoltativamente, copiare il database del nodo di amministrazione dal nodo di amministrazione primario al nodo di amministrazione di espansione se si desidera mantenere costanti le informazioni di attributo e controllo su ciascun nodo di amministrazione. Vedere Copiare il database Admin Node.
   d. Facoltativamente, copiare il database Prometheus dal nodo di amministrazione primario al nodo di

amministrazione di espansione se si desidera mantenere costanti le metriche storiche su ciascun nodo di amministrazione. Vedere Copia le metriche Prometheus.

e. Facoltativamente, copiare i registri di controllo esistenti dal nodo di amministrazione principale al nodo di amministrazione dell'espansione se si desidera mantenere coerenti le informazioni di registro cronologiche su ciascun nodo di amministrazione. Vedere Copia dei registri di audit.

f. Facoltativamente, configurare l'accesso al sistema per scopi di controllo tramite una condivisione file NFS o CIFS. Vedere Amministrare StorageGRID.

> L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

g. Facoltativamente, modificare il mittente preferito per le notifiche. È possibile impostare l'Admin Node di espansione come mittente preferito. In caso contrario, un nodo amministrativo esistente configurato come mittente preferito continua a inviare notifiche, tra cui messaggi AutoSupport, notifiche SNMP, e-mail di avviso ed e-mail di allarme (sistema legacy). Vedere Amministrare StorageGRID.

4. Se è stato aggiunto un nodo di archiviazione, completare le seguenti attività di configurazione.

   a. Configurare la connessione del nodo di archiviazione al sistema di archiviazione esterno di destinazione. Una volta completata l'espansione, i nodi di archiviazione si trovano in uno stato di allarme fino a quando non si configurano le informazioni di connessione tramite il componente **ARC** > **Target**. Vedere Amministrare StorageGRID.

   b. Aggiornare il criterio ILM per archiviare i dati dell'oggetto attraverso il nuovo nodo di archivio. Vedere Gestire gli oggetti con ILM.

   c. Configurare gli allarmi personalizzati per gli attributi utilizzati per monitorare la velocità e l'efficienza del recupero dei dati degli oggetti dai nodi di archiviazione. Vedere Amministrare StorageGRID.

5. Per verificare se i nodi di espansione sono stati aggiunti con una rete client non attendibile o per modificare se la rete client di un nodo è non attendibile o attendibile, andare a **CONFIGURAZIONE** > **rete** > **rete client non attendibile**.

   Se la rete client sul nodo di espansione non è attendibile, le connessioni al nodo sulla rete client devono essere effettuate utilizzando un endpoint di bilanciamento del carico. Vedere Amministrare StorageGRID.

6. Configurare il DNS (Domain Name System).

   Se le impostazioni DNS sono state specificate separatamente per ciascun nodo della griglia, è necessario aggiungere impostazioni DNS personalizzate per nodo per i nuovi nodi. Vedere Modificare la configurazione DNS per un nodo griglia singolo.

   La procedura consigliata prevede che l'elenco dei server DNS a livello di griglia contenga alcuni server DNS accessibili localmente da ciascun sito. Se è stato appena aggiunto un nuovo sito, aggiungere nuovi server DNS per il sito alla configurazione DNS a livello di griglia.

   > Fornire da due a sei indirizzi IPv4 per i server DNS. Selezionare i server DNS ai quali ciascun sito può accedere localmente in caso di rete. In questo modo si garantisce che un sito islanded continui ad avere accesso al servizio DNS. Dopo aver configurato l'elenco dei server DNS a livello di griglia, è possibile personalizzare ulteriormente l'elenco dei server DNS per ciascun nodo. Per ulteriori informazioni, vedere Modificare la configurazione DNS per un nodo griglia singolo..

7. Se è stato aggiunto un nuovo sito, verificare che i server NTP (Network Time Protocol) siano accessibili da tale sito. Vedere Configurare i server NTP.

> Assicurarsi che almeno due nodi di ciascun sito possano accedere ad almeno quattro origini NTP esterne. Se solo un nodo di un sito può raggiungere le origini NTP, si verificheranno problemi di tempistica se tale nodo non funziona. Inoltre, la designazione di due nodi per sito come origini NTP primarie garantisce tempi precisi se un sito viene isolato dal resto della rete.

Verificare che il nodo di storage sia attivo

Al termine di un'operazione di espansione che aggiunge nuovi nodi di storage, il sistema StorageGRID dovrebbe avviarsi automaticamente utilizzando i nuovi nodi di storage. È necessario utilizzare il sistema StorageGRID per verificare che il nuovo nodo di storage sia attivo.

Fasi

1. Accedere a Grid Manager utilizzando un browser web supportato.
2. Selezionare **NODES** > ***Expansion Storage Node*** > **Storage**.
3. Spostare il cursore sul grafico **Storage used - Object Data** (archiviazione utilizzata - dati oggetto) per visualizzare il valore di **Used**, che corrisponde alla quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
4. Verificare che il valore di **used** aumenti man mano che si sposta il cursore a destra sul grafico.

Copia database nodo amministratore

Quando si aggiungono nodi di amministrazione tramite una procedura di espansione, è possibile copiare il database dal nodo di amministrazione primario al nuovo nodo di amministrazione. La copia del database consente di conservare informazioni cronologiche su attributi, avvisi e avvisi.

Di cosa hai bisogno

- Sono state completate le fasi di espansione richieste per aggiungere un nodo di amministrazione.
- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

Il processo di attivazione del software StorageGRID crea un database vuoto per il servizio NMS sul nodo di amministrazione dell'espansione. Quando il servizio NMS viene avviato nel nodo di amministrazione dell'espansione, registra le informazioni relative ai server e ai servizi che fanno parte del sistema o che vengono aggiunti in seguito. Questo database del nodo di amministrazione include le seguenti informazioni:

- Cronologia degli avvisi
- Cronologia degli allarmi
- Dati storici degli attributi, utilizzati nei grafici e nei report di testo disponibili nella pagina **SUPPORTO** > **Strumenti** > **topologia griglia**

Per garantire che il database Admin Node sia coerente tra i nodi, è possibile copiare il database dal nodo Admin primario al nodo Admin di espansione.

> La copia del database dal nodo di amministrazione principale (il nodo di amministrazione___ di origine) a un nodo di amministrazione di espansione può richiedere fino a diverse ore per il completamento. Durante questo periodo, il Grid Manager non è accessibile.

Prima di copiare il database, attenersi alla procedura descritta di seguito per arrestare il servizio MI e il servizio API di gestione sul nodo di amministrazione primario e sul nodo di amministrazione dell'espansione.

Fasi

1. Completare i seguenti passaggi sul nodo di amministrazione principale:
   a. Accedere al nodo di amministrazione:
      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.
   b. Eseguire il seguente comando: `recover-access-points`
   c. Inserire la passphrase di provisioning.
   d. Arrestare il servizio MI: `service mi stop`
   e. Arrestare il servizio Management Application Program Interface (mgmt-api): `service mgmt-api stop`
2. Completare i seguenti passaggi sul nodo di amministrazione dell'espansione:
   a. Accedere al nodo di amministrazione dell'espansione:
      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.
   b. Arrestare il servizio MI: `service mi stop`
   c. Arrestare il servizio mgmt-api: `service mgmt-api stop`
   d. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`
   e. Inserire la password di accesso SSH elencata in `Passwords.txt` file.
   f. Copiare il database dal nodo Admin di origine al nodo Admin di espansione: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Quando richiesto, confermare che si desidera sovrascrivere il database MI nel nodo di amministrazione dell'espansione.

      Il database e i relativi dati storici vengono copiati nel nodo di amministrazione dell'espansione. Al termine dell'operazione di copia, lo script avvia l'espansione Admin Node.

   h. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`
3. Riavviare i servizi sul nodo di amministrazione primario: `service servermanager start`

Copia le metriche Prometheus

Dopo aver aggiunto un nuovo nodo di amministrazione, è possibile copiare facoltativamente le metriche storiche gestite da Prometheus dal nodo di amministrazione primario al nuovo nodo di amministrazione. La copia delle metriche garantisce che le metriche storiche siano coerenti tra i nodi di amministrazione.

Di cosa hai bisogno

- Il nuovo nodo di amministrazione è installato e in esecuzione.
- Hai il `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

Quando si aggiunge un nodo di amministrazione, il processo di installazione del software crea un nuovo database Prometheus. È possibile mantenere costanti le metriche storiche tra i nodi copiando il database Prometheus dal nodo di amministrazione primario (il *nodo di amministrazione di origine*) al nuovo nodo di amministrazione.

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
   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.
2. Dal nodo Admin di origine, arrestare il servizio Prometheus: `service prometheus stop`
3. Completare i seguenti passaggi sul nuovo nodo di amministrazione:
   a. Accedere al nuovo nodo di amministrazione:
      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.
   b. Interrompere il servizio Prometheus: `service prometheus stop`
   c. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`
   d. Inserire la password di accesso SSH elencata in `Passwords.txt` file.
   e. Copiare il database Prometheus dal nodo Admin di origine al nuovo nodo Admin: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Quando richiesto, premere **Invio** per confermare che si desidera distruggere il nuovo database Prometheus nel nuovo nodo di amministrazione.

Il database Prometheus originale e i relativi dati storici vengono copiati nel nuovo nodo di amministrazione. Al termine dell'operazione di copia, lo script avvia il nuovo nodo di amministrazione. Viene visualizzato il seguente stato:

```
Database cloned, starting services
```

a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:

```
ssh-add -D
```

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.

```
service prometheus start
```

Copia dei registri di audit

Quando si aggiunge un nuovo nodo amministratore mediante una procedura di espansione, il servizio AMS registra solo gli eventi e le azioni che si verificano dopo l'accesso al sistema. Se necessario, è possibile copiare i registri di controllo da un nodo amministratore precedentemente installato nel nuovo nodo amministratore di espansione in modo che sia sincronizzato con il resto del sistema StorageGRID.

Di cosa hai bisogno

- Sono state completate le fasi di espansione richieste per aggiungere un nodo di amministrazione.
- Hai il `Passwords.txt` file.

A proposito di questa attività

Per rendere disponibili i messaggi di audit storici su un nuovo nodo di amministrazione, è necessario copiare manualmente i file di log di audit da un nodo di amministrazione esistente al nodo di amministrazione dell'espansione.

> Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:
>
> - È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
> - È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.
>
> Vedere Configurare i messaggi di audit e le destinazioni dei log per ulteriori informazioni.

Fasi

1. 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. `#`.

2. Arrestare il servizio AMS per impedire la creazione di un nuovo file: `service ams stop`
3. Rinominare il `audit.log` File per assicurarsi che non sovrascriva il file sul nodo di amministrazione dell'espansione in cui si sta copiando:

```
cd /var/local/audit/export
ls -l
mv audit.log new_name.txt
```

4. Copiare tutti i file di log dell'audit nel nodo di amministrazione dell'espansione:

```
scp -p * IP_address:/var/local/audit/export
```

5. Se viene richiesta la passphrase per `/root/.ssh/id_rsa`, Immettere la password di accesso SSH per il nodo di amministrazione principale elencato in `Passwords.txt` file.
6. Ripristinare l'originale `audit.log` file:

```
mv new_name.txt audit.log
```

7. Avviare il servizio AMS:

```
service ams start
```

8. Disconnettersi dal server:

```
exit
```

9. Accedere al nodo di amministrazione dell'espansione:
   a. Immettere il seguente comando: `ssh admin@expansion_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. `#`.

10. Aggiornare le impostazioni dell'utente e del gruppo per i file di log di controllo:

```
cd /var/local/audit/export
chown ams-user:bycast *
```

11. Disconnettersi dal server:

```
exit
```

Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage

In alcuni casi, potrebbe essere necessario ribilanciare i dati con codifica di cancellazione dopo aver aggiunto nuovi nodi di storage.

Di cosa hai bisogno

- Sono state completate le fasi di espansione per aggiungere i nuovi nodi di storage.
- Hai esaminato il considerazioni per il ribilanciamento dei dati con codifica erasure.

> Eseguire questa procedura solo se l'avviso **Low Object Storage** è stato attivato per uno o più nodi di storage in un sito e non è stato possibile aggiungere il numero consigliato di nuovi nodi di storage.

- Si comprende che i dati degli oggetti replicati non verranno spostati da questa procedura e che la procedura di ribilanciamento EC non prende in considerazione l'utilizzo dei dati replicati su ciascun nodo di storage quando si determina dove spostare i dati con codifica di cancellazione.
- Hai il `Passwords.txt` file.

A proposito di questa attività

Quando la procedura di ribilanciamento EC è in esecuzione, è probabile che le prestazioni delle operazioni ILM e delle operazioni dei client S3 e Swift ne risentano. Per questo motivo, questa procedura deve essere eseguita solo in casi limitati.

> La procedura di ribilanciamento EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine del ribilanciamento. Se lo storage non è sufficiente per la prenotazione, la procedura di ribilanciamento EC non avrà esito positivo. Le riserve di storage vengono rilasciate al termine della procedura di ribilanciamento EC, indipendentemente dal fatto che la procedura abbia avuto esito negativo o positivo.

> Le operazioni S3 e Swift API per caricare oggetti (o parti di oggetti) potrebbero non riuscire durante la procedura di ribilanciamento EC se richiedono più di 24 ore per essere completate. Le operazioni PUT di lunga durata non avranno esito positivo se la regola ILM applicabile utilizza un posizionamento rigoroso o bilanciato all'acquisizione. Viene segnalato il seguente errore:
>
> `500 Internal Server Error`

Fasi

1. Rivedi i dettagli dello storage a oggetti corrente per il sito che intendi ribilanciare.
   a. Selezionare **NODI**.
   b. Selezionare il primo nodo di storage nel sito.
   c. Selezionare la scheda **Storage**.
   d. Spostare il cursore del mouse sul grafico Storage Used - Object Data (Storage utilizzato - dati oggetto) per visualizzare la quantità corrente di dati replicati e i dati con codifica di cancellazione sul nodo di storage.
   e. Ripetere questa procedura per visualizzare gli altri nodi di storage del sito.
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. Immettere il seguente comando:

   ```
   rebalance-data start --site "site-name"
   ```

   Per `"site-name"`, Specificare il primo sito in cui sono stati aggiunti nuovi nodi o nodi di storage. Racchiudere `site-name` tra virgolette.

   Viene avviata la procedura di ribilanciamento EC e viene restituito un ID lavoro.

4. Copiare l'ID lavoro.
5. Monitorare lo stato della procedura di ribilanciamento EC.

   - Per visualizzare lo stato di una singola procedura di ribilanciamento EC:

     ```
     rebalance-data status --job-id job-id
     ```

     Per `job-id`, Specificare l'ID restituito all'avvio della procedura.

   - Per visualizzare lo stato della procedura di ribilanciamento EC corrente e delle procedure precedentemente completate:

     ```
     rebalance-data status
     ```

     > Per ottenere assistenza sul comando ribilanciamento-dati:
     >
     > ```
     > rebalance-data --help
     > ```

   - Per visualizzare il tempo stimato di completamento e la percentuale di completamento per il lavoro corrente, selezionare **SUPPORTO** > **Strumenti** > **metriche**. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).

6. Eseguire ulteriori operazioni in base allo stato restituito:

   - Se lo stato è `In progress`, L'operazione di ribilanciamento EC è ancora in esecuzione. È necessario monitorare periodicamente la procedura fino al completamento.
   - Se lo stato è `Failure`, eseguire fasi di guasto.
   - Se lo stato è `Success`, eseguire fase di successo.

7. Se la procedura di ribilanciamento EC genera un carico eccessivo (ad esempio, le operazioni di acquisizione sono interessate), sospendere la procedura.

   ```
   rebalance-data pause --job-id job-id
   ```

8. Se è necessario terminare la procedura di ribilanciamento EC (ad esempio, in modo da poter eseguire un aggiornamento del software StorageGRID), immettere quanto segue:

   `rebalance-data terminate --job-id job-id`

   > Quando si termina una procedura di ribilanciamento EC, tutti i frammenti di dati che sono già stati spostati rimangono nella nuova posizione. I dati non vengono spostati di nuovo nella posizione originale.

9. [[ribilanciamento_non riuscito]]se lo stato della procedura di ribilanciamento EC è `Failure`, attenersi alla seguente procedura:
   a. Verificare che tutti i nodi di storage del sito siano connessi alla rete.
   b. Controllare e risolvere eventuali avvisi che potrebbero influire su questi nodi di storage.

      Per informazioni su avvisi specifici, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi.

   c. Riavviare la procedura di ribilanciamento EC:
      `rebalance-data start --job-id job-id`
   d. Se lo stato della procedura di ribilanciamento EC è ancora `Failure`, contattare il supporto tecnico.
10. se lo stato della procedura di ribilanciamento EC è `Success`, facoltativamente esaminare lo storage a oggetti per visualizzare i dettagli aggiornati del sito.

    I dati con codifica erasure dovrebbero ora essere più bilanciati tra i nodi di storage del sito.

11. Se si utilizza la codifica erasure in più siti, eseguire questa procedura per tutti gli altri siti interessati.

Contattare il supporto tecnico

Se durante il processo di espansione della griglia si verificano errori che non è possibile risolvere o se un'attività della griglia non riesce, contattare il supporto tecnico.

A proposito di questa attività

Quando si contatta il supporto tecnico, è necessario fornire i file di registro necessari per la risoluzione degli errori riscontrati.

Fasi

1. Connettersi al nodo di espansione che ha riscontrato errori:
   a. Immettere il seguente comando:`ssh -p 8022 admin@grid_node_IP`

      > La porta 8022 è la porta SSH del sistema operativo di base, mentre la porta 22 è la porta SSH del motore dei container che esegue StorageGRID.

   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. `#`.

2. A seconda della fase di installazione raggiunta, recuperare uno dei seguenti log disponibili nel nodo grid:

Piattaforma	Registri
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf` (per ogni nodo guasto) • `/var/log/storagegrid/nodes/<node-name>.log` (per ogni nodo guasto; potrebbe non esistere)

Ripristino e manutenzione

Recovery and maintain (Ripristino e manutenzione): Panoramica

Attenersi alle seguenti istruzioni per la manutenzione del sistema StorageGRID e per il ripristino in caso di guasti.

A proposito di queste istruzioni

Queste istruzioni descrivono come applicare una correzione rapida del software, ripristinare i nodi della griglia, ripristinare un sito guasto, decommissionare i nodi della griglia o un intero sito, eseguire la manutenzione della rete, eseguire le procedure di manutenzione del middleware e a livello di host ed eseguire le procedure dei nodi della griglia.

> In queste istruzioni, “Linux” si riferisce a una distribuzione Red Hat® Enterprise Linux®, Ubuntu®, CentOS o Debian®. Utilizzare "Tool di matrice di interoperabilità NetApp" per ottenere un elenco delle versioni supportate.

Prima di iniziare

- Hai una vasta conoscenza del sistema StorageGRID.
- Hai esaminato la topologia del sistema StorageGRID e hai compreso la configurazione della griglia.
- Si comprende che è necessario seguire tutte le istruzioni con precisione e prestare attenzione a tutte le avvertenze.
- L’utente è consapevole del fatto che le procedure di manutenzione non descritte non sono supportate o richiedono un intervento di assistenza.

Procedure di manutenzione per le appliance

Per le procedure relative all’hardware, consultare le istruzioni di installazione e manutenzione dell’appliance StorageGRID.

- Appliance di servizi SG100 e SG1000
- Appliance di storage SG6000
- Appliance di storage SG5700
- Appliance di storage SG5600

Scarica Recovery Package

Il file del pacchetto di ripristino consente di ripristinare il sistema StorageGRID in caso di errore.

Di cosa hai bisogno

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

Scaricare il file del pacchetto di ripristino corrente prima di apportare modifiche alla topologia della griglia al sistema StorageGRID o prima di aggiornare il software. Quindi, scaricare una nuova copia del pacchetto di ripristino dopo aver apportato modifiche alla topologia della griglia o dopo aver aggiornato il software.

Fasi

1. Selezionare **MANUTENZIONE sistema pacchetto di ripristino**.
2. Inserire la passphrase di provisioning e selezionare **Avvia download**.

   Il download viene avviato immediatamente.

3. Al termine del download:
   a. Aprire `.zip` file.
   b. Confermare che includa una directory di backup gpt e una interna `.zip` file.
   c. Estrarre l'interno `.zip` file.
   d. Confermare che è possibile aprire `Passwords.txt` file.
4. Copiare il file del pacchetto di ripristino scaricato (`.zip`) in due posizioni sicure e separate.

> Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

Informazioni correlate

Amministrare StorageGRID

Procedura di hotfix StorageGRID

Potrebbe essere necessario applicare una hotfix al sistema StorageGRID se vengono rilevati e risolti problemi relativi al software tra una versione e l'altra.

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. Inoltre, ogni release di hotfix contiene un rolup di tutti gli hotfix precedenti all'interno della funzionalità o della release di patch.

Considerazioni per l'applicazione di una correzione rapida

Quando si applica una correzione rapida, ai nodi del sistema StorageGRID viene applicata una serie cumulativa di aggiornamenti software.

Non è possibile applicare una correzione rapida StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare una correzione rapida mentre è in esecuzione una procedura di decommissionamento, espansione o ripristino.

> Se la procedura di decommissionamento di un nodo o di un sito è in pausa, è possibile applicare una correzione rapida in tutta sicurezza. Inoltre, potrebbe essere possibile applicare una correzione rapida durante le fasi finali di una procedura di aggiornamento di StorageGRID. Per ulteriori informazioni, consultare le istruzioni per l'aggiornamento del software StorageGRID.

Dopo aver caricato la correzione rapida in Grid Manager, la correzione rapida viene applicata automaticamente al nodo di amministrazione primario. Quindi, è possibile approvare l'applicazione della correzione rapida agli altri nodi nel sistema StorageGRID.

Se una correzione rapida non viene applicata a uno o più nodi, il motivo dell'errore viene visualizzato nella colonna Dettagli della tabella di avanzamento della correzione rapida. È necessario risolvere i problemi che hanno causato gli errori e riprovare l'intero processo. I nodi con un'applicazione della correzione rapida precedentemente riuscita verranno ignorati nelle applicazioni successive. È possibile riprovare il processo di hotfix tutte le volte necessarie fino a quando tutti i nodi non sono stati aggiornati. Per completare l'applicazione, la correzione rapida deve essere installata correttamente su tutti i nodi della griglia.

Mentre i nodi della griglia vengono aggiornati con la nuova versione di hotfix, le modifiche effettive di una hotfix potrebbero interessare solo servizi specifici su tipi specifici di nodi. Ad esempio, una correzione rapida potrebbe influire solo sul servizio LDR sui nodi di storage.

Modalità di applicazione degli hotfix per il ripristino e l'espansione

Una volta applicata una correzione rapida alla griglia, il nodo di amministrazione primario installa automaticamente la stessa versione della correzione rapida su qualsiasi nodo ripristinato mediante operazioni di ripristino o aggiunto in un'espansione.

Tuttavia, se è necessario ripristinare il nodo di amministrazione primario, è necessario installare manualmente la versione corretta di StorageGRID e applicare la correzione rapida. La versione finale di StorageGRID del nodo di amministrazione primario deve corrispondere alla versione degli altri nodi nella griglia.

Nell'esempio seguente viene illustrato come applicare una correzione rapida durante il ripristino del nodo di amministrazione primario:

1. Si supponga che la griglia stia eseguendo una versione di StorageGRID 11.*A.B* con la correzione rapida più recente. La "grid version" è 11.*A.B.y*.
2. Si verifica un errore nel nodo di amministrazione primario.
3. Il nodo di amministrazione primario viene ridistribuita utilizzando StorageGRID 11.*A.B* ed è possibile eseguire la procedura di ripristino.

   > In base alle esigenze della versione grid, è possibile utilizzare una release minore durante la distribuzione del nodo; non è necessario implementare prima la release principale.

4. Quindi, applicare la correzione rapida 11.*A.B.y* al nodo di amministrazione primario.

Informazioni correlate

Configurare il nodo amministrativo primario sostitutivo

Pianificare e preparare una correzione rapida

È necessario pianificare prima di applicare una correzione rapida per garantire un'interruzione minima del sistema StorageGRID.

Fasi

- Impatto del sistema quando si applica una correzione rapida
- Ottenere il materiale necessario per una correzione rapida
- Download del file della correzione rapida in corso
- Verifica delle condizioni del sistema prima di applicare una correzione rapida

Impatto del sistema quando si applica una correzione rapida

Quando si applica una hotfix, è necessario comprendere in che modo il sistema StorageGRID verrà influenzato.

Le applicazioni client potrebbero riscontrare interruzioni a breve termine

Il sistema StorageGRID è in grado di acquisire e recuperare i dati dalle applicazioni client durante l'intero processo di hotfix; tuttavia, le connessioni client a singoli nodi gateway o nodi di storage potrebbero essere temporaneamente interrottate se la hotfix deve riavviare i servizi su tali nodi. La connettività verrà ripristinata al termine del processo di hotfix e i servizi riprenderanno sui singoli nodi.

Potrebbe essere necessario pianificare il downtime per applicare una correzione rapida se la perdita di connettività per un breve periodo non è accettabile. È possibile utilizzare l'approvazione selettiva per pianificare l'aggiornamento di determinati nodi.

> È possibile utilizzare più gateway e gruppi ad alta disponibilità (ha) per fornire il failover automatico durante il processo di hotfix. Consultare le istruzioni per configurazione di gruppi ad alta disponibilità.

Potrebbero essere attivati avvisi e notifiche SNMP

Gli avvisi e le notifiche SNMP potrebbero essere attivati al riavvio dei servizi e quando il sistema StorageGRID funziona come ambiente a versione mista (alcuni nodi di griglia che eseguono una versione precedente, mentre altri sono stati aggiornati a una versione successiva). In generale, al termine della correzione rapida, gli avvisi e le notifiche verranno deselezionati.

Le modifiche alla configurazione sono limitate

Quando si applica una correzione rapida a StorageGRID:

- Non apportare alcuna modifica alla configurazione della griglia (ad esempio, specificando le subnet Grid Network o approvando i nodi della griglia in sospeso) fino a quando la correzione rapida non è stata applicata a tutti i nodi.
- Non aggiornare la configurazione ILM fino a quando la correzione rapida non è stata applicata a tutti i nodi.

Ottenere il materiale necessario per la correzione rapida

Prima di applicare una hotfix, è necessario procurarsi tutti i materiali necessari.

Elemento	Note
File di hotfix StorageGRID	È necessario scaricare il file di hotfix StorageGRID.
• Porta di rete • Browser Web supportato • Client SSH (ad esempio, putty)	
Pacchetto di ripristino (`.zip`)	Prima di applicare una correzione rapida, Scaricare il file del pacchetto di ripristino più recente In caso di problemi durante la correzione rapida.una volta applicata la correzione rapida, scaricare una nuova copia del file del pacchetto di ripristino e salvarlo in una posizione sicura. Il file Recovery Package aggiornato consente di ripristinare il sistema in caso di errore.
File Passwords.txt	Facoltativo e utilizzato solo se si applica manualmente una correzione rapida utilizzando il client SSH. Il `Passwords.txt` Il file è incluso NEL pacchetto, che fa parte del pacchetto di ripristino `.zip` file.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è elencata in `Passwords.txt` file.
Documentazione correlata	`readme.txt` file per la correzione rapida. Questo file è incluso nella pagina di download della correzione rapida. Assicurarsi di esaminare `readme` archiviare attentamente prima di applicare la correzione rapida.

Informazioni correlate

Scaricare il file hotfix

Scaricare il file hotfix

Prima di applicare la correzione rapida, è necessario scaricare il file della correzione rapida.

Fasi

1. Vai alla pagina dei download NetApp per StorageGRID.

   "Download NetApp: StorageGRID"

2. Selezionare la freccia verso il basso sotto **Software disponibile** per visualizzare un elenco di hotfix disponibili per il download.

   Le versioni dei file hotfix hanno il formato: 11.4.*x.y*.

3. Esaminare le modifiche incluse nell'aggiornamento.

> Se è stato appena ripristinato il nodo di amministrazione primario ed è necessario applicare una correzione rapida, selezionare la stessa versione della correzione rapida installata sugli altri nodi della griglia.

   a. Selezionare la versione della correzione rapida che si desidera scaricare e selezionare **Go**.
   b. Accedi utilizzando il nome utente e la password del tuo account NetApp.
   c. Leggere e accettare il Contratto di licenza con l'utente finale.

      Viene visualizzata la pagina di download della versione selezionata.

   d. Scaricare la correzione rapida `readme.txt` file per visualizzare un riepilogo delle modifiche incluse nella correzione rapida.
4. Selezionare il pulsante di download per la correzione rapida e salvare il file.

> Non modificare il nome del file.

> Se si utilizza un dispositivo macOS, il file hotfix potrebbe essere salvato automaticamente come `.txt` file. In tal caso, è necessario rinominare il file senza `.txt` interno.

5. Selezionare una posizione per il download e selezionare **Salva**.

Informazioni correlate

Configurare il nodo amministrativo primario sostitutivo

Controllare le condizioni del sistema prima di applicare la correzione rapida

Verificare che il sistema sia pronto per la correzione rapida.

1. Accedere a Grid Manager utilizzando un browser web supportato.
2. Se possibile, assicurarsi che il sistema funzioni correttamente e che tutti i nodi della rete siano collegati alla rete.

   I nodi connessi presentano segni di spunta verdi Nella pagina nodi.

3. Controllare e risolvere eventuali avvisi correnti, se possibile.

   Per informazioni su avvisi specifici, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

4. Assicurarsi che non siano in corso altre procedure di manutenzione, ad esempio una procedura di upgrade, recovery, espansione o decommissionamento.

   Prima di applicare una correzione rapida, attendere il completamento delle procedure di manutenzione attive.

   Non è possibile applicare una correzione rapida StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare una correzione rapida mentre è in esecuzione una procedura di decommissionamento, espansione o ripristino.

Se la procedura di decommissionamento di un nodo o di un sito è in pausa, è possibile applicare una correzione rapida in tutta sicurezza. Inoltre, potrebbe essere possibile applicare una correzione rapida durante le fasi finali di una procedura di aggiornamento di StorageGRID. Per ulteriori informazioni, consultare le istruzioni per l'aggiornamento del software StorageGRID.

Informazioni correlate

Monitorare e risolvere i problemi

Mettere in pausa e riprendere il processo di decommissionamento per i nodi di storage

Applicare la correzione rapida

La correzione rapida viene applicata automaticamente al nodo di amministrazione primario. Quindi, è necessario approvare l'applicazione della correzione rapida ad altri nodi della griglia fino a quando tutti i nodi non eseguono la stessa versione software. È possibile personalizzare la sequenza di approvazione selezionando per approvare singoli nodi della griglia, gruppi di nodi della griglia o tutti i nodi della griglia.

Di cosa hai bisogno

- Le considerazioni sono state esaminate e sono state completate le fasi descritte in Pianificare e preparare una correzione rapida.
- Si dispone della passphrase di provisioning.
- Si dispone dell'autorizzazione Root Access o Maintenance.

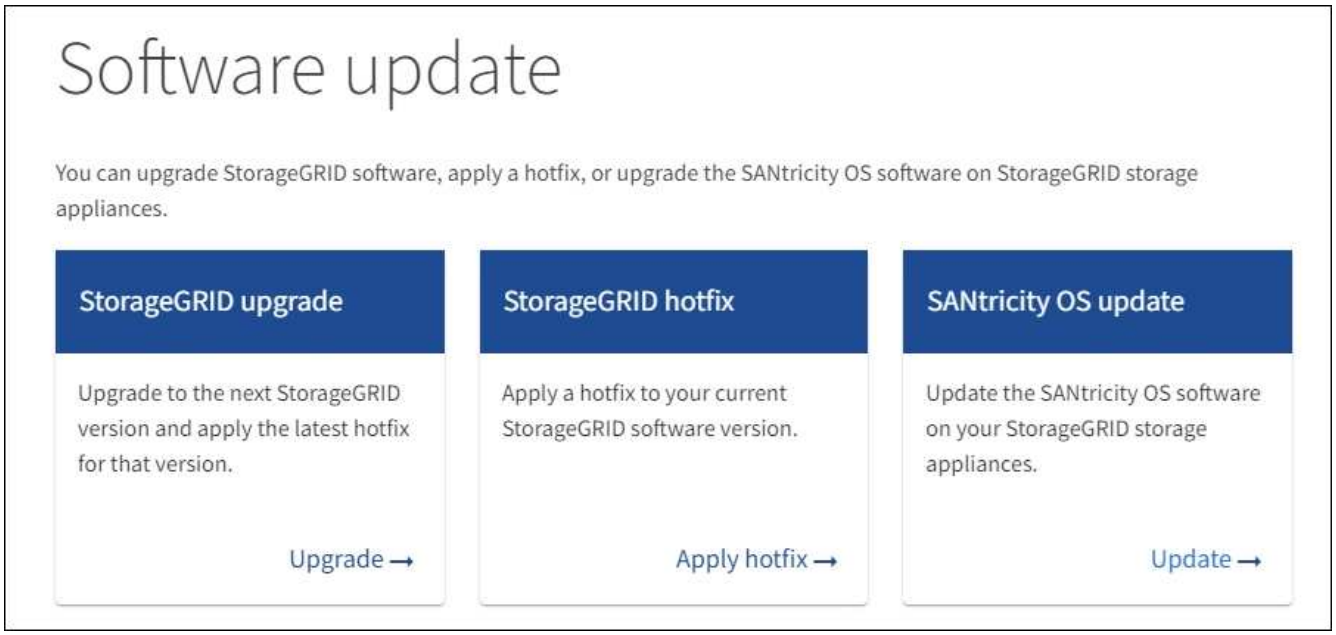
A proposito di questa attività

- È possibile ritardare l'applicazione di una hotfix a un nodo, ma il processo di hotfix non viene completato fino a quando non si applica la hotfix a tutti i nodi.
- Non è possibile eseguire un aggiornamento del software StorageGRID o del sistema operativo SANtricity fino a quando non viene completata la procedura di correzione rapida.

Fasi

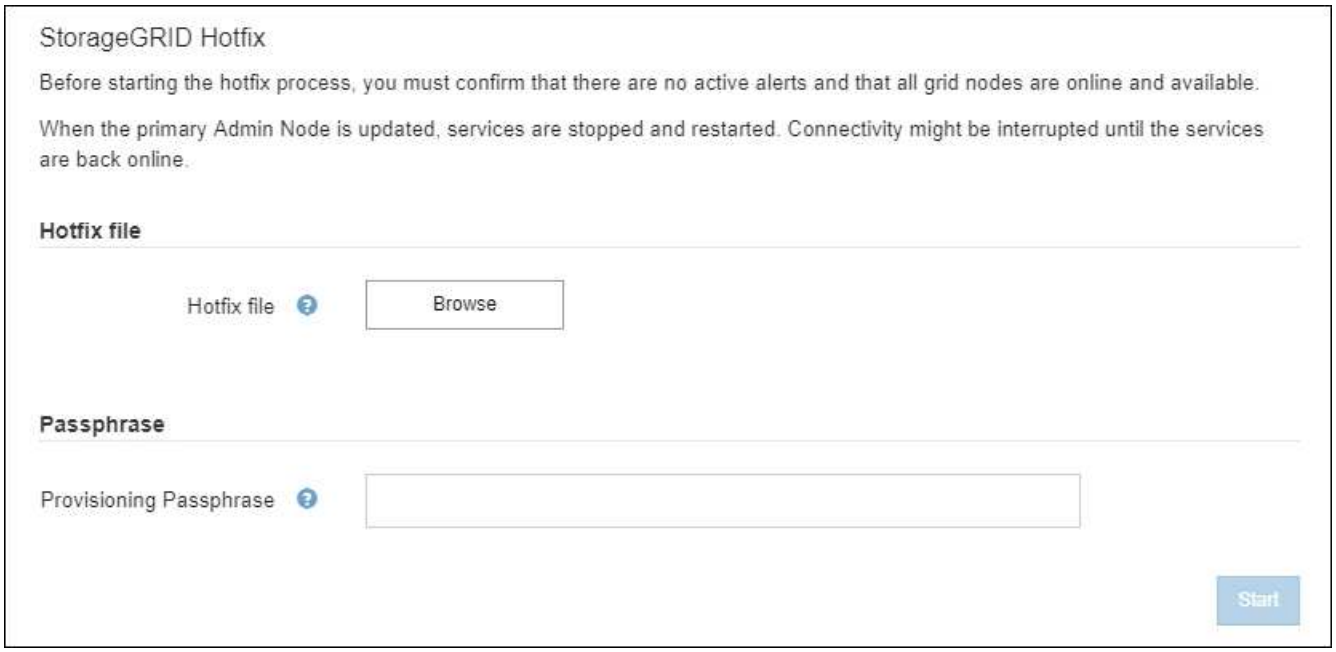
1. Accedere a Grid Manager utilizzando un browser web supportato.
2. Selezionare **MANUTENZIONE** > **sistema** > **aggiornamento software**.

   Viene visualizzata la pagina Software Update (aggiornamento software).



3. Selezionare **Apply Hotfix** (Applica correzione rapida).

   Viene visualizzata la pagina Hotfix StorageGRID.



4. Selezionare il file di hotfix scaricato dal sito di supporto NetApp.

   a. Selezionare **Sfoglia**.
   b. Individuare e selezionare il file.

      `hotfix-install-`*`version`*

   c. Selezionare **Apri**.

      Il file viene caricato. Al termine del caricamento, il nome del file viene visualizzato nel campo Dettagli.

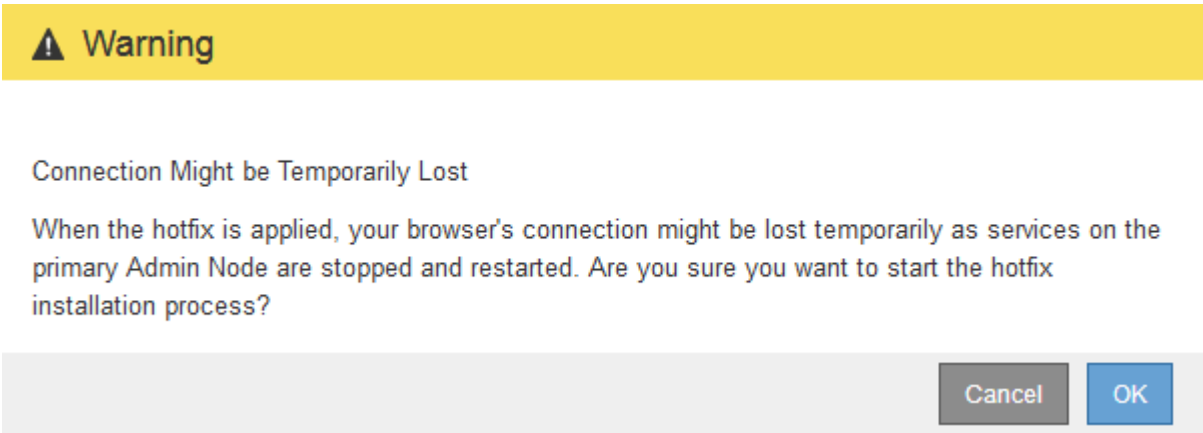
> Non modificare il nome del file poiché fa parte del processo di verifica.

5. Inserire la passphrase di provisioning nella casella di testo.

   Il pulsante **Start** viene attivato.

6. Selezionare **Start**.

   Viene visualizzato un avviso che indica che la connessione del browser potrebbe andare persa temporaneamente quando i servizi sul nodo di amministrazione primario vengono riavviati.



7. Selezionare **OK** per avviare l'applicazione della correzione rapida al nodo di amministrazione primario.

   All'avvio della correzione rapida:

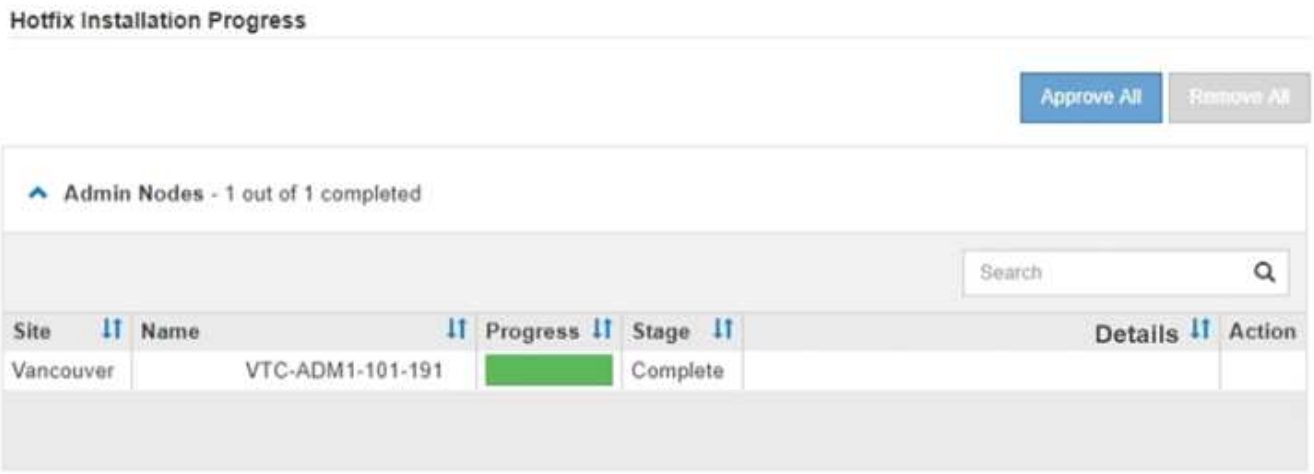
   a. Vengono eseguite le validazioni della correzione rapida.

      > Se vengono segnalati errori, risolverli, caricare nuovamente il file di correzione rapida e selezionare di nuovo **Avvia**.

   b. Viene visualizzata la tabella di avanzamento dell'installazione della correzione rapida. Questa tabella mostra tutti i nodi della griglia e la fase corrente dell'installazione della correzione rapida per ciascun nodo. I nodi nella tabella sono raggruppati per tipo:

      - Nodi di amministrazione
      - Nodi gateway
      - Nodi di storage
      - Nodi di archiviazione

      > La barra di avanzamento raggiunge il completamento, quindi il nodo di amministrazione principale viene visualizzato per primo con la fase "complete".



8. Facoltativamente, ordinare gli elenchi di nodi in ciascun raggruppamento in ordine crescente o decrescente per **Sito**, **Nome**, **avanzamento**, **fase** o **Dettagli**. In alternativa, inserire un termine nella casella **Search** per cercare nodi specifici.
9. Approvare i nodi della griglia pronti per l'aggiornamento. I nodi approvati dello stesso tipo vengono aggiornati uno alla volta.

> Non approvare la correzione rapida per un nodo a meno che non si sia certi che il nodo sia pronto per essere aggiornato.quando la correzione rapida viene applicata a un nodo Grid, alcuni servizi su quel nodo potrebbero essere riavviati. Queste operazioni potrebbero causare interruzioni del servizio per i client che comunicano con il nodo.

- Selezionare uno o più pulsanti **approva** per aggiungere uno o più singoli nodi alla coda degli aggiornamenti rapidi.
- Selezionare il pulsante **approva tutto** all'interno di ciascun gruppo per aggiungere tutti i nodi dello stesso tipo alla coda degli hotfix. Se sono stati immessi criteri di ricerca nella casella **Cerca**, il pulsante **approva tutto** si applica a tutti i nodi selezionati dai criteri di ricerca.

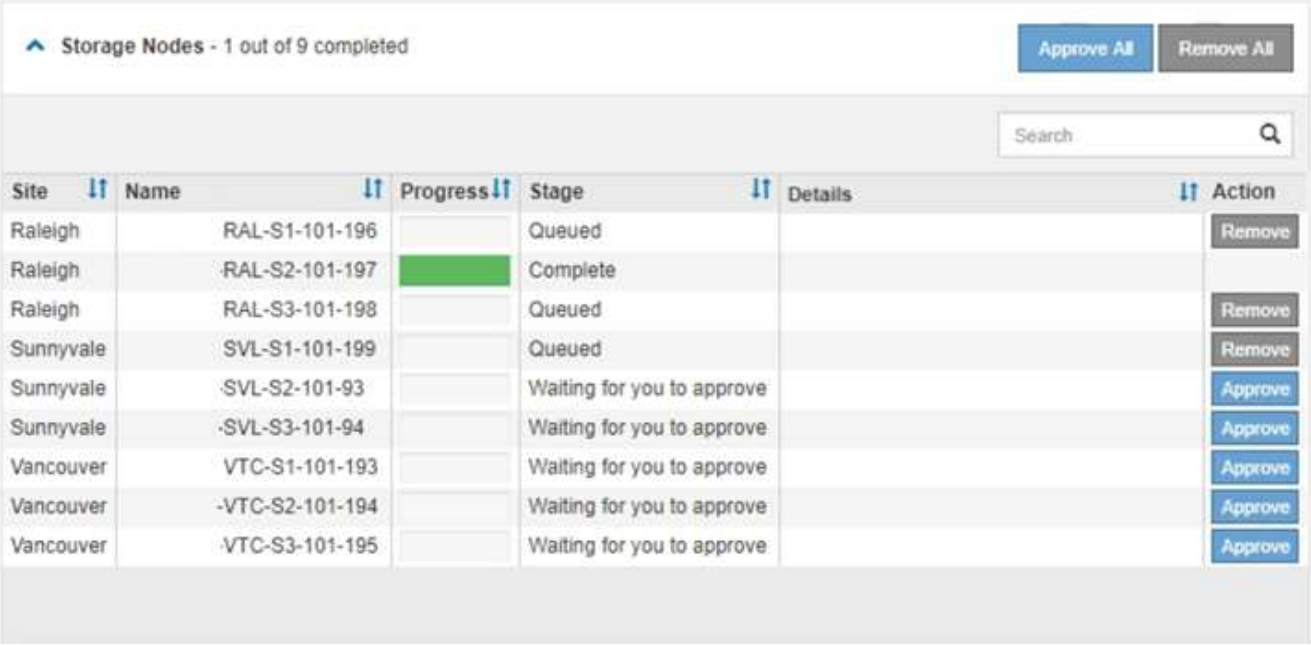
> Il pulsante **approva tutto** nella parte superiore della pagina approva tutti i nodi elencati nella pagina, mentre il pulsante **approva tutto** nella parte superiore di un raggruppamento di tabelle approva solo tutti i nodi di quel gruppo. Se l'ordine in cui i nodi vengono aggiornati è importante, approvare i nodi o i gruppi di nodi uno alla volta e attendere il completamento dell'aggiornamento su ciascun nodo prima di approvare i nodi successivi.

- Selezionare il pulsante di primo livello **approva tutto** nella parte superiore della pagina per aggiungere tutti i nodi della griglia alla coda degli aggiornamenti rapidi.

> È necessario completare la correzione rapida StorageGRID prima di poter avviare un aggiornamento software diverso. Se non si riesce a completare la correzione rapida, contattare il supporto tecnico.

- Selezionare **Remove** o **Remove All** per rimuovere un nodo o tutti i nodi dalla coda di hotfix.

  Quando la fase procede oltre "in coda", il pulsante **Remove** (Rimuovi) viene nascosto e non è più possibile rimuovere il nodo dal processo di correzione rapida.



10. Attendere che la correzione rapida venga applicata a ciascun nodo della griglia approvato.

    Una volta che la correzione rapida è stata installata correttamente su tutti i nodi, la tabella di avanzamento dell'installazione della correzione rapida si chiude. Un banner verde mostra la data e l'ora in cui la correzione rapida è stata completata.

11. Se la correzione rapida non può essere applicata a nessun nodo, esaminare l'errore per ciascun nodo, risolvere il problema e ripetere la procedura.

    La procedura non è completa fino a quando la correzione rapida non viene applicata correttamente a tutti i nodi. È possibile riprovare il processo di correzione rapida tutte le volte necessarie fino al completamento.

Informazioni correlate

Amministrare StorageGRID

Monitorare e risolvere i problemi

Procedure di ripristino del nodo Grid

In caso di guasto di un nodo Grid, è possibile ripristinarlo sostituendo il server fisico o virtuale guasto, reinstallando il software StorageGRID e ripristinando i dati ripristinabili.

I nodi Grid possono non funzionare se un guasto hardware, virtualizzazione, sistema operativo o software rende il nodo inutilizzabile o inaffidabile. Esistono diversi tipi di errore che possono attivare la necessità di ripristinare un nodo di rete.

I passaggi per il ripristino di un nodo di rete variano a seconda della piattaforma in cui è ospitato il nodo di rete e del tipo di nodo di rete. Ogni tipo di nodo della griglia dispone di una procedura di ripristino specifica, che è necessario seguire con precisione.

In genere, se possibile, si tenta di conservare i dati dal nodo della griglia guasto, riparare o sostituire il nodo guasto, utilizzare Grid Manager per configurare il nodo sostitutivo e ripristinare i dati del nodo.

In caso di guasto di un intero sito StorageGRID, contattare il supporto tecnico. Il supporto tecnico collaborerà con te per sviluppare ed eseguire un piano di ripristino del sito che massimizzi la quantità di dati recuperati e soddisfi i tuoi obiettivi di business.

Informazioni correlate

Come viene eseguito il ripristino del sito dal supporto tecnico

Avvertenze e considerazioni per il ripristino del nodo grid

In caso di guasto di un nodo della griglia, è necessario ripristinarlo il prima possibile. Prima di iniziare, è necessario esaminare tutti gli avvisi e le considerazioni per il ripristino del nodo.

StorageGRID è un sistema distribuito composto da più nodi che lavorano l'uno con l'altro. Non utilizzare le snapshot dei dischi per ripristinare i nodi della griglia. Fare invece riferimento alle procedure di ripristino e manutenzione per ciascun tipo di nodo.

Di seguito sono riportati alcuni dei motivi per cui è stato eseguito il ripristino di un nodo Grid guasto il prima possibile:

- Un nodo Grid guasto può ridurre la ridondanza dei dati di sistema e dei dati a oggetti, lasciando l'utente vulnerabile al rischio di perdita permanente dei dati in caso di guasto di un altro nodo.
- Un nodo Grid guasto può influire sull'efficienza delle operazioni giornaliere da-a-.
- Un nodo Grid guasto può ridurre la capacità di monitorare le operazioni del sistema.
- Un nodo Grid guasto può causare un errore del server interno 500 se sono in vigore regole ILM rigide.
- Se un nodo di rete non viene recuperato tempestivamente, i tempi di ripristino potrebbero aumentare. Ad esempio, potrebbero svilupparsi code che devono essere cancellate prima del completamento del ripristino.

Seguire sempre la procedura di ripristino per il tipo specifico di nodo della griglia che si sta ripristinando. Le procedure di recovery variano per i nodi di amministrazione primari o non primari, i nodi gateway, i nodi di archivio, i nodi appliance e i nodi storage.

Condizioni preliminari per il ripristino dei nodi di rete

Quando si ripristinano i nodi della griglia, si presume che siano presenti tutte le seguenti condizioni:

- L'hardware fisico o virtuale guasto è stato sostituito e configurato.
- La versione del programma di installazione dell'appliance StorageGRID installata sull'appliance sostitutiva corrisponde alla versione software del sistema StorageGRID, come descritto in Installazione e manutenzione dell'hardware per la verifica e l'aggiornamento della versione del programma di installazione dell'appliance StorageGRID.
  - Appliance di servizi SG100 e SG1000
  - Appliance di storage SG5600
  - Appliance di storage SG5700
  - Appliance di storage SG6000
- Se si sta ripristinando un nodo Grid diverso dal nodo Admin primario, esiste una connessione tra il nodo Grid da ripristinare e il nodo Admin primario.

Ordine di recovery del nodo in caso di guasto di un server che ospita più di un nodo griglia

Se un server che ospita più di un nodo di rete si guasta, è possibile ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server guasto ospita il nodo di amministrazione primario, è necessario ripristinare prima tale nodo. Il ripristino del nodo di amministrazione primario impedisce prima agli altri ripristini del nodo di interrompere l'attesa di contattare il nodo di amministrazione primario.

Indirizzi IP per i nodi ripristinati

Non tentare di ripristinare un nodo utilizzando un indirizzo IP attualmente assegnato a un altro nodo. Quando si implementa il nuovo nodo, utilizzare l'indirizzo IP corrente del nodo guasto o un indirizzo IP inutilizzato.

Se si utilizza un nuovo indirizzo IP per implementare il nuovo nodo e ripristinarlo, il nuovo indirizzo IP continuerà a essere utilizzato per il nodo recuperato. Se si desidera ripristinare l'indirizzo IP originale, utilizzare lo strumento Cambia IP al termine del ripristino.

Raccogliere i materiali necessari per il ripristino dei nodi grid

Prima di eseguire le procedure di manutenzione, assicurarsi di disporre dei materiali necessari per ripristinare un nodo della griglia guasto.

Elemento	Note
Archivio di installazione di StorageGRID	Se è necessario ripristinare un nodo Grid, è necessario Scaricare i file di installazione di StorageGRID per la tua piattaforma. **Nota:** non è necessario scaricare i file se si stanno ripristinando volumi di storage guasti su un nodo di storage.
Laptop di assistenza	Il laptop di assistenza deve disporre di quanto segue: • Porta di rete • Client SSH (ad esempio, putty) • Browser Web supportato

Elemento	Note
Pacchetto di ripristino `.zip` file	Ottenere una copia del pacchetto di ripristino più recente `.zip` file: `sgws-recovery-package-`*`id-revision`*`.zip` Il contenuto di `.zip` i file vengono aggiornati ogni volta che si modifica il sistema. Dopo aver apportato tali modifiche, viene richiesto di memorizzare la versione più recente del pacchetto di ripristino in una posizione sicura. Utilizzare la copia più recente per eseguire il ripristino in caso di errori della griglia. Se il nodo di amministrazione primario funziona normalmente, è possibile scaricare il pacchetto di ripristino da Grid Manager. Selezionare **MANUTENZIONE sistema pacchetto di ripristino**. Se non è possibile accedere a Grid Manager, è possibile trovare copie crittografate del pacchetto di ripristino su alcuni nodi di storage che contengono il servizio ADC. Su ciascun nodo di storage, esaminare questa posizione per il pacchetto di ripristino: `/var/local/install/sgws-recovery-package-`*`grid-id-revision`*`.zip.gpg` Utilizzare il pacchetto di ripristino con il numero di revisione più alto.
`Passwords.txt` file	Contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando. Incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.
Documentazione aggiornata per la piattaforma	Per la documentazione, visitare il sito Web del vendor della piattaforma. Per le versioni correnti supportate della piattaforma, consultare "Tool di matrice di interoperabilità NetApp".

Scaricare ed estrarre i file di installazione di StorageGRID

Scaricare il software ed estrarre i file, a meno che non si trovino Ripristino dei volumi di storage guasti in un nodo di storage.

È necessario utilizzare la versione di StorageGRID attualmente in esecuzione sulla griglia.

Fasi

1. Determinare la versione del software attualmente installata. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **About** (informazioni su).
2. Accedere alla "Pagina dei download NetApp per StorageGRID".
3. Selezionare la versione di StorageGRID attualmente in esecuzione nella griglia.

   Le versioni del software StorageGRID hanno questo formato: `11.x.y`.

4. Accedi con il nome utente e la password del tuo account NetApp.

5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
6. Nella colonna **Installa StorageGRID** della pagina di download, selezionare `.tgz` oppure `.zip` file per la tua piattaforma.

   La versione mostrata nel file di archivio dell'installazione deve corrispondere alla versione del software attualmente installato.

   Utilizzare `.zip` Se si utilizza Windows.

Piattaforma	Archivio di installazione

Red Hat Enterprise Linux o CentOS	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Ubuntu o Debian o appliance	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

7. Scaricare ed estrarre il file di archivio.
8. Segui la procedura appropriata per la tua piattaforma per scegliere i file di cui hai bisogno, in base alla piattaforma e ai nodi grid da ripristinare.

   I percorsi elencati nella fase per ciascuna piattaforma sono relativi alla directory di primo livello installata dal file di archivio.

9. Se si sta ripristinando un Sistema Red Hat Enterprise Linux o CentOS, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	PACCHETTO RPM per l'installazione delle immagini dei nodi StorageGRID sugli host RHEL o CentOS.
	PACCHETTO RPM per l'installazione del servizio host StorageGRID sugli host RHEL o CentOS.
Tool di scripting per la distribuzione	Descrizione

Percorso e nome del file	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di manuale e ruolo Ansible per la configurazione degli host RHEL o CentOS per l'implementazione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta ripristinando un Ubuntu o sistema Debian, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.

Percorso e nome del file	Descrizione
	Checksum MD5 per il file `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PACCHETTO DEB per l'installazione del servizio host StorageGRID su host Ubuntu o Debian.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta ripristinando un Sistema VMware, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.

Percorso e nome del file	Descrizione
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file di modello Open Virtualization Format (`.ovf`) e il file manifest (`.mf`) Per l'implementazione del nodo di amministrazione primario.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi amministrativi non primari.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi di archiviazione.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione dei nodi gateway.
	Il file di modello (`.ovf`) e il file manifest (`.mf`) Per l'implementazione di nodi di storage basati su macchine virtuali.
Tool di scripting per la distribuzione	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
	Un file di configurazione di esempio da utilizzare con `deploy-vsphere-ovftool.sh` script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on.
	Un file di configurazione di esempio da utilizzare con `configure-storagegrid.py` script.

Percorso e nome del file	Descrizione
	Un file di configurazione vuoto da utilizzare con `configure-storagegrid.py` script.
	Schemi API per StorageGRID. **Nota**: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta ripristinando un sistema basato su appliance StorageGRID, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	PACCHETTO DEB per l'installazione delle immagini del nodo StorageGRID sulle appliance.
	Checksum del pacchetto di installazione DEB utilizzato dal programma di installazione dell'appliance StorageGRID per verificare che il pacchetto sia intatto dopo il caricamento.

> Per l'installazione dell'appliance, questi file sono necessari solo se è necessario evitare il traffico di rete. L'appliance può scaricare i file richiesti dal nodo di amministrazione principale.

Selezionare la procedura di ripristino del nodo

Selezionare la procedura di ripristino corretta per il tipo di nodo che ha avuto esito negativo.

Nodo della griglia	Procedura di recovery
Più di un nodo di storage	Contattare il supporto tecnico. Se più di un nodo di storage si è guastato, il supporto tecnico deve fornire assistenza per il ripristino per evitare incoerenze del database che potrebbero causare la perdita di dati. Potrebbe essere necessaria una procedura di ripristino del sito. Come viene eseguito il ripristino del sito dal supporto tecnico
Un singolo nodo di storage	La procedura di recovery di Storage Node dipende dal tipo e dalla durata dell'errore. Ripristino da guasti del nodo di storage

Nodo della griglia	Procedura di recovery
Nodo Admin	La procedura Admin Node (nodo amministratore) dipende dalla necessità di ripristinare il nodo amministratore primario o un nodo amministratore non primario. Ripristino da errori del nodo di amministrazione
Nodo gateway	Ripristino da guasti del nodo gateway.
Nodo di archiviazione	Ripristino da errori del nodo di archiviazione.

Se un server che ospita più di un nodo di rete si guasta, è possibile ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server guasto ospita il nodo di amministrazione primario, è necessario ripristinare prima tale nodo. Il ripristino del nodo di amministrazione primario impedisce prima agli altri ripristini del nodo di interrompere l'attesa di contattare il nodo di amministrazione primario.

Ripristino da guasti del nodo di storage

La procedura per il ripristino di un nodo di storage guasto dipende dal tipo di guasto e dal tipo di nodo di storage guasto.

Utilizzare questa tabella per selezionare la procedura di ripristino per un nodo di storage guasto.

Problema	Azione	Note
• Si è verificato un errore in più di un nodo di storage. • Un secondo nodo di storage si è guastato meno di 15 giorni dopo un guasto o un ripristino di un nodo di storage. Questo include il caso in cui un nodo di storage si guasta mentre il ripristino di un altro nodo di storage è ancora in corso.	È necessario contattare il supporto tecnico.	Se tutti i nodi di storage guasti si trovano nello stesso sito, potrebbe essere necessario eseguire una procedura di ripristino del sito. Il supporto tecnico valuterà la tua situazione e svilupperà un piano di recovery. Come viene eseguito il ripristino del sito dal supporto tecnico Il ripristino di più di un nodo di storage (o di più nodi di storage entro 15 giorni) potrebbe influire sull'integrità del database Cassandra, causando la perdita di dati. Il supporto tecnico può determinare quando è sicuro iniziare il ripristino di un secondo nodo di storage. **Nota**: Se più di un nodo di storage che contiene il servizio ADC si guasta in un sito, si perdono le richieste di servizio della piattaforma in sospeso per quel sito.
Un nodo di storage è stato offline per più di 15 giorni.	Recovery Storage Node Down per più di 15 giorni	Questa procedura è necessaria per garantire l'integrità del database Cassandra.
Si è verificato un errore in un nodo di storage dell'appliance.	Ripristinare il nodo storage dell'appliance	La procedura di ripristino per i nodi di storage dell'appliance è la stessa per tutti i guasti.
Uno o più volumi di storage sono guasti, ma il disco di sistema è intatto	Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto	Questa procedura viene utilizzata per i nodi di storage basati su software.
Il disco di sistema è guasto.	Ripristino in caso di guasto al disco di sistema	La procedura di sostituzione del nodo dipende dalla piattaforma di implementazione e dal fatto che anche i volumi di storage abbiano avuto un guasto.

Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona “reaper” o “Cassandra repair”. Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

Recovery Storage Node Down per più di 15 giorni

Se un singolo nodo di storage è stato offline e non connesso ad altri nodi di storage per più di 15 giorni, è necessario ricostruire Cassandra sul nodo.

Di cosa hai bisogno

- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).
- Hai verificato che non è in corso un’espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).

A proposito di questa attività

I nodi di storage dispongono di un database Cassandra che include metadati a oggetti. Se un nodo di storage non è stato in grado di comunicare con altri nodi di storage per più di 15 giorni, StorageGRID presume che il database Cassandra del nodo sia obsoleta. Il nodo di storage non può ricongiungersi alla griglia fino a quando Cassandra non viene ricostruita utilizzando le informazioni provenienti da altri nodi di storage.

Utilizzare questa procedura per ricostruire Cassandra solo se un singolo nodo di storage non è attivo. Contattare il supporto tecnico se altri nodi di storage sono offline o se Cassandra è stato ricostruito su un altro nodo di storage negli ultimi 15 giorni; ad esempio, Cassandra potrebbe essere stato ricostruito come parte delle procedure per ripristinare i volumi di storage guasti o per ripristinare un nodo di storage guasto.

Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Contattare il supporto tecnico.

Come viene eseguito il ripristino del sito dal supporto tecnico

Fasi

1. Se necessario, accendere il nodo di storage che deve essere ripristinato.
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. `#`.+

> Se non si riesce ad accedere al nodo Grid, il disco di sistema potrebbe non essere intatto. Passare alla procedura per ripristino in caso di guasto al disco di sistema.

1. Eseguire i seguenti controlli sul nodo di storage:

   a. Eseguire questo comando: `nodetool status`

      L'output deve essere `Connection refused`

   b. In Grid Manager, selezionare **SUPPORT Tools Grid topology**.

   c. Selezionare ***Site* Storage Node SSM Services**. Verificare che venga visualizzato il servizio Cassandra `Not Running`.

   d. Selezionare **Storage Node SSM Resources**. Verificare che non vi sia stato di errore nella sezione Volumes (volumi).

   e. Eseguire questo comando: `grep -i Cassandra /var/local/log/servermanager.log`

      Nell'output dovrebbe essere visualizzato il seguente messaggio:

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

2. Eseguire questo comando e monitorare l'output dello script: `check-cassandra-rebuild`

   - Se i servizi di storage sono in esecuzione, viene richiesto di interromperli. Immettere: **Y**
   - Esaminare gli avvisi nello script. Se non sono applicabili, confermare che si desidera ricostruire Cassandra. Immettere: **Y**

> Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "Cassandra repair". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

3. Al termine della ricostruzione, eseguire i seguenti controlli:

   a. In Grid Manager, selezionare **SUPPORT Tools Grid topology**.

   b. Selezionare ***Site* recuperato nodo di storage SSM servizi**.

   c. Verificare che tutti i servizi siano in esecuzione.

   d. Selezionare **DDS Data Store**.

   e. Verificare che lo stato **Data Store Status** sia "Up" e che lo stato **Data Store state** sia "Normal".

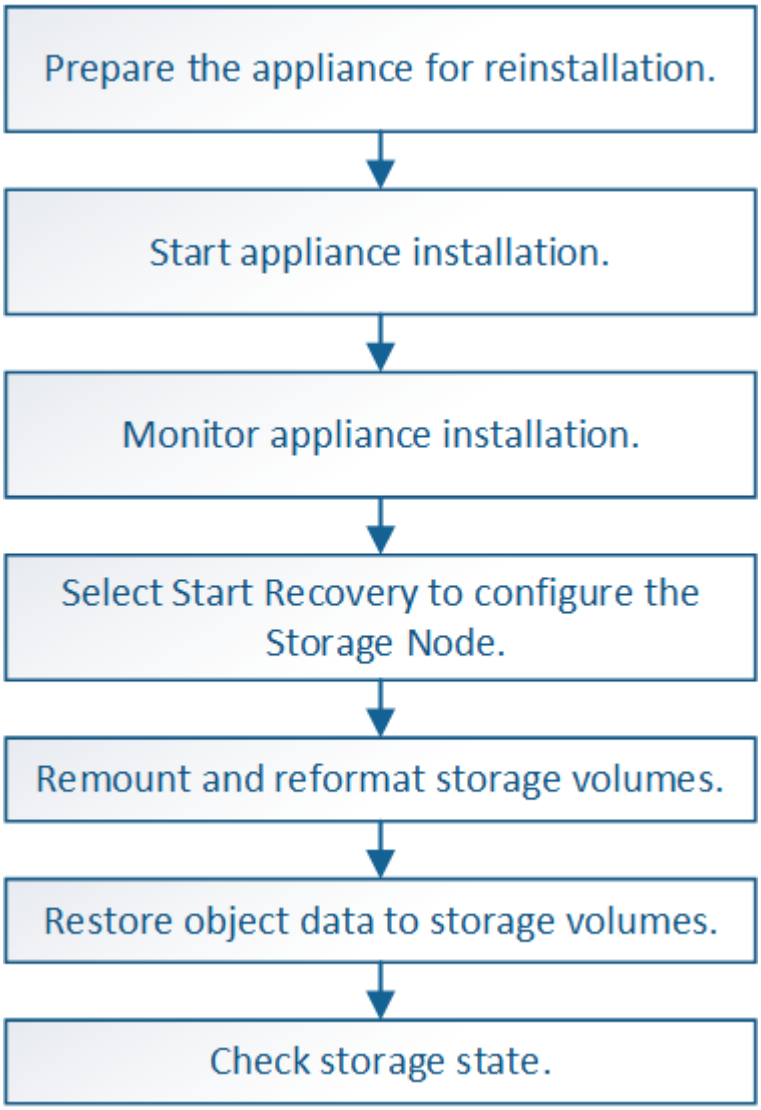
Ripristinare il nodo storage dell'appliance

La procedura per il ripristino di un nodo di storage dell'appliance StorageGRID guasto è

la stessa, sia che si stia ripristinando dalla perdita del disco di sistema che dalla perdita dei soli volumi di storage.

A proposito di questa attività

È necessario preparare l'appliance e reinstallare il software, configurare il nodo in modo che si riunisca di nuovo nella griglia, riformattare lo storage e ripristinare i dati dell'oggetto.



Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni può causare la perdita di dati.

Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Contattare il supporto tecnico.

Come viene eseguito il ripristino del sito dal supporto tecnico

Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.

Se si verifica un allarme Services: Status - Cassandra (SVST) durante il ripristino, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi per ripristinare l'allarme mediante la ricostruzione di Cassandra. Dopo la ricostruzione di Cassandra, gli allarmi devono essere disattivati. Se gli allarmi non vengono disattivati, contattare il supporto tecnico.

Per le procedure di manutenzione dell'hardware, come ad esempio la sostituzione di un controller o la reinstallazione di SANtricity OS, consultare le istruzioni di installazione e manutenzione dell'appliance di storage.

Informazioni correlate

Monitorare e risolvere i problemi

Appliance di storage SG6000

Appliance di storage SG5700

Appliance di storage SG5600

Preparare l'appliance Storage Node per la reinstallazione

Quando si ripristina un nodo di storage dell'appliance, è necessario prima preparare l'appliance per la reinstallazione del software StorageGRID.

1. Accedere al nodo di storage guasto:

   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. `#`.

2. Preparare il nodo di storage dell'appliance per l'installazione del software StorageGRID. `sgareinstall`

3. Quando viene richiesto di continuare, immettere: `y`

   L'apparecchio si riavvia e la sessione SSH termina. In genere, il programma di installazione dell'appliance StorageGRID richiede circa 5 minuti, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.

   Il nodo di storage dell'appliance StorageGRID viene ripristinato e i dati sul nodo di storage non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale devono rimanere intatti; tuttavia, si consiglia di confermarli al termine della procedura.

   Dopo aver eseguito il `sgareinstall` Comando, tutti gli account, le password e le chiavi SSH forniti da StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avviare l'installazione dell'appliance StorageGRID

Per installare StorageGRID su un nodo di storage dell'appliance, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance.

Di cosa hai bisogno

- L'appliance è stata installata in un rack, collegata alla rete e accesa.
- I collegamenti di rete e gli indirizzi IP sono stati configurati per l'appliance mediante il programma di installazione dell'appliance StorageGRID.
- Si conosce l'indirizzo IP del nodo di amministrazione principale per la griglia StorageGRID.
- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete griglia nel nodo di amministrazione principale.
- Per completare queste attività preliminari, seguire le istruzioni di installazione e manutenzione dell'appliance di storage:
  - Appliance di storage SG5600
  - Appliance di storage SG5700
  - Appliance di storage SG6000
- Si sta utilizzando un browser web supportato.
- Conosci uno degli indirizzi IP assegnati al controller di calcolo nell'appliance. È possibile utilizzare l'indirizzo IP per Admin Network (porta di gestione 1 sul controller), Grid Network o Client Network.

A proposito di questa attività

Per installare StorageGRID su un nodo di storage dell'appliance:

- Specificare o confermare l'indirizzo IP del nodo di amministrazione primario e il nome del nodo.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.
- Durante il processo, l'installazione viene interrotta. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo di storage in sospeso come sostituzione del nodo guasto.
- Una volta configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di calcolo nell'appliance.

   ```
   https://Controller_IP:8443
   ```

   Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Nella sezione Primary Admin Node Connection (connessione nodo amministratore primario), determinare se è necessario specificare l'indirizzo IP per il nodo amministratore primario.

   Il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, presupponendo che il nodo amministratore primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente nella stessa sottorete.

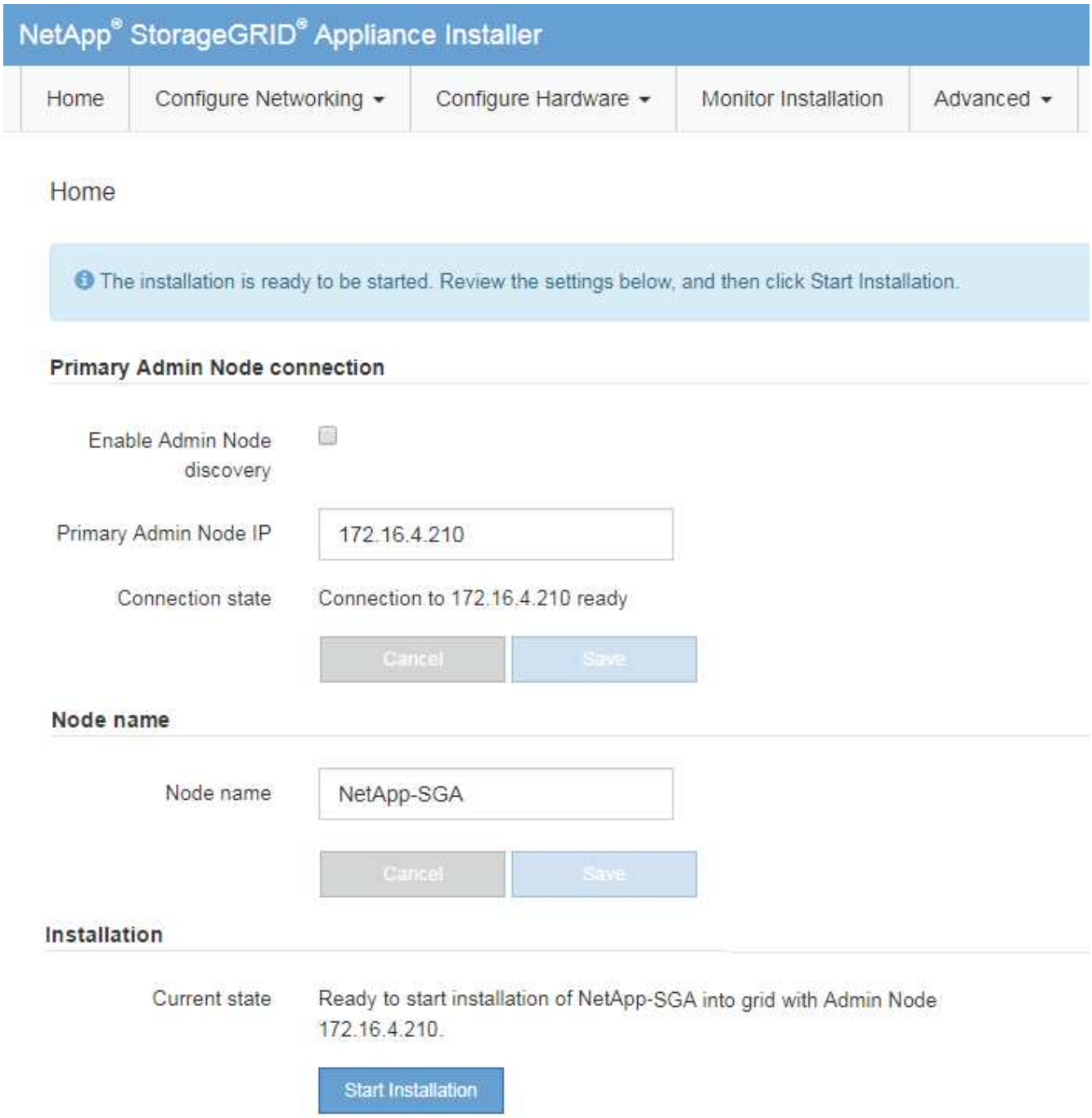
3. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Fasi
Immissione manuale dell'IP	a. Deselezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Fare clic su **Save** (Salva). d. Attendere che lo stato di connessione del nuovo indirizzo IP diventi "ready".
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Dall'elenco degli indirizzi IP rilevati, selezionare il nodo di amministrazione principale per la griglia in cui verrà implementato il nodo di storage dell'appliance. c. Fare clic su **Save** (Salva). d. Attendere che lo stato di connessione del nuovo indirizzo IP diventi "ready".

4. Nel campo **Node Name** (Nome nodo), immettere lo stesso nome utilizzato per il nodo che si sta ripristinando e fare clic su **Save** (Salva).
5. Nella sezione Installazione, verificare che lo stato corrente sia "Ready to start installation of node name into grid with Primary Admin Node admin_ip" e che il pulsante **Start Installation** sia attivato.

   Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di installazione e manutenzione dell'apparecchio.

6. Dalla home page del programma di installazione dell'appliance StorageGRID, fare clic su **Avvia installazione**.



Lo stato corrente cambia in “Installation is in Progress” (Installazione in corso) e viene visualizzata la pagina Monitor Installation (Installazione monitor).

> Per accedere manualmente alla pagina Installazione monitor, fare clic su **Installazione monitor** dalla barra dei menu.

Informazioni correlate

Appliance di servizi SG100 e SG1000

Appliance di storage SG6000

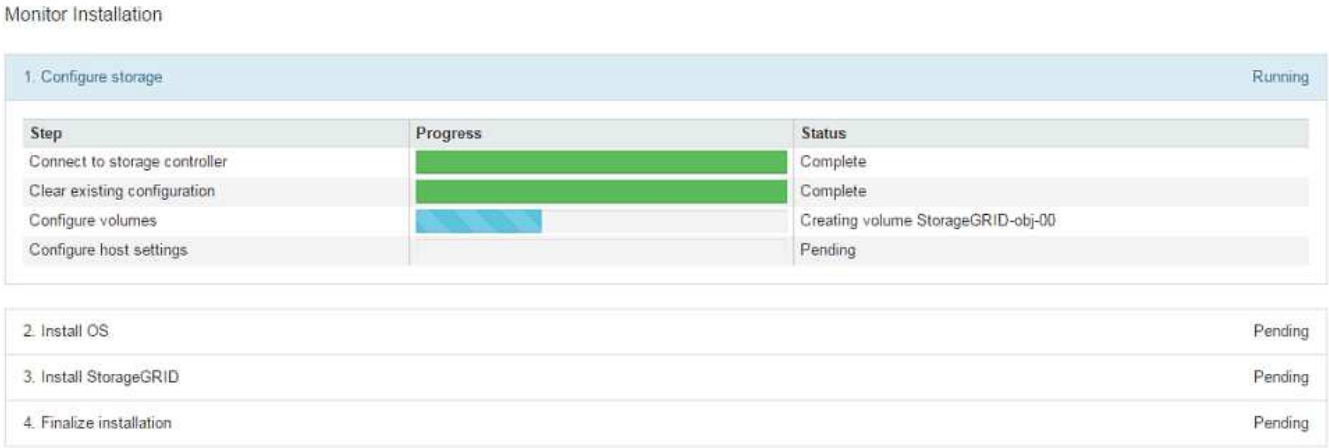
Appliance di storage SG5700

Monitorare l'installazione dell'appliance StorageGRID

Il programma di installazione dell'appliance StorageGRID indica lo stato fino al completamento dell'installazione. Una volta completata l'installazione del software, l'appliance viene riavviata.

1. Per monitorare l'avanzamento dell'installazione, fare clic su **Monitor Installation** (Installazione monitor) nella barra dei menu.

   La pagina Monitor Installation (Installazione monitor) mostra lo stato di avanzamento dell'installazione.

   La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.

   > Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si esegue nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "Skipped".

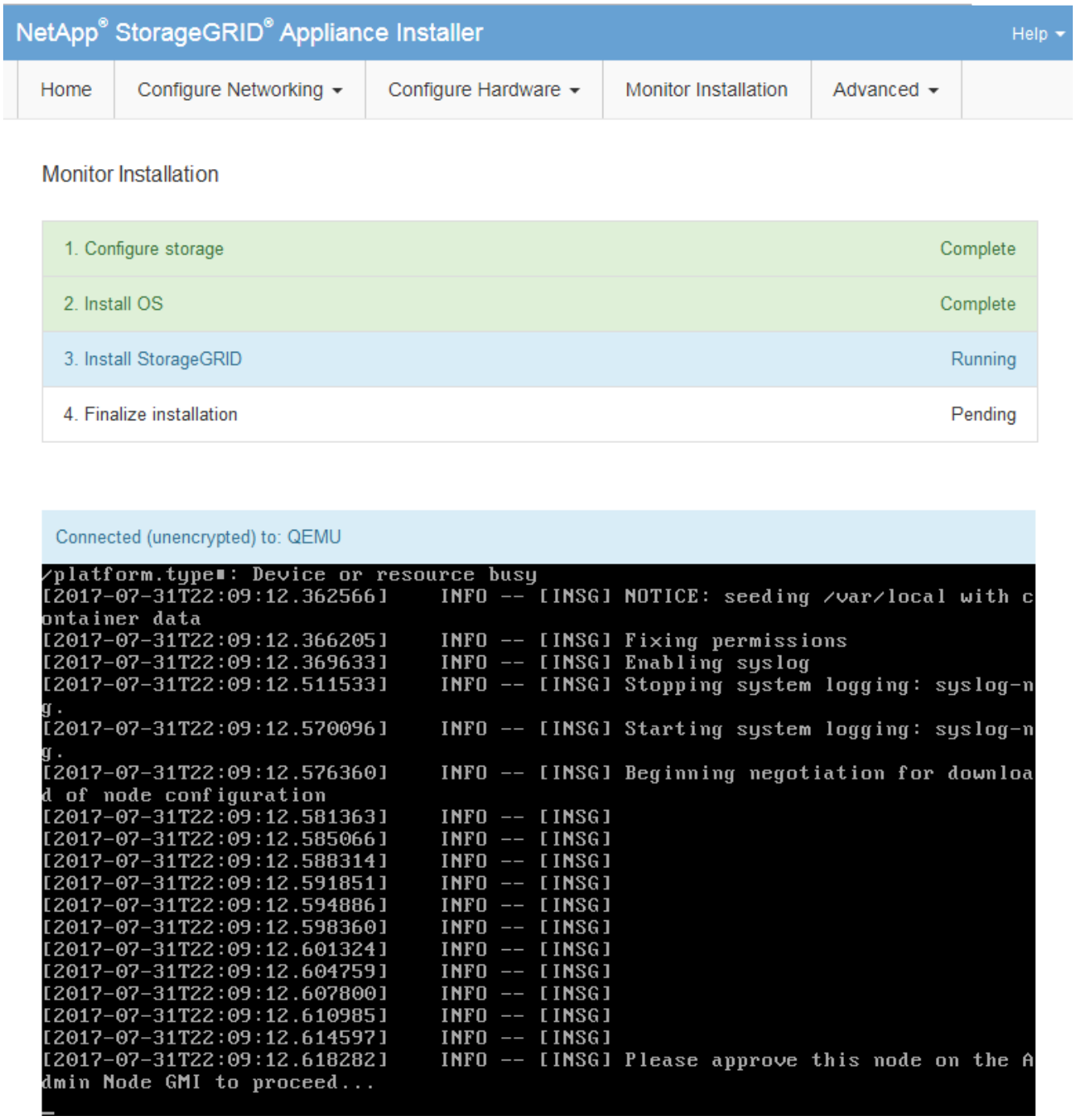
2. Esaminare i progressi delle prime due fasi dell'installazione.
   - **1. Configurare lo storage**

     Durante questa fase, il programma di installazione si connette al controller dello storage, cancella qualsiasi configurazione esistente, comunica con il software SANtricity per configurare i volumi e configura le impostazioni dell'host.

   - **2. Installare il sistema operativo**

     In questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID nell'appliance.

3. Continuare a monitorare lo stato di avanzamento dell'installazione fino a quando la fase **Install StorageGRID** (Installazione guidata) non viene interrotta e sulla console integrata viene visualizzato un messaggio che richiede di approvare questo nodo nel nodo di amministrazione utilizzando Gestione griglia.



4. Passare alla procedura per configurare il nodo di storage dell'appliance.

Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di storage dell'appliance

Selezionare Start Recovery (Avvia ripristino) in Grid Manager (Gestione griglia) per configurare un nodo di storage dell'appliance come sostituzione del nodo guasto.

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).
- È necessario disporre della passphrase di provisioning.

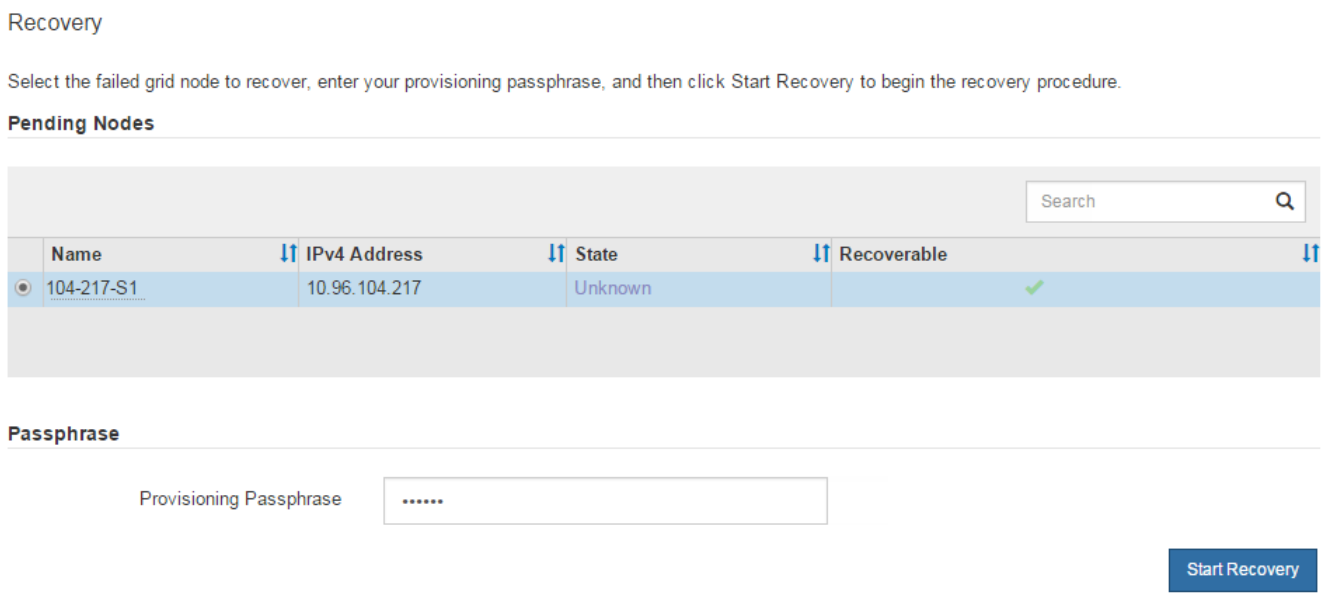
- È necessario aver implementato un nodo di storage dell'appliance di ripristino.
- È necessario conoscere la data di inizio di qualsiasi intervento di riparazione per i dati codificati per la cancellazione.
- È necessario verificare che il nodo di storage non sia stato ricostruito negli ultimi 15 giorni.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE attività Recovery**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

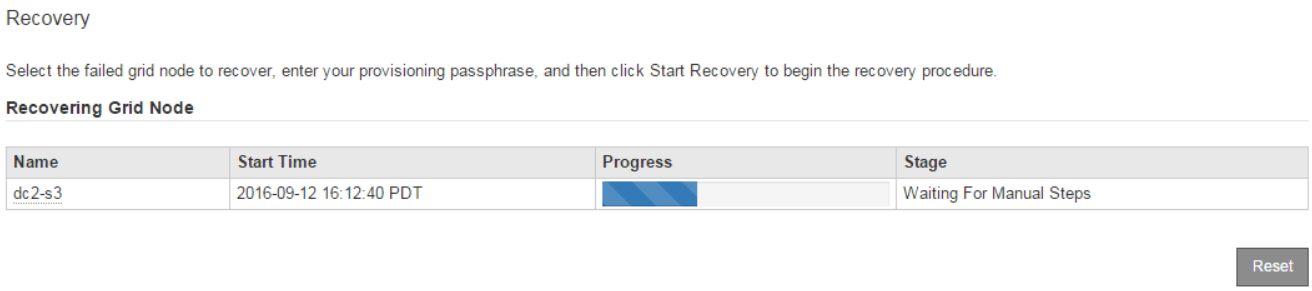
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).

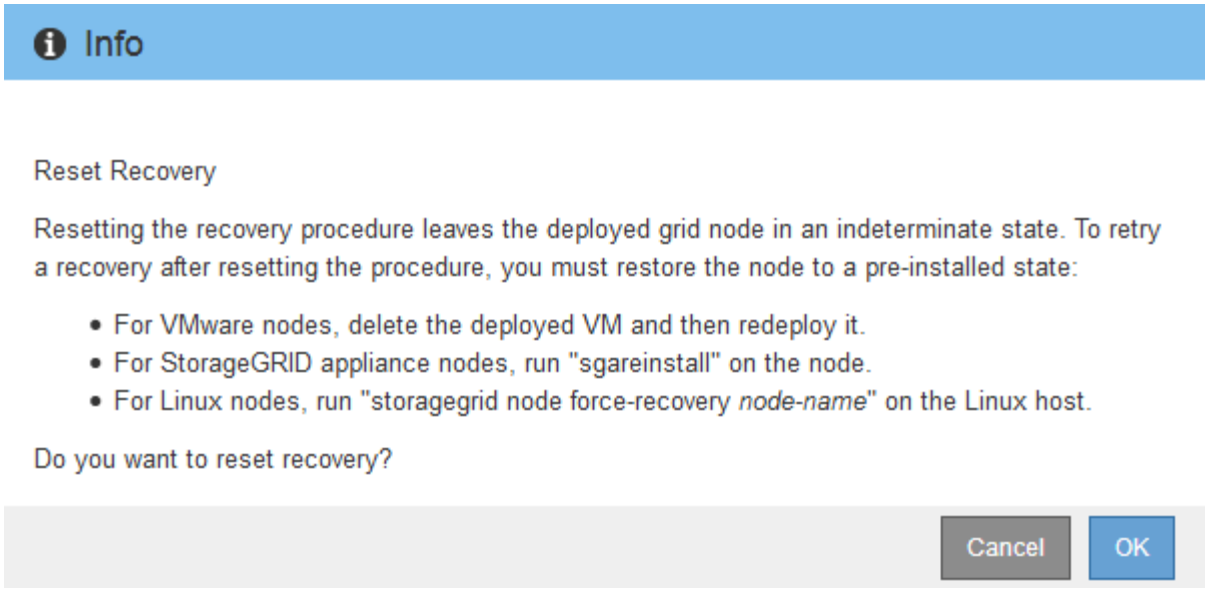


5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

   Quando il nodo Grid raggiunge la fase "Waiting for Manual Steps", passare all'argomento successivo ed eseguire la procedura manuale per rimontare e riformattare i volumi di storage delle appliance.



In qualsiasi momento durante il ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo Info, che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo appliance a uno stato preinstallato eseguendo `sgareinstall` sul nodo.

Rimontare e riformattare i volumi di storage delle appliance ("procedure manuali")

È necessario eseguire manualmente due script per rimontare volumi di storage conservati e riformattare eventuali volumi di storage guasti. Il primo script consente di eseguire il remontaggio dei volumi correttamente formattati come volumi di storage StorageGRID. Il secondo script riformatta tutti i volumi non montati, ricostruisce il database Cassandra, se necessario, e avvia i servizi.

Di cosa hai bisogno

- L'hardware è già stato sostituito per tutti i volumi di storage guasti che è necessario sostituire.

  Esecuzione di `sn-remount-volumes` lo script può aiutare a identificare altri volumi di storage guasti.

- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).
- Hai verificato che non è in corso un'espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).

> Contattare il supporto tecnico se più di un nodo di storage non è in linea o se un nodo di storage in questa griglia è stato ricostruito negli ultimi 15 giorni. Non eseguire `sn-recovery-postinstall.sh` script. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni l'uno dall'altro potrebbe causare la perdita di dati.

A proposito di questa attività

Per completare questa procedura, eseguire le seguenti attività di alto livello:

- Accedere al nodo di storage recuperato.
- Eseguire `sn-remount-volumes` script per il remount di volumi di storage correttamente formattati. Quando viene eseguito, lo script esegue le seguenti operazioni:

- Consente di montare e rimuovere ciascun volume di storage per riprodurre il journal XFS.
- Esegue un controllo di coerenza del file XFS.
- Se il file system è coerente, determina se il volume di storage è un volume di storage StorageGRID formattato correttamente.
- Se il volume di storage è formattato correttamente, esegue il remontaggio del volume di storage. Tutti i dati esistenti sul volume rimangono intatti.

- Esaminare l'output dello script e risolvere eventuali problemi.
- Eseguire `sn-recovery-postinstall.sh` script. Quando viene eseguito, lo script esegue le seguenti operazioni.

> Non riavviare un nodo di storage durante il ripristino prima dell'esecuzione `sn-recovery-postinstall.sh` (fase 4) per riformattare i volumi di storage guasti e ripristinare i metadati degli oggetti. Riavviare il nodo di storage prima `sn-recovery-postinstall.sh` Il completamento causa errori per i servizi che tentano di avviarsi e fa uscire i nodi dell'appliance StorageGRID dalla modalità di manutenzione.

  - Consente di riformattare tutti i volumi di storage di `sn-remount-volumes` impossibile eseguire il montaggio dello script o che è stato trovato formattato in modo errato.

    > Se un volume di storage viene riformattato, tutti i dati presenti in tale volume andranno persi. È necessario eseguire un'ulteriore procedura per ripristinare i dati degli oggetti da altre posizioni nella griglia, supponendo che le regole ILM siano state configurate per memorizzare più copie di un oggetto.

  - Ricostruisce il database Cassandra sul nodo, se necessario.
  - Avvia i servizi sul nodo di storage.

Fasi

1. Accedere al nodo di storage recuperato:

   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. `#`.

2. Eseguire il primo script per rimontare eventuali volumi di storage correttamente formattati.

   > Se tutti i volumi di storage sono nuovi e devono essere formattati, o se tutti i volumi di storage sono guasti, è possibile saltare questa fase ed eseguire il secondo script per riformattare tutti i volumi di storage non montati.

   a. Eseguire lo script: `sn-remount-volumes`

      Questo script potrebbe richiedere ore per essere eseguito su volumi di storage che contengono dati.

   b. Durante l'esecuzione dello script, esaminare l'output e rispondere alle richieste.

Se necessario, è possibile utilizzare `tail -f` per monitorare il contenuto del file di log dello script (`/var/local/log/sn-remount-volumes.log`) . Il file di log contiene informazioni più dettagliate rispetto all'output della riga di comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
```

```
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Nell'output di esempio, un volume di storage è stato rimontato correttamente e tre volumi di storage hanno avuto errori.

- `/dev/sdb` Ha superato il controllo di coerenza del file system XFS e disponeva di una struttura di volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi che vengono rimontati dallo script vengono conservati.
- `/dev/sdc` Verifica della coerenza del file system XFS non riuscita perché il volume di storage era nuovo o corrotto.
- `/dev/sdd` impossibile montare perché il disco non è stato inizializzato o il superblocco del disco è stato danneggiato. Quando lo script non riesce a montare un volume di storage, chiede se si desidera eseguire il controllo di coerenza del file system.
  - Se il volume di storage è collegato a un nuovo disco, rispondere **N** alla richiesta. Non è necessario controllare il file system su un nuovo disco.
  - Se il volume di storage è collegato a un disco esistente, rispondere **Y** alla richiesta. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I

risultati vengono salvati in `/var/local/log/sn-remount-volumes.log` file di log.

- `/dev/sde` Ha superato la verifica di coerenza del file system XFS e disponeva di una struttura di volume valida; tuttavia, l'ID del nodo LDR in `volID` Il file non corrisponde all'ID per questo nodo di storage (il `configured LDR noid` visualizzato nella parte superiore). Questo messaggio indica che questo volume appartiene a un altro nodo di storage.

3. Esaminare l'output dello script e risolvere eventuali problemi.

> Se un volume di storage non ha superato il controllo di coerenza del file system XFS o non è stato possibile montarlo, esaminare attentamente i messaggi di errore nell'output. È necessario comprendere le implicazioni dell'esecuzione di `sn-recovery-postinstall.sh` creare script su questi volumi.

a. Verificare che i risultati includano una voce per tutti i volumi previsti. Se alcuni volumi non sono elencati, eseguire nuovamente lo script.

b. Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indichino che un volume di storage non appartiene a questo nodo di storage.

   Nell'esempio, l'output per /dev/sde include il seguente messaggio di errore:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Se un volume di storage viene segnalato come appartenente a un altro nodo di storage, contattare il supporto tecnico. Se si esegue `sn-recovery-postinstall.sh` script, il volume di storage verrà riformattato, causando la perdita di dati.

c. Se non è stato possibile montare alcun dispositivo di storage, annotare il nome del dispositivo e riparare o sostituire il dispositivo.

> È necessario riparare o sostituire i dispositivi di storage che non possono essere montati.

   Il nome del dispositivo viene utilizzato per cercare l'ID del volume, che è necessario immettere quando si esegue `repair-data` script per ripristinare i dati dell'oggetto nel volume (la procedura successiva).

d. Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire `sn-remount-volumes` eseguire nuovamente lo script per confermare che tutti i volumi di storage che possono essere rimontati sono stati rimontati.

> Se un volume di storage non può essere montato o non è formattato correttamente e si passa alla fase successiva, il volume e i dati presenti nel volume verranno eliminati. Se si dispone di due copie di dati oggetto, si disporrà di una sola copia fino al completamento della procedura successiva (ripristino dei dati oggetto).

> Non eseguire `sn-recovery-postinstall.sh` Eseguire uno script se si ritiene che i dati rimanenti su un volume di storage guasto non possano essere ricostruiti da un'altra parte della griglia (ad esempio, se il criterio ILM utilizza una regola che esegue una sola copia o se i volumi sono guasti su più nodi). Contattare invece il supporto tecnico per determinare come ripristinare i dati.

4. Eseguire `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

   Questo script riformatta tutti i volumi di storage che non possono essere montati o che sono stati trovati per essere formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; avvia i servizi sul nodo di storage.

   Tenere presente quanto segue:

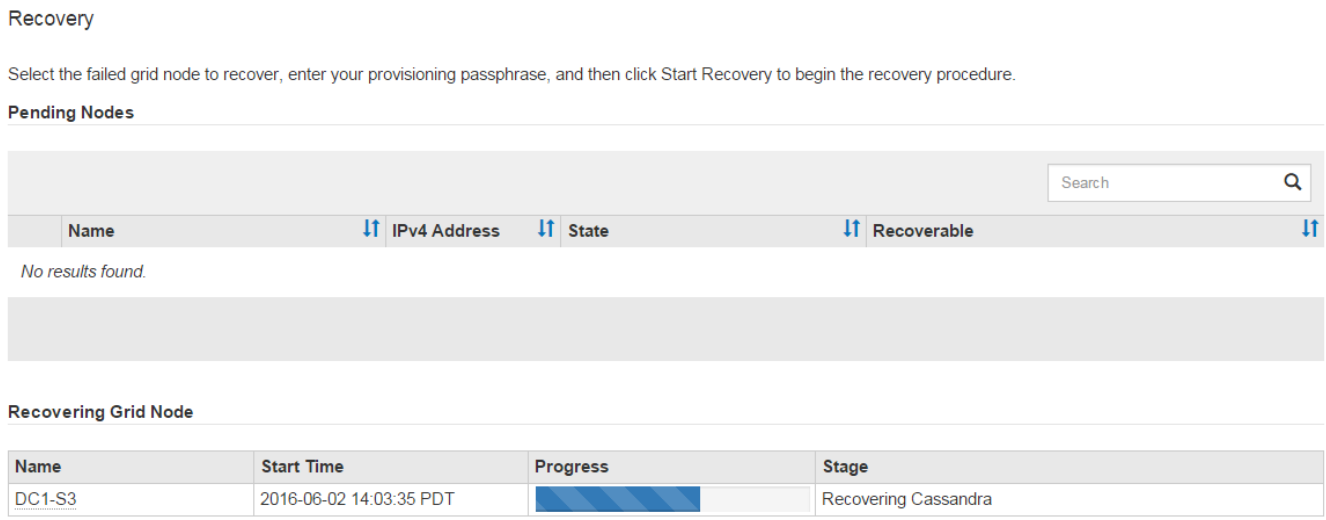
   - L'esecuzione dello script potrebbe richiedere ore.
   - In generale, si consiglia di lasciare la sessione SSH da sola mentre lo script è in esecuzione.
   - Non premere **Ctrl+C** mentre la sessione SSH è attiva.
   - Lo script viene eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzarne l'avanzamento dalla pagina Recovery (Ripristino).
   - Se Storage Node utilizza il servizio RSM, lo script potrebbe sembrare bloccato per 5 minuti quando i servizi del nodo vengono riavviati. Questo ritardo di 5 minuti è previsto ogni volta che il servizio RSM viene avviato per la prima volta.

     > Il servizio RSM è presente sui nodi di storage che includono il servizio ADC.

   > Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "Cassandra repair". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

5. Come `sn-recovery-postinstall.sh` Viene eseguito lo script, monitorare la pagina Recovery in Grid Manager.

   La barra di avanzamento e la colonna fase della pagina di ripristino forniscono uno stato di alto livello di `sn-recovery-postinstall.sh` script.



Dopo il `sn-recovery-postinstall.sh` lo script ha avviato i servizi sul nodo. è possibile ripristinare i dati degli oggetti su qualsiasi volume di storage formattato dallo script, come descritto nella procedura successiva.

Informazioni correlate

Esaminare gli avvisi per il ripristino del disco di sistema Storage Node

Ripristinare i dati dell'oggetto nel volume di storage per l'appliance

Ripristinare i dati dell'oggetto nel volume di storage per l'appliance

Dopo il ripristino dei volumi di storage per il nodo di storage dell'appliance, è possibile ripristinare i dati dell'oggetto persi in caso di guasto del nodo di storage.

Di cosa hai bisogno

- È necessario confermare che il nodo di storage recuperato ha uno stato di connessione di **connesso** Nella scheda **NODI** > **Panoramica** di Grid Manager.

A proposito di questa attività

I dati degli oggetti possono essere ripristinati da altri nodi di storage, da un nodo di archiviazione o da un pool di storage cloud, supponendo che le regole ILM del grid siano state configurate in modo da rendere disponibili le copie degli oggetti.

Tenere presente quanto segue:

- Se una regola ILM è stata configurata per memorizzare solo una copia replicata e tale copia esisteva su un volume di storage che non ha superato il test, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi di ripristino e dei relativi costi.
- Se l'unica copia rimanente di un oggetto si trova su un nodo di archiviazione, i dati dell'oggetto vengono recuperati dal nodo di archiviazione. Il ripristino dei dati degli oggetti in un nodo di storage da un nodo di archiviazione richiede più tempo rispetto al ripristino delle copie da altri nodi di storage a causa della latenza associata ai recuperi da sistemi di storage di archiviazione esterni.

A proposito di `repair-data` script

Per ripristinare i dati dell'oggetto, eseguire `repair-data` script. Questo script inizia il processo di ripristino dei dati degli oggetti e lavora con la scansione ILM per garantire che le regole ILM siano soddisfatte.

Selezionare **Replicated data** o **Erasure-Coded (EC) data** per apprendere le diverse opzioni di `repair-data` script, in base al ripristino di dati replicati o a dati con codifica di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.

> Per ulteriori informazioni su `repair-data` script, invio `repair-data --help` Dalla riga di comando del nodo di amministrazione primario.

Dati replicati

Sono disponibili due comandi per il ripristino dei dati replicati, a seconda che sia necessario riparare l'intero nodo o solo alcuni volumi sul nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

> Il `show-replicated-repair-status` L'opzione è disponibile per l'anteprima tecnica in StorageGRID 11.6. Questa funzionalità è in fase di sviluppo e il valore restituito potrebbe essere errato o ritardato. Per determinare se una riparazione è completa, utilizzare **in attesa di – tutto**, **riparazioni tentate (XRPA)** e **periodo di scansione — stimato (XSCM)** come descritto in Monitorare le riparazioni.

Cancellazione dei dati codificati (EC)

Sono disponibili due comandi per il ripristino dei dati con codifica erasure, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

È possibile tenere traccia delle riparazioni dei dati con codifica per la cancellazione con questo comando:

```
repair-data show-ec-repair-status
```

> Il lavoro di riparazione EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine della riparazione. Se lo storage non è sufficiente per la prenotazione, il lavoro di riparazione EC non avrà esito positivo. Le prenotazioni di storage vengono rilasciate al termine del lavoro di riparazione EC, indipendentemente dal fatto che il lavoro abbia avuto esito negativo o positivo.

Trovare il nome host per il nodo di storage

1. 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. `#`.

2. Utilizzare `/etc/hosts` File per trovare il nome host del nodo di storage per i volumi di storage ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat /etc/hosts`.

Riparare i dati se tutti i volumi sono guasti

Se tutti i volumi di storage si sono guastati, riparare l'intero nodo. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se solo alcuni volumi hanno avuto problemi, passare a. Riparare i dati se solo alcuni volumi sono guasti.

> Impossibile eseguire `repair-data` operazioni per più di un nodo contemporaneamente. Per ripristinare più nodi, contattare il supporto tecnico.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` con il `--nodes` Opzione per riparare l'intero nodo di storage.

Questo comando ripara i dati replicati su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non è in grado di individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Vedere Monitorare e risolvere i problemi.

Cancellazione dei dati codificati (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `repair-data start-ec-node-repair` con il `--nodes` Opzione per riparare l'intero nodo di storage.

Questo comando ripara i dati con codifica di cancellazione su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono guasti

Se solo alcuni volumi hanno avuto problemi, riparare i volumi interessati. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati

con codifica di cancellazione (EC) o entrambi.

Se tutti i volumi non sono riusciti, passare a. Riparare i dati se tutti i volumi sono guasti.

Inserire gli ID del volume in formato esadecimale. Ad esempio, `0000` è il primo volume e. `000F` è il sedicesimo volume. È possibile specificare un volume, un intervallo di volumi o più volumi che non si trovano in una sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di storage. Se è necessario ripristinare i volumi per più di un nodo di storage, contattare il supporto tecnico.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` con il `--nodes` opzione per identificare il nodo. Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati replicati nel volume `0002` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati replicati in tutti i volumi dell'intervallo `0003` a. `0009` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumi multipli non in sequenza: Questo comando ripristina i dati replicati nei volumi `0001`, `0005`, e. `0008` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non è in grado di individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

Cancellazione dei dati codificati (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `start-ec-volume-repair` con il `--nodes` opzione per identificare il nodo. Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati con codifica erasure nel volume `0007` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati con codifica di cancellazione su tutti i volumi dell'intervallo `0004` a. `0006` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Volumi multipli non in sequenza: Questo comando ripristina i dati con codifica erasure nei volumi `000A`, `000C`, e. `000E` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Il `repair-data` l'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di

ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Monitorare le riparazioni

Monitorare lo stato dei lavori di riparazione, in base all'utilizzo di **dati replicati**, **dati EC (erasure-coded)** o entrambi.

Dati replicati

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

    > Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

    - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

      > Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

    - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.
- Facoltativamente, per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

  > Il `show-replicated-repair-status` L'opzione è disponibile per l'anteprima tecnica in StorageGRID 11.6. Questa funzionalità è in fase di sviluppo e il valore restituito potrebbe essere errato o ritardato. Per determinare se una riparazione è completa, utilizzare **in attesa di – tutto**, **riparazioni tentate (XRPA)** e **periodo di scansione — stimato (XSCM)** come descritto in Monitorare le riparazioni.

Cancellazione dei dati codificati (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:

   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).
   - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

     ```
     repair-data show-ec-repair-status --repair-id repair ID
     ```

   - Utilizzare questo comando per elencare tutte le riparazioni:

     ```
     repair-data show-ec-repair-status
     ```

   L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Controllare lo stato dello storage dopo il ripristino del nodo di storage dell'appliance

Dopo aver ripristinato un nodo di storage dell'appliance, è necessario verificare che lo stato desiderato del nodo di storage dell'appliance sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che si riavvia il server del nodo di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Controllare i valori di **Recovery Storage Node LDR Storage Storage state — Desired** e **Storage state — Current**.

   Il valore di entrambi gli attributi deve essere Online.

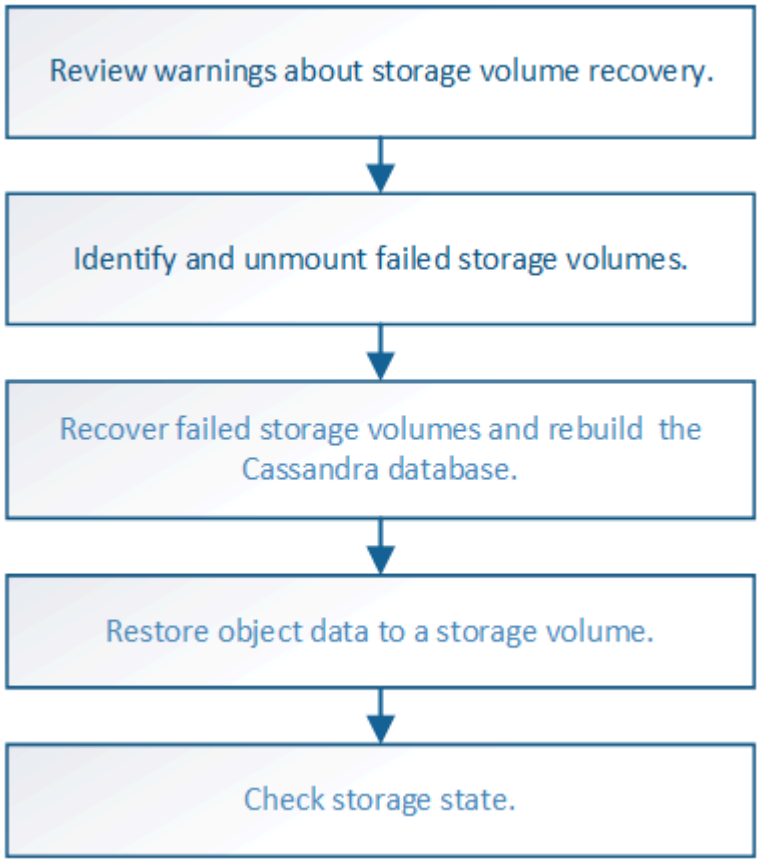
3. Se lo stato di storage — desiderato è impostato su sola lettura, attenersi alla seguente procedura:
   a. Fare clic sulla scheda **Configurazione**.
   b. Dall'elenco a discesa **Storage state — Desired** (Stato storage — desiderato*), selezionare **Online**.
   c. Fare clic su **Applica modifiche**.
   d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato dello storage — desiderato** e **Stato dello storage — corrente** siano aggiornati a Online.

Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto

È necessario completare una serie di attività per ripristinare un nodo di storage basato su software in cui uno o più volumi di storage sul nodo di storage si sono guastati, ma il disco di sistema è intatto. Se solo i volumi di storage sono guasti, il nodo di storage è ancora disponibile per il sistema StorageGRID.

A proposito di questa attività

Questa procedura di ripristino si applica solo ai nodi di storage basati su software. Se i volumi di storage si sono guastati su un nodo di storage dell'appliance, utilizzare la procedura "Recover appliance Storage Node" (Ripristina nodo di storage dell'appliance).



Informazioni correlate

Ripristinare il nodo storage dell'appliance

Esaminare gli avvisi relativi al ripristino del volume di storage

Prima di ripristinare i volumi di storage guasti per un nodo di storage, è necessario

esaminare i seguenti avvisi.

I volumi di storage (o rangedb) in un nodo di storage sono identificati da un numero esadecimale, noto come ID del volume. Ad esempio, 0000 è il primo volume e 000F è il sedicesimo volume. Il primo archivio di oggetti (volume 0) su ciascun nodo di storage utilizza fino a 4 TB di spazio per i metadati degli oggetti e le operazioni del database Cassandra; qualsiasi spazio rimanente su tale volume viene utilizzato per i dati degli oggetti. Tutti gli altri volumi di storage vengono utilizzati esclusivamente per i dati a oggetti.

Se il volume 0 non funziona e deve essere ripristinato, il database Cassandra potrebbe essere ricostruito come parte della procedura di ripristino del volume. Cassandra potrebbe essere ricostruita anche nelle seguenti circostanze:

- Un nodo di storage viene riportato online dopo essere stato offline per più di 15 giorni.
- Il disco di sistema e uno o più volumi di storage si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di storage. Se troppi nodi di storage sono offline, alcuni dati Cassandra potrebbero non essere disponibili. Se Cassandra è stata ricostruita di recente, i dati Cassandra potrebbero non essere ancora coerenti in tutta la griglia. La perdita di dati può verificarsi se Cassandra viene ricostruita quando troppi nodi di storage sono offline o se due o più nodi di storage vengono ricostruiti entro 15 giorni l'uno dall'altro.

Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni può causare la perdita di dati.

Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Contattare il supporto tecnico.

Come viene eseguito il ripristino del sito dal supporto tecnico

Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.

Se si verifica un allarme Services: Status - Cassandra (SVST) durante il ripristino, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi per ripristinare l'allarme mediante la ricostruzione di Cassandra. Dopo la ricostruzione di Cassandra, gli allarmi devono essere disattivati. Se gli allarmi non vengono disattivati, contattare il supporto tecnico.

Informazioni correlate

Monitorare e risolvere i problemi

Avvertenze e considerazioni per il ripristino del nodo grid

Identificare e smontare i volumi di storage guasti

Durante il ripristino di un nodo di storage con volumi di storage guasti, è necessario identificare e smontare i volumi guasti. È necessario verificare che solo i volumi di

storage guasti vengano riformattati come parte della procedura di ripristino.

Di cosa hai bisogno

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

A proposito di questa attività

È necessario ripristinare i volumi di storage guasti il prima possibile.

La prima fase del processo di ripristino consiste nel rilevare i volumi che sono stati scollegati, che devono essere disinstallati o che presentano errori di i/O. Se i volumi guasti sono ancora collegati ma hanno un file system corrotto in modo casuale, il sistema potrebbe non rilevare alcun danneggiamento nelle parti del disco non utilizzate o non allocate.

> È necessario completare questa procedura prima di eseguire la procedura manuale per ripristinare i volumi, ad esempio aggiungere o ricollegare i dischi, arrestare il nodo, avviare il nodo o riavviare. In caso contrario, quando si esegue `reformat_storage_block_devices.rb` script, potrebbe verificarsi un errore del file system che causa il blocco o l'errore dello script.

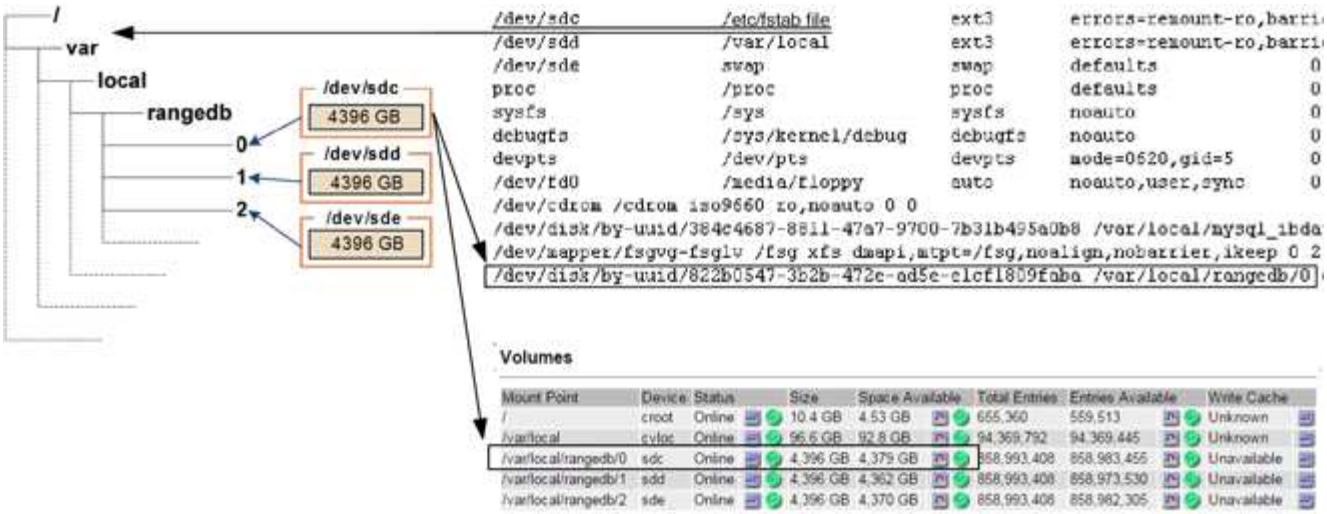
> Riparare l'hardware e collegare correttamente i dischi prima di eseguire `reboot` comando.

> Identificare con attenzione i volumi di storage guasti. Queste informazioni verranno utilizzate per verificare quali volumi devono essere riformattati. Una volta riformattato un volume, i dati sul volume non possono essere ripristinati.

Per ripristinare correttamente i volumi di storage guasti, è necessario conoscere i nomi dei dispositivi dei volumi di storage guasti e i relativi ID dei volumi.

Al momento dell'installazione, a ciascun dispositivo di storage viene assegnato un UID (Universal Unique Identifier) del file system e viene montato in una directory rangedb sul nodo di storage utilizzando l'UID del file system assegnato. L'UUID del file system e la directory rangedb sono elencati in `/etc/fstab` file. Il nome del dispositivo, la directory rangedb e le dimensioni del volume montato vengono visualizzati in Grid Manager.

Nell'esempio seguente, dispositivo `/dev/sdc` Ha un volume di 4 TB, è montato su `/var/local/rangedb/0`, utilizzando il nome del dispositivo `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` in `/etc/fstab` file:



Fasi

1. Completare i seguenti passaggi per registrare i volumi di storage guasti e i relativi nomi dei dispositivi:

   a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.

   b. Selezionare **sito nodo di storage guasto LDR Storage Panoramica principale** e cercare gli archivi di oggetti con allarmi.

   Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

   c. Selezionare **sito nodo storage guasto SSM risorse Panoramica principale**. Determinare il punto di montaggio e le dimensioni del volume di ciascun volume di storage guasto identificato nel passaggio precedente.

   Gli archivi di oggetti sono numerati in notazione esadecimale. Ad esempio, 0000 è il primo volume e 000F è il sedicesimo volume. Nell'esempio, l'archivio di oggetti con un ID di 0000 corrisponde a. `/var/local/rangedb/0` Con nome periferica sdc e una dimensione di 107 GB.

   Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. Accedere al nodo di storage guasto:

   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. Eseguire il seguente script per arrestare i servizi di storage e smontare un volume di storage guasto:

```
sn-unmount-volume object_store_ID
```

Il `object_store_ID` È l'ID del volume di storage guasto. Ad esempio, specificare `0` Nel comando per un archivio di oggetti con ID 0000.

4. Se richiesto, premere **y** per arrestare i servizi di storage sul nodo di storage.

> Se i servizi di storage sono già stati arrestati, non viene richiesto. Il servizio Cassandra viene arrestato solo per il volume 0.

```
root@Storage-180:~ # sn-unmount-volume 0
Storage services (ldr, chunk, dds, cassandra) are not down.
Storage services must be stopped before running this script.
Stop storage services [y/N]? y
Shutting down storage services.
Storage services stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

In pochi secondi, i servizi di storage vengono arrestati e il volume viene dismontato. Vengono visualizzati messaggi che indicano ogni fase del processo. Il messaggio finale indica che il volume è stato dismontato.

Ripristinare i volumi di storage guasti e ricostruire il database Cassandra

È necessario eseguire uno script che riformatta e rimontana lo storage su volumi di storage guasti e ricostruisce il database Cassandra sul nodo di storage, se il sistema lo ritiene necessario.

- È necessario disporre di `Passwords.txt` file.
- I dischi di sistema sul server devono essere intatti.
- La causa del guasto deve essere stata identificata e, se necessario, l'hardware di storage sostitutivo deve essere già stato acquistato.
- La dimensione totale dello storage sostitutivo deve essere uguale a quella dell'originale.
- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).

- Hai verificato che non è in corso un'espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).
- Lo hai fatto analisi degli avvisi relativi al ripristino del volume di storage.

a. Se necessario, sostituire lo storage fisico o virtuale guasto associato ai volumi di storage guasti identificati e non montati in precedenza.

   Dopo aver sostituito lo storage, assicurarsi di eseguire nuovamente la scansione o il riavvio per assicurarsi che sia riconosciuto dal sistema operativo, ma non rimontare i volumi. Lo storage viene rimontato e aggiunto a. `/etc/fstab` in un passaggio successivo.

b. Accedere al nodo di storage guasto:

   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. `#`.

c. Utilizzare un editor di testo (vi o vim) per eliminare i volumi guasti da `/etc/fstab` quindi salvare il file.

   > Commenti su un volume guasto in `/etc/fstab` file insufficiente. Il volume deve essere cancellato da `fstab` mentre il processo di ripristino verifica che tutte le linee in `fstab` il file corrisponde ai file system montati.

d. Riformattare eventuali volumi di storage guasti e ricostruire il database Cassandra, se necessario. Inserire: `reformat_storage_block_devices.rb`

   - Se i servizi di storage sono in esecuzione, viene richiesto di interromperli. Immettere: **Y**
   - Se necessario, viene richiesto di ricostruire il database Cassandra.
     - Esaminare gli avvisi. Se non sono applicabili, ricostruire il database Cassandra. Immettere: **Y**
     - Se più di un nodo di storage non è in linea o se un altro nodo di storage è stato ricostruito negli ultimi 15 giorni. Immettere: **N**

       Lo script verrà chiuso senza ricostruire Cassandra. Contattare il supporto tecnico.
   - Per ogni disco rangedb sul nodo di storage, quando viene richiesto: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, immettere una delle seguenti risposte:
     - **y** per riformattare un disco con errori. In questo modo, il volume di storage viene riformattato e il volume di storage riformattato viene aggiunto a. `/etc/fstab` file.
     - **n** se il disco non contiene errori e non si desidera riformattarlo.

       > Selezionando **n** si esce dallo script. Montare il disco (se si ritiene che i dati sul disco debbano essere conservati e il disco non è stato montato per errore) oppure rimuoverlo. Quindi, eseguire `reformat_storage_block_devices.rb` di nuovo comando.

> Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona “reaper” o “Cassandra repair”. Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

Nel seguente esempio di output, il disco `/dev/sdf` Deve essere riformattato e Cassandra non ha bisogno di essere ricostruito:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

Ripristinare i dati degli oggetti nel volume di storage in cui il disco di sistema è intatto

Dopo il ripristino di un volume di storage su un nodo di storage in cui il disco di sistema è intatto, è possibile ripristinare i dati dell’oggetto persi in caso di guasto del volume di storage.

Di cosa hai bisogno

- È necessario confermare che il nodo di storage recuperato ha uno stato di connessione di **connesso** Nella scheda **NODI** > **Panoramica** di Grid Manager.

A proposito di questa attività

I dati degli oggetti possono essere ripristinati da altri nodi di storage, da un nodo di archiviazione o da un pool di storage cloud, supponendo che le regole ILM del grid siano state configurate in modo da rendere disponibili le copie degli oggetti.

Tenere presente quanto segue:

- Se una regola ILM è stata configurata per memorizzare solo una copia replicata e tale copia esisteva su un volume di storage che non ha superato il test, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi di ripristino e dei relativi costi.
- Se l'unica copia rimanente di un oggetto si trova su un nodo di archiviazione, i dati dell'oggetto vengono recuperati dal nodo di archiviazione. Il ripristino dei dati degli oggetti in un nodo di storage da un nodo di archiviazione richiede più tempo rispetto al ripristino delle copie da altri nodi di storage a causa della latenza associata ai recuperi da sistemi di storage di archiviazione esterni.

A proposito di `repair-data` script

Per ripristinare i dati dell'oggetto, eseguire `repair-data` script. Questo script inizia il processo di ripristino dei dati degli oggetti e lavora con la scansione ILM per garantire che le regole ILM siano soddisfatte.

Selezionare **Replicated data** o **Erasure-Coded (EC) data** per apprendere le diverse opzioni di `repair-data` script, in base al ripristino di dati replicati o a dati con codifica di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.

> Per ulteriori informazioni su `repair-data` script, invio `repair-data --help` Dalla riga di comando del nodo di amministrazione primario.

Dati replicati

Sono disponibili due comandi per il ripristino dei dati replicati, a seconda che sia necessario riparare l'intero nodo o solo alcuni volumi sul nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

> Il `show-replicated-repair-status` L'opzione è disponibile per l'anteprima tecnica in StorageGRID 11.6. Questa funzionalità è in fase di sviluppo e il valore restituito potrebbe essere errato o ritardato. Per determinare se una riparazione è completa, utilizzare **in attesa di – tutto**, **riparazioni tentate (XRPA)** e **periodo di scansione — stimato (XSCM)** come descritto in Monitorare le riparazioni.

Cancellazione dei dati codificati (EC)

Sono disponibili due comandi per il ripristino dei dati con codifica erasure, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

È possibile tenere traccia delle riparazioni dei dati con codifica per la cancellazione con questo comando:

```
repair-data show-ec-repair-status
```

> Il lavoro di riparazione EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine della riparazione. Se lo storage non è sufficiente per la prenotazione, il lavoro di riparazione EC non avrà esito positivo. Le prenotazioni di storage vengono rilasciate al termine del lavoro di riparazione EC, indipendentemente dal fatto che il lavoro abbia avuto esito negativo o positivo.

Trovare il nome host per il nodo di storage

1. 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. `#`.

2. Utilizzare `/etc/hosts` File per trovare il nome host del nodo di storage per i volumi di storage ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat /etc/hosts`.

Riparare i dati se tutti i volumi sono guasti

Se tutti i volumi di storage si sono guastati, riparare l'intero nodo. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se solo alcuni volumi hanno avuto problemi, passare a. Riparare i dati se solo alcuni volumi sono guasti.

> Impossibile eseguire `repair-data` operazioni per più di un nodo contemporaneamente. Per ripristinare più nodi, contattare il supporto tecnico.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` con il `--nodes` Opzione per riparare l'intero nodo di storage.

Questo comando ripara i dati replicati su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non è in grado di individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Vedere Monitorare e risolvere i problemi.

Cancellazione dei dati codificati (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `repair-data start-ec-node-repair` con il `--nodes` Opzione per riparare l'intero nodo di storage.

Questo comando ripara i dati con codifica di cancellazione su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono guasti

Se solo alcuni volumi hanno avuto problemi, riparare i volumi interessati. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati

con codifica di cancellazione (EC) o entrambi.

Se tutti i volumi non sono riusciti, passare a. Riparare i dati se tutti i volumi sono guasti.

Inserire gli ID del volume in formato esadecimale. Ad esempio, `0000` è il primo volume e. `000F` è il sedicesimo volume. È possibile specificare un volume, un intervallo di volumi o più volumi che non si trovano in una sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di storage. Se è necessario ripristinare i volumi per più di un nodo di storage, contattare il supporto tecnico.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` con il `--nodes` opzione per identificare il nodo. Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati replicati nel volume `0002` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati replicati in tutti i volumi dell'intervallo `0003` a. `0009` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumi multipli non in sequenza: Questo comando ripristina i dati replicati nei volumi `0001`, `0005`, e. `0008` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non è in grado di individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

Cancellazione dei dati codificati (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `start-ec-volume-repair` con il `--nodes` opzione per identificare il nodo. Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati con codifica erasure nel volume `0007` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati con codifica di cancellazione su tutti i volumi dell'intervallo `0004` a. `0006` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Volumi multipli non in sequenza: Questo comando ripristina i dati con codifica erasure nei volumi `000A`, `000C`, e. `000E` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Il `repair-data` l'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di

ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Monitorare le riparazioni

Monitorare lo stato dei lavori di riparazione, in base all'utilizzo di **dati replicati**, **dati EC (erasure-coded)** o entrambi.

Dati replicati

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

> Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

    - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

> Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

    - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.
- Facoltativamente, per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

```
repair-data show-replicated-repair-status
```

> Il `show-replicated-repair-status` L'opzione è disponibile per l'anteprima tecnica in StorageGRID 11.6. Questa funzionalità è in fase di sviluppo e il valore restituito potrebbe essere errato o ritardato. Per determinare se una riparazione è completa, utilizzare **in attesa di – tutto**, **riparazioni tentate (XRPA)** e **periodo di scansione — stimato (XSCM)** come descritto in Monitorare le riparazioni.

Cancellazione dei dati codificati (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:

   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).
   - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

     ```
     repair-data show-ec-repair-status --repair-id repair ID
     ```

   - Utilizzare questo comando per elencare tutte le riparazioni:

     ```
     repair-data show-ec-repair-status
     ```

   L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Controllare lo stato dello storage dopo il ripristino dei volumi di storage

Dopo il ripristino dei volumi di storage, è necessario verificare che lo stato desiderato del nodo di storage sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che si riavvia il server del nodo di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Controllare i valori di **Recovery Storage Node LDR Storage Storage state — Desired** e **Storage state — Current**.

   Il valore di entrambi gli attributi deve essere Online.

3. Se lo stato di storage — desiderato è impostato su sola lettura, attenersi alla seguente procedura:

a. Fare clic sulla scheda **Configurazione**.
b. Dall'elenco a discesa **Storage state — Desired** (Stato storage — desiderato*), selezionare **Online**.
c. Fare clic su **Applica modifiche**.
d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato dello storage — desiderato** e **Stato dello storage — corrente** siano aggiornati a Online.

Ripristino in caso di guasto al disco di sistema

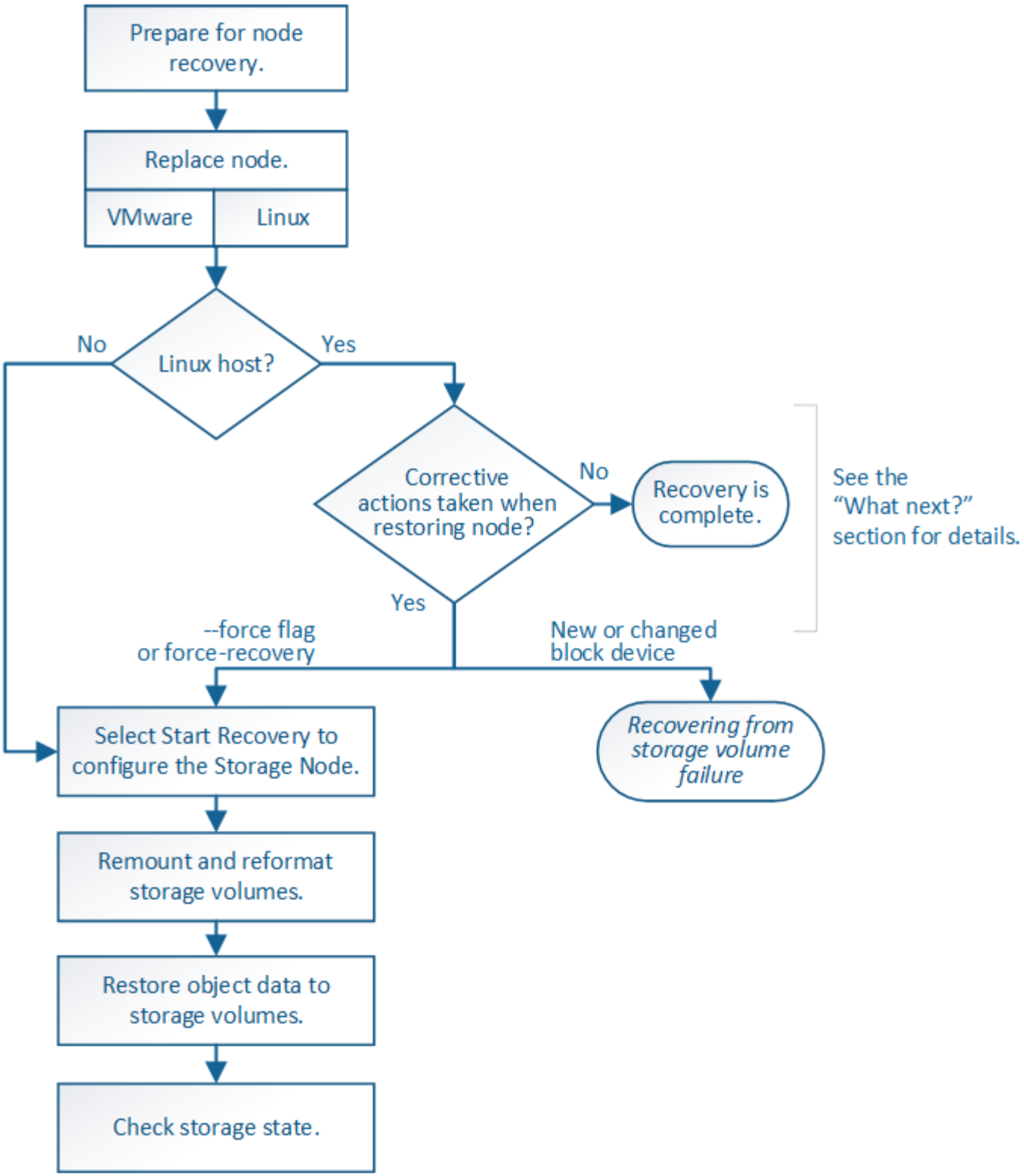
Se il disco di sistema su un nodo di storage basato su software si è guastato, il nodo di storage non è disponibile per il sistema StorageGRID. È necessario completare una serie specifica di attività per eseguire il ripristino da un guasto al disco di sistema.

A proposito di questa attività

Utilizzare questa procedura per eseguire il ripristino da un guasto del disco di sistema su un nodo di storage basato su software. Questa procedura include i passaggi da seguire se anche i volumi di storage non sono riusciti o non possono essere rimontati.

> Questa procedura si applica solo ai nodi di storage basati su software. Per ripristinare un nodo di storage dell'appliance, è necessario seguire un'altra procedura.

Ripristinare il nodo storage dell'appliance



Esaminare gli avvisi per il ripristino del disco di sistema Storage Node

Prima di ripristinare un disco di sistema guasto di un nodo di storage, è necessario esaminare i seguenti avvisi.

I nodi di storage dispongono di un database Cassandra che include metadati a oggetti. Il database Cassandra potrebbe essere ricostruito nei seguenti casi:

- Un nodo di storage viene riportato online dopo essere stato offline per più di 15 giorni.
- Un volume di storage ha subito un errore e è stato ripristinato.
- Il disco di sistema e uno o più volumi di storage si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di storage. Se troppi nodi di storage sono offline, alcuni dati Cassandra potrebbero non essere disponibili. Se Cassandra è stata ricostruita di recente, i dati Cassandra potrebbero non essere ancora coerenti in tutta la griglia. La perdita di dati può verificarsi se Cassandra viene ricostruita quando troppi nodi di storage sono offline o se due o più nodi di storage vengono ricostruiti entro 15 giorni l'uno dall'altro.

Se più di un nodo di storage si è guastato (o non è in linea), contattare il supporto tecnico. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati.

Se si tratta del secondo guasto del nodo di storage in meno di 15 giorni dopo un guasto o un ripristino del nodo di storage, contattare il supporto tecnico. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni può causare la perdita di dati.

Se più di un nodo di storage in un sito si è guastato, potrebbe essere necessaria una procedura di ripristino del sito. Contattare il supporto tecnico.

Come viene eseguito il ripristino del sito dal supporto tecnico

Se questo nodo di storage è in modalità di manutenzione in sola lettura per consentire il recupero di oggetti da parte di un altro nodo di storage con volumi di storage guasti, ripristinare i volumi sul nodo di storage con volumi di storage guasti prima di ripristinare questo nodo di storage guasto. Consultare le istruzioni per il ripristino dalla perdita di volumi di storage in cui il disco di sistema è intatto.

Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.

Se si verifica un allarme Services: Status - Cassandra (SVST) durante il ripristino, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi per ripristinare l'allarme mediante la ricostruzione di Cassandra. Dopo la ricostruzione di Cassandra, gli allarmi devono essere disattivati. Se gli allarmi non vengono disattivati, contattare il supporto tecnico.

Informazioni correlate

Monitorare e risolvere i problemi

Avvertenze e considerazioni per il ripristino del nodo grid

Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto

Sostituire il nodo di storage

Se il disco di sistema presenta un guasto, è necessario sostituire il nodo di storage.

Selezionare la procedura di sostituzione del nodo per la piattaforma. I passaggi per sostituire un nodo sono gli stessi per tutti i tipi di nodi griglia.

Questa procedura si applica solo ai nodi di storage basati su software. Per ripristinare un nodo di storage dell'appliance, è necessario seguire un'altra procedura.

Ripristinare il nodo storage dell'appliance

Linux: se non si è sicuri che il disco di sistema sia guasto, seguire le istruzioni per sostituire il nodo per determinare quali passaggi di ripristino sono necessari.

Piattaforma	Procedura
VMware	Sostituire un nodo VMware
Linux	Sostituire un nodo Linux
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per sostituire un nodo Linux.

Selezionare Avvia ripristino per configurare il nodo di storage

Dopo aver sostituito un nodo di storage, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

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).
- È necessario disporre della passphrase di provisioning.
- È necessario aver implementato e configurato il nodo sostitutivo.
- È necessario conoscere la data di inizio di qualsiasi intervento di riparazione per i dati codificati per la cancellazione.
- È necessario verificare che il nodo di storage non sia stato ricostruito negli ultimi 15 giorni.

A proposito di questa attività

Se Storage Node è installato come container su un host Linux, eseguire questa operazione solo se si verifica una delle seguenti condizioni:

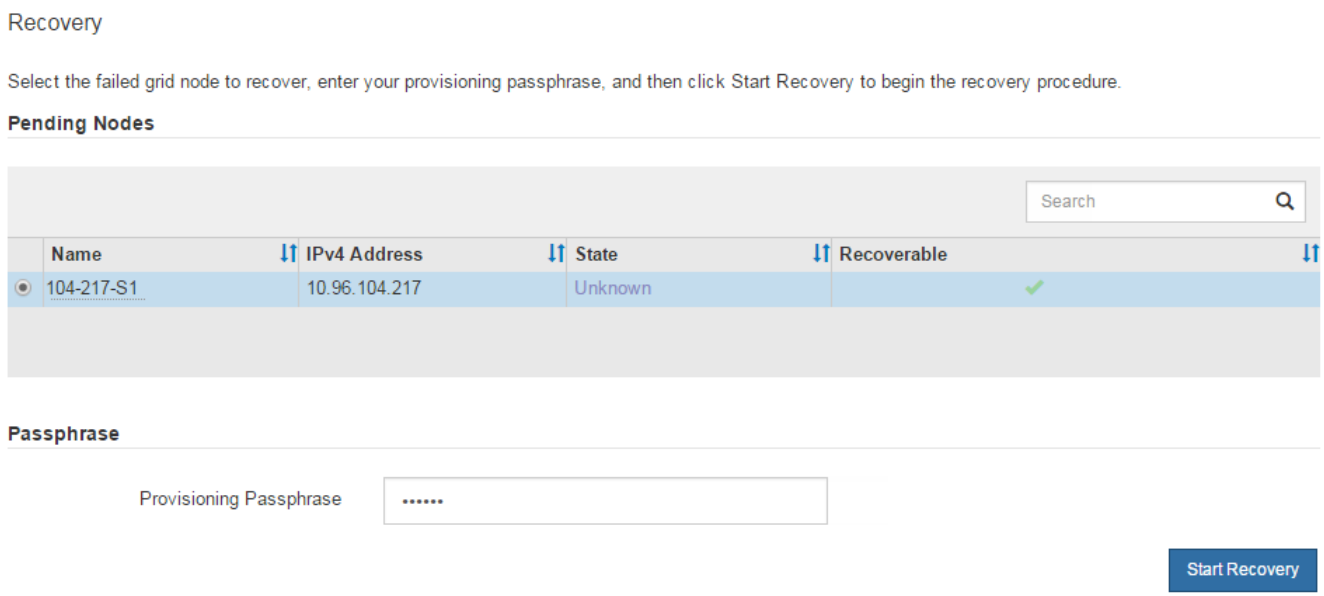
- È stato necessario utilizzare `--force` contrassegno per importare il nodo o emesso `storagegrid node force-recovery` *`node-name`*
- Era necessario eseguire una reinstallazione completa del nodo oppure ripristinare /var/local.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE attività Recovery**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

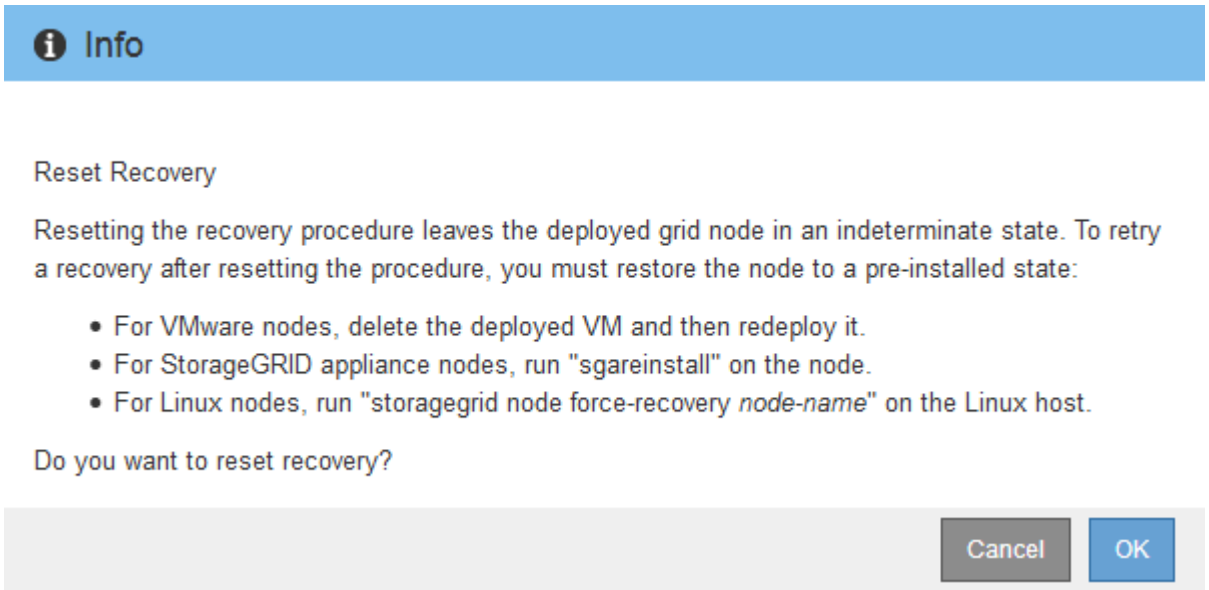
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

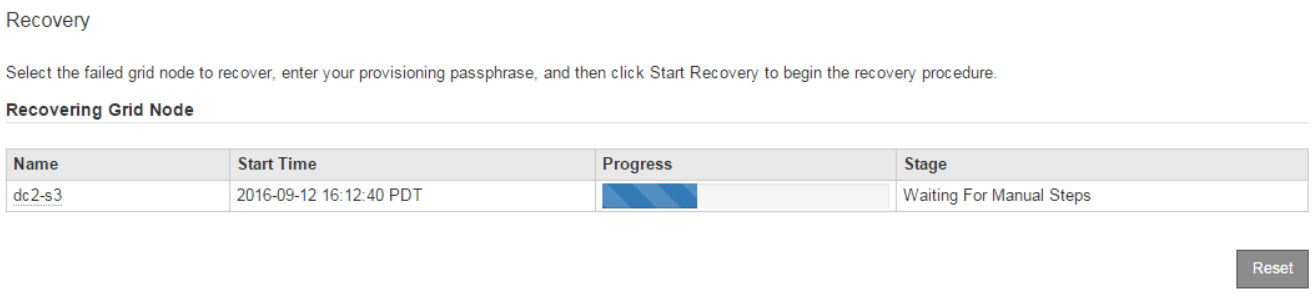
> Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo Info, che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`

6. Quando il nodo di storage raggiunge la fase “Waiting for Manual Steps”, passare all’attività successiva della procedura di recovery per il remount e la riformattazione dei volumi di storage.



Informazioni correlate

Preparazione dell’appliance per la reinstallazione (solo sostituzione della piattaforma)

Rimontare e riformattare i volumi di storage ("procedure manuali")

È necessario eseguire manualmente due script per rimontare volumi di storage conservati e riformattare eventuali volumi di storage guasti. Il primo script consente di eseguire il remontaggio dei volumi correttamente formattati come volumi di storage StorageGRID. Il secondo script riformatta tutti i volumi non montati, ricostruisce Cassandra, se necessario, e avvia i servizi.

Di cosa hai bisogno

- L’hardware è già stato sostituito per tutti i volumi di storage guasti che è necessario sostituire.

  Esecuzione di `sn-remount-volumes` lo script può aiutare a identificare altri volumi di storage guasti.

- È stato verificato che non è in corso la decommissionamento di un nodo di storage oppure che la procedura di decommissionamento del nodo è stata sospesa. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **smantellamento**).
- Hai verificato che non è in corso un’espansione. (In Grid Manager, selezionare **MANUTENZIONE** > **attività** > **espansione**).
- Lo hai fatto Esaminate le avvertenze relative al ripristino del disco di sistema Storage Node.

> Contattare il supporto tecnico se più di un nodo di storage non è in linea o se un nodo di storage in questa griglia è stato ricostruito negli ultimi 15 giorni. Non eseguire `sn-recovery-postinstall.sh` script. La ricostruzione di Cassandra su due o più nodi di storage entro 15 giorni l’uno dall’altro potrebbe causare la perdita di dati.

A proposito di questa attività

Per completare questa procedura, eseguire le seguenti attività di alto livello:

- Accedere al nodo di storage recuperato.
- Eseguire `sn-remount-volumes` script per il remount di volumi di storage correttamente formattati. Quando viene eseguito, lo script esegue le seguenti operazioni:
  - Consente di montare e rimuovere ciascun volume di storage per riprodurre il journal XFS.
  - Esegue un controllo di coerenza del file XFS.

- Se il file system è coerente, determina se il volume di storage è un volume di storage StorageGRID formattato correttamente.
- Se il volume di storage è formattato correttamente, esegue il remontaggio del volume di storage. Tutti i dati esistenti sul volume rimangono intatti.

- Esaminare l'output dello script e risolvere eventuali problemi.
- Eseguire `sn-recovery-postinstall.sh` script. Quando viene eseguito, lo script esegue le seguenti operazioni.

> Non riavviare un nodo di storage durante il ripristino prima dell'esecuzione `sn-recovery-postinstall.sh` per riformattare i volumi di storage guasti e ripristinare i metadati degli oggetti. Riavviare il nodo di storage prima `sn-recovery-postinstall.sh` Il completamento causa errori per i servizi che tentano di avviarsi e fa uscire i nodi dell'appliance StorageGRID dalla modalità di manutenzione. Vedere la fase per script post-installazione.

  - Consente di riformattare tutti i volumi di storage di `sn-remount-volumes` impossibile eseguire il montaggio dello script o che è stato trovato formattato in modo errato.

    > Se un volume di storage viene riformattato, tutti i dati presenti in tale volume andranno persi. È necessario eseguire un'ulteriore procedura per ripristinare i dati degli oggetti da altre posizioni nella griglia, supponendo che le regole ILM siano state configurate per memorizzare più copie di un oggetto.

  - Ricostruisce il database Cassandra sul nodo, se necessario.
  - Avvia i servizi sul nodo di storage.

Fasi

1. Accedere al nodo di storage recuperato:

   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. `#`.

2. Eseguire il primo script per rimontare eventuali volumi di storage correttamente formattati.

   > Se tutti i volumi di storage sono nuovi e devono essere formattati, o se tutti i volumi di storage sono guasti, è possibile saltare questa fase ed eseguire il secondo script per riformattare tutti i volumi di storage non montati.

   a. Eseguire lo script: `sn-remount-volumes`

      Questo script potrebbe richiedere ore per essere eseguito su volumi di storage che contengono dati.

   b. Durante l'esecuzione dello script, esaminare l'output e rispondere alle richieste.

Se necessario, è possibile utilizzare `tail -f` per monitorare il contenuto del file di log dello script (`/var/local/log/sn-remount-volumes.log`) . Il file di log contiene informazioni più dettagliate rispetto all'output della riga di comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.
```

```
====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Nell’output di esempio, un volume di storage è stato rimontato correttamente e tre volumi di storage

hanno avuto errori.

- `/dev/sdb` Ha superato il controllo di coerenza del file system XFS e disponeva di una struttura di volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi che vengono rimontati dallo script vengono conservati.
- `/dev/sdc` Verifica della coerenza del file system XFS non riuscita perché il volume di storage era nuovo o corrotto.
- `/dev/sdd` impossibile montare perché il disco non è stato inizializzato o il superblocco del disco è stato danneggiato. Quando lo script non riesce a montare un volume di storage, chiede se si desidera eseguire il controllo di coerenza del file system.
  - Se il volume di storage è collegato a un nuovo disco, rispondere **N** alla richiesta. Non è necessario controllare il file system su un nuovo disco.
  - Se il volume di storage è collegato a un disco esistente, rispondere **Y** alla richiesta. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I risultati vengono salvati in `/var/local/log/sn-remount-volumes.log` file di log.
- `/dev/sde` Ha superato la verifica di coerenza del file system XFS e disponeva di una struttura di volume valida; tuttavia, l'ID del nodo LDR nel file volID non corrisponde all'ID per questo nodo di storage (la `configured LDR noid` visualizzato nella parte superiore). Questo messaggio indica che questo volume appartiene a un altro nodo di storage.

3. Esaminare l'output dello script e risolvere eventuali problemi.

> Se un volume di storage non ha superato il controllo di coerenza del file system XFS o non è stato possibile montarlo, esaminare attentamente i messaggi di errore nell'output. È necessario comprendere le implicazioni dell'esecuzione di `sn-recovery-postinstall.sh` creare script su questi volumi.

a. Verificare che i risultati includano una voce per tutti i volumi previsti. Se alcuni volumi non sono elencati, eseguire nuovamente lo script.
b. Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indichino che un volume di storage non appartiene a questo nodo di storage.

   Nell'esempio, l'output per `/dev/sde` include il seguente messaggio di errore:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Se un volume di storage viene segnalato come appartenente a un altro nodo di storage, contattare il supporto tecnico. Se si esegue `sn-recovery-postinstall.sh` script, il volume di storage verrà riformattato, causando la perdita di dati.

c. Se non è stato possibile montare alcun dispositivo di storage, annotare il nome del dispositivo e riparare o sostituire il dispositivo.

> È necessario riparare o sostituire i dispositivi di storage che non possono essere montati.

   Il nome del dispositivo viene utilizzato per cercare l'ID del volume, che è necessario immettere quando

si esegue `repair-data` script per ripristinare i dati dell'oggetto nel volume (la procedura successiva).

d. Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire `sn-remount-volumes` eseguire nuovamente lo script per confermare che tutti i volumi di storage che possono essere rimontati sono stati rimontati.

> Se un volume di storage non può essere montato o non è formattato correttamente e si passa alla fase successiva, il volume e i dati presenti nel volume verranno eliminati. Se si dispone di due copie di dati oggetto, si disporrà di una sola copia fino al completamento della procedura successiva (ripristino dei dati oggetto).

> Non eseguire `sn-recovery-postinstall.sh` Eseguire uno script se si ritiene che i dati rimanenti su un volume di storage guasto non possano essere ricostruiti da un'altra parte della griglia (ad esempio, se il criterio ILM utilizza una regola che esegue una sola copia o se i volumi sono guasti su più nodi). Contattare invece il supporto tecnico per determinare come ripristinare i dati.

4. Eseguire `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

   Questo script riformatta tutti i volumi di storage che non possono essere montati o che sono stati trovati per essere formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; avvia i servizi sul nodo di storage.

   Tenere presente quanto segue:

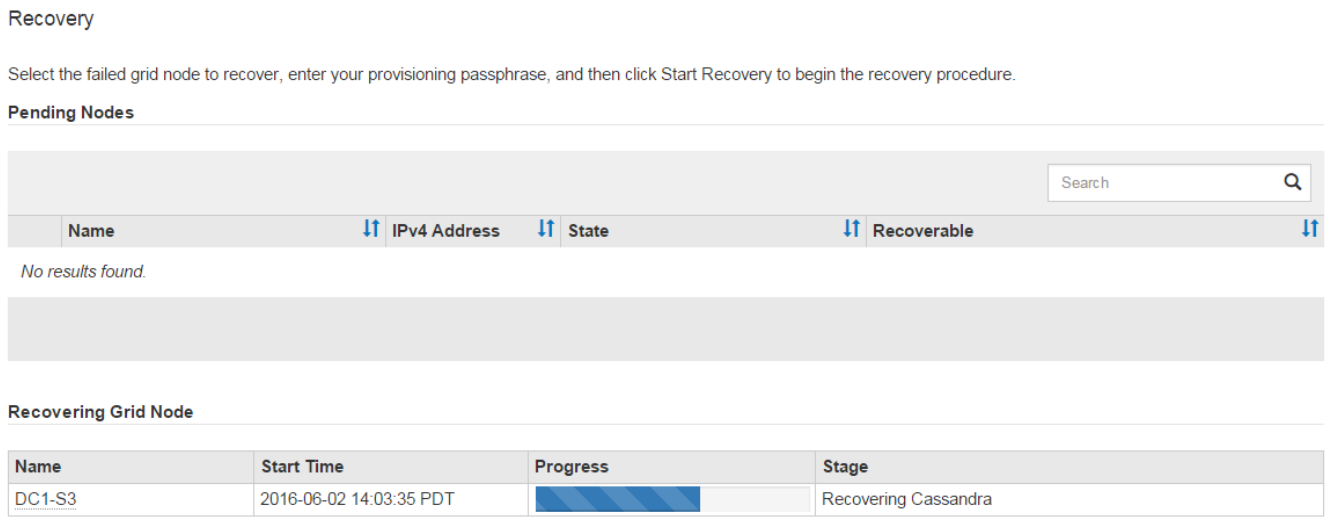
   - L'esecuzione dello script potrebbe richiedere ore.
   - In generale, si consiglia di lasciare la sessione SSH da sola mentre lo script è in esecuzione.
   - Non premere **Ctrl+C** mentre la sessione SSH è attiva.
   - Lo script viene eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzarne l'avanzamento dalla pagina Recovery (Ripristino).
   - Se Storage Node utilizza il servizio RSM, lo script potrebbe sembrare bloccato per 5 minuti quando i servizi del nodo vengono riavviati. Questo ritardo di 5 minuti è previsto ogni volta che il servizio RSM viene avviato per la prima volta.

     > Il servizio RSM è presente sui nodi di storage che includono il servizio ADC.

   > Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "Cassandra repair". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

5. come `sn-recovery-postinstall.sh` Viene eseguito lo script, monitorare la pagina Recovery in Grid Manager.

   La barra di avanzamento e la colonna fase della pagina di ripristino forniscono uno stato di alto livello di `sn-recovery-postinstall.sh` script.



Dopo il `sn-recovery-postinstall.sh` lo script ha avviato i servizi sul nodo, è possibile ripristinare i dati degli oggetti in qualsiasi volume di storage formattato dallo script, come descritto in tale procedura.

Informazioni correlate

Esaminare gli avvisi per il ripristino del disco di sistema Storage Node

Ripristinare i dati dell'oggetto nel volume di storage, se necessario

Ripristinare i dati dell'oggetto nel volume di storage, se necessario

Se il `sn-recovery-postinstall.sh` Lo script è necessario per riformattare uno o più volumi di storage guasti; è necessario ripristinare i dati degli oggetti nel volume di storage riformattato da altri nodi di storage e nodi di archivio. Questi passaggi non sono necessari a meno che uno o più volumi di storage non siano stati riformattati.

Di cosa hai bisogno

- È necessario confermare che il nodo di storage recuperato ha uno stato di connessione di **connesso** Nella scheda **NODI** > **Panoramica** di Grid Manager.

A proposito di questa attività

I dati degli oggetti possono essere ripristinati da altri nodi di storage, da un nodo di archiviazione o da un pool di storage cloud, supponendo che le regole ILM del grid siano state configurate in modo da rendere disponibili le copie degli oggetti.

Tenere presente quanto segue:

- Se una regola ILM è stata configurata per memorizzare solo una copia replicata e tale copia esisteva su un volume di storage che non ha superato il test, non sarà possibile ripristinare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto. Prima di eseguire questa procedura, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi di ripristino e dei relativi costi.
- Se l'unica copia rimanente di un oggetto si trova su un nodo di archiviazione, i dati dell'oggetto vengono recuperati dal nodo di archiviazione. Il ripristino dei dati degli oggetti in un nodo di storage da un nodo di archiviazione richiede più tempo rispetto al ripristino delle copie da altri nodi di storage a causa della

latenza associata ai recuperi da sistemi di storage di archiviazione esterni.

A proposito di `repair-data` script

Per ripristinare i dati dell'oggetto, eseguire `repair-data` script. Questo script inizia il processo di ripristino dei dati degli oggetti e lavora con la scansione ILM per garantire che le regole ILM siano soddisfatte.

Selezionare **Replicated data** o **Erasure-Coded (EC) data** per apprendere le diverse opzioni di `repair-data` script, in base al ripristino di dati replicati o a dati con codifica di cancellazione. Se è necessario ripristinare entrambi i tipi di dati, è necessario eseguire entrambi i set di comandi.

> Per ulteriori informazioni su `repair-data` script, invio `repair-data --help` Dalla riga di comando del nodo di amministrazione primario.

Dati replicati

Sono disponibili due comandi per il ripristino dei dati replicati, a seconda che sia necessario riparare l'intero nodo o solo alcuni volumi sul nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

È possibile tenere traccia delle riparazioni dei dati replicati con questo comando:

```
repair-data show-replicated-repair-status
```

> Il `show-replicated-repair-status` L'opzione è disponibile per l'anteprima tecnica in StorageGRID 11.6. Questa funzionalità è in fase di sviluppo e il valore restituito potrebbe essere errato o ritardato. Per determinare se una riparazione è completa, utilizzare **in attesa di – tutto**, **riparazioni tentate (XRPA)** e **periodo di scansione — stimato (XSCM)** come descritto in Monitorare le riparazioni.

Cancellazione dei dati codificati (EC)

Sono disponibili due comandi per il ripristino dei dati con codifica erasure, a seconda che sia necessario riparare l'intero nodo o solo determinati volumi sul nodo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

È possibile tenere traccia delle riparazioni dei dati con codifica per la cancellazione con questo comando:

```
repair-data show-ec-repair-status
```

> Il lavoro di riparazione EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine della riparazione. Se lo storage non è sufficiente per la prenotazione, il lavoro di riparazione EC non avrà esito positivo. Le prenotazioni di storage vengono rilasciate al termine del lavoro di riparazione EC, indipendentemente dal fatto che il lavoro abbia avuto esito negativo o positivo.

Trovare il nome host per il nodo di storage

1. 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. `#`.

2. Utilizzare `/etc/hosts` File per trovare il nome host del nodo di storage per i volumi di storage ripristinati. Per visualizzare un elenco di tutti i nodi nella griglia, immettere quanto segue: `cat /etc/hosts`.

Riparare i dati se tutti i volumi sono guasti

Se tutti i volumi di storage si sono guastati, riparare l'intero nodo. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati con codifica di cancellazione (EC) o entrambi.

Se solo alcuni volumi hanno avuto problemi, passare a. Riparare i dati se solo alcuni volumi sono guasti.

> Impossibile eseguire `repair-data` operazioni per più di un nodo contemporaneamente. Per ripristinare più nodi, contattare il supporto tecnico.

Dati replicati

Se la griglia include dati replicati, utilizzare `repair-data start-replicated-node-repair` con il `--nodes` Opzione per riparare l'intero nodo di storage.

Questo comando ripara i dati replicati su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non è in grado di individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Vedere Monitorare e risolvere i problemi.

Cancellazione dei dati codificati (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `repair-data start-ec-node-repair` con il `--nodes` Opzione per riparare l'intero nodo di storage.

Questo comando ripara i dati con codifica di cancellazione su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Riparare i dati se solo alcuni volumi sono guasti

Se solo alcuni volumi hanno avuto problemi, riparare i volumi interessati. Seguire le istruzioni per **dati replicati**, **dati con codifica di cancellazione (EC)** o entrambi, a seconda che si utilizzino dati replicati, dati

con codifica di cancellazione (EC) o entrambi.

Se tutti i volumi non sono riusciti, passare a. Riparare i dati se tutti i volumi sono guasti.

Inserire gli ID del volume in formato esadecimale. Ad esempio, `0000` è il primo volume e. `000F` è il sedicesimo volume. È possibile specificare un volume, un intervallo di volumi o più volumi che non si trovano in una sequenza.

Tutti i volumi devono trovarsi sullo stesso nodo di storage. Se è necessario ripristinare i volumi per più di un nodo di storage, contattare il supporto tecnico.

Dati replicati

Se la griglia contiene dati replicati, utilizzare `start-replicated-volume-repair` con il `--nodes` opzione per identificare il nodo. Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati replicati nel volume `0002` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati replicati in tutti i volumi dell'intervallo `0003` a. `0009` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumi multipli non in sequenza: Questo comando ripristina i dati replicati nei volumi `0001`, `0005`, e. `0008` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Quando i dati dell'oggetto vengono ripristinati, l'avviso **oggetti persi** viene attivato se il sistema StorageGRID non è in grado di individuare i dati dell'oggetto replicati. Gli avvisi potrebbero essere attivati sui nodi di storage all'interno del sistema. È necessario determinare la causa della perdita e se è possibile eseguire il ripristino. Consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

Cancellazione dei dati codificati (EC)

Se la griglia contiene dati con codifica per la cancellazione, utilizzare `start-ec-volume-repair` con il `--nodes` opzione per identificare il nodo. Quindi, aggiungere il `--volumes` oppure `--volume-range` come illustrato negli esempi seguenti.

Volume singolo: Questo comando ripristina i dati con codifica erasure nel volume `0007` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Range of Volumes (intervallo di volumi): Questo comando ripristina i dati con codifica di cancellazione su tutti i volumi dell'intervallo `0004` a. `0006` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Volumi multipli non in sequenza: Questo comando ripristina i dati con codifica erasure nei volumi `000A`, `000C`, e. `000E` Su un nodo di storage denominato SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Il `repair-data` l'operazione restituisce un valore univoco `repair ID` questo lo identifica `repair_data` operazione. Utilizzare questo `repair ID` per tenere traccia dell'avanzamento e dei risultati di `repair_data` operazione. Non viene restituito alcun altro feedback al termine del processo di

ripristino.

> Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.

Monitorare le riparazioni

Monitorare lo stato dei lavori di riparazione, in base all'utilizzo di **dati replicati**, **dati EC (erasure-coded)** o entrambi.

Dati replicati

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

> Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

    - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

> Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

    - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.
- Facoltativamente, per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

```
repair-data show-replicated-repair-status
```

> Il `show-replicated-repair-status` L'opzione è disponibile per l'anteprima tecnica in StorageGRID 11.6. Questa funzionalità è in fase di sviluppo e il valore restituito potrebbe essere errato o ritardato. Per determinare se una riparazione è completa, utilizzare **in attesa di – tutto**, **riparazioni tentate (XRPA)** e **periodo di scansione — stimato (XSCM)** come descritto in Monitorare le riparazioni.

Cancellazione dei dati codificati (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:

   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).
   - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

     ```
     repair-data show-ec-repair-status --repair-id repair ID
     ```

   - Utilizzare questo comando per elencare tutte le riparazioni:

     ```
     repair-data show-ec-repair-status
     ```

   L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Controllare lo stato dello storage dopo il ripristino del disco di sistema Storage Node

Dopo aver ripristinato l'unità di sistema per un nodo di storage, è necessario verificare che lo stato desiderato del nodo di storage sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che il server del nodo di storage viene riavviato.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Controllare i valori di **Recovery Storage Node LDR Storage Storage state — Desired** e **Storage state — Current**.

   Il valore di entrambi gli attributi deve essere Online.

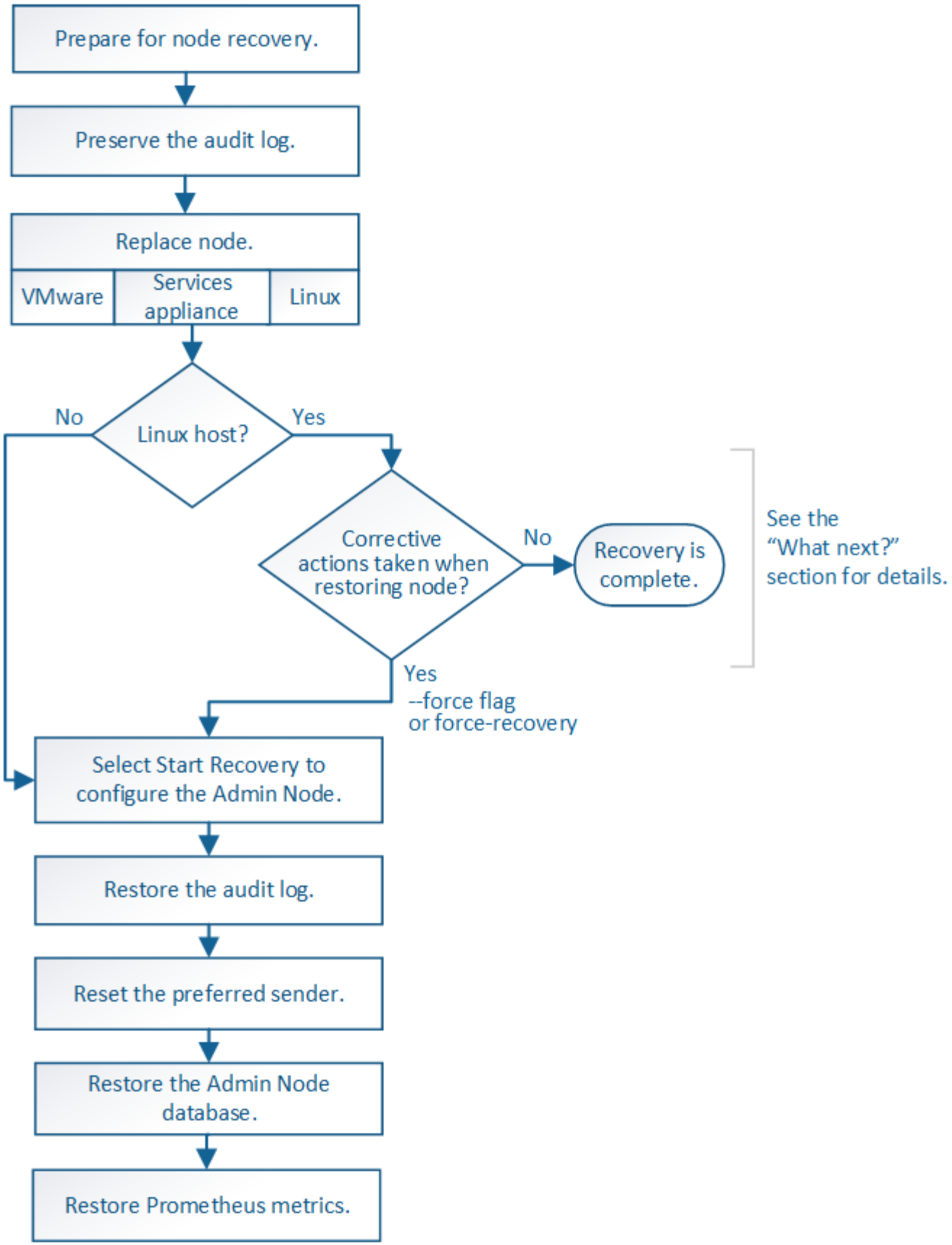
3. Se lo stato di storage — desiderato è impostato su sola lettura, attenersi alla seguente procedura:
   a. Fare clic sulla scheda **Configurazione**.
   b. Dall'elenco a discesa **Storage state — Desired** (Stato storage — desiderato*), selezionare **Online**.
   c. Fare clic su **Applica modifiche**.
   d. Fare clic sulla scheda **Panoramica** e verificare che i valori di **Stato dello storage — desiderato** e **Stato dello storage — corrente** siano aggiornati a Online.

Ripristino da errori del nodo di amministrazione

Il processo di ripristino per un nodo di amministrazione dipende dal fatto che si tratti del nodo di amministrazione primario o di un nodo di amministrazione non primario.

A proposito di questa attività

I passaggi di alto livello per il ripristino di un nodo di amministrazione primario o non primario sono gli stessi, anche se i dettagli dei passaggi differiscono.



Seguire sempre la procedura di ripristino corretta per l'Admin Node che si sta ripristinando. Le procedure hanno lo stesso aspetto ad un livello elevato, ma differiscono nei dettagli.

Informazioni correlate

Appliance di servizi SG100 e SG1000

Scelte

- Ripristino da guasti principali del nodo di amministrazione
- Ripristino da guasti non primari del nodo di amministrazione

Ripristino da guasti principali del nodo di amministrazione

È necessario completare un set specifico di attività per eseguire il ripristino da un guasto primario del nodo di amministrazione. Il nodo di amministrazione primario ospita il servizio CMN (Configuration Management Node) per la griglia.

A proposito di questa attività

Un nodo di amministrazione primario guasto deve essere sostituito tempestivamente. Il servizio CMN (Configuration Management Node) sul nodo di amministrazione primario è responsabile dell'emissione di blocchi di identificatori di oggetti per la griglia. Questi identificatori vengono assegnati agli oggetti man mano che vengono acquisiti. Non è possibile acquisire nuovi oggetti a meno che non siano disponibili identificatori. L'acquisizione degli oggetti può continuare anche quando la CMN non è disponibile, poiché la fornitura di identificatori di circa un mese viene memorizzata nella cache della griglia. Tuttavia, una volta esauriti gli identificatori memorizzati nella cache, non è possibile aggiungere nuovi oggetti.

> È necessario riparare o sostituire un nodo di amministrazione primario guasto entro circa un mese, altrimenti la griglia potrebbe perdere la capacità di acquisire nuovi oggetti. Il periodo di tempo esatto dipende dal tasso di acquisizione degli oggetti: Se hai bisogno di una valutazione più accurata del periodo di tempo per la tua griglia, contatta il supporto tecnico.

Copia i registri di controllo dal nodo di amministrazione primario non riuscito

Se è possibile copiare i registri di controllo dal nodo di amministrazione primario guasto, è necessario conservarli per mantenere il record dell'attività e dell'utilizzo del sistema della griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione primario recuperato dopo che è attivo e in esecuzione.

Questa procedura copia i file di log di audit dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo griglia separato. Questi registri di controllo conservati possono quindi essere copiati nel nodo di amministrazione sostitutivo. I registri di controllo non vengono copiati automaticamente nel nuovo nodo di amministrazione.

A seconda del tipo di errore, potrebbe non essere possibile copiare i registri di controllo da un nodo di amministrazione non riuscito. Se l'implementazione ha un solo nodo di amministrazione, il nodo di amministrazione recuperato avvia la registrazione degli eventi nel registro di controllo in un nuovo file vuoto e i dati precedentemente registrati vengono persi. Se l'implementazione include più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione.

> Se i registri di controllo non sono ora accessibili sul nodo di amministrazione guasto, potrebbe essere possibile accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

1. Se possibile, accedere al nodo Admin non riuscito. In caso contrario, accedere al nodo di amministrazione primario o a un altro nodo di amministrazione, se disponibile.
   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. `#`.

2. Arrestare il servizio AMS per impedire la creazione di un nuovo file di log:`service ams stop`
3. Rinominare il file audit.log in modo che non sovrascriva il file esistente quando lo si copia nel nodo di amministrazione recuperato.

   Rinominare il file audit.log con un nome di file univoco numerato, ad esempio yyyy-mm-dd.txt.1. Ad esempio, è possibile rinominare il file audit.log in 2015-10-25.txt.1`cd /var/local/audit/export/`

4. Riavviare il servizio AMS: `service ams start`
5. Creare la directory per copiare tutti i file di log dell'audit in una posizione temporanea su un nodo griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.

6. Copia tutti i file di log di audit: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.

7. Disconnettersi come root: `exit`

Sostituire nodo amministratore primario

Per ripristinare un nodo di amministrazione primario, è necessario prima sostituire l'hardware fisico o virtuale.

È possibile sostituire un nodo di amministrazione primario guasto con un nodo di amministrazione primario in esecuzione sulla stessa piattaforma oppure sostituire un nodo di amministrazione primario in esecuzione su VMware o su un host Linux con un nodo di amministrazione primario in hosting su un'appliance di servizi.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino primario del nodo di amministrazione.

Piattaforma sostitutiva	Procedura
VMware	Sostituire un nodo VMware
Linux	Sostituire un nodo Linux
Appliance di servizi SG100 e SG1000	Sostituire un'appliance di servizi

Piattaforma sostitutiva	Procedura
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per sostituire un nodo Linux.

Configurare il nodo amministrativo primario sostitutivo

Il nodo sostitutivo deve essere configurato come nodo amministratore primario per il sistema StorageGRID.

Di cosa hai bisogno

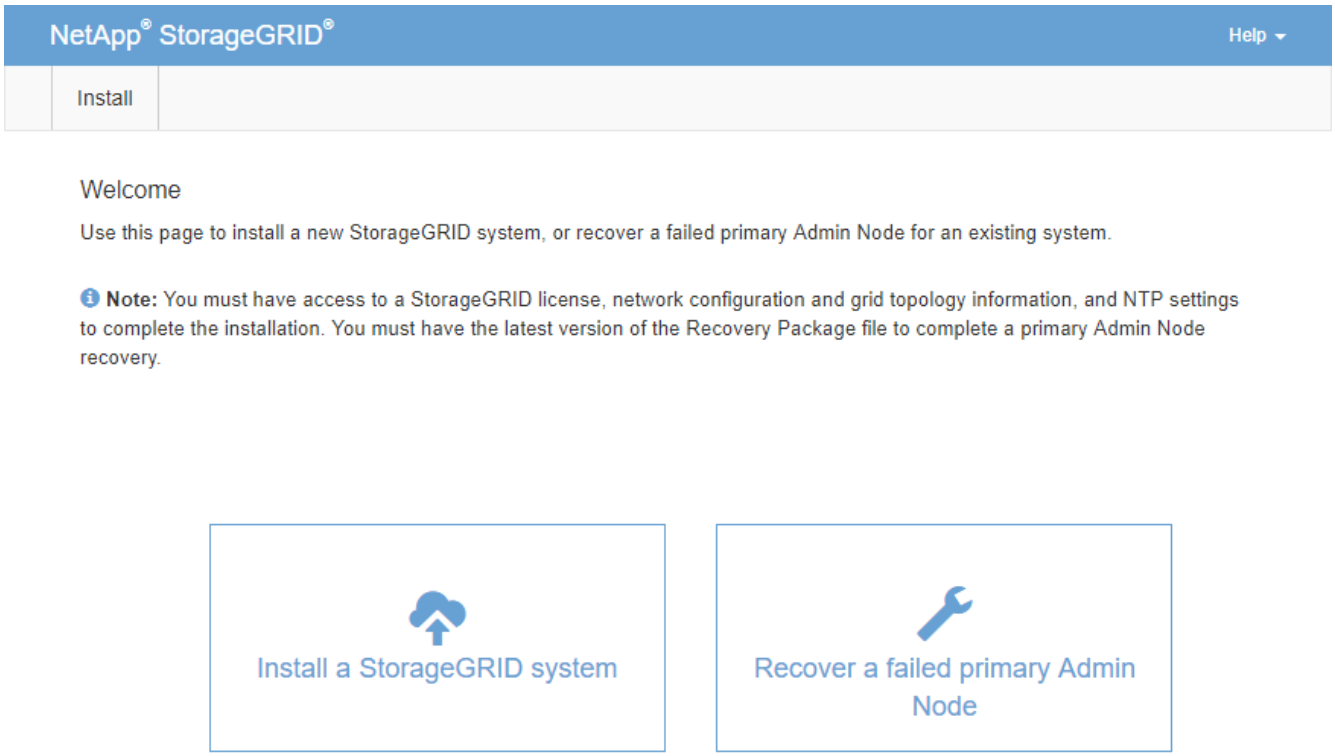
- Per i nodi di amministrazione primari ospitati su macchine virtuali, la macchina virtuale deve essere implementata, accesa e inizializzata.
- Per i nodi di amministrazione primari ospitati su un'appliance di servizi, l'appliance è stata sostituita e il software è stato installato. Consultare la guida all'installazione dell'appliance.

  Appliance di servizi SG100 e SG1000

- È necessario disporre dell'ultimo backup del file del pacchetto di ripristino (`sgws-recovery-package-id-revision.zip`).
- È necessario disporre della passphrase di provisioning.

Fasi

1. Aprire il browser Web e accedere a. `https://primary_admin_node_ip`.



2. Fare clic su **Recover a failed primary Admin Node** (Ripristina nodo amministratore primario guasto
3. Caricare il backup più recente del pacchetto di ripristino:
   a. Fare clic su **Sfoglia**.
   b. Individuare il file del pacchetto di ripristino più recente per il sistema StorageGRID in uso e fare clic su **Apri**.
4. Inserire la passphrase di provisioning.
5. Fare clic su **Start Recovery** (Avvia ripristino).

   Viene avviato il processo di ripristino. Grid Manager potrebbe non essere disponibile per alcuni minuti all'avvio dei servizi richiesti. Al termine del ripristino, viene visualizzata la pagina di accesso.

6. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e il trust della parte di base per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinita, aggiornare (o eliminare e ricreare) il trust della parte di base del nodo in Active Directory Federation Services (ad FS). Utilizzare il nuovo certificato server predefinito generato durante il processo di ripristino del nodo di amministrazione.

   > Per configurare un trust di parte, consultare le istruzioni per l'amministrazione di StorageGRID. Per accedere al certificato del server predefinito, accedere alla shell dei comandi del nodo di amministrazione. Accedere alla `/var/local/mgmt-api` e selezionare `server.crt` file.

7. Determinare se è necessario applicare una correzione rapida.
   a. Accedere a Grid Manager utilizzando un browser web supportato.
   b. Selezionare **NODI**.
   c. Dall'elenco a sinistra, selezionare il nodo di amministrazione principale.
   d. Nella scheda Overview (Panoramica), annotare la versione visualizzata nel campo **Software Version** (versione software).
   e. Selezionare qualsiasi altro nodo della griglia.
   f. Nella scheda Overview (Panoramica), annotare la versione visualizzata nel campo **Software Version** (versione software).
      - Se le versioni visualizzate nei campi **versione software** sono identiche, non è necessario applicare una correzione rapida.
      - Se le versioni visualizzate nei campi **versione software** sono diverse, è necessario applicare una correzione rapida per aggiornare il nodo amministratore primario recuperato alla stessa versione.

Informazioni correlate

Amministrare StorageGRID

Procedura di hotfix StorageGRID

Ripristinare il log di audit sul nodo di amministrazione primario recuperato

Se è stato possibile conservare il registro di controllo dal nodo di amministrazione primario guasto, è possibile copiarlo nel nodo di amministrazione primario che si sta ripristinando.

- Il nodo Admin recuperato deve essere installato e in esecuzione.
- È necessario aver copiato i registri di controllo in un'altra posizione dopo l'errore del nodo di amministrazione originale.

In caso di errore di un nodo amministratore, i registri di controllo salvati in quel nodo amministratore potrebbero andare persi. Potrebbe essere possibile conservare i dati in caso di perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e ripristinando questi registri di controllo nel nodo di amministrazione ripristinato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se l'implementazione ha più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione, poiché i registri di controllo vengono replicati in tutti i nodi di amministrazione.

Se è presente un solo nodo amministratore e non è possibile copiare il registro di controllo dal nodo guasto, il nodo amministratore recuperato inizia a registrare gli eventi nel registro di controllo come se l'installazione fosse nuova.

Per ripristinare la funzionalità di registrazione, è necessario ripristinare un nodo amministratore il prima possibile.

> Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:
>
> - È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
> - È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.
>
> Vedere Configurare i messaggi di audit e le destinazioni dei log per ulteriori informazioni.

Fasi

1. Accedere al nodo di amministrazione recuperato:

   a. Immettere il seguente comando: `ssh admin@recovery_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. `#`.

2. Controllare quali file di audit sono stati conservati: `cd /var/local/audit/export`

3. Copiare i file di log di controllo conservati nel nodo di amministrazione recuperato: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Quando richiesto, inserire la password per admin.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.

5. Aggiornare le impostazioni di utente e gruppo dei file di log di controllo sul nodo di amministrazione recuperato: `chown ams-user:bycast *`

6. Disconnettersi come root: `exit`

È inoltre necessario ripristinare qualsiasi accesso client preesistente alla condivisione di controllo. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

Amministrare StorageGRID

Ripristinare il mittente preferito sul nodo di amministrazione primario recuperato

Se il nodo amministratore primario che si sta ripristinando è attualmente impostato come mittente preferito di notifiche di avviso, notifiche di allarme e messaggi AutoSupport, è necessario riconfigurare questa impostazione.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Il nodo Admin recuperato deve essere installato e in esecuzione.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Opzioni di visualizzazione**.
2. Selezionare il nodo di amministrazione recuperato dall'elenco a discesa **Preferred Sender** (mittente preferito).
3. Fare clic su **Applica modifiche**.

Informazioni correlate

Amministrare StorageGRID

Ripristinare il database Admin Node durante il ripristino del nodo Admin primario

Se si desidera conservare le informazioni cronologiche relative ad attributi, allarmi e avvisi su un nodo di amministrazione primario che ha avuto esito negativo, è possibile ripristinare il database del nodo di amministrazione. È possibile ripristinare questo database solo se il sistema StorageGRID include un altro nodo amministratore.

- Il nodo Admin recuperato deve essere installato e in esecuzione.
- Il sistema StorageGRID deve includere almeno due nodi di amministrazione.
- È necessario disporre di `Passwords.txt` file.
- È necessario disporre della passphrase di provisioning.

In caso di errore di un nodo amministratore, le informazioni storiche memorizzate nel database del nodo amministratore andranno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Cronologia degli allarmi
- Dati storici degli attributi, utilizzati nei grafici e nei report di testo disponibili nella pagina **SUPPORTO Strumenti topologia griglia**.

Quando si ripristina un nodo amministratore, il processo di installazione del software crea un database Admin Node vuoto sul nodo recuperato. Tuttavia, il nuovo database include solo le informazioni relative ai server e ai servizi attualmente presenti nel sistema o aggiunti successivamente.

Se è stato ripristinato un nodo di amministrazione primario e il sistema StorageGRID dispone di un altro nodo di amministrazione, è possibile ripristinare le informazioni storiche copiando il database del nodo di amministrazione da un nodo di amministrazione non primario (il *nodo di amministrazione di origine*) al nodo di amministrazione primario recuperato. Se il sistema dispone solo di un nodo di amministrazione primario, non è possibile ripristinare il database del nodo di amministrazione.

> La copia del database Admin Node potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

1. Accedere al nodo di amministrazione di origine:
   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.
2. Dal nodo Admin di origine, arrestare il servizio MI: `service mi stop`
3. Dal nodo di amministrazione di origine, arrestare il servizio Management Application Program Interface (mgmt-api): `service mgmt-api stop`
4. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:
   a. Accedere al nodo di amministrazione recuperato:
      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.
   b. Arrestare il servizio MI: `service mi stop`
   c. Arrestare il servizio mgmt-api: `service mgmt-api stop`
   d. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`
   e. Inserire la password di accesso SSH elencata in `Passwords.txt` file.
   f. Copiare il database dal nodo Admin di origine al nodo Admin recuperato: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Quando richiesto, confermare che si desidera sovrascrivere il database MI nel nodo Admin recuperato.

      Il database e i relativi dati storici vengono copiati nel nodo di amministrazione recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato.

   h. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`
5. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristinare le metriche Prometheus durante il ripristino del nodo di amministrazione primario

Facoltativamente, è possibile conservare le metriche storiche gestite da Prometheus su un nodo di amministrazione primario che ha avuto problemi. Le metriche Prometheus possono essere ripristinate solo se il sistema StorageGRID include un altro nodo di amministrazione.

- Il nodo Admin recuperato deve essere installato e in esecuzione.
- Il sistema StorageGRID deve includere almeno due nodi di amministrazione.
- È necessario disporre di `Passwords.txt` file.
- È necessario disporre della passphrase di provisioning.

In caso di guasto di un nodo di amministrazione, le metriche mantenute nel database Prometheus sul nodo di amministrazione andranno perse. Quando si ripristina l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Una volta avviato il nodo di amministrazione recuperato, vengono registrate le metriche come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se è stato ripristinato un nodo di amministrazione primario e il sistema StorageGRID dispone di un altro nodo di amministrazione, è possibile ripristinare le metriche storiche copiando il database Prometheus da un nodo di amministrazione non primario (il *nodo di amministrazione di origine*) al nodo di amministrazione primario recuperato. Se il sistema dispone solo di un nodo di amministrazione primario, non è possibile ripristinare il database Prometheus.

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

1. Accedere al nodo di amministrazione di origine:
   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.
2. Dal nodo Admin di origine, arrestare il servizio Prometheus: `service prometheus stop`
3. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:
   a. Accedere al nodo di amministrazione recuperato:
      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.
   b. Interrompere il servizio Prometheus: `service prometheus stop`
   c. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`
   d. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

e. Copiare il database Prometheus dal nodo di amministrazione di origine al nodo di amministrazione recuperato: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Quando richiesto, premere **Invio** per confermare che si desidera distruggere il nuovo database Prometheus nel nodo di amministrazione recuperato.

   Il database Prometheus originale e i relativi dati storici vengono copiati nel nodo Admin recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.`service prometheus start`

Ripristino da guasti non primari del nodo di amministrazione

È necessario completare le seguenti attività per eseguire il ripristino da un errore non primario del nodo di amministrazione. Un nodo amministratore ospita il servizio CMN (Configuration Management Node) ed è noto come nodo amministratore primario. Sebbene sia possibile avere più nodi di amministrazione, ogni sistema StorageGRID include un solo nodo di amministrazione primario. Tutti gli altri nodi Admin non sono nodi Admin primari.

Informazioni correlate

Appliance di servizi SG100 e SG1000

Copia i registri di controllo dal nodo di amministrazione non primario non riuscito

Se è possibile copiare i registri di controllo dal nodo di amministrazione non riuscito, è necessario conservarli per mantenere il record dell'attività e dell'utilizzo del sistema della griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione non primario recuperato una volta attivato e in esecuzione.

Questa procedura copia i file di log di audit dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo griglia separato. Questi registri di controllo conservati possono quindi essere copiati nel nodo di amministrazione sostitutivo. I registri di controllo non vengono copiati automaticamente nel nuovo nodo di amministrazione.

A seconda del tipo di errore, potrebbe non essere possibile copiare i registri di controllo da un nodo di amministrazione non riuscito. Se l'implementazione ha un solo nodo di amministrazione, il nodo di amministrazione recuperato avvia la registrazione degli eventi nel registro di controllo in un nuovo file vuoto e i dati precedentemente registrati vengono persi. Se l'implementazione include più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione.

> Se i registri di controllo non sono ora accessibili sul nodo di amministrazione guasto, potrebbe essere possibile accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

1. Se possibile, accedere al nodo Admin non riuscito. In caso contrario, accedere al nodo di amministrazione

primario o a un altro nodo di amministrazione, se disponibile.

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. `#`.

2. Arrestare il servizio AMS per impedire la creazione di un nuovo file di log:`service ams stop`
3. Rinominare il file audit.log in modo che non sovrascriva il file esistente quando lo si copia nel nodo di amministrazione recuperato.

   Rinominare il file audit.log con un nome di file univoco numerato, ad esempio yyyy-mm-dd.txt.1. Ad esempio, è possibile rinominare il file audit.log in 2015-10-25.txt.1`cd /var/local/audit/export/`

4. Riavviare il servizio AMS: `service ams start`
5. Creare la directory per copiare tutti i file di log dell'audit in una posizione temporanea su un nodo griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.

6. Copia tutti i file di log di audit: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Quando richiesto, inserire la password per admin.

7. Disconnettersi come root: `exit`

Sostituire nodo amministratore non primario

Per ripristinare un nodo di amministrazione non primario, è necessario sostituire l'hardware fisico o virtuale.

È possibile sostituire un nodo di amministrazione non primario guasto con un nodo di amministrazione non primario in esecuzione sulla stessa piattaforma oppure sostituire un nodo di amministrazione non primario in esecuzione su VMware o su un host Linux con un nodo di amministrazione non primario in hosting su un'appliance di servizi.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino del nodo Admin non primario.

Piattaforma sostitutiva	Procedura
VMware	Sostituire un nodo VMware
Linux	Sostituire un nodo Linux

Piattaforma sostitutiva	Procedura
Appliance di servizi SG100 e SG1000	Sostituire un'appliance di servizi
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per sostituire un nodo Linux.

Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario

Dopo aver sostituito un nodo Admin non primario, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Di cosa hai bisogno

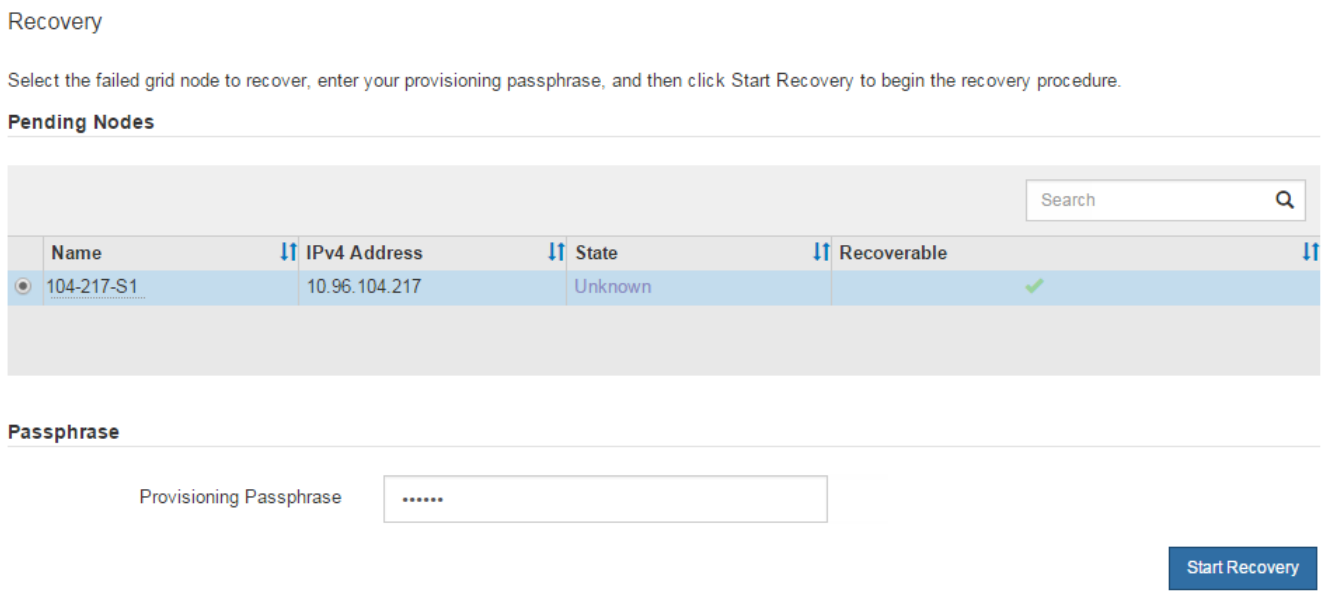
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Maintenance (manutenzione) o Root Access (accesso root).
- È necessario disporre della passphrase di provisioning.
- È necessario aver implementato e configurato il nodo sostitutivo.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE attività Recovery**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

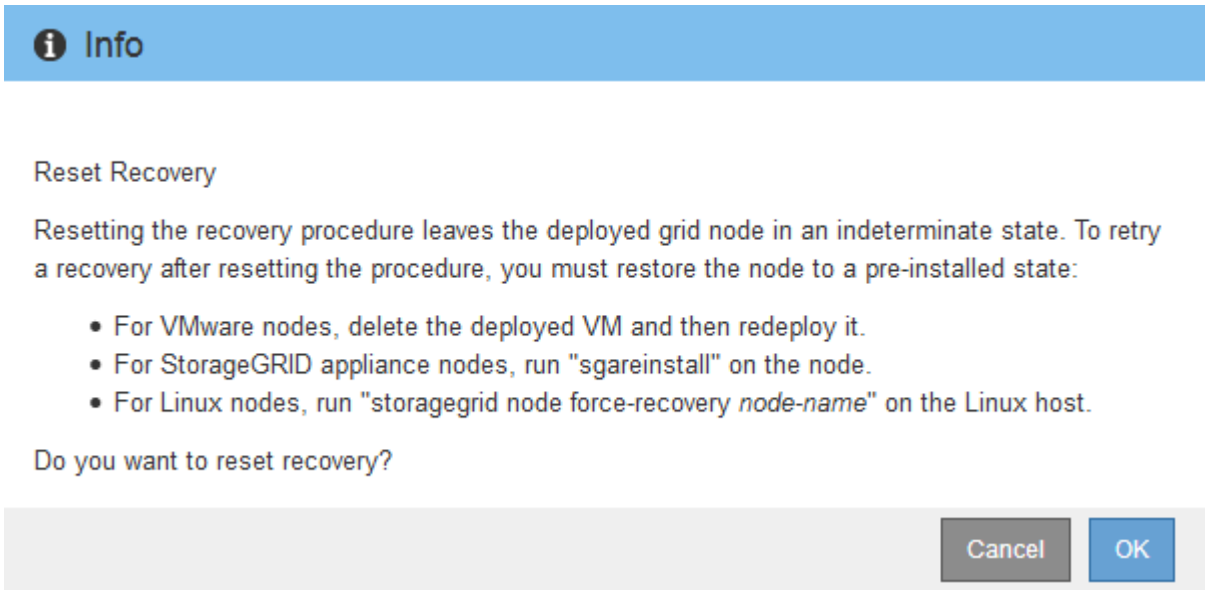
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

> Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo Info, che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery` *`node-name`*
- **Appliance**: Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo appliance a uno stato preinstallato eseguendo `sgareinstall` sul nodo.

6. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e il trust della parte di base per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinita, aggiornare (o eliminare e ricreare) il trust della parte di base del nodo in Active Directory Federation Services (ad FS). Utilizzare il nuovo certificato server predefinito generato durante il processo di ripristino del nodo di amministrazione.

> Per configurare un trust di parte, consultare le istruzioni per l'amministrazione di StorageGRID. Per accedere al certificato del server predefinito, accedere alla shell dei comandi del nodo di amministrazione. Accedere alla `/var/local/mgmt-api` e selezionare `server.crt` file.

Informazioni correlate

Amministrare StorageGRID

Preparazione dell'appliance per la reinstallazione (solo sostituzione della piattaforma)

Ripristina log di audit su nodo Admin non primario recuperato

Se è stato possibile conservare il registro di controllo dal nodo di amministrazione non primario non riuscito, in modo da conservare le informazioni del registro di controllo cronologico, è possibile copiarle nel nodo di amministrazione non primario che si sta ripristinando.

- Il nodo Admin recuperato deve essere installato e in esecuzione.
- È necessario aver copiato i registri di controllo in un'altra posizione dopo l'errore del nodo di amministrazione originale.

In caso di errore di un nodo amministratore, i registri di controllo salvati in quel nodo amministratore potrebbero andare persi. Potrebbe essere possibile conservare i dati in caso di perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e ripristinando questi registri di controllo nel nodo di amministrazione ripristinato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se l'implementazione ha più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione, poiché i registri di controllo vengono replicati in tutti i nodi di amministrazione.

Se è presente un solo nodo amministratore e non è possibile copiare il registro di controllo dal nodo guasto, il nodo amministratore recuperato inizia a registrare gli eventi nel registro di controllo come se l'installazione fosse nuova.

Per ripristinare la funzionalità di registrazione, è necessario ripristinare un nodo amministratore il prima possibile.

> Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:
>
> - È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
> - È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.
>
> Vedere Configurare i messaggi di audit e le destinazioni dei log per ulteriori informazioni.

Fasi

1. Accedere al nodo di amministrazione recuperato:

   a. Immettere il seguente comando:
   `ssh admin@recovery_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. `#`.

2. Controllare quali file di audit sono stati conservati:

   ```
   cd /var/local/audit/export
   ```

3. Copiare i file di log di controllo conservati nel nodo di amministrazione recuperato:

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   Quando richiesto, inserire la password per admin.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.
5. Aggiornare le impostazioni di utente e gruppo dei file di log di controllo sul nodo di amministrazione recuperato:

   ```
   chown ams-user:bycast *
   ```

6. Disconnettersi come root: `exit`

È inoltre necessario ripristinare qualsiasi accesso client preesistente alla condivisione di controllo. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

Amministrare StorageGRID

Ripristinare il mittente preferito sul nodo di amministrazione non primario recuperato

Se il nodo amministrativo non primario che si sta ripristinando è attualmente impostato come mittente preferito di notifiche di avviso, notifiche di allarme e messaggi AutoSupport, è necessario riconfigurare questa impostazione nel 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.
- Il nodo Admin recuperato deve essere installato e in esecuzione.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Opzioni di visualizzazione**.
2. Selezionare il nodo di amministrazione recuperato dall'elenco a discesa **Preferred Sender** (mittente preferito).
3. Fare clic su **Applica modifiche**.

Informazioni correlate

Amministrare StorageGRID

Ripristinare il database Admin Node durante il ripristino del nodo Admin non primario

Se si desidera conservare le informazioni cronologiche relative ad attributi, allarmi e avvisi su un nodo di amministrazione non primario che ha avuto esito negativo, è possibile ripristinare il database del nodo di amministrazione dal nodo di amministrazione primario.

- Il nodo Admin recuperato deve essere installato e in esecuzione.

- Il sistema StorageGRID deve includere almeno due nodi di amministrazione.
- È necessario disporre di `Passwords.txt` file.
- È necessario disporre della passphrase di provisioning.

In caso di errore di un nodo amministratore, le informazioni storiche memorizzate nel database del nodo amministratore andranno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Cronologia degli allarmi
- Dati storici degli attributi, utilizzati nei grafici e nei report di testo disponibili nella pagina **SUPPORTO Strumenti topologia griglia**.

Quando si ripristina un nodo amministratore, il processo di installazione del software crea un database Admin Node vuoto sul nodo recuperato. Tuttavia, il nuovo database include solo le informazioni relative ai server e ai servizi attualmente presenti nel sistema o aggiunti successivamente.

Se è stato ripristinato un nodo Admin non primario, è possibile ripristinare le informazioni storiche copiando il database del nodo Admin dal nodo Admin primario (il *nodo Admin di origine*) nel nodo recuperato.

> La copia del database Admin Node potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di origine.

1. Accedere al nodo di amministrazione di origine:
   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.
2. Eseguire il seguente comando dal nodo di amministrazione di origine. Quindi, inserire la passphrase di provisioning, se richiesto. `recover-access-points`
3. Dal nodo Admin di origine, arrestare il servizio MI: `service mi stop`
4. Dal nodo di amministrazione di origine, arrestare il servizio Management Application Program Interface (mgmt-api): `service mgmt-api stop`
5. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:
   a. Accedere al nodo di amministrazione recuperato:
      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.
   b. Arrestare il servizio MI: `service mi stop`
   c. Arrestare il servizio mgmt-api: `service mgmt-api stop`
   d. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`
   e. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

f. Copiare il database dal nodo Admin di origine al nodo Admin recuperato: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Quando richiesto, confermare che si desidera sovrascrivere il database MI nel nodo Admin recuperato.

   Il database e i relativi dati storici vengono copiati nel nodo di amministrazione recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato.

h. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

6. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristinare le metriche Prometheus durante il ripristino del nodo di amministrazione non primario

In alternativa, è possibile conservare le metriche storiche gestite da Prometheus su un nodo amministrativo non primario che ha avuto problemi.

- Il nodo Admin recuperato deve essere installato e in esecuzione.
- Il sistema StorageGRID deve includere almeno due nodi di amministrazione.
- È necessario disporre di `Passwords.txt` file.
- È necessario disporre della passphrase di provisioning.

In caso di guasto di un nodo di amministrazione, le metriche mantenute nel database Prometheus sul nodo di amministrazione andranno perse. Quando si ripristina l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Una volta avviato il nodo di amministrazione recuperato, vengono registrate le metriche come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se è stato ripristinato un nodo di amministrazione non primario, è possibile ripristinare le metriche storiche copiando il database Prometheus dal nodo di amministrazione primario (il *nodo di amministrazione di origine*) al nodo di amministrazione recuperato.

> La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

1. Accedere al nodo di amministrazione di origine:
   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.
2. Dal nodo Admin di origine, arrestare il servizio Prometheus: `service prometheus stop`
3. Completare i seguenti passaggi sul nodo di amministrazione ripristinato:
   a. Accedere al nodo di amministrazione recuperato:
      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.

b. Interrompere il servizio Prometheus: `service prometheus stop`

c. Aggiungere la chiave privata SSH all'agente SSH. Inserire:`ssh-add`

d. Inserire la password di accesso SSH elencata in `Passwords.txt` file.

e. Copiare il database Prometheus dal nodo di amministrazione di origine al nodo di amministrazione recuperato: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Quando richiesto, premere **Invio** per confermare che si desidera distruggere il nuovo database Prometheus nel nodo di amministrazione recuperato.

   Il database Prometheus originale e i relativi dati storici vengono copiati nel nodo Admin recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato. Viene visualizzato il seguente stato:

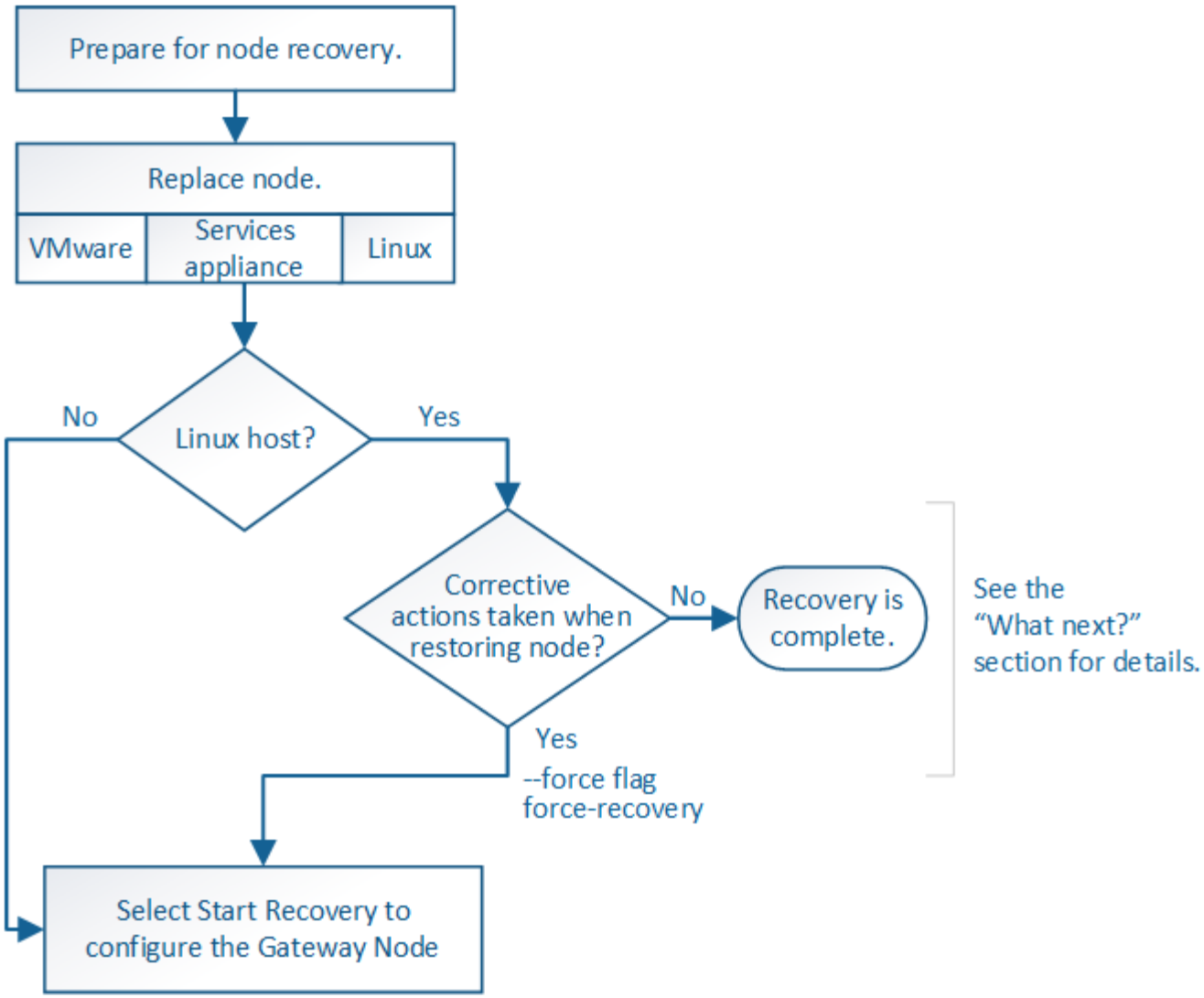
Database clonato, avvio dei servizi

a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:`ssh-add -D`

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.`service prometheus start`

Ripristino da guasti del nodo gateway

È necessario completare una sequenza di attività nell'ordine esatto per eseguire il ripristino in caso di guasto di un nodo gateway.



Informazioni correlate

Appliance di servizi SG100 e SG1000

Sostituire il nodo gateway

È possibile sostituire un nodo gateway guasto con un nodo gateway in esecuzione sullo stesso hardware fisico o virtuale oppure sostituire un nodo gateway in esecuzione su VMware o su un host Linux con un nodo gateway in hosting su un'appliance di servizi.

La procedura di sostituzione del nodo da seguire dipende dalla piattaforma utilizzata dal nodo sostitutivo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino del nodo gateway.

Piattaforma sostitutiva	Procedura
VMware	Sostituire un nodo VMware
Linux	Sostituire un nodo Linux

Piattaforma sostitutiva	Procedura
Appliance di servizi SG100 e SG1000	Sostituire un'appliance di servizi
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per sostituire un nodo Linux.

Selezionare Avvia ripristino per configurare il nodo gateway

Dopo aver sostituito un nodo gateway, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Di cosa hai bisogno

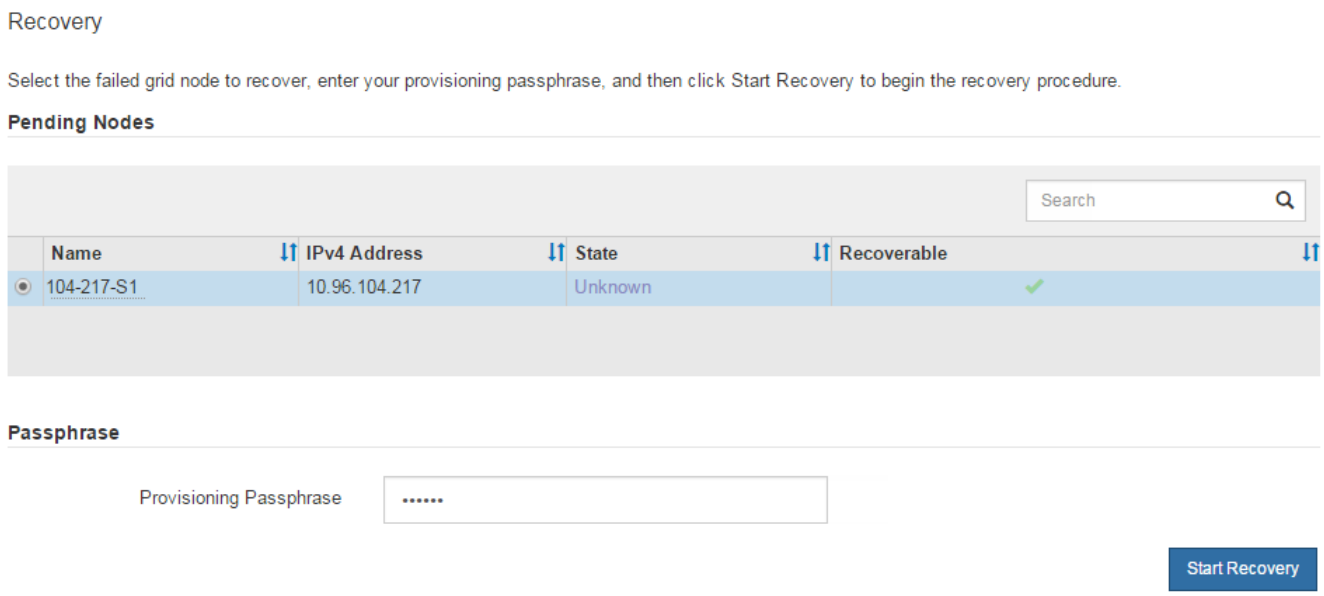
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Maintenance (manutenzione) o Root Access (accesso root).
- È necessario disporre della passphrase di provisioning.
- È necessario aver implementato e configurato il nodo sostitutivo.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE attività Recovery**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

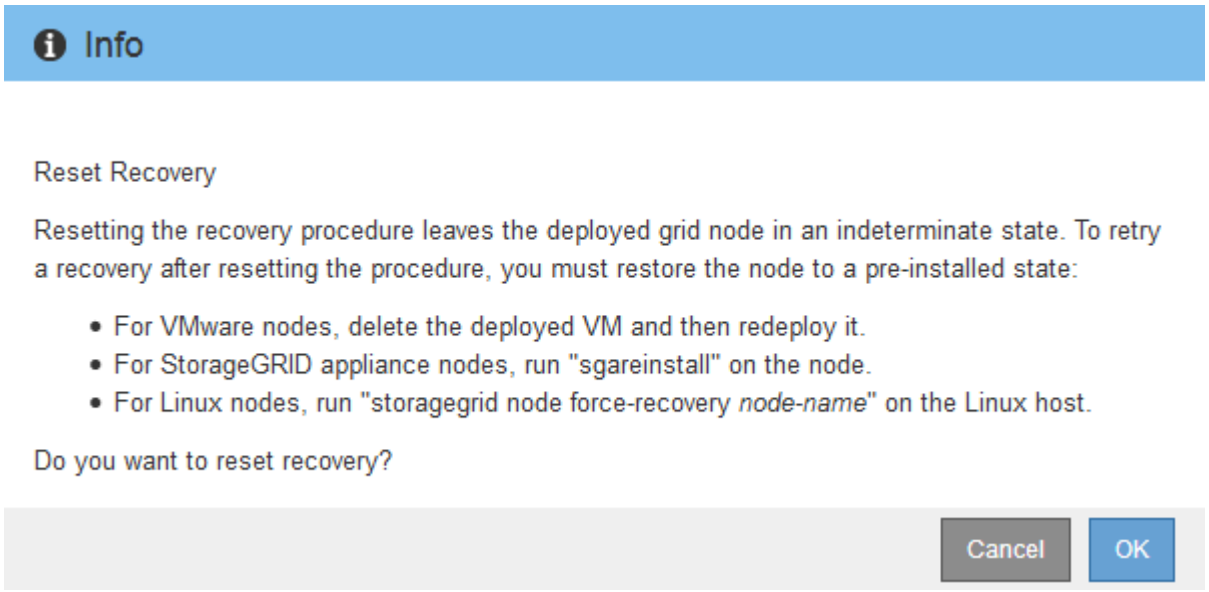
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

> Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo Info, che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

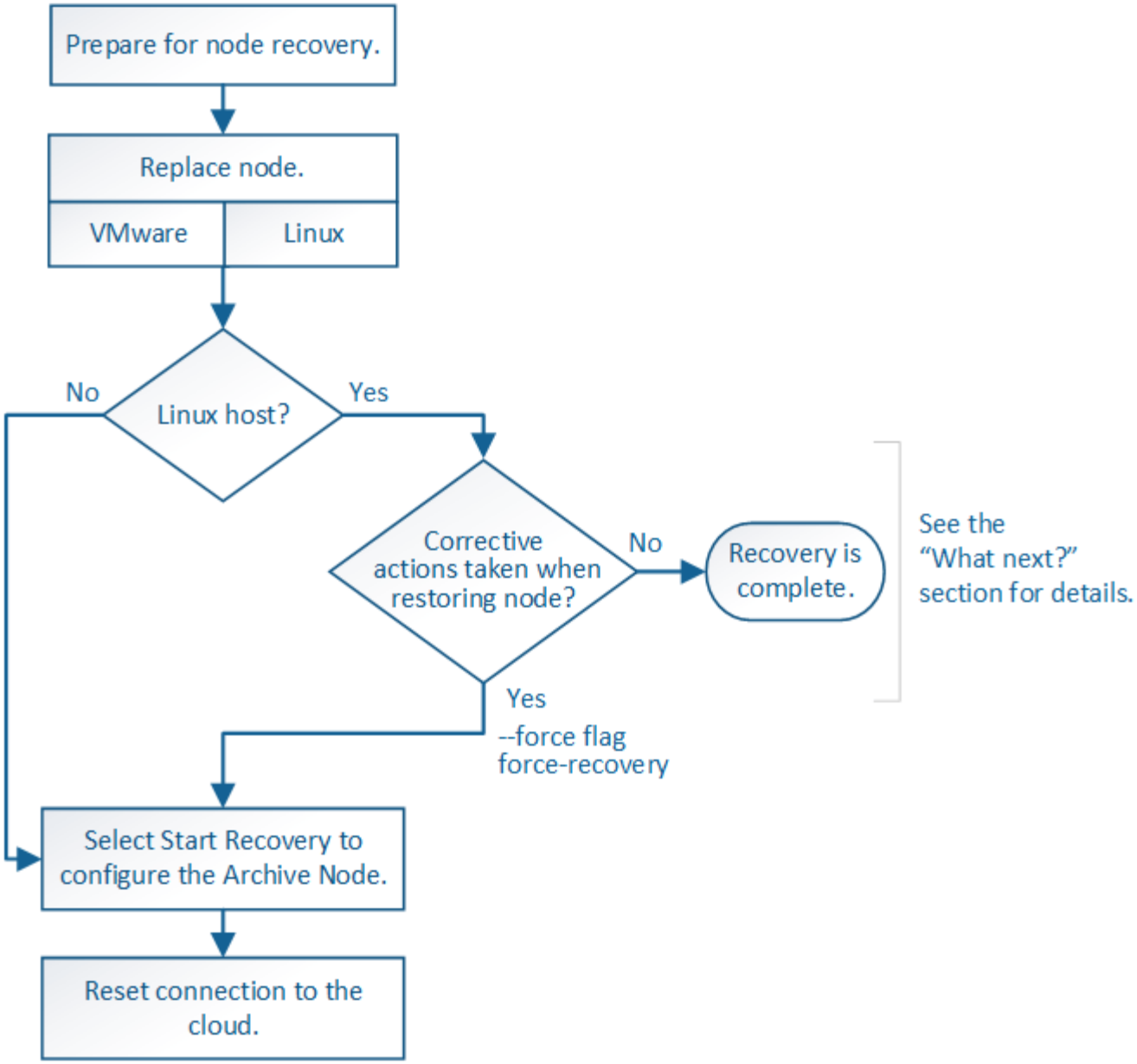
- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`
- **Appliance**: Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo appliance a uno stato preinstallato eseguendo `sgareinstall` sul nodo.

Informazioni correlate

Preparazione dell'appliance per la reinstallazione (solo sostituzione della piattaforma)

Ripristino da errori del nodo di archiviazione

È necessario completare una sequenza di attività nell'ordine esatto per eseguire il ripristino in caso di guasto di un nodo di archiviazione.



A proposito di questa attività

Il ripristino del nodo di archiviazione è interessato dai seguenti problemi:

- Se il criterio ILM è configurato per replicare una singola copia.

  In un sistema StorageGRID configurato per eseguire una singola copia di oggetti, un guasto al nodo di archiviazione potrebbe causare una perdita di dati irreversibile. Se si verifica un errore, tutti questi oggetti vengono persi; tuttavia, è necessario eseguire le procedure di ripristino per "ripulire" il sistema StorageGRID ed eliminare le informazioni sugli oggetti persi dal database.

- Se si verifica un errore del nodo di archiviazione durante il ripristino del nodo di storage.

  Se il nodo di archiviazione non riesce durante l'elaborazione di recuperi in blocco come parte di un ripristino del nodo di storage, È necessario ripetere la procedura per ripristinare le copie dei dati dell'oggetto nel nodo di storage dall'inizio per garantire che tutti i dati dell'oggetto recuperati dal nodo di archiviazione vengano ripristinati nel nodo di storage.

Sostituisci nodo archivio

Per ripristinare un nodo di archiviazione, è necessario sostituirlo.

Selezionare la procedura di sostituzione del nodo per la piattaforma. I passaggi per sostituire un nodo sono gli stessi per tutti i tipi di nodi griglia.

Piattaforma	Procedura
VMware	Sostituire un nodo VMware
Linux	Sostituire un nodo Linux
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per sostituire un nodo Linux.

Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di archiviazione

Dopo aver sostituito un nodo di archiviazione, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Di cosa hai bisogno

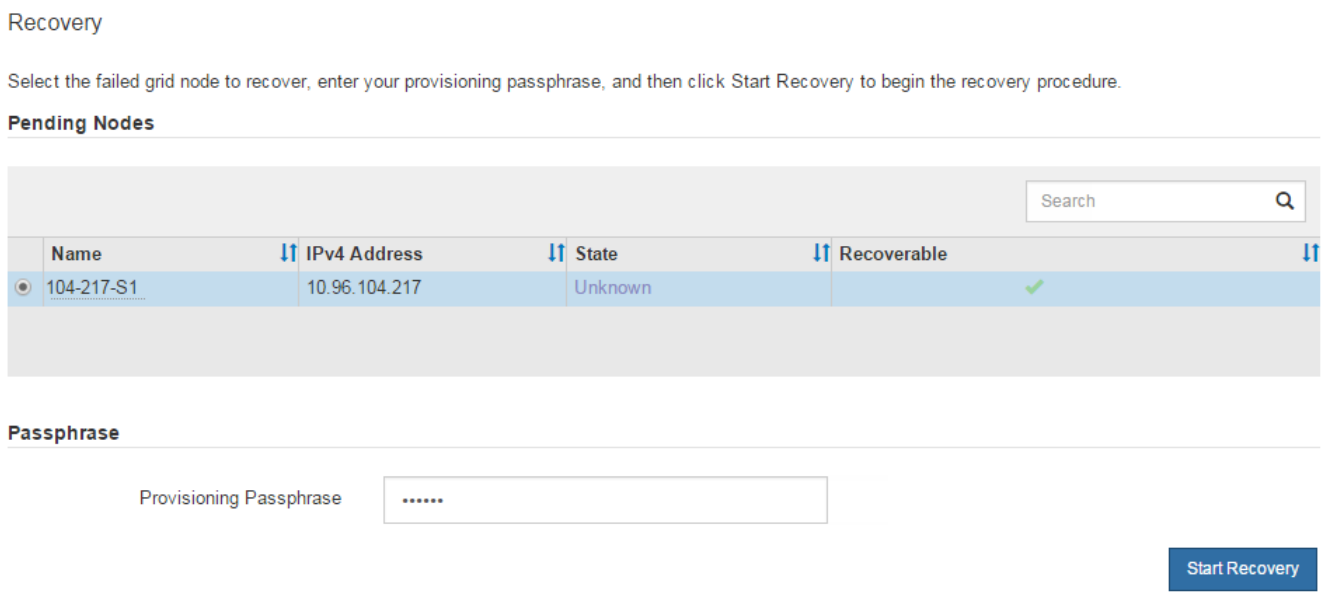
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Maintenance (manutenzione) o Root Access (accesso root).
- È necessario disporre della passphrase di provisioning.
- È necessario aver implementato e configurato il nodo sostitutivo.

Fasi

1. In Grid Manager, selezionare **MANUTENZIONE attività Recovery**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

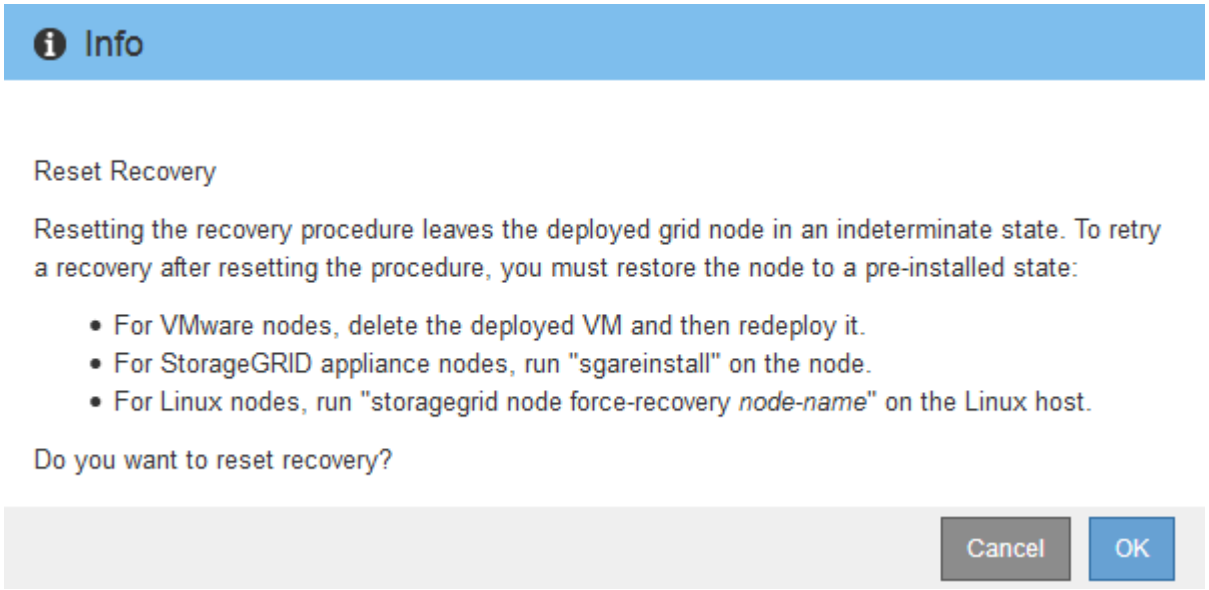
   I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Immettere la **Provisioning Passphrase**.
4. Fare clic su **Start Recovery** (Avvia ripristino).



5. Monitorare l'avanzamento del ripristino nella tabella Recovery Grid Node (nodo griglia di ripristino).

> Durante l'esecuzione della procedura di ripristino, fare clic su **Reset** (Ripristina) per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo Info, che indica che il nodo viene lasciato in uno stato indeterminato se si ripristina la procedura.



Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware**: Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux**: Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`

Ripristinare la connessione del nodo di archiviazione al cloud

Dopo aver ripristinato un nodo di archiviazione che ha come destinazione il cloud tramite l'API S3, è necessario modificare le impostazioni di configurazione per ripristinare le connessioni. Un allarme ORSU (Outbound Replication Status) viene attivato se il nodo di archiviazione non è in grado di recuperare i dati dell'oggetto.

> Se il nodo di archiviazione si connette allo storage esterno tramite il middleware TSM, il nodo si ripristina automaticamente e non è necessario riconfigurare.

Di cosa hai bisogno

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

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare **Archive Node ARC Target**.
3. Modificare il campo **Access Key** inserendo un valore errato e fare clic su **Apply Changes** (Applica modifiche).
4. Modificare il campo **Access Key** inserendo il valore corretto e fare clic su **Apply Changes** (Applica modifiche).

Tutti i tipi di nodi grid: Sostituire il nodo VMware

Quando si ripristina un nodo StorageGRID guasto ospitato su VMware, è necessario rimuovere il nodo guasto e implementare un nodo di ripristino.

Di cosa hai bisogno

È necessario aver determinato che la macchina virtuale non può essere ripristinata e deve essere sostituita.

A proposito di questa attività

VMware vSphere Web Client viene utilizzato per rimuovere prima la macchina virtuale associata al nodo Grid guasto. Quindi, è possibile implementare una nuova macchina virtuale.

Questa procedura è solo una fase del processo di ripristino del nodo grid. La procedura di rimozione e implementazione dei nodi è la stessa per tutti i nodi VMware, inclusi i nodi Admin, i nodi Storage, i nodi Gateway e i nodi Archive.

Fasi

1. Accedere a VMware vSphere Web Client.
2. Passare alla macchina virtuale del nodo della griglia guasto.
3. Prendere nota di tutte le informazioni necessarie per implementare il nodo di ripristino.
   a. Fare clic con il pulsante destro del mouse sulla macchina virtuale, selezionare la scheda **Edit Settings** (Modifica impostazioni) e annotare le impostazioni in uso.
   b. Selezionare la scheda **vApp Options** per visualizzare e registrare le impostazioni di rete del nodo della griglia.
4. Se il nodo Grid guasto è un nodo Storage, determinare se uno dei dischi rigidi virtuali utilizzati per lo storage dei dati non è danneggiato e conservarlo per il ricollegamento al nodo Grid ripristinato.

5. Spegnere la macchina virtuale.
6. Selezionare **azioni** > **tutte le azioni vCenter** > **Elimina dal disco** per eliminare la macchina virtuale.
7. Implementare una nuova macchina virtuale come nodo sostitutivo e connetterla a una o più reti StorageGRID.

   Quando si implementa il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.

   > Dopo aver implementato il nuovo nodo, è possibile aggiungere nuovi dischi virtuali in base ai requisiti di storage, ricollegare eventuali dischi rigidi virtuali conservati dal nodo Grid guasto precedentemente rimosso o da entrambi.

   Per istruzioni:

   Installare VMware > implementazione di un nodo StorageGRID come macchina virtuale

8. Completare la procedura di ripristino del nodo, in base al tipo di nodo che si sta ripristinando.

Tipo di nodo	Passare a.
Nodo amministratore primario	Configurare il nodo amministrativo primario sostitutivo
Nodo amministrativo non primario	Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario
Nodo gateway	Selezionare Avvia ripristino per configurare il nodo gateway
Nodo di storage	Selezionare Avvia ripristino per configurare il nodo di storage
Nodo di archiviazione	Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di archiviazione

Tutti i tipi di nodi grid: Sostituire il nodo Linux

Se un errore richiede l'implementazione di uno o più nuovi host fisici o virtuali o la reinstallazione di Linux su un host esistente, è necessario implementare e configurare l'host sostitutivo prima di poter ripristinare il nodo grid. Questa procedura è una fase del processo di ripristino del nodo grid per tutti i tipi di nodi grid.

"Linux" si riferisce a una distribuzione Red Hat® Enterprise Linux®, Ubuntu®, CentOS o Debian®. Utilizza NetApp Interoperability Matrix Tool per ottenere un elenco delle versioni supportate.

Questa procedura viene eseguita solo come una fase del processo di ripristino dei nodi di storage basati su software, dei nodi di amministrazione primari o non primari, dei nodi gateway o dei nodi di archivio. I passaggi sono identici indipendentemente dal tipo di nodo di griglia che si sta ripristinando.

Se su un host Linux fisico o virtuale sono ospitati più nodi grid, è possibile ripristinare i nodi grid in qualsiasi ordine. Tuttavia, il ripristino di un nodo di amministrazione primario, se presente, impedisce il blocco del ripristino di altri nodi della griglia quando tentano di contattare il nodo di amministrazione primario per la

registrazione per il ripristino.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Implementare nuovi host Linux

Con alcune eccezioni, è possibile preparare i nuovi host come durante il processo di installazione iniziale.

Per implementare host Linux fisici o virtuali nuovi o reinstallati, seguire la procedura per la preparazione degli host nelle istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso.

Questa procedura include i passaggi per eseguire le seguenti attività:

1. Installare Linux.
2. Configurare la rete host.
3. Configurare lo storage host.
4. Installare il motore del container.
5. Installare il servizio host StorageGRID.

> Interrompere il processo dopo aver completato l'attività "Installazione del servizio host StorageGRID" nelle istruzioni di installazione. Non avviare l'attività "Deploying grid nodes".

Durante l'esecuzione di questi passaggi, prendere nota delle seguenti importanti linee guida:

- Assicurarsi di utilizzare gli stessi nomi di interfaccia host utilizzati sull'host originale.
- Se si utilizza lo storage condiviso per supportare i nodi StorageGRID o se alcuni o tutti i dischi o gli SSD sono stati spostati dai nodi guasti ai nodi sostitutivi, è necessario ristabilire le stesse mappature dello storage presenti sull'host originale. Ad esempio, se sono stati utilizzati WWID e alias in `/etc/multipath.conf` Come consigliato nelle istruzioni di installazione, assicurarsi di utilizzare le stesse coppie alias/WWID in `/etc/multipath.conf` sull'host sostitutivo.
- Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verificare che il volume non disponga di un criterio di tiering FabricPool attivato. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

> Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

Informazioni correlate

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Ripristinare i nodi della griglia nell'host

Per ripristinare un nodo Grid guasto in un nuovo host Linux, ripristinare il file di configurazione del nodo utilizzando i comandi appropriati.

Quando si esegue una nuova installazione, si crea un file di configurazione del nodo per ciascun nodo della griglia da installare su un host. Quando si ripristina un nodo della griglia su un host sostitutivo, il file di configurazione del nodo viene ripristinato o sostituito per eventuali nodi della griglia guasti.

Se sono stati conservati volumi di storage a blocchi dall'host precedente, potrebbe essere necessario eseguire ulteriori procedure di ripristino. I comandi di questa sezione consentono di determinare quali procedure aggiuntive sono necessarie.

Fasi

- Ripristinare e validare i nodi della griglia
- Avviare il servizio host StorageGRID
- Ripristinare i nodi che non si avviano normalmente

Ripristinare e validare i nodi della griglia

È necessario ripristinare i file di configurazione della griglia per eventuali nodi della griglia guasti, quindi validare i file di configurazione della griglia e risolvere eventuali errori.

A proposito di questa attività

È possibile importare qualsiasi nodo di griglia che dovrebbe essere presente sull'host, a condizione che sia `/var/local` il volume non è stato perso a causa del guasto dell'host precedente. Ad esempio, il `/var/local` Il volume potrebbe ancora esistere se si utilizza lo storage condiviso per i volumi di dati del sistema StorageGRID, come descritto nelle istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso. L'importazione del nodo ripristina il file di configurazione del nodo sull'host.

Se non è possibile importare nodi mancanti, è necessario ricreare i file di configurazione della griglia.

È quindi necessario convalidare il file di configurazione della griglia e risolvere eventuali problemi di rete o storage che potrebbero verificarsi prima di riavviare StorageGRID. Quando si crea nuovamente il file di configurazione per un nodo, è necessario utilizzare lo stesso nome per il nodo sostitutivo utilizzato per il nodo che si sta ripristinando.

Per ulteriori informazioni sulla posizione di, consultare le istruzioni di installazione di `/var/local` volume per un nodo.

Fasi

1. Nella riga di comando dell'host recuperato, elencare tutti i nodi della griglia StorageGRID attualmente configurati:`sudo storagegrid node list`

   Se non sono configurati nodi di griglia, non verrà generato alcun output. Se alcuni nodi della griglia sono configurati, l'output deve essere nel seguente formato:

   ```
   Name                Metadata-Volume
   ==================================================================
   dc1-adm1            /dev/mapper/sgws-adm1-var-local
   dc1-gw1             /dev/mapper/sgws-gw1-var-local
   dc1-sn1             /dev/mapper/sgws-sn1-var-local
   dc1-arc1            /dev/mapper/sgws-arc1-var-local
   ```

   Se alcuni o tutti i nodi della griglia che devono essere configurati sull'host non sono elencati, è necessario

ripristinare i nodi della griglia mancanti.

2. Per importare nodi griglia che hanno un `/var/local` volume:

   a. Eseguire il seguente comando per ciascun nodo da importare:`sudo storagegrid node import node-var-local-volume-path`

      Il `storagegrid node import` il comando ha esito positivo solo se il nodo di destinazione è stato chiuso correttamente sull'host su cui è stato eseguito l'ultima volta. In caso contrario, si verificherà un errore simile al seguente:

      `This node (node-name) appears to be owned by another host (UUID host-uuid).`

   `Use the --force flag if you are sure import is safe.`

   a. Se viene visualizzato un errore relativo al nodo di proprietà di un altro host, eseguire nuovamente il comando con `--force` contrassegno per completare l'importazione:`sudo storagegrid --force node import node-var-local-volume-path`

      > Tutti i nodi importati con `--force` flag richiederà ulteriori passaggi di ripristino prima che possano ricongiungersi alla griglia, come descritto in Cosa c'è di seguito: Se necessario, eseguire ulteriori passaggi di ripristino.

3. Per i nodi griglia che non dispongono di `/var/local` ricreare il file di configurazione del nodo per ripristinarlo nell'host.

   Seguire le linee guida in "Create node Configuration Files" (Crea file di configurazione del nodo) nelle istruzioni di installazione.

   > Quando si crea nuovamente il file di configurazione per un nodo, è necessario utilizzare lo stesso nome per il nodo sostitutivo utilizzato per il nodo che si sta ripristinando. Per le implementazioni Linux, assicurarsi che il nome del file di configurazione contenga il nome del nodo. Se possibile, utilizzare le stesse interfacce di rete, le mappature dei dispositivi a blocchi e gli stessi indirizzi IP. Questa procedura riduce al minimo la quantità di dati che devono essere copiati nel nodo durante il ripristino, il che potrebbe rendere il ripristino molto più rapido (in alcuni casi, minuti piuttosto che settimane).

   > Se si utilizzano nuovi dispositivi a blocchi (dispositivi che il nodo StorageGRID non ha utilizzato in precedenza) come valori per una qualsiasi delle variabili di configurazione che iniziano con `BLOCK_DEVICE_` quando si ricreano i file di configurazione per un nodo, attenersi a tutte le linee guida riportate in Correggere gli errori del dispositivo a blocchi mancanti.

4. Eseguire il seguente comando sull'host ripristinato per elencare tutti i nodi StorageGRID.

   `sudo storagegrid node list`

5. Convalidare il file di configurazione del nodo per ogni nodo della griglia il cui nome è stato visualizzato nell'output dell'elenco dei nodi StorageGRID:

   `sudo storagegrid node validate node-name`

Prima di avviare il servizio host StorageGRID, è necessario risolvere eventuali errori o avvisi. Le sezioni seguenti forniscono ulteriori dettagli sugli errori che potrebbero avere un significato speciale durante il ripristino.

Informazioni correlate

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Correggere gli errori di interfaccia di rete mancanti

Correggere gli errori di interfaccia di rete mancanti

Se la rete host non è configurata correttamente o se un nome viene scritto in modo errato, si verifica un errore quando StorageGRID controlla la mappatura specificata in `/etc/storagegrid/nodes/node-name.conf` file.

Potrebbe essere visualizzato un errore o un avviso corrispondente a questo modello:

`Checking configuration file `/etc/storagegrid/nodes/node-name.conf` per il nodo *node-name*...` `ERROR: node-name: GRID_NETWORK_TARGET = host-interface-name` *node-name*: L'interfaccia '*host-interface-name*' non esiste`

L'errore potrebbe essere segnalato per Grid Network, Admin Network o Client Network. Questo errore indica che `/etc/storagegrid/nodes/node-name.conf` Il file associa la rete StorageGRID indicata all'interfaccia host denominata `host-interface-name`, ma non esiste alcuna interfaccia con questo nome sull'host corrente.

Se viene visualizzato questo errore, verificare di aver completato la procedura descritta in Implementare nuovi host Linux. Utilizzare gli stessi nomi per tutte le interfacce host utilizzati sull'host originale.

Se non è possibile assegnare un nome alle interfacce host in modo che corrispondano al file di configurazione del nodo, è possibile modificare il file di configurazione del nodo e modificare il valore DI GRID_NETWORK_TARGET, ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET in modo che corrisponda a un'interfaccia host esistente.

Assicurarsi che l'interfaccia host fornisca l'accesso alla porta di rete fisica o alla VLAN appropriata e che l'interfaccia non faccia riferimento direttamente a un dispositivo di collegamento o di bridge. È necessario configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond sull'host oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).

Correggere gli errori del dispositivo a blocchi mancanti

Il sistema verifica che ciascun nodo recuperato sia mappato a un file speciale valido per il dispositivo a blocchi o a un softlink valido a un file speciale per il dispositivo a blocchi. Se StorageGRID rileva una mappatura non valida in `/etc/storagegrid/nodes/node-name.conf` file, viene visualizzato un errore di dispositivo a blocchi mancante.

Se si verifica un errore corrispondente a questo modello:

`Checking configuration file /etc/storagegrid/nodes/node-name.conf for node node-name... ERROR: node-name: BLOCK_DEVICE_PURPOSE = path-name` *nome-nodo*: *nome-percorso* non

esiste`

Significa che `/etc/storagegrid/nodes/node-name.conf` Esegue la mappatura del dispositivo a blocchi utilizzato da *node-name* A SCOPO con il nome percorso specificato nel file system Linux, ma non esiste un file speciale valido per il dispositivo a blocchi o un softlink a un file speciale per il dispositivo a blocchi in tale posizione.

Verificare di aver completato le operazioni descritte in Implementare nuovi host Linux. Utilizzare gli stessi nomi persistenti dei dispositivi per tutti i dispositivi a blocchi utilizzati sull'host originale.

Se non si riesce a ripristinare o ricreare il file speciale del dispositivo a blocchi mancante, è possibile allocare un nuovo dispositivo a blocchi della dimensione e della categoria di storage appropriate e modificare il file di configurazione del nodo per modificare il valore DI BLOCK_DEVICE_PURPOSE in modo che punti al nuovo file speciale del dispositivo a blocchi.

Determinare le dimensioni e la categoria di storage appropriate dalle tabelle nella sezione "Srequisiti di torage" delle istruzioni di installazione per il sistema operativo Linux in uso. Prima di procedere con la sostituzione del dispositivo a blocchi, consultare le raccomandazioni contenute in "Configuring host storage" (Configurazione dello storage host).

> Se è necessario fornire un nuovo dispositivo di storage a blocchi per qualsiasi variabile del file di configurazione che inizia con `BLOCK_DEVICE_` poiché il dispositivo a blocchi originale è stato perso con l'host guasto, assicurarsi che il nuovo dispositivo a blocchi non sia formattato prima di tentare ulteriori procedure di ripristino. Il nuovo dispositivo a blocchi non verrà formattato se si utilizza lo storage condiviso e si è creato un nuovo volume. In caso di dubbi, eseguire il seguente comando per tutti i nuovi file speciali del dispositivo di storage a blocchi.

ATTENZIONE:

Eseguire il seguente comando solo per i nuovi dispositivi di storage a blocchi. Non eseguire questo comando se si ritiene che lo storage a blocchi contenga ancora dati validi per il nodo da ripristinare, in quanto i dati sul dispositivo andranno persi.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Informazioni correlate

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Avviare il servizio host StorageGRID

Per avviare i nodi StorageGRID e assicurarsi che vengano riavviati dopo un riavvio dell'host, è necessario attivare e avviare il servizio host StorageGRID.

1. Eseguire i seguenti comandi su ciascun host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Eseguire il seguente comando per assicurarsi che l'implementazione stia procedendo:

   `sudo storagegrid node status node-name`

   Per qualsiasi nodo che restituisca uno stato di non in esecuzione o interrotto, eseguire il seguente comando:

   `sudo storagegrid node start node-name`

3. Se in precedenza è stato attivato e avviato il servizio host StorageGRID (o se non si è certi che il servizio sia stato attivato e avviato), eseguire anche il seguente comando:

   ```
   sudo systemctl reload-or-restart storagegrid
   ```

Ripristinare i nodi che non si avviano normalmente

Se un nodo StorageGRID non si ricongiungerà normalmente alla griglia e non verrà visualizzato come ripristinabile, potrebbe essere danneggiato. È possibile forzare il nodo in modalità di ripristino.

Per forzare il nodo in modalità di ripristino:

`sudo storagegrid node force-recovery node-name`

> Prima di eseguire questo comando, verificare che la configurazione di rete del nodo sia corretta; potrebbe non essere riuscito a riconnettersi alla griglia a causa di mappature dell'interfaccia di rete non corrette o di un gateway o indirizzo IP Grid Network non corretto.

> Dopo l'emissione di `storagegrid node force-recovery node-name` eseguire ulteriori operazioni di ripristino per *node-name*.

Informazioni correlate

Cosa c'è di seguito: Se necessario, eseguire ulteriori passaggi di ripristino

Cosa succederà dopo: Se necessario, eseguire ulteriori passaggi di ripristino

A seconda delle azioni specifiche intraprese per eseguire i nodi StorageGRID sull'host sostitutivo, potrebbe essere necessario eseguire ulteriori operazioni di ripristino per ciascun nodo.

Il ripristino del nodo è completo se non è stato necessario intraprendere alcuna azione correttiva durante la sostituzione dell'host Linux o il ripristino del nodo Grid guasto nel nuovo host.

Azioni correttive e passi successivi

Durante la sostituzione del nodo, potrebbe essere necessario intraprendere una delle seguenti azioni correttive:

- È stato necessario utilizzare `--force` flag per importare il nodo.

- Per qualsiasi `<PURPOSE>`, il valore di `BLOCK_DEVICE_<PURPOSE>` la variabile del file di configurazione si riferisce a un dispositivo a blocchi che non contiene gli stessi dati che ha fatto prima dell'errore dell'host.
- Hai emesso `storagegrid node force-recovery node-name` per il nodo.
- È stato aggiunto un nuovo dispositivo a blocchi.

Se è stata eseguita una di queste azioni correttive, è necessario eseguire ulteriori operazioni di ripristino.

Tipo di ripristino	Passo successivo
Nodo amministratore primario	Configurare il nodo amministrativo primario sostitutivo
Nodo amministrativo non primario	Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario
Nodo gateway	Selezionare Avvia ripristino per configurare il nodo gateway
Nodo di archiviazione	Selezionare Start Recovery (Avvia ripristino) per configurare il nodo di archiviazione
Nodo di storage (basato su software): • Se è stato necessario utilizzare `--force` contrassegno per importare il nodo o emesso `storagegrid node force-recovery node-name` • Se è stata eseguita una reinstallazione completa del nodo o se è stato necessario ripristinare /var/local	Selezionare Avvia ripristino per configurare il nodo di storage
Nodo di storage (basato su software): • Se è stato aggiunto un nuovo dispositivo a blocchi. • Se, per qualsiasi `<PURPOSE>`, il valore di `BLOCK_DEVICE_<PURPOSE>` la variabile del file di configurazione si riferisce a un dispositivo a blocchi che non contiene gli stessi dati che ha fatto prima dell'errore dell'host.	Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto

Sostituire il nodo guasto con l'appliance di servizi

È possibile utilizzare un'appliance di servizi SG100 o SG1000 per ripristinare un nodo gateway guasto, un nodo Admin non primario guasto o un nodo Admin primario guasto ospitato su VMware, un host Linux o un'appliance di servizi. Questa procedura è una fase della procedura di ripristino del nodo di rete.

Di cosa hai bisogno

- È necessario aver stabilito che è vera una delle seguenti situazioni:
  - Impossibile ripristinare la macchina virtuale che ospita il nodo.
  - L'host Linux fisico o virtuale per il nodo grid è guasto e deve essere sostituito.
  - L'appliance di servizi che ospita il nodo Grid deve essere sostituita.
- Assicurarsi che la versione del programma di installazione dell'appliance StorageGRID sul dispositivo di servizi corrisponda alla versione software del sistema StorageGRID, come descritto in Installazione e manutenzione dell'hardware per la verifica e l'aggiornamento della versione del programma di installazione dell'appliance StorageGRID.

  Appliance di servizi SG100 e SG1000

> Non implementare sia un'appliance SG100 che un'appliance di servizio SG1000 nello stesso sito. Potrebbero verificarsi performance imprevedibili.

A proposito di questa attività

È possibile utilizzare un'appliance di servizi SG100 o SG1000 per ripristinare un nodo di rete guasto nei seguenti casi:

- Il nodo guasto è stato ospitato su VMware o Linux (modifica della piattaforma)
- Il nodo guasto era ospitato su un'appliance di servizi (sostituzione della piattaforma)

Installare l'appliance di servizi (solo modifica della piattaforma)

Durante il ripristino di un nodo Grid guasto ospitato su VMware o su un host Linux e si utilizza un'appliance di servizi SG100 o SG1000 per il nodo sostitutivo, è necessario installare prima il nuovo hardware dell'appliance utilizzando lo stesso nome del nodo guasto.

È necessario disporre delle seguenti informazioni sul nodo guasto:

- **Node name** (Nome nodo): È necessario installare l'appliance di servizi utilizzando lo stesso nome di nodo del nodo guasto.
- **Indirizzi IP**: È possibile assegnare al dispositivo di servizi gli stessi indirizzi IP del nodo guasto, che è l'opzione preferita, oppure selezionare un nuovo indirizzo IP inutilizzato su ciascuna rete.

Eseguire questa procedura solo se si sta ripristinando un nodo guasto ospitato su VMware o Linux e lo si sta sostituendo con un nodo ospitato su un'appliance di servizi.

1. Seguire le istruzioni per l'installazione di una nuova appliance di servizi SG100 o SG1000.
2. Quando viene richiesto il nome di un nodo, utilizzare il nome del nodo guasto.

Informazioni correlate

Appliance di servizi SG100 e SG1000

Preparazione dell'appliance per la reinstallazione (solo sostituzione della piattaforma)

Durante il ripristino di un nodo Grid ospitato su un'appliance di servizi, è necessario preparare l'appliance per la reinstallazione del software StorageGRID.

Eseguire questa procedura solo se si sta sostituendo un nodo guasto ospitato su un'appliance di servizi. Non seguire questi passi se il nodo guasto era originariamente ospitato su un host VMware o Linux.

1. Accedere al nodo Grid guasto:

   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. `#`.

2. Preparare l'appliance per l'installazione del software StorageGRID. Inserire: `sgareinstall`

3. Quando viene richiesto di continuare, immettere: `y`

   L'apparecchio si riavvia e la sessione SSH termina. In genere, il programma di installazione dell'appliance StorageGRID richiede circa 5 minuti, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.

   L'appliance di servizi viene reimpostata e i dati sul nodo Grid non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale devono rimanere intatti; tuttavia, si consiglia di confermarli al termine della procedura.

   Dopo aver eseguito il `sgareinstall` Comando, tutti gli account, le password e le chiavi SSH forniti da StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avviare l'installazione del software sull'appliance di servizi

Per installare un nodo gateway o un nodo amministratore su un'appliance di servizi SG100 o SG1000, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance.

Di cosa hai bisogno

- L'appliance deve essere installata in un rack, collegata alla rete e accesa.
- I collegamenti di rete e gli indirizzi IP devono essere configurati per l'appliance mediante il programma di installazione dell'appliance StorageGRID.
- Se si installa un nodo gateway o un nodo amministratore non primario, si conosce l'indirizzo IP del nodo amministratore primario per la griglia StorageGRID.
- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID devono essere definite nell'elenco subnet della rete griglia sul nodo amministratore primario.

Per istruzioni su come completare queste attività prerequisite, consultare le istruzioni di installazione e manutenzione di un'appliance di servizi SG100 o SG1000.

- È necessario utilizzare un browser web supportato.
- È necessario conoscere uno degli indirizzi IP assegnati all'appliance. È possibile utilizzare l'indirizzo IP per Admin Network, Grid Network o Client Network.
- Se si installa un nodo amministrativo primario, sono disponibili i file di installazione di Ubuntu o Debian per

questa versione di StorageGRID.

> Una versione recente del software StorageGRID viene precaricata sull'appliance di servizi durante la produzione. Se la versione precaricata del software corrisponde alla versione utilizzata nella distribuzione di StorageGRID, non sono necessari i file di installazione.

A proposito di questa attività

Per installare il software StorageGRID su un'appliance di servizi SG100 o SG1000:

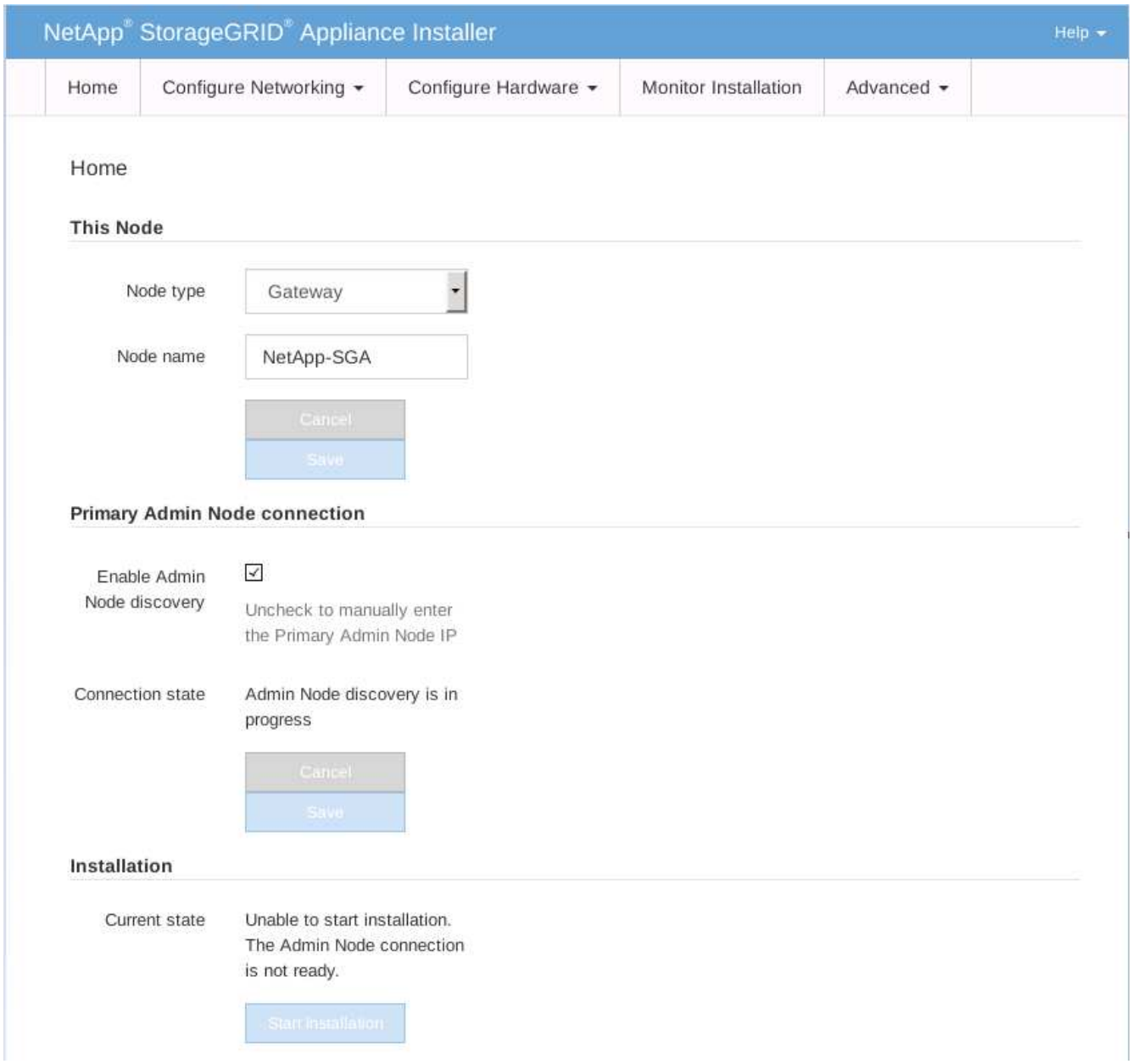
- Per un nodo amministrativo primario, specificare il nome del nodo e caricare i pacchetti software appropriati (se necessario).
- Per un nodo Admin non primario o un nodo gateway, specificare o confermare l'indirizzo IP del nodo Admin primario e il nome del nodo.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.
- Durante il processo, l'installazione viene interrotta. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo in sospeso come sostituzione del nodo guasto.
- Una volta configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Fasi

1. Aprire un browser e inserire uno degli indirizzi IP per l'appliance di servizi SG100 o SG1000.

   ```
   https://Controller_IP:8443
   ```

   Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.



2. Per installare un nodo di amministrazione primario:

   a. Nella sezione questo nodo, per **Node Type**, selezionare **Primary Admin**.

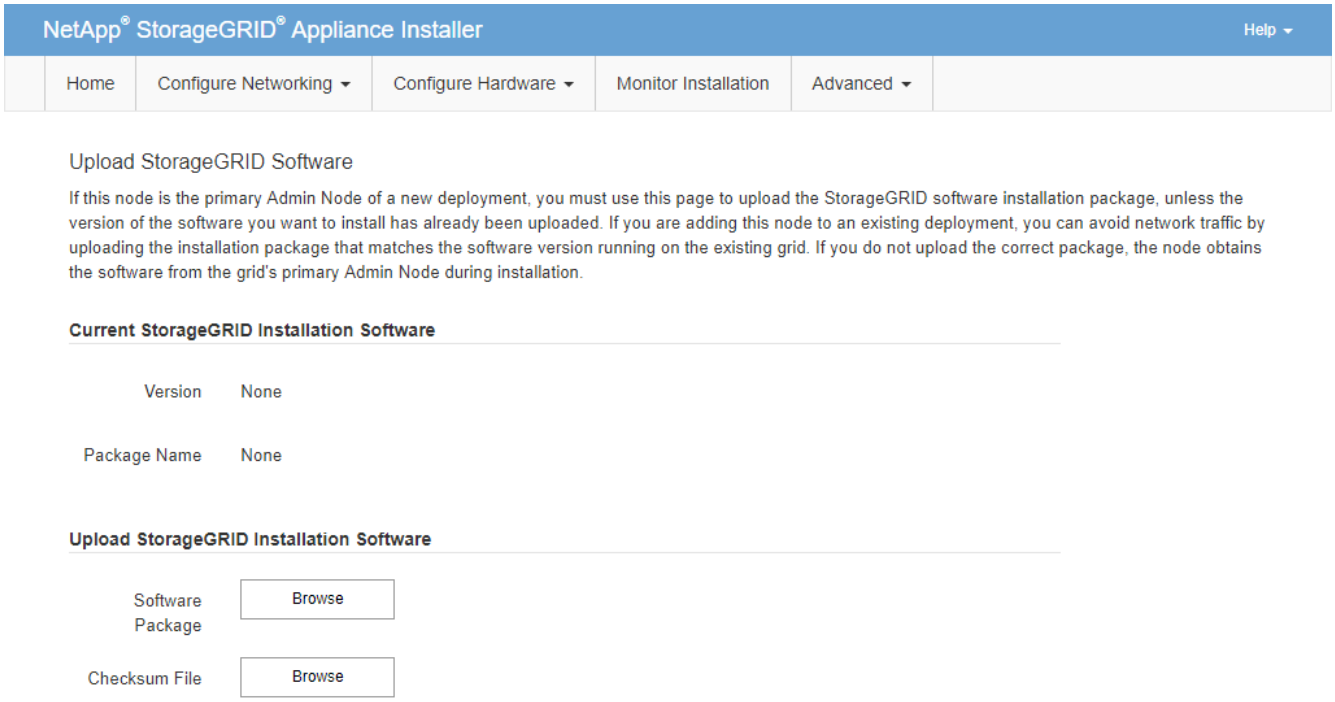
   b. Nel campo **Node Name** (Nome nodo), immettere lo stesso nome utilizzato per il nodo che si sta ripristinando e fare clic su **Save** (Salva).

   c. Nella sezione Installazione, controllare la versione del software elencata sotto Stato corrente

      Se la versione del software pronta per l'installazione è corretta, passare alla Fase di installazione.

   d. Per caricare una versione diversa del software, nel menu **Avanzate**, selezionare **carica software StorageGRID**.

      Viene visualizzata la pagina Caricamento del software StorageGRID.



a. Fare clic su **Browse** (Sfoglia) per caricare i file **pacchetto software** e **checksum file** per il software StorageGRID.

   I file vengono caricati automaticamente dopo averli selezionati.

b. Fare clic su **Home** per tornare alla home page del programma di installazione dell'appliance StorageGRID.

3. Per installare un nodo gateway o un nodo amministratore non primario:

   a. Nella sezione questo nodo, per **Node Type**, selezionare **Gateway** o **non-Primary Admin**, a seconda del tipo di nodo che si sta ripristinando.

   b. Nel campo **Node Name** (Nome nodo), immettere lo stesso nome utilizzato per il nodo che si sta ripristinando e fare clic su **Save** (Salva).

   c. Nella sezione Primary Admin Node Connection (connessione nodo amministratore primario), determinare se è necessario specificare l'indirizzo IP per il nodo amministratore primario.

      Il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, presupponendo che il nodo amministratore primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente nella stessa sottorete.

   d. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Immissione manuale dell'IP	a. Deselezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Fare clic su **Save** (Salva). d. Attendere che lo stato di connessione del nuovo indirizzo IP diventi "ready".

Opzione	Descrizione
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo **Enable Admin Node Discovery** (attiva rilevamento nodo amministratore). b. Dall'elenco degli indirizzi IP rilevati, selezionare il nodo di amministrazione principale per la griglia in cui verrà implementata l'appliance di servizi. c. Fare clic su **Save** (Salva). d. Attendere che lo stato di connessione del nuovo indirizzo IP diventi "ready".

4. nella sezione Installation (Installazione), verificare che lo stato corrente sia Ready to start installation of node name (Pronto per avviare l'installazione del nome del nodo) e che il pulsante **Start Installation** (Avvia installazione) sia attivato.

   Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di installazione e manutenzione dell'apparecchio.

5. Dalla home page del programma di installazione dell'appliance StorageGRID, fare clic su **Avvia installazione**.

   Lo stato corrente cambia in "Installation is in Progress" (Installazione in corso) e viene visualizzata la pagina Monitor Installation (Installazione monitor).

   > Per accedere manualmente alla pagina Installazione monitor, fare clic su **Installazione monitor** dalla barra dei menu.

Informazioni correlate

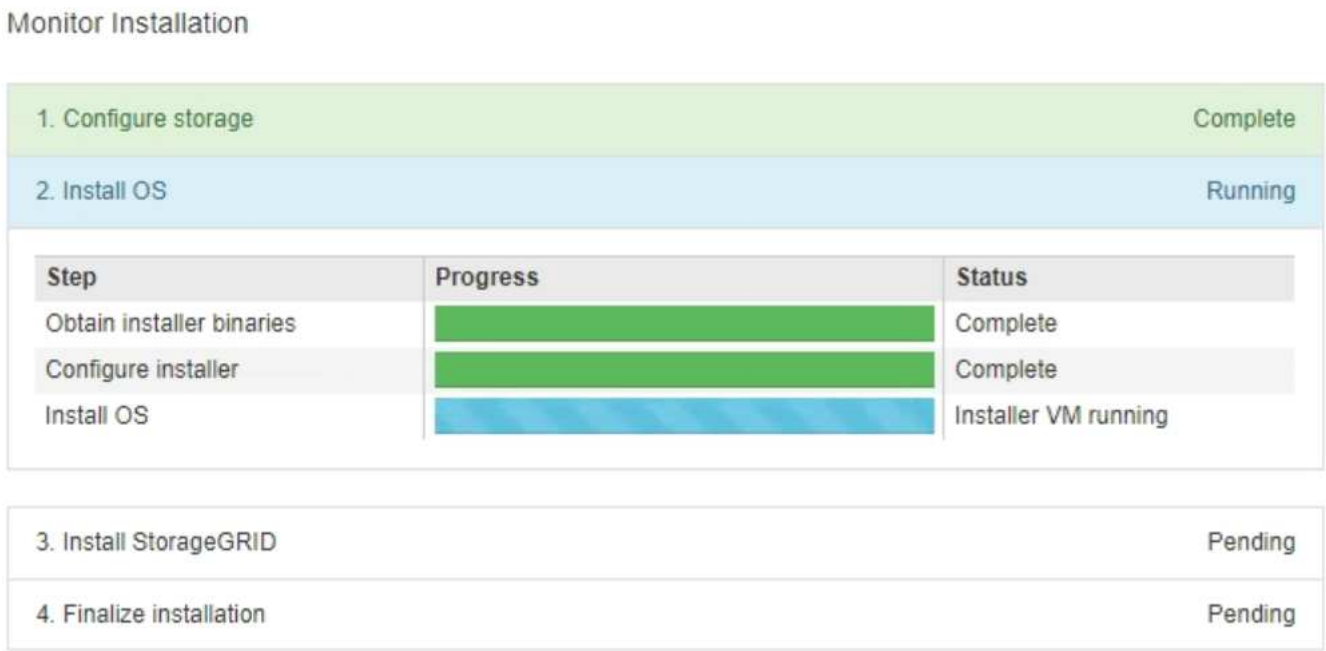
Appliance di servizi SG100 e SG1000

Monitorare l'installazione delle appliance di servizi

Il programma di installazione dell'appliance StorageGRID indica lo stato fino al completamento dell'installazione. Una volta completata l'installazione del software, l'appliance viene riavviata.

1. Per monitorare l'avanzamento dell'installazione, fare clic su **Monitor Installation** (Installazione monitor) nella barra dei menu.

   La pagina Monitor Installation (Installazione monitor) mostra lo stato di avanzamento dell'installazione.



La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.

> Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si esegue nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "Skipped".

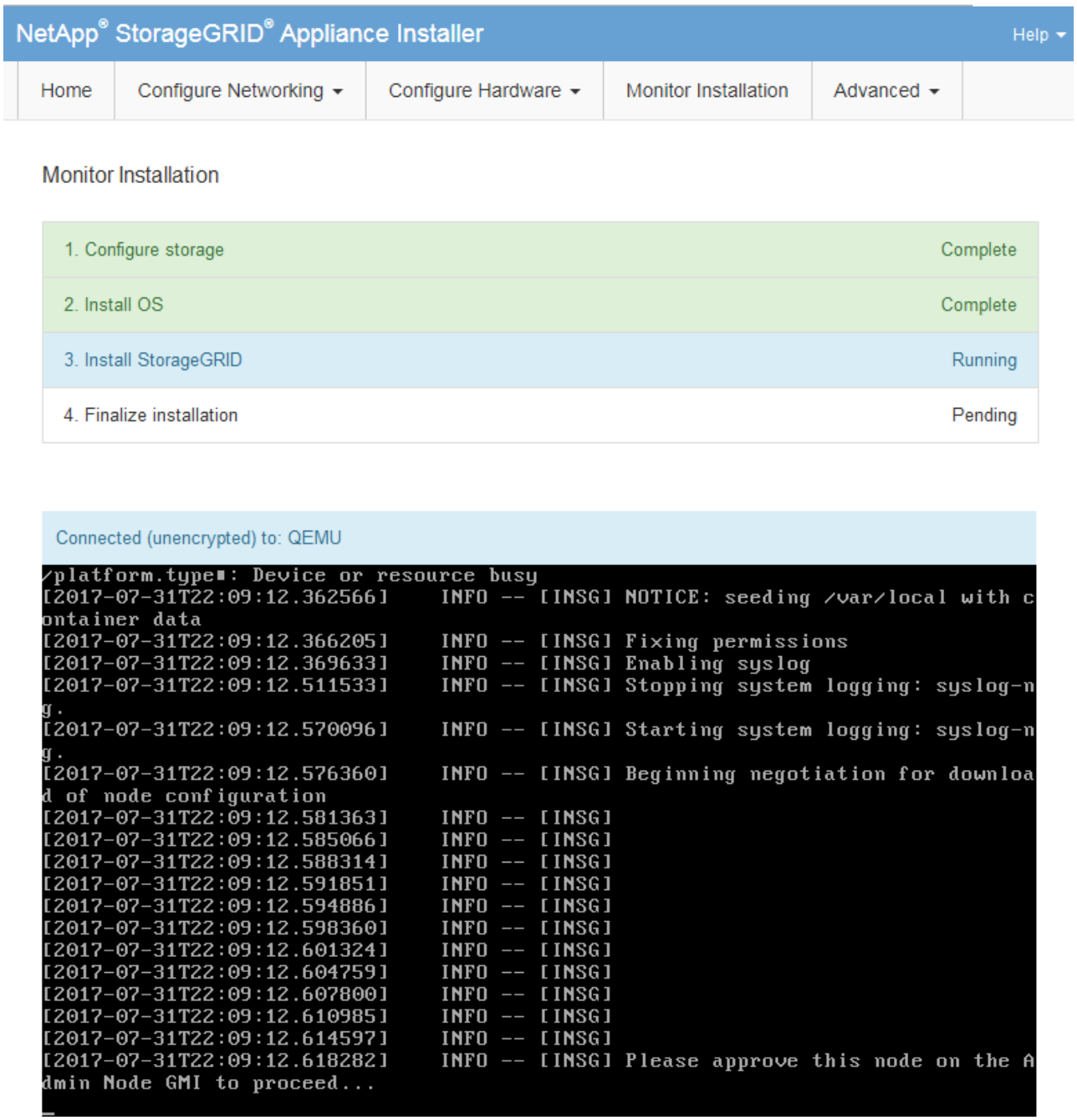
2. Esaminare i progressi delle prime due fasi dell'installazione.
   - **1. Configurare lo storage**

     Durante questa fase, il programma di installazione cancella qualsiasi configurazione esistente dai dischi e configura le impostazioni dell'host.

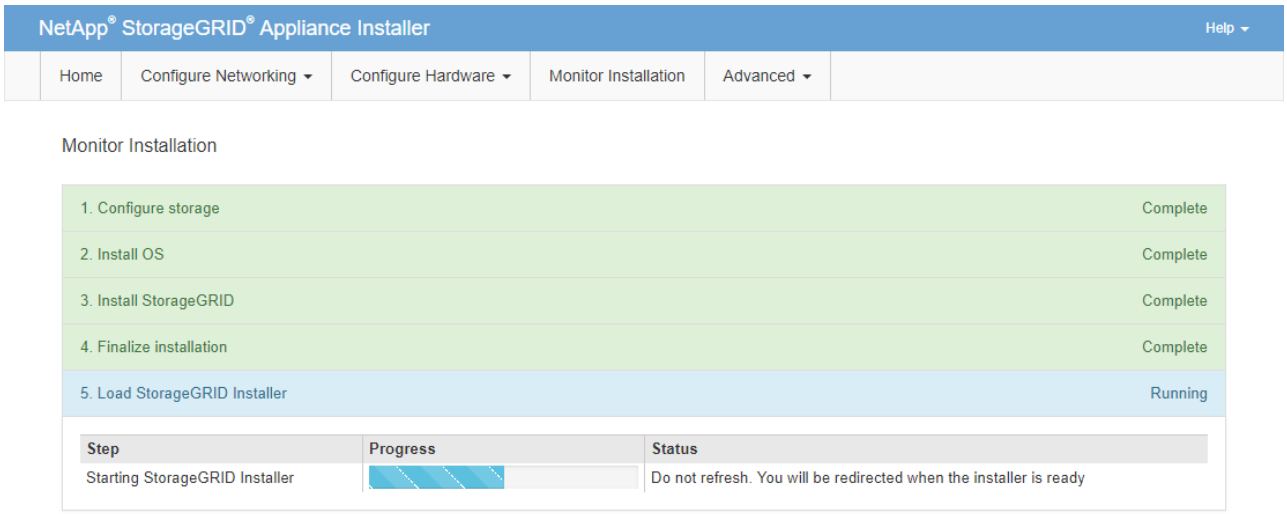
   - **2. Installare il sistema operativo**

     Durante questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID dal nodo di amministrazione primario all'appliance o installa il sistema operativo di base dal pacchetto di installazione per il nodo di amministrazione primario.

3. Continuare a monitorare l'avanzamento dell'installazione fino a quando non si verifica una delle seguenti condizioni:
   - Per i nodi gateway dell'appliance o i nodi di amministrazione dell'appliance non primaria, la fase **Install StorageGRID** (Installazione del nodo) viene sospesa e sulla console integrata viene visualizzato un messaggio che richiede di approvare questo nodo nel nodo di amministrazione utilizzando Gestione griglia.



- Per i nodi di amministrazione primari dell'appliance, viene visualizzata una quinta fase (carica programma di installazione StorageGRID). Se la quinta fase è in corso per più di 10 minuti, aggiornare la pagina manualmente.



4. Passare alla fase successiva del processo di ripristino per il tipo di nodo Grid dell'appliance che si sta ripristinando.

Tipo di ripristino	Riferimento
Nodo gateway	Selezionare Avvia ripristino per configurare il nodo gateway
Nodo amministrativo non primario	Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario
Nodo amministratore primario	Configurare il nodo amministrativo primario sostitutivo

Come viene eseguito il ripristino del sito dal supporto tecnico

In caso di guasto di un intero sito StorageGRID o in caso di guasto di più nodi di storage, è necessario contattare il supporto tecnico. Il supporto tecnico valuterà la tua situazione, svilupperà un piano di recovery e ripristinerà i nodi o il sito guasti in modo da soddisfare gli obiettivi di business, ottimizzare i tempi di recovery e prevenire inutili perdite di dati.

> Il ripristino del sito può essere eseguito solo dal supporto tecnico.

I sistemi StorageGRID sono resilienti a una vasta gamma di guasti e puoi eseguire molte procedure di ripristino e manutenzione autonomamente. Tuttavia, è difficile creare una procedura di ripristino del sito semplice e generalizzata, in quanto i passaggi dettagliati dipendono da fattori specifici della situazione. Ad esempio:

- **I tuoi obiettivi di business**: Dopo la perdita completa di un sito StorageGRID, dovresti valutare come soddisfare al meglio i tuoi obiettivi di business. Ad esempio, si desidera ricostruire il sito smarrito sul posto? Sostituire il sito StorageGRID perso in una nuova posizione? La situazione di ogni cliente è diversa e il tuo piano di recovery deve essere progettato per soddisfare le tue priorità.
- **Natura esatta del guasto**: Prima di iniziare un ripristino del sito, è importante stabilire se i nodi nel sito guasto sono intatti o se i nodi di storage contengono oggetti ripristinabili. Se si ricostruiscono nodi o volumi di storage che contengono dati validi, potrebbe verificarsi una perdita di dati non necessaria.
- **Active ILM policy**: Il numero, il tipo e la posizione delle copie degli oggetti nella griglia sono controllati

dalla policy ILM attiva. Le specifiche della policy ILM possono influire sulla quantità di dati ripristinabili e sulle tecniche specifiche richieste per il ripristino.

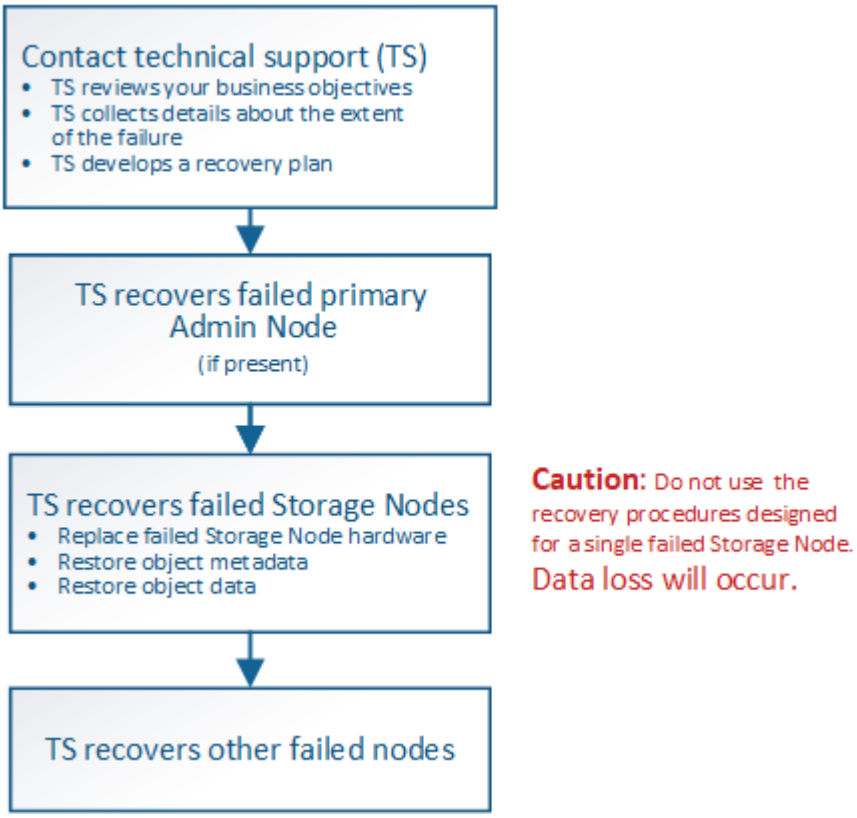
> Se un sito contiene l'unica copia di un oggetto e il sito viene perso, l'oggetto viene perso.

- **Coerenza bucket (o container)**: Il livello di coerenza applicato a un bucket (o container) influenza se StorageGRID replica completamente i metadati degli oggetti in tutti i nodi e siti prima di comunicare a un client che l'acquisizione degli oggetti ha avuto successo. Se il livello di coerenza consente una coerenza finale, alcuni metadati degli oggetti potrebbero essere stati persi in caso di guasto del sito. Ciò può influire sulla quantità di dati ripristinabili e potenzialmente sui dettagli della procedura di ripristino.
- **Cronologia delle modifiche recenti**: I dettagli della procedura di ripristino possono essere influenzati dal fatto che siano in corso procedure di manutenzione al momento dell'errore o se siano state apportate modifiche recenti alla policy ILM. Prima di iniziare un ripristino del sito, il supporto tecnico deve valutare la cronologia recente del tuo grid e la sua situazione attuale.

Panoramica del ripristino del sito

Questa è una panoramica generale del processo utilizzato dal supporto tecnico per ripristinare un sito guasto.

> Il ripristino del sito può essere eseguito solo dal supporto tecnico.



1. Contattare il supporto tecnico.

   Il supporto tecnico effettua una valutazione dettagliata del guasto e collabora con te per rivedere i tuoi obiettivi di business. In base a queste informazioni, il supporto tecnico sviluppa un piano di recovery personalizzato per la tua situazione.

2. Il supporto tecnico ripristina il nodo di amministrazione primario in caso di guasto.

3. Il supporto tecnico recupera tutti i nodi di storage, seguendo questa descrizione:

   a. Sostituire l'hardware o le macchine virtuali del nodo di storage secondo necessità.
   b. Ripristinare i metadati dell'oggetto nel sito guasto.
   c. Ripristinare i dati dell'oggetto nei nodi di storage ripristinati.

   > La perdita di dati si verifica se vengono utilizzate le procedure di ripristino per un singolo nodo di storage guasto.

   > Quando un intero sito ha avuto esito negativo, sono necessari comandi specializzati per ripristinare correttamente oggetti e metadati di oggetti.

4. Il supporto tecnico recupera altri nodi guasti.

   Una volta ripristinati i metadati e i dati dell'oggetto, è possibile ripristinare i nodi Gateway, i nodi Admin non primari o i nodi di archiviazione con procedure standard.

Informazioni correlate

Decommissionare il sito

Procedura di decommissionamento

È possibile eseguire una procedura di decommissionamento per rimuovere in modo permanente i nodi della griglia o un intero sito dal sistema StorageGRID.

Per rimuovere un nodo della griglia o un sito, eseguire una delle seguenti procedure di decommissionamento:

- Eseguire una **decommissionazione del nodo** per rimuovere uno o più nodi, che possono trovarsi in uno o più siti. I nodi rimossi possono essere online e connessi al sistema StorageGRID oppure offline e disconnessi.
- Eseguire una **decommissionazione del sito connesso** per rimuovere un sito in cui tutti i nodi sono connessi a StorageGRID.
- Eseguire una **decommissionazione sito disconnessa** per rimuovere un sito in cui tutti i nodi sono disconnessi da StorageGRID.

> Prima di eseguire la decommissionazione di un sito disconnesso, è necessario contattare il rappresentante commerciale NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site. Non tentare di decommissionare un sito disconnesso se si ritiene possibile ripristinare il sito o i dati degli oggetti dal sito.

Se un sito contiene una combinazione di) e nodi disconnessi (oppure), è necessario riportare tutti i nodi offline in linea.

Se è necessario eseguire una seconda procedura di manutenzione, è possibile Mettere in pausa la procedura di decommissionamento mentre i nodi di storage vengono rimossi. Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background. Una volta completata la seconda procedura di manutenzione, è possibile riprendere la decommissionamento.

Informazioni correlate

Decommissionare il nodo di rete

Decommissionare il sito

Decommissionare il nodo di rete

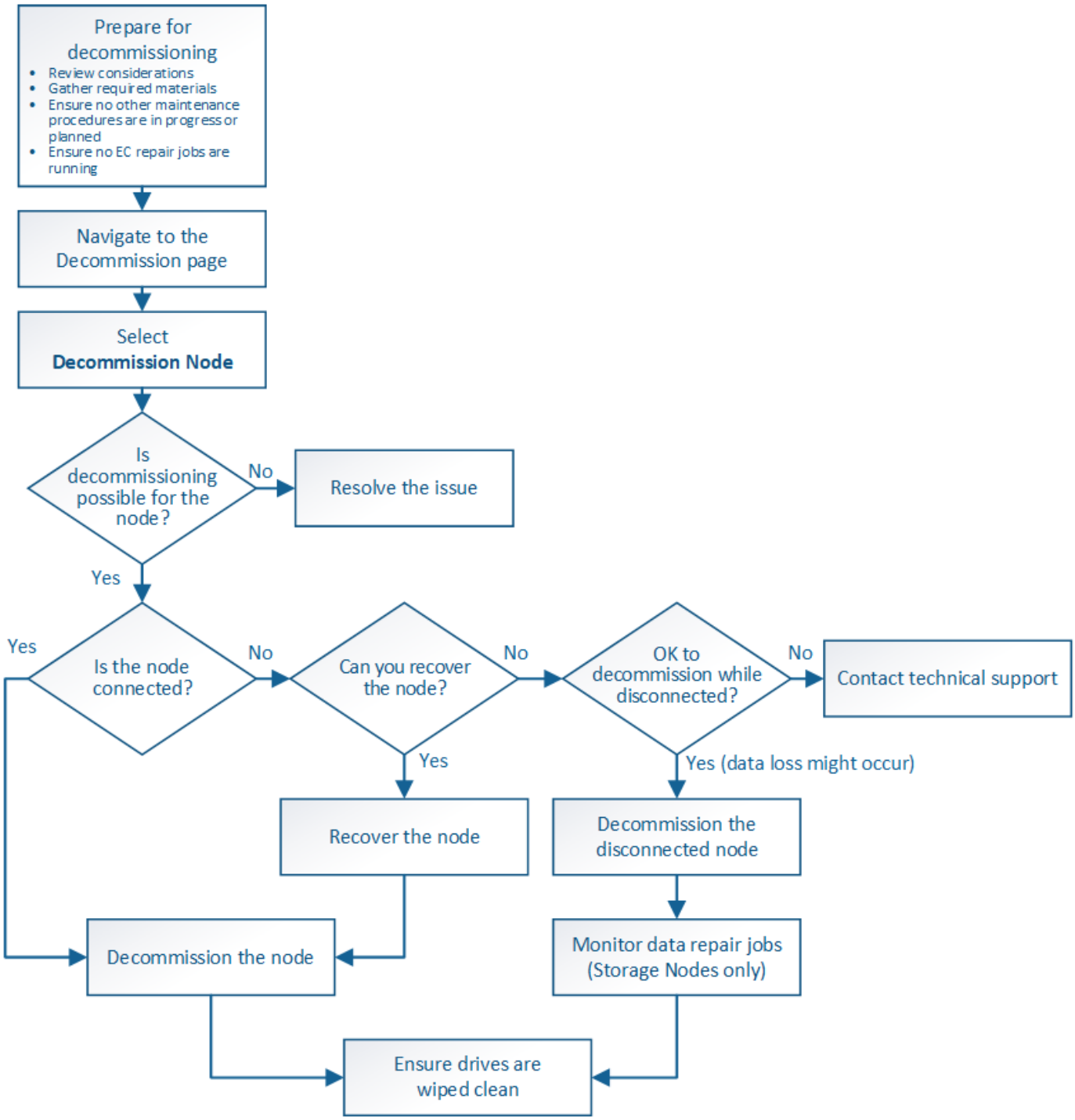
È possibile utilizzare la procedura di decommissionamento dei nodi per rimuovere uno o più nodi di storage, nodi gateway o nodi di amministrazione non primari in uno o più siti. Non è possibile decommissionare il nodo di amministrazione primario o un nodo di archivio.

In generale, è necessario decommissionare i nodi della griglia solo mentre sono connessi al sistema StorageGRID e tutti i nodi sono in condizioni normali (sono presenti icone verdi sulle pagine **NODI** e sulla pagina **nodi di decommissionazione**). Tuttavia, se necessario, è possibile decommissionare un nodo di rete scollegato. Prima di rimuovere un nodo disconnesso, assicurarsi di comprendere le implicazioni e le restrizioni di tale processo.

Utilizzare la procedura di decommissionamento del nodo quando si verifica una delle seguenti condizioni:

- È stato aggiunto un nodo di storage più grande al sistema e si desidera rimuovere uno o più nodi di storage più piccoli, preservando al contempo gli oggetti.
- Richiede meno storage totale.
- Non è più necessario un nodo gateway.
- Non è più necessario un nodo di amministrazione non primario.
- La griglia include un nodo disconnesso che non è possibile ripristinare o ripristinare online.

Il diagramma di flusso mostra le fasi di alto livello per la disattivazione dei nodi della griglia.



Prepararsi a decommissionare i nodi della griglia

È necessario esaminare le considerazioni relative alla rimozione dei nodi di griglia e verificare che non siano attivi lavori di riparazione per i dati con codifica di cancellazione.

Considerazioni per la decommissionazione del nodo grid

Prima di iniziare questa procedura per decommissionare uno o più nodi, è necessario comprendere le implicazioni della rimozione di ciascun tipo di nodo. Una volta decommissionato correttamente un nodo, i relativi servizi verranno disattivati e il nodo verrà automaticamente arrestato.

Non è possibile decommissionare un nodo se così facendo StorageGRID viene lasciato in uno stato non valido. Vengono applicate le seguenti regole:

- Non è possibile decommissionare il nodo di amministrazione primario.
- Non è possibile decommissionare i nodi di archiviazione.
- Non è possibile decommissionare un nodo amministratore o un nodo gateway se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (ha).
- Non è possibile decommissionare un nodo di storage se la sua rimozione influisce sul quorum di ADC.
- Non è possibile decommissionare un nodo di storage se richiesto per il criterio ILM attivo.
- Non è consigliabile decommissionare più di 10 nodi di storage in una singola procedura Decommission Node.
- Non è possibile decommissionare un nodo connesso se la griglia include nodi disconnessi (nodi il cui stato di salute è sconosciuto o amministrativamente inattivo). È necessario prima decommissionare o ripristinare i nodi disconnessi.
- Se la griglia contiene più nodi disconnessi, il software richiede di decommissionarli tutti contemporaneamente, aumentando il potenziale di risultati imprevisti.
- Se non è possibile rimuovere un nodo disconnesso (ad esempio, un nodo di storage necessario per il quorum ADC), non è possibile rimuovere nessun altro nodo disconnesso.
- Se si desidera sostituire un'appliance precedente con un'appliance più recente, prendere in considerazione l'opzione clonare il nodo appliance invece di smantellare il vecchio nodo e aggiungere il nuovo nodo in un'espansione.

> Non rimuovere la macchina virtuale o altre risorse di un nodo di griglia fino a quando non viene richiesto nelle procedure di decommissionamento.

Considerazioni per la decommissionazione del nodo Admin o del nodo gateway

Prima di disattivare un nodo Admin o un nodo gateway, esaminare le seguenti considerazioni.

- La procedura di decommissionamento richiede l'accesso esclusivo ad alcune risorse di sistema, pertanto è necessario verificare che non siano in esecuzione altre procedure di manutenzione.
- Non è possibile decommissionare il nodo di amministrazione primario.
- Non è possibile decommissionare un nodo amministratore o un nodo gateway se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (ha). Rimuovere prima le interfacce di rete dal gruppo ha. Consultare le istruzioni per l'amministrazione di StorageGRID.
- Come richiesto, è possibile modificare in modo sicuro il criterio ILM durante la disattivazione di un nodo gateway o di un nodo amministratore.
- Se si decommissiona un nodo amministratore e si attiva l'accesso singolo (SSO) per il sistema StorageGRID, è necessario ricordare di rimuovere l'attendibilità della parte di base del nodo dai servizi di federazione di Active Directory (ad FS).

Informazioni correlate

Amministrare StorageGRID

Considerazioni per la decommissionazione del nodo di storage

Se si prevede di decommissionare un nodo di storage, è necessario comprendere come StorageGRID gestisce i dati e i metadati dell'oggetto su tale nodo.

Le seguenti considerazioni e restrizioni si applicano quando si decommissiona nodi di storage:

- Il sistema deve sempre includere un numero sufficiente di nodi di storage per soddisfare i requisiti operativi, inclusi il quorum ADC e la policy ILM attiva. Per soddisfare questa restrizione, potrebbe essere necessario aggiungere un nuovo nodo di storage in un'operazione di espansione prima di poter decommissionare un nodo di storage esistente.
- Se il nodo di storage viene disconnesso quando viene decommissionato, il sistema deve ricostruire i dati utilizzando i dati dei nodi di storage connessi, con conseguente perdita di dati.
- Quando si rimuove un nodo di storage, è necessario trasferire grandi volumi di dati a oggetti sulla rete. Sebbene questi trasferimenti non debbano influire sulle normali operazioni di sistema, possono avere un impatto sulla quantità totale di larghezza di banda di rete consumata dal sistema StorageGRID.
- Le attività associate allo smantellamento del nodo di storage hanno una priorità inferiore rispetto alle attività associate alle normali operazioni di sistema. Ciò significa che lo smantellamento non interferisce con le normali operazioni del sistema StorageGRID e non deve essere pianificato per un periodo di inattività del sistema. Poiché lo smantellamento viene eseguito in background, è difficile stimare il tempo necessario per il completamento del processo. In generale, lo smantellamento termina più rapidamente quando il sistema non funziona correttamente o se viene rimosso un solo nodo di storage alla volta.
- La decommissionazione di un nodo di storage potrebbe richiedere giorni o settimane. Pianificare questa procedura di conseguenza. Sebbene il processo di decommissionamento sia progettato per non influire sulle operazioni del sistema, può limitare altre procedure. In generale, prima di rimuovere i nodi di rete, è necessario eseguire eventuali upgrade o espansioni del sistema pianificati.
- Le procedure di decommissionamento che coinvolgono i nodi di storage possono essere messe in pausa durante determinate fasi per consentire l'esecuzione di altre procedure di manutenzione, se necessario, e ripristinarle una volta completate.
- Non è possibile eseguire operazioni di riparazione dei dati su nodi grid quando è in esecuzione un'attività di decommissionamento.
- Non apportare modifiche al criterio ILM durante la disattivazione di un nodo di storage.
- Quando si rimuove un nodo di storage, i dati sul nodo vengono migrati in altri nodi griglia; tuttavia, questi dati non vengono completamente rimossi dal nodo griglia decommissionata. Per rimuovere i dati in modo permanente e sicuro, è necessario cancellare i dischi del nodo della griglia decommissionata al termine della procedura di decommissionamento.
- Quando si decommissiona un nodo di storage, è possibile che vengano generati i seguenti avvisi e allarmi e che si ricevano notifiche e-mail e SNMP correlate:
  - **Impossibile comunicare con l'avviso Node**. Questo avviso viene attivato quando si decommissiona un nodo di storage che include il servizio ADC. L'avviso viene risolto al termine dell'operazione di decommissionamento.
  - Allarme VSTU (Object Verification Status). Questo allarme a livello di avviso indica che il nodo di storage sta entrando in modalità di manutenzione durante il processo di decommissionamento.
  - Allarme CASA (Data Store Status). Questo allarme di livello maggiore indica che il database Cassandra è in stato di inattività a causa dell'interruzione dei servizi.

Informazioni correlate

Ripristinare i dati dell'oggetto nel volume di storage, se necessario

Comprendere il quorum di ADC

Potrebbe non essere possibile decommissionare alcuni nodi di storage in un sito del data center se dopo la disattivazione resterebbero pochi servizi ADC (Administrative Domain Controller). Questo servizio, disponibile in alcuni nodi di storage, mantiene le informazioni sulla topologia della griglia e fornisce servizi di configurazione alla griglia. Il sistema StorageGRID richiede un quorum di servizi ADC per essere sempre disponibile in ogni sito.

Non è possibile decommissionare un nodo di storage se la rimozione del nodo causerebbe il mancato rispetto del quorum di ADC. Per soddisfare il quorum di ADC durante la decommissionamento, è necessario che almeno tre nodi di storage in ciascun sito del data center dispongano del servizio ADC. Se un sito del data center dispone di più di tre nodi di storage con il servizio ADC, la maggior parte di questi nodi deve rimanere disponibile dopo la disattivazione ((0.5 * `Storage Nodes with ADC`) + 1).

Si supponga, ad esempio, che un sito del data center includa attualmente sei nodi di storage con servizi ADC e che si desideri decommissionare tre nodi di storage. A causa del requisito di quorum di ADC, è necessario completare due procedure di decommissionamento, come indicato di seguito:

- Nella prima procedura di decommissionamento, è necessario assicurarsi che i quattro nodi di storage con servizi ADC rimangano disponibili ((0.5 * 6) +1) . Ciò significa che all'inizio è possibile decommissionare solo due nodi di storage.
- Nella seconda procedura di decommissionamento, è possibile rimuovere il terzo nodo di storage perché il quorum ADC richiede ora solo tre servizi ADC per rimanere disponibili ((0.5 * 4) + 1).

Se è necessario decommissionare un nodo di storage ma non è possibile a causa del requisito di quorum di ADC, è necessario aggiungere un nuovo nodo di storage in un'espansione e specificare che deve disporre di un servizio ADC. Quindi, è possibile decommissionare il nodo di storage esistente.

Informazioni correlate

Espandi il tuo grid

Esaminare i criteri ILM e la configurazione dello storage

Se si prevede di decommissionare un nodo di storage, è necessario rivedere la policy ILM del sistema StorageGRID prima di avviare il processo di decommissionamento.

Durante lo smantellamento, tutti i dati degli oggetti vengono migrati dal nodo di storage decommissionato ad altri nodi di storage.

> La policy ILM di cui disponi *durante* la decommissionazione sarà quella utilizzata *dopo* la decommissionazione. È necessario assicurarsi che questa policy soddisfi i requisiti dei dati prima di iniziare la decommissionazione e dopo il completamento della decommissionazione.

È necessario rivedere le regole nel criterio ILM attivo per assicurarsi che il sistema StorageGRID continui a disporre di capacità sufficiente del tipo corretto e nelle posizioni corrette per consentire la disattivazione di un nodo di storage.

Considerare quanto segue:

- I servizi di valutazione ILM potranno copiare i dati degli oggetti in modo che le regole ILM siano soddisfatte?

- Cosa succede se un sito diventa temporaneamente non disponibile mentre è in corso la disattivazione? È possibile eseguire copie aggiuntive in una posizione alternativa?
- In che modo il processo di disattivazione influirà sulla distribuzione finale dei contenuti? Come descritto in Consolidare i nodi di storage, È necessario aggiungere nuovi nodi di storage prima di decommissionare quelli vecchi. Se si aggiunge un nodo di storage sostitutivo più grande dopo la disattivazione di un nodo di storage più piccolo, i vecchi nodi di storage potrebbero essere vicini alla capacità e il nuovo nodo di storage potrebbe non avere quasi alcun contenuto. La maggior parte delle operazioni di scrittura per i nuovi dati a oggetti verrebbe quindi indirizzata al nuovo nodo di storage, riducendo l'efficienza complessiva delle operazioni di sistema.
- Il sistema includerà sempre un numero sufficiente di nodi di storage per soddisfare la policy ILM attiva?

> Un criterio ILM che non può essere soddisfatto porterà a backlog e allarmi e può interrompere il funzionamento del sistema StorageGRID.

Verificare che la topologia proposta risultante dal processo di decommissionamento soddisfi la policy ILM valutando i fattori elencati nella tabella.

Area da valutare	Note
Capacità disponibile	La capacità dello storage è sufficiente per ospitare tutti i dati degli oggetti memorizzati nel sistema StorageGRID, Incluse le copie permanenti dei dati dell'oggetto attualmente memorizzati nel nodo di storage da smantellare?la capacità sarà sufficiente per gestire la crescita prevista dei dati dell'oggetto memorizzato per un intervallo di tempo ragionevole dopo il completamento della disattivazione?
Ubicazione dello storage	Se nel sistema StorageGRID rimane una capacità sufficiente, la capacità è nelle posizioni giuste per soddisfare le regole di business del sistema StorageGRID?
Tipo di storage	Sarà disponibile uno storage sufficiente del tipo appropriato dopo il completamento dello smantellamento? Ad esempio, le regole ILM potrebbero imporre che il contenuto venga spostato da un tipo di storage all'altro in base all'età del contenuto. In tal caso, è necessario assicurarsi che nella configurazione finale del sistema StorageGRID sia disponibile una quantità sufficiente di storage del tipo appropriato.

Informazioni correlate

Gestire gli oggetti con ILM

Espandi il tuo grid

Decommissionare nodi di storage disconnessi

È necessario comprendere cosa può accadere se si decommissiona un nodo di storage mentre è disconnesso (lo stato di salute è sconosciuto o amministrativamente inattivo).

Quando si decommissiona un nodo di storage disconnesso dalla griglia, StorageGRID utilizza i dati di altri nodi di storage per ricostruire i dati dell'oggetto e i metadati presenti nel nodo disconnesso. Ciò avviene avviando automaticamente i lavori di riparazione dei dati al termine del processo di disattivazione.

Prima di smantellare un nodo di storage disconnesso, tenere presente quanto segue:

- Non decommissionare mai un nodo disconnesso a meno che non si sia certi che non possa essere portato online o ripristinato.

> Non eseguire questa procedura se si ritiene che sia possibile ripristinare i dati dell'oggetto dal nodo. Contattare invece il supporto tecnico per determinare se è possibile eseguire il ripristino del nodo.

- Se un nodo di storage disconnesso contiene l'unica copia di un oggetto, tale oggetto verrà perso quando il nodo viene decommissionato. I processi di riparazione dei dati possono ricostruire e ripristinare gli oggetti solo se nei nodi di storage attualmente connessi sono presenti almeno una copia replicata o un numero sufficiente di frammenti con codifica di cancellazione.
- Quando si decommissiona un nodo di storage disconnesso, la procedura di decommissionamento viene completata in modo relativamente rapido. Tuttavia, i lavori di riparazione dei dati possono richiedere giorni o settimane e non sono monitorati dalla procedura di decommissionamento. È necessario monitorare manualmente questi lavori e riavviarli secondo necessità. Vedere Controllare i lavori di riparazione dei dati.
- Se si decommissiona più di un nodo di storage disconnesso alla volta, potrebbe verificarsi una perdita di dati. Il sistema potrebbe non essere in grado di ricostruire i dati se rimangono disponibili troppe copie di dati a oggetti, metadati o frammenti con codifica di cancellazione.

> Se si dispone di più di un nodo di storage disconnesso che non è possibile ripristinare, contattare il supporto tecnico per determinare la procedura migliore.

Consolidare i nodi di storage

È possibile consolidare i nodi di storage per ridurre il numero di nodi di storage per un sito o un'implementazione, aumentando al contempo la capacità di storage.

Quando consolidate i nodi storage, espandete il sistema StorageGRID per aggiungere nuovi nodi storage con capacità maggiore e decommissionare i vecchi nodi storage con capacità inferiore. Durante la procedura di decommissionamento, gli oggetti vengono migrati dai vecchi nodi di storage ai nuovi nodi di storage.

> Se si consolidano appliance più vecchie e più piccole con nuovi modelli o appliance di capacità superiore, molti utilizzano la funzione di clone del nodo o la procedura di clone del nodo e la procedura di decommissionamento se non si sta eseguendo una sostituzione uno a uno.

Ad esempio, è possibile aggiungere due nuovi nodi di storage con capacità maggiore per sostituire tre nodi di storage meno recenti. Prima di tutto, utilizzare la procedura di espansione per aggiungere i due nuovi nodi di storage di dimensioni maggiori, quindi utilizzare la procedura di decommissionamento per rimuovere i tre nodi di storage di capacità inferiore.

Aggiungendo nuova capacità prima di rimuovere i nodi di storage esistenti, è possibile garantire una distribuzione più equilibrata dei dati nel sistema StorageGRID. Inoltre, si riduce la possibilità che un nodo di storage esistente venga spinto oltre il livello di filigrana dello storage.

Informazioni correlate

Espandi il tuo grid

Decommissionare più nodi di storage

Se è necessario rimuovere più di un nodo di storage, è possibile decommissionarli in sequenza o in parallelo.

- Se si decommissionano i nodi di storage in modo sequenziale, è necessario attendere che il primo nodo di storage completi la decommissionamento prima di iniziare a decommissionare il nodo di storage successivo.
- Se i nodi di storage vengono decommissionati in parallelo, i nodi di storage elaborano contemporaneamente le attività di decommissionamento per tutti i nodi di storage da decommissionare. Questo può causare una situazione in cui tutte le copie permanenti di un file sono contrassegnate come “read-only,”, disattivando temporaneamente l’eliminazione nelle griglie in cui questa funzionalità è attivata.

Controllare i lavori di riparazione dei dati

Prima di disattivare un nodo di rete, è necessario confermare che non sono attivi lavori di riparazione dei dati. Se le riparazioni non sono riuscite, è necessario riavviarle e lasciarle completare prima di eseguire la procedura di decommissionamento.

Se è necessario decommissionare un nodo di storage disconnesso, queste fasi verranno completate anche al termine della procedura di decommissionamento per garantire che il lavoro di riparazione dei dati sia stato completato correttamente. È necessario assicurarsi che tutti i frammenti erasure-coded presenti nel nodo rimosso siano stati ripristinati correttamente.

Questi passaggi si applicano solo ai sistemi che dispongono di oggetti con codifica per la cancellazione.

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@grid_node_IP`

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

   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.
2. Verificare la presenza di riparazioni in corso: `repair-data show-ec-repair-status`
   - Se non si è mai eseguito un lavoro di riparazione dei dati, l’output è `No job found`. Non è necessario riavviare alcun lavoro di riparazione.
   - Se il lavoro di riparazione dei dati è stato eseguito in precedenza o è in esecuzione, l’output elenca le informazioni per la riparazione. Ogni riparazione ha un ID di riparazione univoco. Passare alla fase successiva.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
==========================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. Se lo stato per tutte le riparazioni è `Success`, non è necessario riavviare alcun lavoro di riparazione.
4. Se lo stato per qualsiasi riparazione è `Failure`, è necessario riavviare la riparazione.
   a. Ottenere l'ID della riparazione per la riparazione non riuscita dall'output.
   b. Eseguire `repair-data start-ec-node-repair` comando.

      Utilizzare `--repair-id` Opzione per specificare l'ID riparazione. Ad esempio, se si desidera riprovare una riparazione con l'ID riparazione 949292, eseguire questo comando: `repair-data start-ec-node-repair --repair-id 949292`

   c. Continuare a tenere traccia dello stato delle riparazioni dei dati EC fino a quando lo stato di tutte le riparazioni non è `Success`.

Raccogliere il materiale necessario

Prima di eseguire la decommissionazione di un nodo di rete, è necessario ottenere le seguenti informazioni.

Elemento	Note
Pacchetto di ripristino `.zip` file	È necessario Scarica il pacchetto di ripristino più recente `.zip` file (`sgws-recovery-package-`*`id-revision`*`.zip`). È possibile utilizzare il file Recovery Package per ripristinare il sistema in caso di errore.
`Passwords.txt` file	Questo file contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando ed è incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.

Elemento	Note
Descrizione della topologia del sistema StorageGRID prima dello smantellamento	Se disponibile, procurarsi la documentazione che descrive la topologia corrente del sistema.

Informazioni correlate

Requisiti del browser Web

Accedere alla pagina nodi di smantellamento

Quando si accede alla pagina nodi di disattivazione in Grid Manager, è possibile visualizzare a colpo d'occhio i nodi che possono essere disattivati.

Di cosa hai bisogno

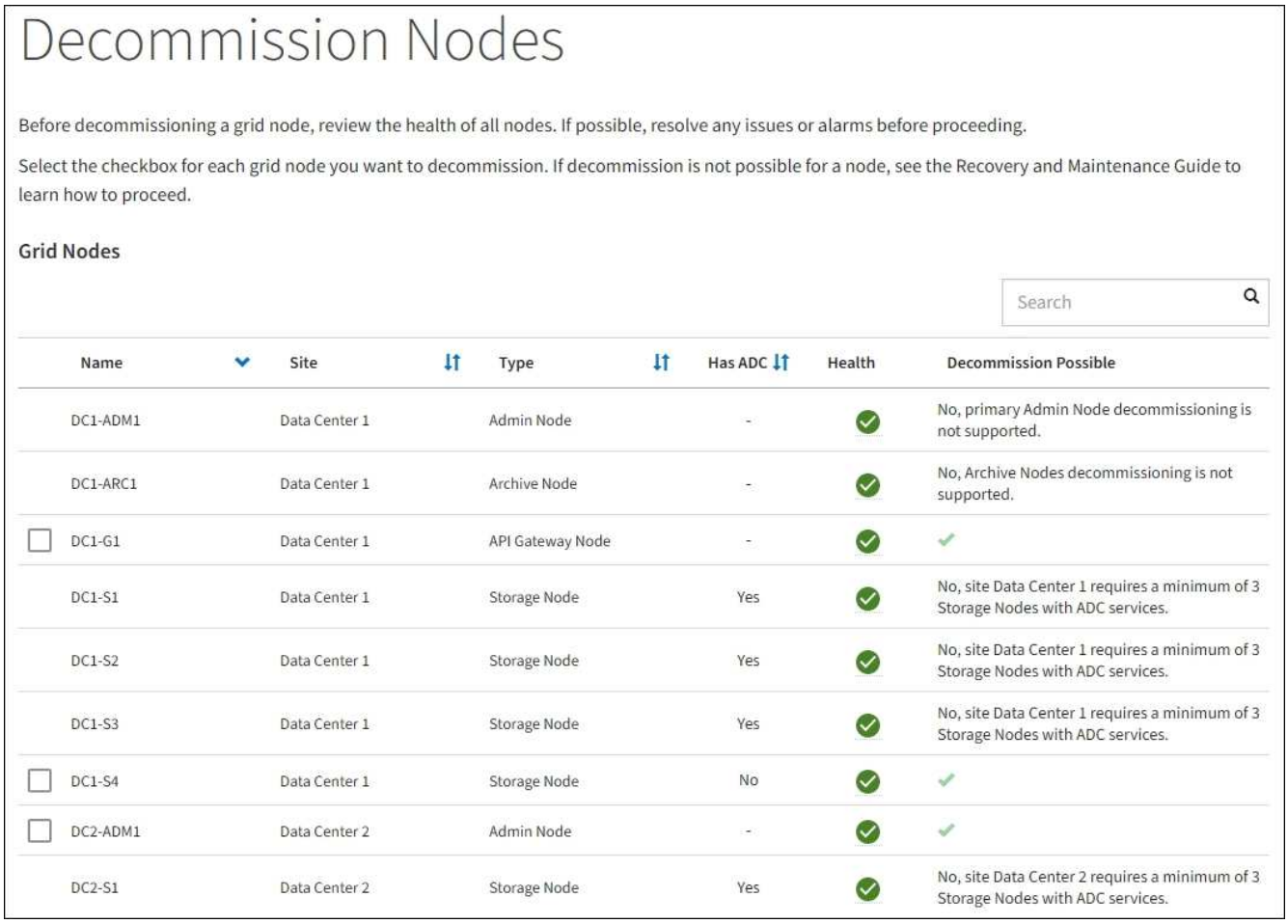
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Maintenance (manutenzione) o Root Access (accesso root).

Fasi

1. Selezionare **MANUTENZIONE attività Smantecazione**.
2. Selezionare **nodi di decommissionazione**.

   Viene visualizzata la pagina nodi di decommissionazione. Da questa pagina è possibile:

   - Determinare quali nodi di rete possono essere attualmente dismessi.
   - Scopri lo stato di salute di tutti i nodi della griglia
   - Ordinare l'elenco in ordine crescente o decrescente per **Nome**, **Sito**, **tipo** o **con ADC**.
   - Inserisci i termini di ricerca per trovare rapidamente nodi specifici. Ad esempio, questa pagina mostra i nodi della griglia in due data center. La colonna Decommissionabile indica che è possibile decommissionare il nodo gateway, uno dei cinque nodi di storage e il nodo di amministrazione non primario.



3. Esaminare la colonna **Dismissione possibile** per ciascun nodo che si desidera decommissionare.

   Se è possibile disattivare un nodo della griglia, questa colonna include un segno di spunta verde e la colonna più a sinistra include una casella di controllo. Se un nodo non può essere decommissionato, questa colonna descrive il problema. Se vi sono più motivi per cui un nodo non può essere dismesso, viene visualizzato il motivo più critico.

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, la disattivazione del tipo di nodo non è supportata.	Non è possibile decommissionare il nodo di amministrazione primario o un nodo di archivio.	Nessuno.

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, almeno un nodo della griglia è scollegato. **Nota:** questo messaggio viene visualizzato solo per i nodi di rete connessi.	Non è possibile decommissionare un nodo di rete connesso se un nodo di rete è scollegato. La colonna **Health** include una di queste icone per i nodi della griglia disconnessi: • (Grigio): Amministrativamente in basso • (Blu): Sconosciuto	Accedere alla fase che elenca le scelte della procedura di decommissionamento.
No, uno o più nodi richiesti sono attualmente disconnessi e devono essere ripristinati. **Nota:** questo messaggio viene visualizzato solo per i nodi della griglia disconnessi.	Non è possibile decommissionare un nodo di rete disconnesso se anche uno o più nodi richiesti sono disconnessi (ad esempio, un nodo di storage necessario per il quorum ADC).	a. Esaminare i messaggi Decommission possible per tutti i nodi disconnessi. b. Determinare quali nodi non possono essere dismessi perché sono necessari. ◦ Se lo stato di salute di un nodo richiesto è amministrativamente inattivo, riportare il nodo in linea. ◦ Se l'integrità di un nodo richiesto è sconosciuta, eseguire una procedura di ripristino del nodo per ripristinare il nodo richiesto.
No, membro dei gruppi ha: *X*. Prima di poter decommissionare questo nodo, è necessario rimuoverlo da tutti i gruppi ha.	Non è possibile decommissionare un nodo amministrativo o un nodo gateway se un'interfaccia di nodo appartiene a un gruppo ad alta disponibilità (ha).	Modificare il gruppo ha per rimuovere l'interfaccia del nodo o rimuovere l'intero gruppo ha. Consultare le istruzioni per l'amministrazione di StorageGRID.
No, il sito *x* richiede un minimo di *n* nodi di storage con servizi ADC.	**Solo nodi di storage.** non è possibile decommissionare un nodo di storage se nel sito rimangono nodi insufficienti per supportare i requisiti di quorum ADC.	Eseguire un'espansione. Aggiungere un nuovo nodo di storage al sito e specificare che deve disporre di un servizio ADC. Vedere le informazioni sul quorum di ADC.

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, uno o più profili di codifica Erasure richiedono almeno *n* nodi di storage. Se il profilo non viene utilizzato in una regola ILM, è possibile disattivarlo.	**Solo nodi di storage.** non è possibile decommissionare un nodo di storage a meno che non resti un numero sufficiente di nodi per i profili di codifica Erasure esistenti. Ad esempio, se esiste un profilo di codifica Erasure per la codifica di cancellazione 4+2, devono rimanere almeno 6 nodi di storage.	Per ciascun profilo di codifica Erasure interessato, eseguire una delle seguenti operazioni in base all'utilizzo del profilo: • **Utilizzato nel criterio ILM attivo**: Eseguire un'espansione. Aggiungere un numero sufficiente di nuovi nodi di storage per consentire la cancellazione del codice. Consultare le istruzioni per espandere StorageGRID. • **Utilizzato in una regola ILM ma non nel criterio ILM attivo**: Modificare o eliminare la regola e disattivare il profilo di codifica Erasure. • **Non utilizzato in alcuna regola ILM**: Disattiva il profilo di codifica Erasure. **Nota:** viene visualizzato un messaggio di errore se si tenta di disattivare un profilo di codifica Erasure e i dati dell'oggetto sono ancora associati al profilo. Potrebbe essere necessario attendere alcune settimane prima di provare di nuovo il processo di disattivazione. Scopri come disattivare un profilo di codifica Erasure nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

4. se è possibile eseguire lo decommissionamento per il nodo, determinare quale procedura eseguire:

Se la griglia include…	Vai a…
Qualsiasi nodo di rete disconnesso	Decommissionare nodi di rete disconnessi
Solo nodi di rete connessi	Decommissionare i nodi di rete connessi

Informazioni correlate

Controllare i lavori di riparazione dei dati

Comprendere il quorum di ADC

Gestire gli oggetti con ILM

Espandi il tuo grid

Amministrare StorageGRID

Decommissionare nodi di rete disconnessi

Potrebbe essere necessario decommissionare un nodo che non è attualmente connesso alla rete (un nodo il cui stato di salute è sconosciuto o amministrativamente inattivo).

Di cosa hai bisogno

- Comprendete i requisiti e. considerazioni per la disattivazione dei nodi di rete.
- Sono stati ottenuti tutti gli elementi prerequisiti.
- Hai garantito che non siano attivi lavori di riparazione dei dati. Vedere Controllare i lavori di riparazione dei dati.
- Hai confermato che il ripristino del nodo di storage non è in corso in nessun punto della griglia. In tal caso, è necessario attendere il completamento di qualsiasi ricostruzione Cassandra eseguita come parte del ripristino. È quindi possibile procedere con lo smantellamento.
- Si è assicurato che non verranno eseguite altre procedure di manutenzione mentre la procedura di decommissionamento del nodo è in esecuzione, a meno che la procedura di decommissionamento del nodo non sia in pausa.
- La colonna **Dismissione possibile** per il nodo o i nodi disconnessi che si desidera decommissionare include un segno di spunta verde.
- È necessario disporre della passphrase di provisioning.

A proposito di questa attività

È possibile identificare i nodi disconnessi cercando le icone sconosciute (blu) o amministrative (grigie) nella colonna **Health**. Nell'esempio, il nodo di storage denominato DC1-S4 è disconnesso; tutti gli altri nodi sono connessi.

Decommission Nodes

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

A grid node is disconnected (has a blue or gray health icon). Try to bring it back online or recover it. Data loss might occur if you decommission a node that is disconnected.

See the Recovery and Maintenance Guide for details. Contact Support if you cannot recover a node and do not want to decommission it.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes

Search

	Name	Site	Type	Has ADC	Health	Decommission Possible
	DC1-ADM1	Data Center 1	Admin Node	-		No, primary Admin Node decommissioning is not supported.
	DC1-ADM2	Data Center 1	Admin Node	-		No, at least one grid node is disconnected.
	DC1-G1	Data Center 1	API Gateway Node	-		No, at least one grid node is disconnected.
	DC1-S1	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
	DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
	DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
☐	DC1-S4	Data Center 1	Storage Node	No		✔

Passphrase

Provisioning Passphrase

Start Decommission

Prima di disattivare qualsiasi nodo disconnesso, tenere presente quanto segue:

- Questa procedura è principalmente destinata alla rimozione di un singolo nodo disconnesso. Se la griglia contiene più nodi disconnessi, il software richiede di decommissionarli tutti contemporaneamente, aumentando il potenziale di risultati imprevisti.

> Prestare molta attenzione quando si decommissiona più di un nodo di rete disconnesso alla volta, soprattutto se si selezionano più nodi di storage disconnessi.

- Se non è possibile rimuovere un nodo disconnesso (ad esempio, un nodo di storage necessario per il quorum ADC), non è possibile rimuovere nessun altro nodo disconnesso.

Prima di dismettere un nodo di storage * disconnesso, tenere presente quanto segue

- Non decommissionare mai un nodo di storage disconnesso, a meno che non si sia certi che non possa essere portato online o ripristinato.

> Se si ritiene che i dati dell'oggetto possano essere ancora ripristinati dal nodo, non eseguire questa procedura. Contattare invece il supporto tecnico per determinare se è possibile eseguire il ripristino del nodo.

- Se si decommissiona più di un nodo di storage disconnesso, potrebbe verificarsi una perdita di dati. Il sistema potrebbe non essere in grado di ricostruire i dati se non sono disponibili un numero sufficiente di copie di oggetti, frammenti con codifica di cancellazione o metadati di oggetti.

> Se si dispone di più di un nodo di storage disconnesso che non è possibile ripristinare, contattare il supporto tecnico per determinare la procedura migliore.

- Quando si decommissiona un nodo di storage disconnesso, StorageGRID avvia i lavori di riparazione dei dati al termine del processo di decommissionamento. Questi processi tentano di ricostruire i dati dell'oggetto e i metadati memorizzati nel nodo disconnesso.
- Quando si decommissiona un nodo di storage disconnesso, la procedura di decommissionamento viene completata in modo relativamente rapido. Tuttavia, i lavori di riparazione dei dati possono richiedere giorni o settimane e non sono monitorati dalla procedura di decommissionamento. È necessario monitorare manualmente questi lavori e riavviarli secondo necessità. Vedere Controllare i lavori di riparazione dei dati.
- Se si decommissiona un nodo di storage disconnesso che contiene l'unica copia di un oggetto, l'oggetto andrà perso. I processi di riparazione dei dati possono ricostruire e ripristinare gli oggetti solo se nei nodi di storage attualmente connessi sono presenti almeno una copia replicata o un numero sufficiente di frammenti con codifica di cancellazione.

Prima di smantellare un nodo **Admin Node** o **Gateway Node** disconnesso, tenere presente quanto segue:

- Quando si decommissiona un nodo di amministrazione disconnesso, i registri di controllo andranno persi da quel nodo; tuttavia, questi registri dovrebbero esistere anche nel nodo di amministrazione primario.
- È possibile decommissionare in modo sicuro un nodo gateway mentre è disconnesso.

Fasi

1. Tentare di riportare in linea eventuali nodi di rete disconnessi o di ripristinarli.

   Per istruzioni, consultare le procedure di ripristino.

2. Se non si riesce a ripristinare un nodo di rete disconnesso e si desidera decommissionarlo mentre è disconnesso, selezionare la casella di controllo corrispondente.

   > Se la griglia contiene più nodi disconnessi, il software richiede di decommissionarli tutti contemporaneamente, aumentando il potenziale di risultati imprevisti.

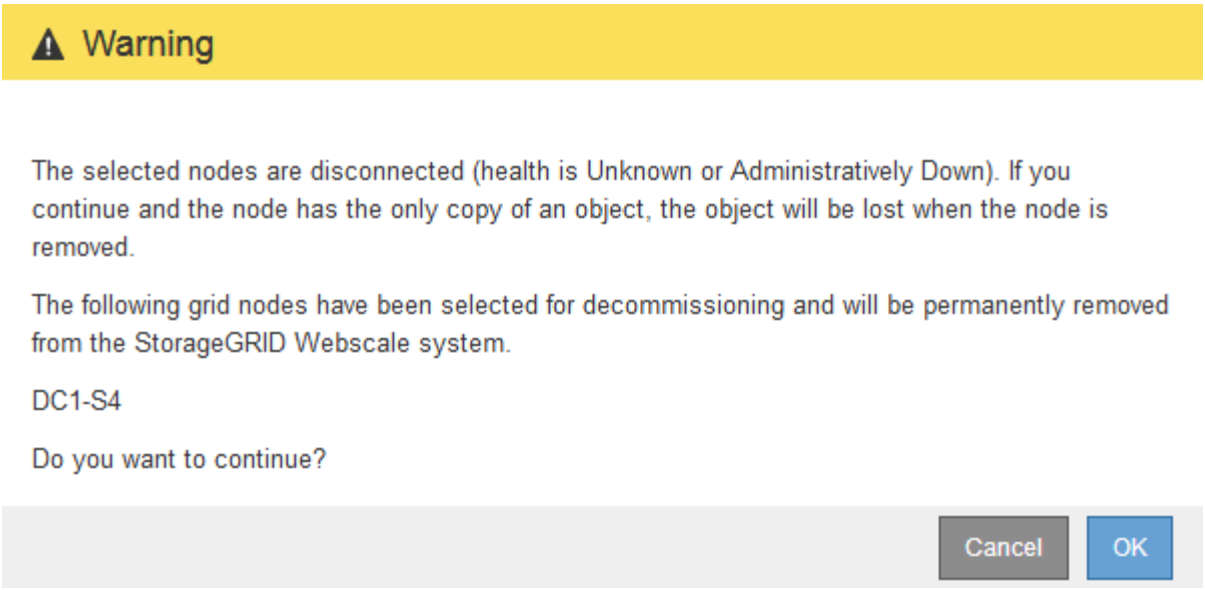
   > Prestare molta attenzione quando si sceglie di decommissionare più nodi di griglia disconnessi alla volta, soprattutto se si selezionano più nodi di storage disconnessi. Se si dispone di più di un nodo di storage disconnesso che non è possibile ripristinare, contattare il supporto tecnico per determinare la procedura migliore.

3. Inserire la passphrase di provisioning.

   Il pulsante **Avvia decommissionazione** è attivato.

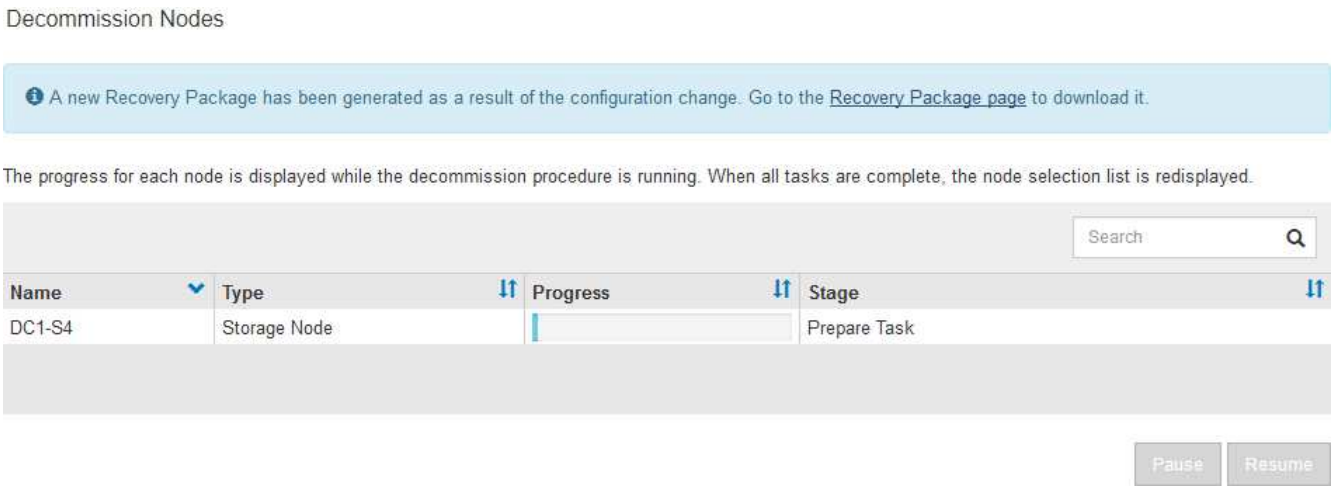
4. Fare clic su **Avvia decommissionazione**.

   Viene visualizzato un avviso che indica che è stato selezionato un nodo disconnesso e che i dati dell'oggetto andranno persi se il nodo dispone dell'unica copia di un oggetto.



5. Esaminare l'elenco dei nodi e fare clic su **OK**.

   Viene avviata la procedura di decommissionamento e l'avanzamento viene visualizzato per ciascun nodo. Durante la procedura, viene generato un nuovo pacchetto di ripristino contenente la modifica della configurazione della griglia.



6. Non appena il nuovo pacchetto di ripristino sarà disponibile, fare clic sul collegamento o selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino** per accedere alla pagina del pacchetto di ripristino. Quindi, scaricare `.zip` file.

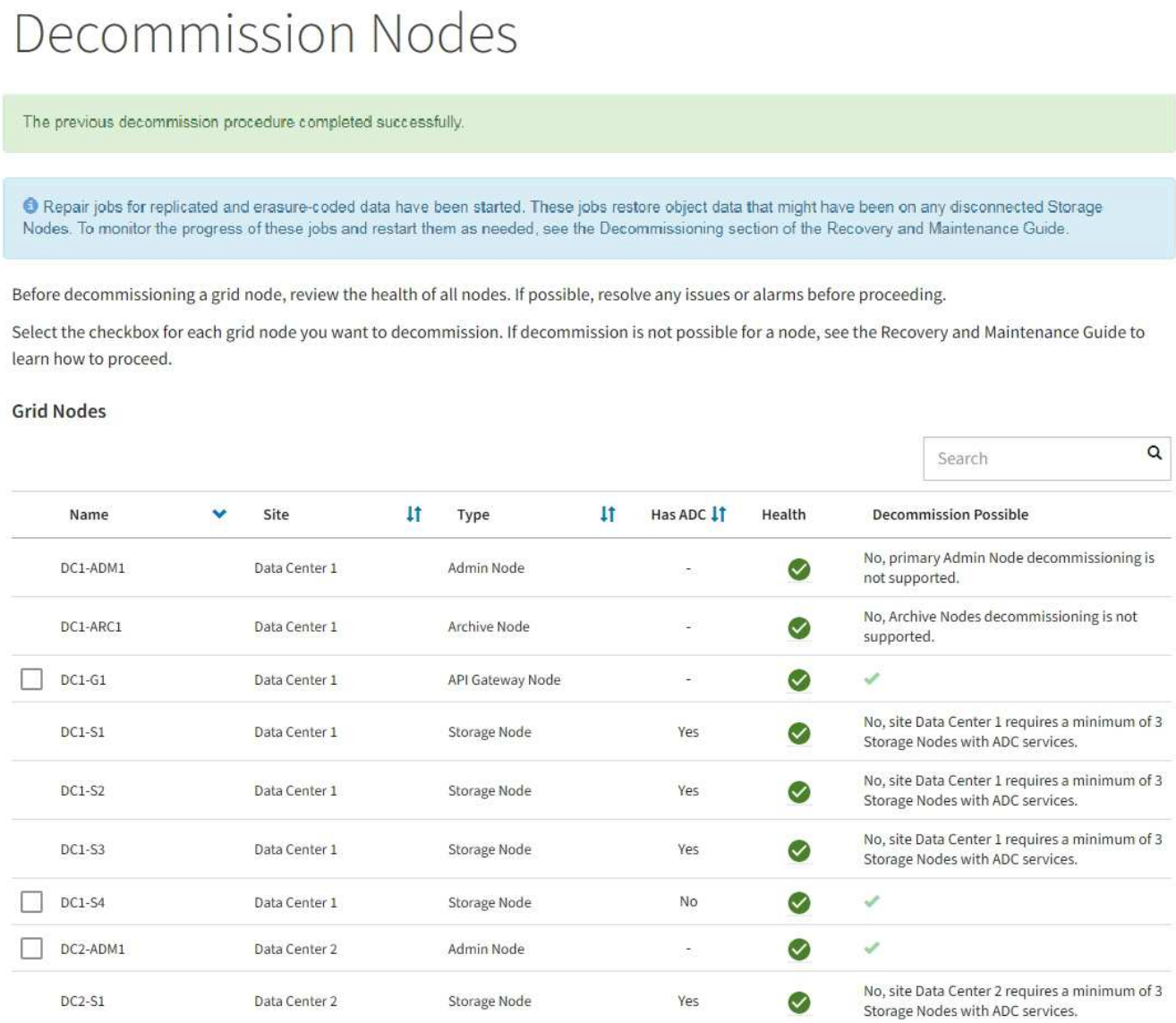
   Consultare le istruzioni per Download del pacchetto di ripristino.

   > Scarica il pacchetto di ripristino il prima possibile per assicurarti di ripristinare la griglia in caso di problemi durante la procedura di decommissionamento.

   > Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

7. Monitorare periodicamente la pagina Decommissionare per assicurarsi che tutti i nodi selezionati siano dismessi correttamente.

I nodi di storage possono richiedere giorni o settimane per la decommissionazione. Una volta completate tutte le attività, viene visualizzato nuovamente l'elenco di selezione dei nodi con un messaggio di esito positivo. Se si decommissiona un nodo di storage disconnesso, un messaggio di informazioni indica che i lavori di riparazione sono stati avviati.



8. Dopo che i nodi si sono spenti automaticamente nell'ambito della procedura di decommissionamento, rimuovere eventuali macchine virtuali o altre risorse rimanenti associate al nodo decommissionato.

   Non eseguire questa operazione fino a quando i nodi non si sono spenti automaticamente.

9. Se si sta smantellando un nodo di storage, monitorare lo stato dei lavori di riparazione di **dati replicati** e **dati con codifica di cancellazione (EC)** che vengono avviati automaticamente durante il processo di decommissionamento.

Dati replicati

- Per determinare se le riparazioni sono state completate:
  a. Selezionare **NODI** > ***nodo di storage in riparazione*** > **ILM**.
  b. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
  a. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
  b. Selezionare ***Grid*** > ***Storage Node in riparazione*** > **LDR** > **Data Store**.
  c. Utilizzare una combinazione dei seguenti attributi per determinare, come possibile, se le riparazioni replicate sono complete.

    > Le incongruenze di Cassandra potrebbero essere presenti e le riparazioni non riuscite non vengono monitorate.

    - **Tentativi di riparazione (XRPA)**: Utilizzare questo attributo per tenere traccia dell'avanzamento delle riparazioni replicate. Questo attributo aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Quando questo attributo non aumenta per un periodo superiore al periodo di scansione corrente (fornito dall'attributo **Scan Period — Estimated**), significa che la scansione ILM non ha rilevato oggetti ad alto rischio che devono essere riparati su alcun nodo.

      > Gli oggetti ad alto rischio sono oggetti che rischiano di essere completamente persi. Non sono inclusi oggetti che non soddisfano la configurazione ILM.

    - **Periodo di scansione — stimato (XSCM)**: Utilizzare questo attributo per stimare quando verrà applicata una modifica di policy agli oggetti precedentemente acquisiti. Se l'attributo **riparazioni tentate** non aumenta per un periodo superiore al periodo di scansione corrente, è probabile che vengano eseguite riparazioni replicate. Si noti che il periodo di scansione può cambiare. L'attributo **Scan Period — Estimated (XSCM)** si applica all'intera griglia ed è il massimo di tutti i periodi di scansione del nodo. È possibile eseguire una query nella cronologia degli attributi **Scan Period — Estimated** per la griglia per determinare un intervallo di tempo appropriato.
- Facoltativamente, per ottenere una percentuale di completamento stimata per la riparazione replicata, aggiungere `show-replicated-repair-status` al comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

  > Il `show-replicated-repair-status` L'opzione è disponibile per l'anteprima tecnica in StorageGRID 11.6. Questa funzionalità è in fase di sviluppo e il valore restituito potrebbe essere errato o ritardato. Per determinare se una riparazione è completa, utilizzare **in attesa di – tutto**, **riparazioni tentate (XRPA)** e **periodo di scansione — stimato (XSCM)** come descritto in Monitorare le riparazioni.

Cancellazione dei dati codificati (EC)

Per monitorare la riparazione dei dati con codifica erasure e riprovare eventuali richieste che potrebbero non essere riuscite:

1. Determinare lo stato delle riparazioni dei dati con codice di cancellazione:

   - Selezionare **SUPPORTO** > **Strumenti** > **metriche** per visualizzare il tempo stimato per il completamento e la percentuale di completamento per il lavoro corrente. Quindi, selezionare **EC Overview** (Panoramica EC) nella sezione Grafana. Esaminare le dashboard **Grid EC Job Estimated Time to Completion** (tempo stimato per il completamento della commessa EC) e **Grid EC Job Percentage Completed** (percentuale lavoro EC completata).
   - Utilizzare questo comando per visualizzare lo stato di uno specifico `repair-data` funzionamento:

     ```
     repair-data show-ec-repair-status --repair-id repair ID
     ```

   - Utilizzare questo comando per elencare tutte le riparazioni:

     ```
     repair-data show-ec-repair-status
     ```

   L'output elenca le informazioni, tra cui `repair ID`, per tutte le riparazioni precedentemente e attualmente in esecuzione.

2. Se l'output mostra che l'operazione di riparazione non è riuscita, utilizzare `--repair-id` opzione per riprovare la riparazione.

   Questo comando prova di nuovo una riparazione del nodo non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Questo comando prova di nuovo una riparazione del volume non riuscita, utilizzando l'ID riparazione 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Al termine

Non appena i nodi disconnessi sono stati decommissionati e tutti i lavori di riparazione dei dati sono stati completati, è possibile decommissionare qualsiasi nodo di rete connesso secondo necessità.

Quindi, completare questi passaggi dopo aver completato la procedura di decommissionamento:

- Assicurarsi che i dischi del nodo della griglia decommissionata siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.
- Se un nodo dell'appliance è stato disattivato e i dati dell'appliance sono stati protetti mediante la crittografia del nodo, utilizzare il programma di installazione dell'appliance StorageGRID per cancellare la configurazione del server di gestione delle chiavi (Cancella KMS). Se si desidera aggiungere l'appliance a un'altra griglia, è necessario cancellare la configurazione KMS.
  - Appliance di servizi SG100 e SG1000
  - Appliance di storage SG5600
  - Appliance di storage SG5700
  - Appliance di storage SG6000

Informazioni correlate

Procedure di ripristino del nodo Grid

Decommissionare i nodi di rete connessi

È possibile decommissionare e rimuovere in modo permanente i nodi collegati alla rete.

- È necessario comprendere i requisiti e. considerazioni per la disattivazione dei nodi di rete.
- È necessario aver raccolto tutti i materiali necessari.
- È necessario assicurarsi che non siano attivi lavori di riparazione dei dati.
- È necessario aver confermato che il ripristino del nodo di storage non è in corso in alcun punto della griglia. In tal caso, è necessario attendere il completamento di qualsiasi ricostruzione Cassandra eseguita come parte del ripristino. È quindi possibile procedere con lo smantellamento.
- È necessario assicurarsi che non vengano eseguite altre procedure di manutenzione mentre la procedura di decommissionamento del nodo è in esecuzione, a meno che la procedura di decommissionamento del nodo non sia in pausa.
- È necessario disporre della passphrase di provisioning.
- I nodi della griglia sono connessi.
- La colonna **Dismissione possibile** per il nodo o i nodi che si desidera decommissionare deve includere un segno di spunta verde.
- Tutti i nodi della griglia devono avere uno stato di salute normale (verde) . Se nella colonna **Health** viene visualizzata una di queste icone, provare a risolvere il problema:

Icona	Colore	Severità
	Giallo	Avviso
	Arancione chiaro	Minore
	Arancione scuro	Maggiore
	Rosso	Critico

- Se in precedenza è stato dismesso un nodo di storage disconnesso, tutti i lavori di riparazione dei dati sono stati completati correttamente. Vedere Controllare i lavori di riparazione dei dati.

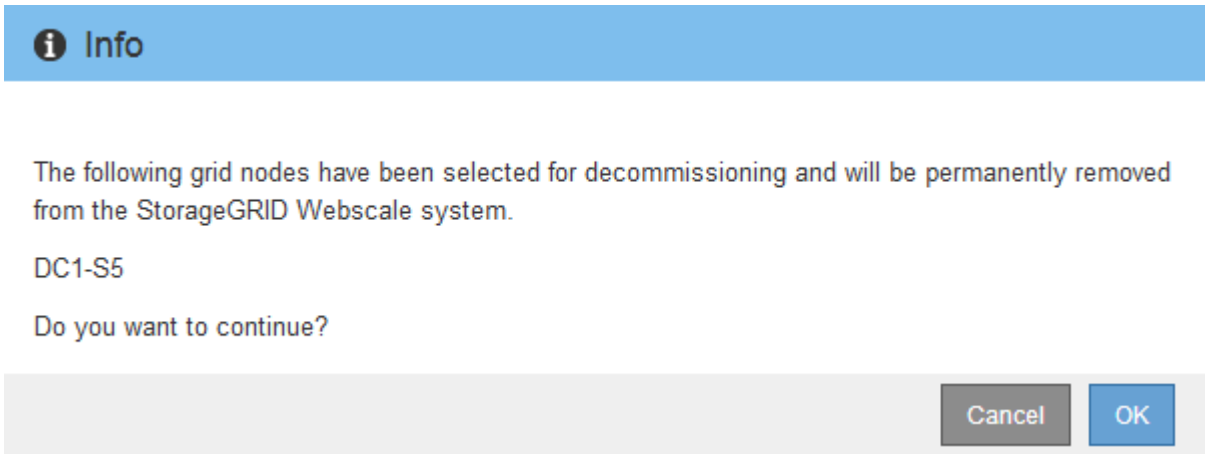
> Non rimuovere la macchina virtuale o altre risorse di un nodo griglia fino a quando non viene richiesto in questa procedura.

1. Nella pagina nodi di decommissionazione, selezionare la casella di controllo per ciascun nodo della griglia che si desidera decommissionare.
2. Inserire la passphrase di provisioning.

   Il pulsante **Avvia decommissionazione** è attivato.

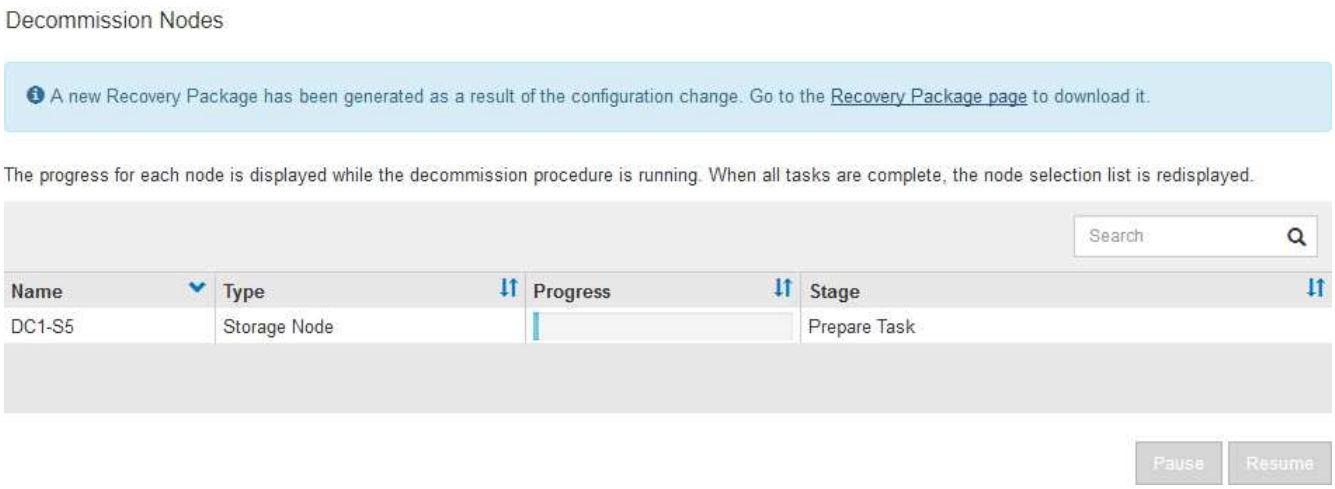
3. Fare clic su **Avvia decommissionazione**.

   Viene visualizzata una finestra di dialogo di conferma.



4. Esaminare l'elenco dei nodi selezionati e fare clic su **OK**.

   Viene avviata la procedura di decommissionamento del nodo e viene visualizzato l'avanzamento per ciascun nodo. Durante la procedura, viene generato un nuovo pacchetto di ripristino per mostrare la modifica della configurazione della griglia.



   Non scollegare un nodo di storage dopo l'avvio della procedura di decommissionamento. La modifica dello stato potrebbe causare la mancata copia di alcuni contenuti in altre posizioni.

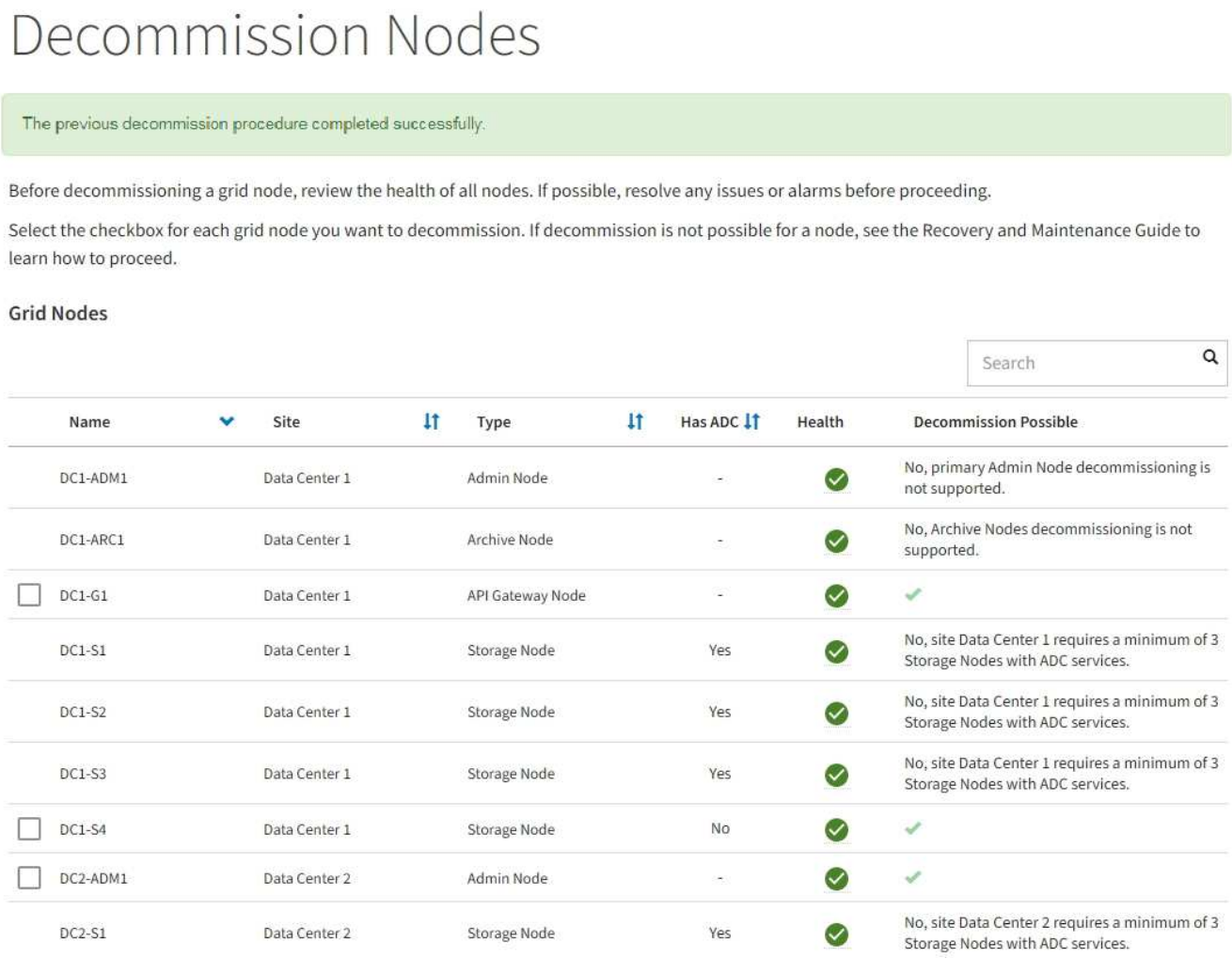
5. Non appena il nuovo pacchetto di ripristino sarà disponibile, fare clic sul collegamento o selezionare **MANUTENZIONE** > **sistema** > **pacchetto di ripristino** per accedere alla pagina del pacchetto di ripristino. Quindi, scaricare `.zip` file.

   Consultare le istruzioni per Download del pacchetto di ripristino.

   Scarica il pacchetto di ripristino il prima possibile per assicurarti di ripristinare la griglia in caso di problemi durante la procedura di decommissionamento.

6. Monitorare periodicamente la pagina nodi di decommissionazione per assicurarsi che tutti i nodi selezionati vengano decommissionati correttamente.

I nodi di storage possono richiedere giorni o settimane per la decommissionazione. Una volta completate tutte le attività, viene visualizzato nuovamente l'elenco di selezione dei nodi con un messaggio di esito positivo.



7. Seguire la fase appropriata per la piattaforma. Ad esempio:
   - **Linux**: Si consiglia di scollegare i volumi ed eliminare i file di configurazione del nodo creati durante l'installazione.
   - **VMware**: Per eliminare la macchina virtuale, utilizzare l'opzione "DElimina dal disco" di vCenter. Potrebbe essere necessario eliminare anche i dischi dati indipendenti dalla macchina virtuale.
   - **Appliance StorageGRID**: Il nodo appliance torna automaticamente allo stato non distribuito, dove è possibile accedere al programma di installazione dell'appliance StorageGRID. È possibile spegnere l'apparecchio o aggiungerlo a un altro sistema StorageGRID.

Completare questi passaggi dopo aver completato la procedura di decommissionamento del nodo:

- Assicurarsi che i dischi del nodo della griglia decommissionata siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.
- Se un nodo dell'appliance è stato disattivato e i dati dell'appliance sono stati protetti mediante la crittografia del nodo, utilizzare il programma di installazione dell'appliance StorageGRID per cancellare la configurazione del server di gestione delle chiavi (Cancella KMS). Se si desidera utilizzare l'appliance in un'altra griglia, è necessario cancellare la configurazione KMS.

Appliance di servizi SG100 e SG1000

Appliance di storage SG5600

Appliance di storage SG5700

Appliance di storage SG6000

Informazioni correlate

Installare Red Hat Enterprise Linux o CentOS

Mettere in pausa e riprendere il processo di decommissionamento per i nodi di storage

Se è necessario eseguire una seconda procedura di manutenzione, è possibile sospendere la procedura di decommissionamento per un nodo di storage durante determinate fasi. Al termine dell'altra procedura, è possibile riprendere la decommissionamento.

> Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background.

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).

Fasi

1. Selezionare **MANUTENZIONE attività Smantecazione**.

   Viene visualizzata la pagina Decommission.

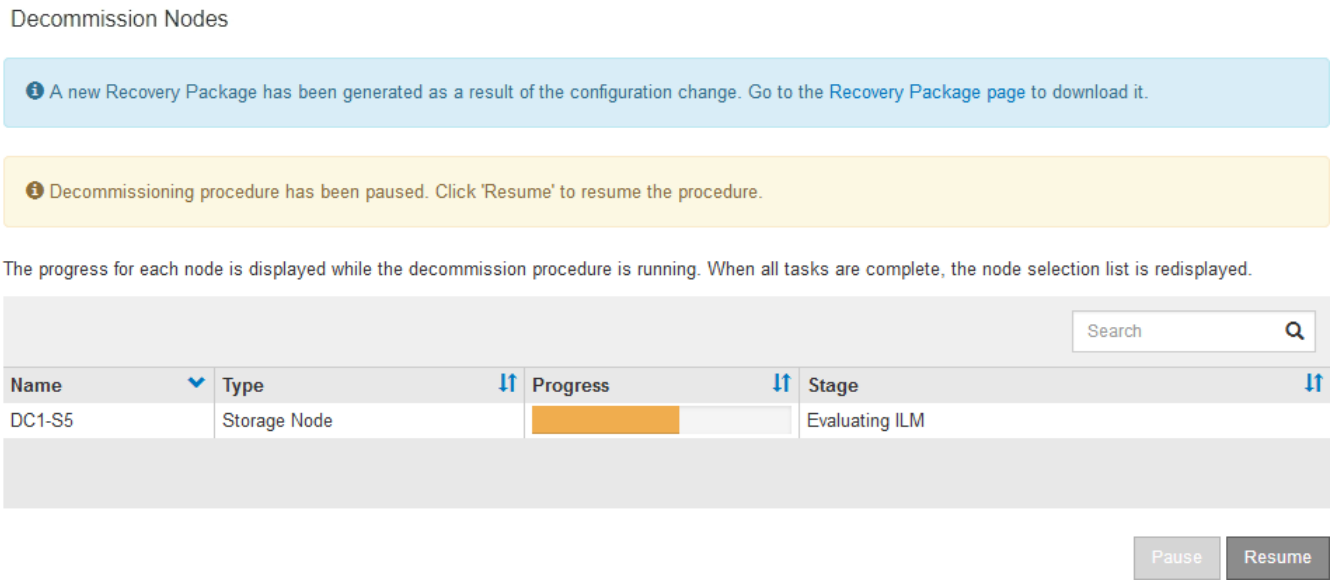
2. Selezionare **nodi di decommissionazione**.

   Viene visualizzata la pagina nodi di decommissionazione. Quando la procedura di decommissionamento raggiunge una delle seguenti fasi, il pulsante **Pause** (Pausa) viene attivato.

   - Valutazione di ILM
   - Decommissionamento Erasure coded data (Cancella dati codificati)

3. Selezionare **Pausa** per sospendere la procedura.

   La fase corrente viene messa in pausa e il pulsante **Riprendi** viene attivato.



4. Al termine dell'altra procedura di manutenzione, selezionare **Riprendi** per procedere con la decommissionazione.

Risolvere i problemi relativi alla disattivazione del nodo

Se la procedura di decommissionamento del nodo si interrompe a causa di un errore, è possibile eseguire operazioni specifiche per risolvere il problema.

Di cosa hai bisogno

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

A proposito di questa attività

Se si arresta il nodo della griglia da smantellare, l'attività si interrompe fino al riavvio del nodo della griglia. Il nodo Grid deve essere in linea.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Nell'albero Grid Topology, espandere ogni voce Storage Node e verificare che i servizi DDS e LDR siano entrambi online.

   Per eseguire la disattivazione dei nodi di storage, tutti i nodi e tutti i servizi devono essere integri all'inizio della disattivazione di un nodo/sito online.

3. Per visualizzare le attività attive della griglia, selezionare **nodo amministratore primario CMN attività griglia Panoramica**.
4. Controllare lo stato dell'attività della griglia di disattivazione.

   a. Se lo stato dell'attività della griglia di decommissionamento indica un problema con il salvataggio dei bundle di attività della griglia, selezionare **nodo amministratore primario CMN Eventi Panoramica**

   b. Controllare il numero di relè di audit disponibili.

      Se l'attributo Available Audit Relay è uno o più, il servizio CMN è connesso ad almeno un servizio ADC. I servizi ADC fungono da relè di audit.

   Il servizio CMN deve essere connesso ad almeno un servizio ADC e la maggior parte (50% più uno) dei

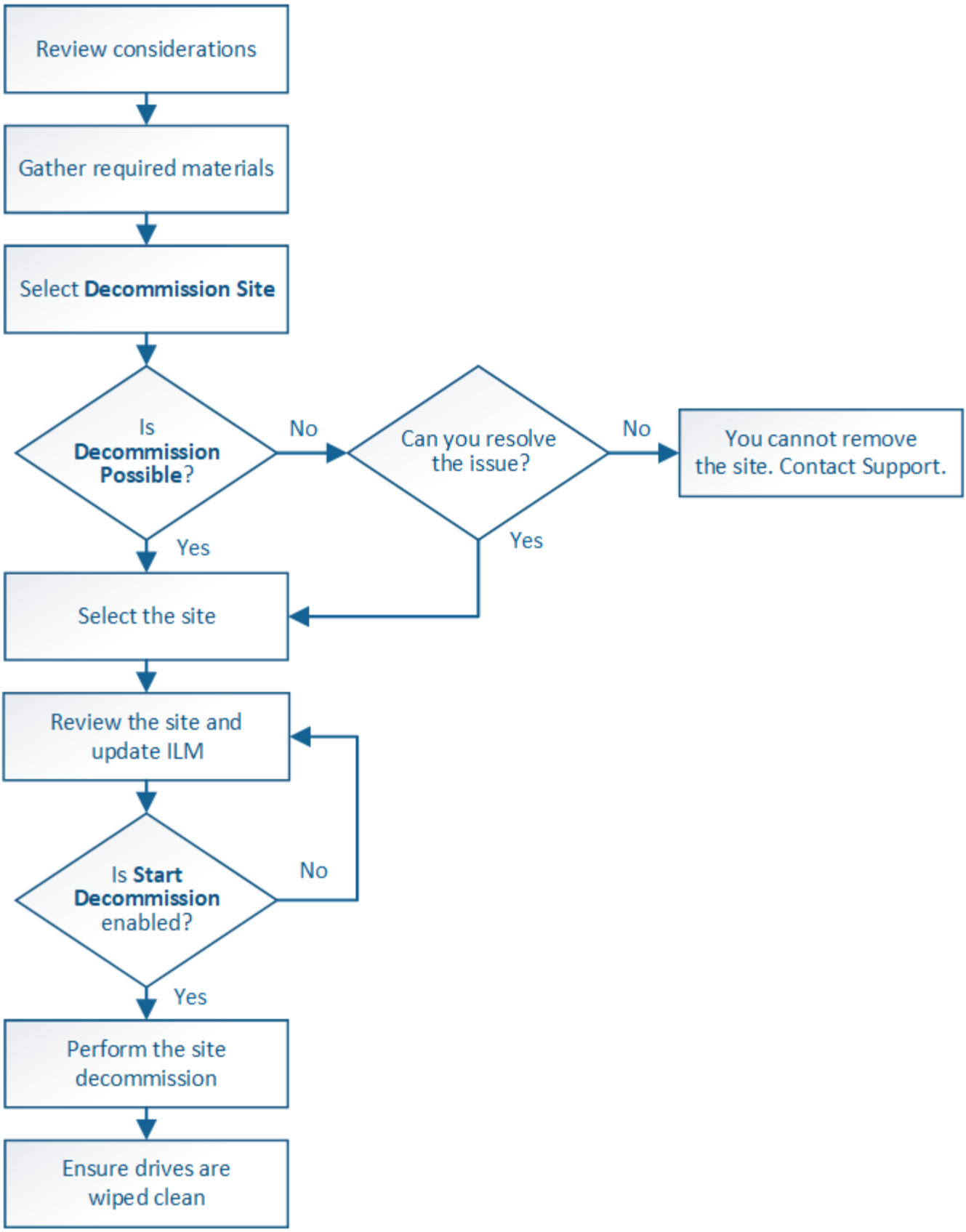
servizi ADC del sistema StorageGRID deve essere disponibile per consentire a un'attività Grid di passare da una fase di disattivazione a un'altra e terminare.

a. Se il servizio CMN non è connesso a un numero sufficiente di servizi ADC, assicurarsi che i nodi di storage siano in linea e controllare la connettività di rete tra il nodo di amministrazione primario e i nodi di storage.

Decommissionare il sito

Potrebbe essere necessario rimuovere un sito del data center dal sistema StorageGRID. Per rimuovere un sito, è necessario decommissionarlo.

Il diagramma di flusso mostra le fasi di alto livello per la disattivazione di un sito.



Considerazioni per la rimozione di un sito

Prima di utilizzare la procedura di decommissionamento del sito per rimuovere un sito, è necessario esaminare le considerazioni.

Cosa accade quando si decommissiona un sito

Quando si decommissiona un sito, StorageGRID rimuove in modo permanente tutti i nodi del sito e del sito stesso dal sistema StorageGRID.

Una volta completata la procedura di decommissionamento del sito:

- Non è più possibile utilizzare StorageGRID per visualizzare o accedere al sito o a uno qualsiasi dei nodi del sito.
- Non è più possibile utilizzare pool di storage o profili di codifica Erasure relativi al sito. Quando StorageGRID decommissiona un sito, rimuove automaticamente questi pool di storage e disattiva questi profili di codifica di cancellazione.

Differenze tra le procedure di decommissionamento del sito connesso e disconnesso

È possibile utilizzare la procedura di decommissionamento del sito per rimuovere un sito in cui tutti i nodi sono connessi a StorageGRID (chiamata decommissionazione di un sito connesso) o per rimuovere un sito in cui tutti i nodi sono disconnessi da StorageGRID (chiamata decommissionazione di un sito disconnesso). Prima di iniziare, è necessario comprendere le differenze tra queste procedure.

> Se un sito contiene una combinazione di) e nodi disconnessi (oppure), è necessario riportare tutti i nodi offline in linea.

- La decommissionazione di un sito connesso consente di rimuovere un sito operativo dal sistema StorageGRID. Ad esempio, è possibile eseguire la decommissionazione di un sito connesso per rimuovere un sito funzionante ma non più necessario.
- Quando StorageGRID rimuove un sito connesso, utilizza ILM per gestire i dati dell'oggetto nel sito. Prima di avviare la decommissionazione di un sito connesso, è necessario rimuovere il sito da tutte le regole ILM e attivare una nuova policy ILM. I processi ILM per la migrazione dei dati degli oggetti e i processi interni per la rimozione di un sito possono essere eseguiti contemporaneamente, ma la procedura consigliata consiste nel consentire il completamento dei passaggi ILM prima di avviare la procedura di decommissionamento effettiva.
- La decommissionazione di un sito disconnesso consente di rimuovere un sito guasto dal sistema StorageGRID. Ad esempio, è possibile eseguire la decommissionazione di un sito disconnesso per rimuovere un sito distrutto da un incendio o un'inondazione.

  Quando StorageGRID rimuove un sito disconnesso, considera tutti i nodi irripristinabili e non tenta di conservare i dati. Tuttavia, prima di avviare una decommissionazione disconnessa del sito, è necessario rimuovere il sito da tutte le regole ILM e attivare una nuova policy ILM.

> Prima di eseguire una procedura di decommissionamento del sito disconnesso, è necessario contattare il rappresentante commerciale NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site. Non tentare di decommissionare un sito disconnesso se si ritiene possibile ripristinare il sito o i dati degli oggetti dal sito.

Requisiti generali per la rimozione di un sito connesso o disconnesso

Prima di rimuovere un sito connesso o disconnesso, è necessario conoscere i seguenti requisiti:

- Non è possibile decommissionare un sito che include il nodo di amministrazione primario.

- Non è possibile decommissionare un sito che include un nodo di archiviazione.
- Non è possibile decommissionare un sito se uno dei nodi dispone di un'interfaccia che appartiene a un gruppo ad alta disponibilità (ha). È necessario modificare il gruppo ha per rimuovere l'interfaccia del nodo o rimuovere l'intero gruppo ha.
- Non è possibile decommissionare un sito se contiene una combinazione di connesso ( ) e disconnessi (oppure).
- Non è possibile decommissionare un sito se un nodo di un altro sito è disconnesso (oppure).
- Non è possibile avviare la procedura di decommissionamento del sito se è in corso un'operazione di riparazione del nodo ec. Vedere Controllare i lavori di riparazione dei dati per tenere traccia delle riparazioni dei dati con codice di cancellazione.
- Durante l'esecuzione della procedura di decommissionamento del sito:
  - Non è possibile creare regole ILM che si riferiscono al sito da smantellare. Non è inoltre possibile modificare una regola ILM esistente per fare riferimento al sito.
  - Non è possibile eseguire altre procedure di manutenzione, ad esempio l'espansione o l'aggiornamento.

    > Se è necessario eseguire un'altra procedura di manutenzione durante la decommissionazione di un sito connesso, è possibile Sospendere la procedura durante la rimozione dei nodi di storage. Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background. Una volta completata la seconda procedura di manutenzione, è possibile riprendere la decommissionamento.

  - Se è necessario ripristinare un nodo dopo aver avviato la procedura di decommissionamento del sito, contattare il supporto.
- Non è possibile decommissionare più di un sito alla volta.
- Se il sito include uno o più nodi di amministrazione ed è abilitato il Single Sign-on (SSO) per il sistema StorageGRID, è necessario rimuovere tutti i trust delle parti che si basano sul sito dai servizi di federazione Active Directory (ad FS).

Requisiti per la gestione del ciclo di vita delle informazioni (ILM)

Durante la rimozione di un sito, è necessario aggiornare la configurazione ILM. La procedura guidata Decommission Site (Sito di rimozione) guida l'utente attraverso una serie di passaggi necessari per garantire quanto segue:

- Il sito non è indicato dalla policy ILM attiva. In tal caso, è necessario creare e attivare un nuovo criterio ILM con nuove regole ILM.
- Non esiste alcun criterio ILM proposto. Se si dispone di una policy proposta, è necessario eliminarla.
- Nessuna regola ILM fa riferimento al sito, anche se tali regole non vengono utilizzate nella policy attiva o proposta. È necessario eliminare o modificare tutte le regole che fanno riferimento al sito.

Quando StorageGRID decommissiona il sito, disattiva automaticamente i profili di codifica di cancellazione non utilizzati che fanno riferimento al sito e elimina automaticamente i pool di storage inutilizzati che fanno riferimento al sito. Il pool di storage di tutti i nodi di storage predefinito del sistema viene rimosso perché utilizza tutti i siti.

> Prima di rimuovere un sito, potrebbe essere necessario creare nuove regole ILM e attivare un nuovo criterio ILM. Queste istruzioni presuppongono una buona comprensione del funzionamento di ILM e una buona conoscenza della creazione di pool di storage, dei profili di codifica Erasure, delle regole ILM e della simulazione e attivazione di un criterio ILM. Consultare le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Gestire gli oggetti con ILM

Considerazioni per i dati dell'oggetto in un sito connesso

Se si sta eseguendo una decommissionazione del sito connesso, è necessario decidere cosa fare con i dati dell'oggetto esistenti nel sito quando si creano nuove regole ILM e un nuovo criterio ILM. È possibile eseguire una o entrambe le operazioni seguenti:

- Sposta i dati degli oggetti dal sito selezionato a uno o più altri siti della griglia.

  Esempio per lo spostamento dei dati: Supponiamo di voler decommissionare un sito in Raleigh perché hai aggiunto un nuovo sito in Sunnyvale. In questo esempio, si desidera spostare tutti i dati dell'oggetto dal sito precedente al nuovo sito. Prima di aggiornare le regole ILM e i criteri ILM, è necessario rivedere la capacità di entrambi i siti. È necessario assicurarsi che il sito Sunnyvale disponga di capacità sufficiente per ospitare i dati dell'oggetto provenienti dal sito Raleigh e che la capacità di Sunnyvale rimanga adeguata per la crescita futura.

  > Per garantire che sia disponibile una capacità adeguata, potrebbe essere necessario aggiungere volumi di storage o nodi di storage a un sito esistente o aggiungere un nuovo sito prima di eseguire questa procedura. Consultare le istruzioni per espandere un sistema StorageGRID.

- Elimina le copie degli oggetti dal sito selezionato.

  Esempio per l'eliminazione dei dati: Si supponga di utilizzare una regola ILM a 3 copie per replicare i dati degli oggetti su tre siti. Prima di smantellare un sito, è possibile creare una regola ILM equivalente a 2 copie per memorizzare i dati solo in due siti. Quando si attiva un nuovo criterio ILM che utilizza la regola 2-copy, StorageGRID elimina le copie dal terzo sito perché non soddisfano più i requisiti ILM. Tuttavia, i dati dell'oggetto rimangono protetti e la capacità dei due siti rimanenti rimane invariata.

  > Non creare mai una regola ILM a copia singola per consentire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Requisiti aggiuntivi per la decommissionazione di un sito connesso

Prima che StorageGRID possa rimuovere un sito connesso, è necessario assicurarsi che:

- Tutti i nodi nel sistema StorageGRID devono avere uno stato di connessione di **connesso** ( ); tuttavia, i nodi possono avere avvisi attivi.

> Se uno o più nodi sono disconnessi, è possibile completare i passaggi 1-4 della procedura guidata Smantella sito. Tuttavia, non è possibile completare la fase 5 della procedura guidata, che avvia il processo di decommissionamento, a meno che tutti i nodi non siano connessi.

- Se il sito che si intende rimuovere contiene un nodo gateway o un nodo amministratore utilizzato per il bilanciamento del carico, potrebbe essere necessario eseguire una procedura di espansione per aggiungere un nuovo nodo equivalente in un altro sito. Assicurarsi che i client possano connettersi al nodo sostitutivo prima di avviare la procedura di decommissionamento del sito.
- Se il sito che si intende rimuovere contiene nodi gateway o nodi amministratore che si trovano in un gruppo ad alta disponibilità (ha), è possibile completare i passaggi 1-4 della procedura guidata Decommission Site. Tuttavia, non è possibile completare la fase 5 della procedura guidata, che avvia il processo di decommissionamento, fino a quando non si rimuovono questi nodi da tutti i gruppi ha. Se i client esistenti si connettono a un gruppo ha che include nodi dal sito, è necessario assicurarsi che possano continuare a connettersi a StorageGRID dopo la rimozione del sito.
- Se i client si connettono direttamente ai nodi di storage nel sito che si intende rimuovere, è necessario assicurarsi che possano connettersi ai nodi di storage in altri siti prima di avviare la procedura di decommissionamento del sito.
- È necessario fornire spazio sufficiente sui siti rimanenti per ospitare i dati degli oggetti che verranno spostati a causa delle modifiche apportate al criterio ILM attivo. In alcuni casi, potrebbe essere necessario espandere il sistema StorageGRID aggiungendo nodi di storage, volumi di storage o nuovi siti prima di completare la decommissionazione di un sito connesso.
- Per completare la procedura di decommissionamento, è necessario attendere il tempo necessario. I processi ILM di StorageGRID potrebbero richiedere giorni, settimane o persino mesi per spostare o eliminare i dati degli oggetti dal sito prima che il sito possa essere disattivato.

> Lo spostamento o l'eliminazione dei dati degli oggetti da un sito potrebbe richiedere giorni, settimane o persino mesi, a seconda della quantità di dati nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

- Se possibile, completare i passaggi 1-4 della procedura guidata Decommission Site il prima possibile. La procedura di decommissionamento viene completata più rapidamente e con meno interruzioni e impatti sulle performance se si consente lo spostamento dei dati dal sito prima di avviare la procedura di decommissionamento effettiva (selezionando **Avvia decommissionamento** nella fase 5 della procedura guidata).

Requisiti aggiuntivi per la decommissionazione di un sito disconnesso

Prima che StorageGRID possa rimuovere un sito disconnesso, è necessario assicurarsi che:

- Hai contattato il tuo rappresentante commerciale NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site.

> Non tentare di decommissionare un sito disconnesso se si ritiene che sia possibile ripristinare il sito o i dati degli oggetti dal sito.

- Tutti i nodi del sito devono avere uno stato di connessione di uno dei seguenti:
  - **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.

- **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 chiusi.

- Tutti i nodi di tutti gli altri siti devono avere uno stato di connessione di **connesso** ( ); tuttavia, questi altri nodi possono avere avvisi attivi.
- È necessario comprendere che non sarà più possibile utilizzare StorageGRID per visualizzare o recuperare i dati degli oggetti memorizzati nel sito. Quando StorageGRID esegue questa procedura, non tenta di conservare i dati del sito disconnesso.

> Se le regole e i criteri ILM sono stati progettati per proteggere dalla perdita di un singolo sito, le copie degli oggetti rimangono nei siti rimanenti.

- È necessario comprendere che se il sito conteneva l'unica copia di un oggetto, l'oggetto viene perso e non può essere recuperato.

Considerazioni sui controlli di coerenza quando si rimuove un sito

Il livello di coerenza per un bucket S3 o un container Swift determina se StorageGRID replica completamente i metadati degli oggetti in tutti i nodi e siti prima di comunicare a un client che l'acquisizione degli oggetti ha avuto successo. I controlli di coerenza forniscono un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage.

Quando StorageGRID rimuove un sito, deve assicurarsi che non vengano scritti dati sul sito da rimuovere. Di conseguenza, sovrascrive temporaneamente il livello di coerenza per ciascun bucket o container. Dopo aver avviato il processo di decommissionamento del sito, StorageGRID utilizza temporaneamente una forte coerenza del sito per impedire che i metadati degli oggetti vengano scritti nel sito.

Come risultato di questa override temporanea, tenere presente che le operazioni di scrittura, aggiornamento ed eliminazione dei client che si verificano durante la decommissionazione di un sito possono avere esito negativo se più nodi diventano non disponibili negli altri siti.

Informazioni correlate

Come viene eseguito il ripristino del sito dal supporto tecnico

Gestire gli oggetti con ILM

Espandi il tuo grid

Raccogliere il materiale necessario

Prima di decommissionare un sito, è necessario procurarsi i seguenti materiali.

Elemento	Note
Pacchetto di ripristino `.zip` file	È necessario scaricare il pacchetto di ripristino più recente `.zip` file (`sgws-recovery-package-id-revision.zip`). È possibile utilizzare il file Recovery Package per ripristinare il sistema in caso di errore.

`Passwords.txt` file	Questo file contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando ed è incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non si trova in `Passwords.txt` file.
Descrizione della topologia del sistema StorageGRID prima dello smantellamento	Se disponibile, procurarsi la documentazione che descrive la topologia corrente del sistema.

Informazioni correlate

Requisiti del browser Web

Scaricare il pacchetto di ripristino

Fase 1: Selezionare Site (Sito)

Per determinare se un sito può essere decommissionato, iniziare accedendo alla procedura guidata Decommissionare il sito.

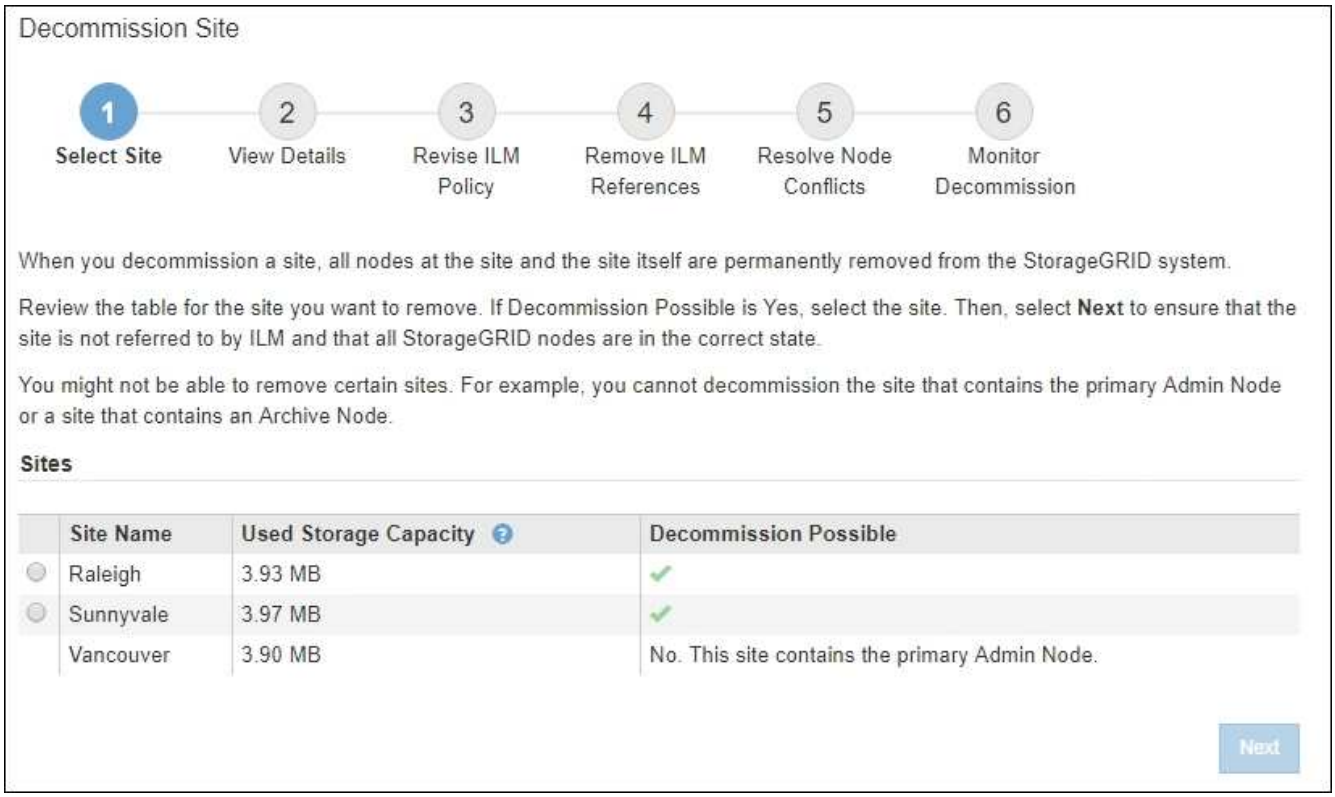
Di cosa hai bisogno

- È necessario aver ottenuto tutti i materiali richiesti.
- È necessario aver esaminato le considerazioni relative alla rimozione di un sito.
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Root Access o delle autorizzazioni Maintenance e ILM.

Fasi

1. Selezionare **MANUTENZIONE attività Smantecazione**.
2. Selezionare **Smantella sito**.

   Viene visualizzata la fase 1 (Seleziona sito) della procedura guidata Smantella sito. Questo passaggio include un elenco alfabetico dei siti nel sistema StorageGRID.



3. Visualizzare i valori nella colonna **capacità di storage utilizzata** per determinare la quantità di storage attualmente utilizzata per i dati a oggetti in ogni sito.

   La capacità di storage utilizzata è una stima. Se i nodi sono offline, la capacità di storage utilizzata è l'ultimo valore noto per il sito.

   - Per la decommissionazione di un sito connesso, questo valore rappresenta la quantità di dati dell'oggetto da spostare in altri siti o da eliminare da ILM prima di poter decommissionare il sito in modo sicuro.
   - Per la decommissionazione di un sito disconnesso, questo valore rappresenta la quantità di storage dei dati del sistema che diventa inaccessibile quando si decommissiona questo sito.

   > Se la policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, le copie dei dati dell'oggetto dovrebbero comunque esistere sui siti rimanenti.

4. Esaminare i motivi nella colonna **Smantella possibile** per determinare quali siti possono essere attualmente dismessi.

   > Se vi sono più motivi per cui un sito non può essere dismesso, viene visualizzato il motivo più critico.

Motivo possibile della decommissionazione	Descrizione	Passo successivo
Segno di spunta verde ( )	È possibile decommissionare questo sito.	Passare a. il passo successivo.

Motivo possibile della decommissionazione	Descrizione	Passo successivo
No Questo sito contiene il nodo di amministrazione principale.	Non è possibile decommissionare un sito contenente il nodo di amministrazione primario.	Nessuno. Non è possibile eseguire questa procedura.
No Questo sito contiene uno o più nodi di archiviazione.	Non è possibile decommissionare un sito contenente un nodo di archiviazione.	Nessuno. Non è possibile eseguire questa procedura.
No Tutti i nodi di questo sito sono disconnessi. Contatta il tuo rappresentante commerciale NetApp.	Non è possibile eseguire la decommissionazione di un sito connesso a meno che tutti i nodi del sito non siano connessi ( ).	Se si desidera eseguire una decommissionazione del sito disconnesso, è necessario contattare il rappresentante commerciale NetApp, che esaminerà i requisiti e attiverà il resto della procedura guidata Decommission Site. **IMPORTANTE**: Non scollegare mai i nodi online per poter rimuovere un sito. I dati andranno persi.

L'esempio mostra un sistema StorageGRID con tre siti. Il segno di spunta verde ( ) Per i siti Raleigh e Sunnyvale indica che è possibile decommissionarli. Tuttavia, non è possibile decommissionare il sito di Vancouver perché contiene il nodo di amministrazione primario.

1. Se è possibile decommissionare, selezionare il pulsante di opzione corrispondente al sito.

   Il pulsante **Avanti** è attivato.

2. Selezionare **Avanti**.

   Viene visualizzato il punto 2 (Visualizza dettagli).

Fase 2: Visualizzare i dettagli

Dalla fase 2 (Visualizza dettagli) della procedura guidata Decommission Site, è possibile esaminare i nodi inclusi nel sito, verificare la quantità di spazio utilizzata su ciascun nodo di storage e valutare la quantità di spazio libero disponibile negli altri siti della griglia.

Di cosa hai bisogno

Prima di decommissionare un sito, è necessario esaminare la quantità di dati oggetto presenti nel sito.

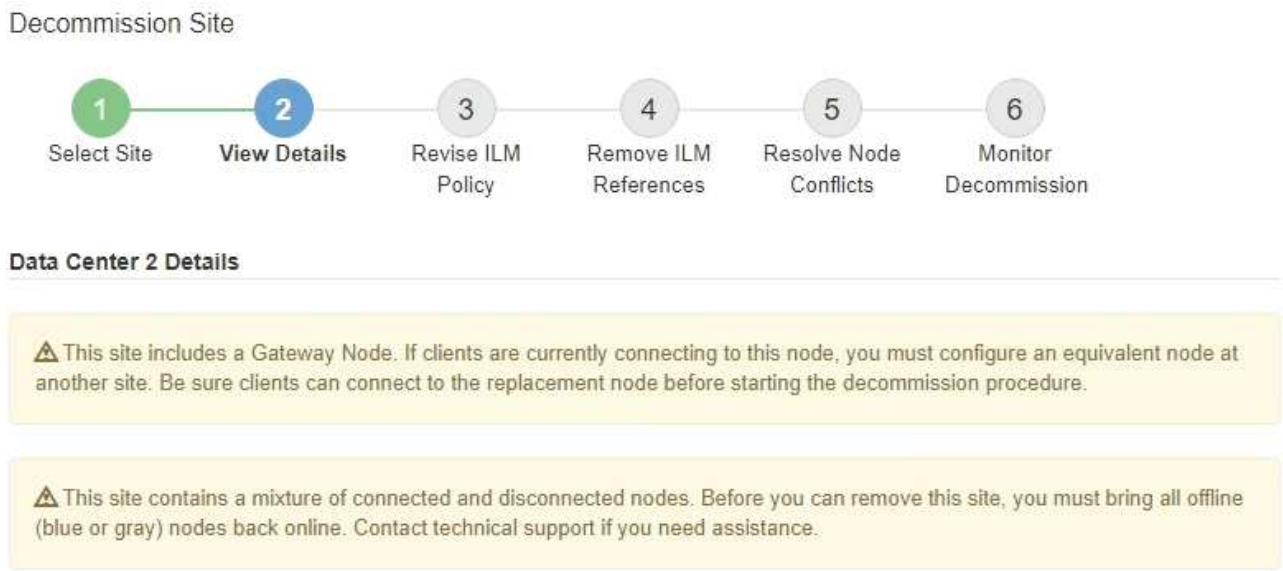
- Se si sta eseguendo una decommissionazione del sito connesso, è necessario comprendere la quantità di dati oggetto attualmente presenti nel sito prima di aggiornare ILM. In base alle capacità del sito e alle esigenze di protezione dei dati, è possibile creare nuove regole ILM per spostare i dati in altri siti o per eliminare i dati degli oggetti dal sito.
- Eseguire le espansioni dei nodi di storage necessarie prima di avviare la procedura di decommissionamento, se possibile.

- Se si esegue una decommissionazione disconnessa del sito, è necessario comprendere la quantità di dati oggetto che diventeranno inaccessibili in modo permanente quando si rimuove il sito.

> Se si sta eseguendo una decommissionazione disconnessa del sito, ILM non può spostare o eliminare i dati dell'oggetto. Tutti i dati che rimangono nel sito andranno persi. Tuttavia, se la policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, le copie dei dati dell'oggetto rimangono nei siti rimanenti.

Fasi

1. Dal passaggio 2 (Visualizza dettagli), esaminare eventuali avvisi relativi al sito selezionato per la rimozione.



   Viene visualizzato un avviso nei seguenti casi:

   - Il sito include un nodo gateway. Se i client S3 e Swift si stanno connettendo a questo nodo, è necessario configurare un nodo equivalente in un altro sito. Assicurarsi che i client possano connettersi al nodo sostitutivo prima di continuare con la procedura di decommissionamento.
   - Il sito contiene una combinazione di) e nodi disconnessi (oppure). Prima di poter rimuovere questo sito, è necessario riportare tutti i nodi offline in linea.

2. Esaminare i dettagli del sito selezionato per la rimozione.

Decommission Site

1 Select Site — 2 View Details — 3 Revise ILM Policy — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

Raleigh Details

Number of Nodes: 3
Free Space: 475.38 GB
Used Space: 3.93 MB
Site Capacity: 475.38 GB

Node Name	Node Type	Connnection State	Details
RAL-S1-101-196	Storage Node	✔	1.30 MB used space
RAL-S2-101-197	Storage Node	✔	1.30 MB used space
RAL-S3-101-198	Storage Node	✔	1.34 MB used space

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	**950.76 GB**	**7.87 MB**	**950.77 GB**

Previous Next

Per il sito selezionato sono incluse le seguenti informazioni:

- Numero di nodi
- Lo spazio utilizzato totale, lo spazio libero e la capacità di tutti i nodi di storage nel sito.
  - Per la decommissionazione di un sito connesso, il valore **Used Space** rappresenta la quantità di dati oggetto che devono essere spostati in altri siti o cancellati con ILM.
  - Per la decommissionazione di un sito disconnesso, il valore **spazio utilizzato** indica la quantità di dati oggetto che diventeranno inaccessibili quando si rimuove il sito.
- Nomi, tipi e stati di connessione dei nodi:
  - (Connesso)
  - (Amministrazione non disponibile)
  - (Sconosciuto)
- Dettagli su ciascun nodo:
  - Per ciascun nodo di storage, la quantità di spazio utilizzata per i dati dell'oggetto.

- Per i nodi Admin e Gateway, se il nodo è attualmente utilizzato in un gruppo ad alta disponibilità (ha). Non è possibile decommissionare un nodo amministratore o un nodo gateway utilizzato in un gruppo ha. Prima di avviare la decommissionazione, è necessario modificare i gruppi ha per rimuovere tutti i nodi nel sito. In alternativa, è possibile rimuovere il gruppo ha se include solo nodi da questo sito.

  Amministrare StorageGRID

3. Nella sezione Dettagli per altri siti della pagina, valuta lo spazio disponibile negli altri siti della griglia.

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Se si sta eseguendo una decommissionazione del sito connesso e si prevede di utilizzare ILM per spostare i dati dell'oggetto dal sito selezionato (invece di eliminarli semplicemente), è necessario assicurarsi che gli altri siti abbiano una capacità sufficiente per ospitare i dati spostati e che rimanga una capacità adeguata per la crescita futura.

> Viene visualizzato un avviso se lo spazio utilizzato * del sito che si desidera rimuovere è maggiore di **spazio libero totale per altri siti**. Per garantire che sia disponibile una capacità di storage adeguata dopo la rimozione del sito, potrebbe essere necessario eseguire un'espansione prima di eseguire questa procedura.

4. Selezionare **Avanti**.

   Viene visualizzato il punto 3 (revisione policy ILM).

Informazioni correlate

Gestire gli oggetti con ILM

Fase 3: Revisione della policy ILM

Dalla fase 3 (revisione policy ILM) della procedura guidata Decommission Site (Sito di rimozione), è possibile determinare se il sito fa riferimento al criterio ILM attivo.

Di cosa hai bisogno

Hai una buona conoscenza del funzionamento di ILM e conosci la creazione di pool di storage, profili di codifica Erasure, regole ILM e la simulazione e l'attivazione di un criterio ILM.

Gestire gli oggetti con ILM

A proposito di questa attività

StorageGRID non è in grado di decommissionare un sito se tale sito è indicato da una regola ILM nel criterio ILM attivo.

Se la policy ILM corrente fa riferimento al sito che si desidera rimuovere, è necessario attivare una nuova policy ILM che soddisfi determinati requisiti. In particolare, la nuova policy ILM:

- Impossibile utilizzare un pool di storage che si riferisce al sito.
- Impossibile utilizzare un profilo di codifica Erasure che si riferisce al sito.
- Impossibile utilizzare il pool di storage predefinito **All Storage Nodes** o il sito predefinito **All Sites**.
- Non è possibile utilizzare la regola di archiviazione **creazione di 2 copie**.
- Deve essere progettato per proteggere completamente tutti i dati degli oggetti.

> Non creare mai una regola ILM a copia singola per consentire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Se si esegue una *decommissionazione del sito connesso*, è necessario considerare come StorageGRID deve gestire i dati dell'oggetto attualmente nel sito che si desidera rimuovere. A seconda dei requisiti di protezione dei dati, le nuove regole possono spostare i dati degli oggetti esistenti in siti diversi o eliminare eventuali copie di oggetti extra non più necessarie.

Contattare il supporto tecnico per ricevere assistenza nella progettazione della nuova policy.

Fasi

1. Dalla fase 3 (revisione policy ILM), determinare se eventuali regole ILM nel criterio ILM attivo fanno riferimento al sito selezionato per la rimozione.

Decommission Site

1 Select Site — 2 View Details — 3 **Revise ILM Policy** — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

If your current ILM policy refers to the site, you must activate a new policy before you can go to the next step.

The new ILM policy:

- Cannot use a storage pool that refers to the site.
- Cannot use an Erasure Coding profile that refers to the site.
- Cannot use the default **All Storage Nodes** storage pool or the default **All Sites** site.
- Cannot use the **Make 2 Copies** rule.
- Must be designed to fully protect all object data after one site is removed.

Contact technical support if you need assistance in designing the new policy.

If you are performing a connected site decommission, StorageGRID will begin to remove object data from the site as soon as you activate the new ILM policy. Moving or deleting all object copies might take weeks, but you can safely start a site decommission while object data still exists at the site.

Rules Referring to Raleigh in the Active ILM Policy

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: Data Protection for Three Sites

The active ILM policy refers to Raleigh. Before you can remove this site, you must propose and activate a new policy.

Name	EC Profiles	Storage Pools
3 copies for S3 tenant	—	Raleigh storage pool
2 copy 2 sites for smaller objects	—	Raleigh storage pool
EC for larger objects	three site EC profile	All 3 Sites

Previous Next

2. Se non sono elencate regole, selezionare **Avanti** per passare alla fase 4 (Rimuovi riferimenti ILM)

Fase 4: Rimuovere i riferimenti ILM

3. Se una o più regole ILM sono elencate nella tabella, selezionare il collegamento accanto a **Active Policy Name**.

   La pagina ILM Policies (Criteri ILM) viene visualizzata in una nuova scheda del browser. Utilizzare questa scheda per aggiornare ILM. La pagina Decommission Site rimane aperta nella scheda Other (Altro).

   a. Se necessario, selezionare **ILM** > **Storage Pools** per creare uno o più pool di storage che non fanno riferimento al sito.

> Per ulteriori informazioni, consulta le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

b. Se si intende utilizzare la codifica di cancellazione, selezionare **ILM** > **Erasure coding** per creare uno o più profili di codifica di cancellazione.

   È necessario selezionare i pool di storage che non fanno riferimento al sito.

> Non utilizzare il pool di storage **All Storage Node** nei profili di codifica Erasure.

4. Selezionare **ILM** > **Rules** e clonare ciascuna delle regole elencate nella tabella per la fase 3 (rivedere la policy ILM).

> Per ulteriori informazioni, consulta le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

   a. Utilizzare nomi che semplificino la selezione di queste regole in una nuova policy.
   b. Aggiornare le istruzioni di posizionamento.

      Rimuovere eventuali pool di storage o profili di codifica Erasure che fanno riferimento al sito e sostituirli con nuovi pool di storage o profili di codifica Erasure.

> Non utilizzare il pool di storage **All Storage Node** nelle nuove regole.

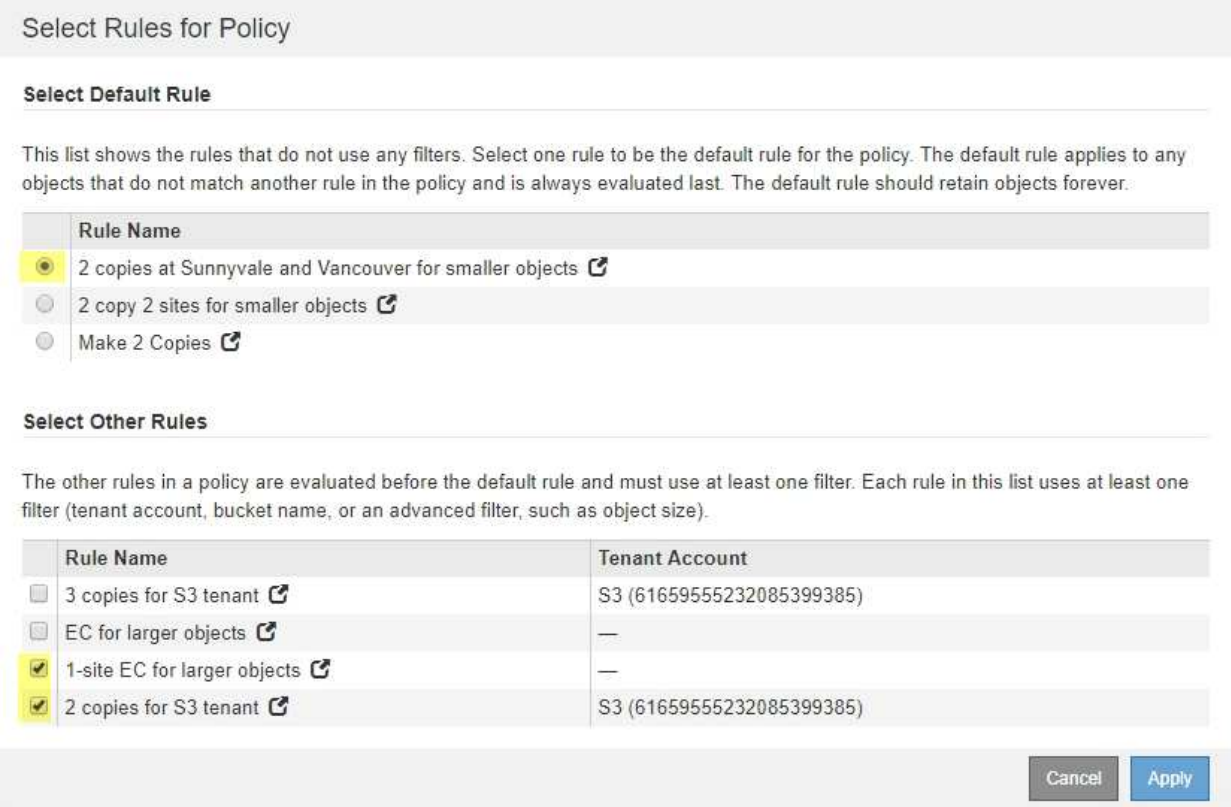
5. Selezionare **ILM** > **Policies** e creare una nuova policy che utilizzi le nuove regole.

> Per ulteriori informazioni, consulta le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

   a. Selezionare il criterio attivo e selezionare **Clone**.
   b. Specificare il nome di un criterio e il motivo della modifica.
   c. Selezionare le regole per il criterio clonato.
      - Deselezionare tutte le regole elencate per la fase 3 (revisione policy ILM) della pagina Decommission Site.
      - Selezionare una regola predefinita che non si riferisce al sito.

> Non selezionare la regola **Crea 2 copie** perché questa regola utilizza il pool di storage **tutti i nodi di storage**, che non è consentito.

      - Selezionare le altre regole di sostituzione create. Queste regole non devono fare riferimento al sito.



d. Selezionare **Applica**.

e. Trascinare e rilasciare le righe per riordinare le regole nel criterio.

   Non è possibile spostare la regola predefinita.

> Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

a. Salvare la policy proposta.

6. Acquisire oggetti di test e simulare il criterio proposto per garantire l'applicazione delle regole corrette.

> Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.

> Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

7. Attivare la nuova policy.

   Se si sta eseguendo una decommissionazione del sito connesso, StorageGRID inizia a rimuovere i dati dell'oggetto dal sito selezionato non appena si attiva il nuovo criterio ILM. Lo spostamento o l'eliminazione di tutte le copie degli oggetti potrebbe richiedere settimane. Sebbene sia possibile avviare in sicurezza la decommissionazione di un sito mentre i dati degli oggetti sono ancora presenti nel sito, la procedura di

decommissionazione viene completata più rapidamente e con meno interruzioni e impatti sulle performance se si consente di spostare i dati dal sito prima di avviare la procedura di decommissionazione effettiva (Selezionando **Avvia decommissionazione** nella fase 5 della procedura guidata).

8. Tornare al passaggio 3 (revisione policy ILM)* per assicurarsi che nessuna regola ILM nel nuovo criterio attivo faccia riferimento al sito e che il pulsante **Avanti** sia attivato.

> Se sono elencate delle regole, è necessario creare e attivare una nuova policy ILM prima di poter continuare.

9. Se non sono elencate regole, selezionare **Avanti**.

   Viene visualizzato il punto 4 (Rimuovi riferimenti ILM).

Fase 4: Rimuovere i riferimenti ILM

Dalla fase 4 (Rimuovi riferimenti ILM) della procedura guidata Decommission Site, è possibile rimuovere la policy proposta, se esistente, ed eliminare o modificare eventuali regole ILM inutilizzate che fanno ancora riferimento al sito.

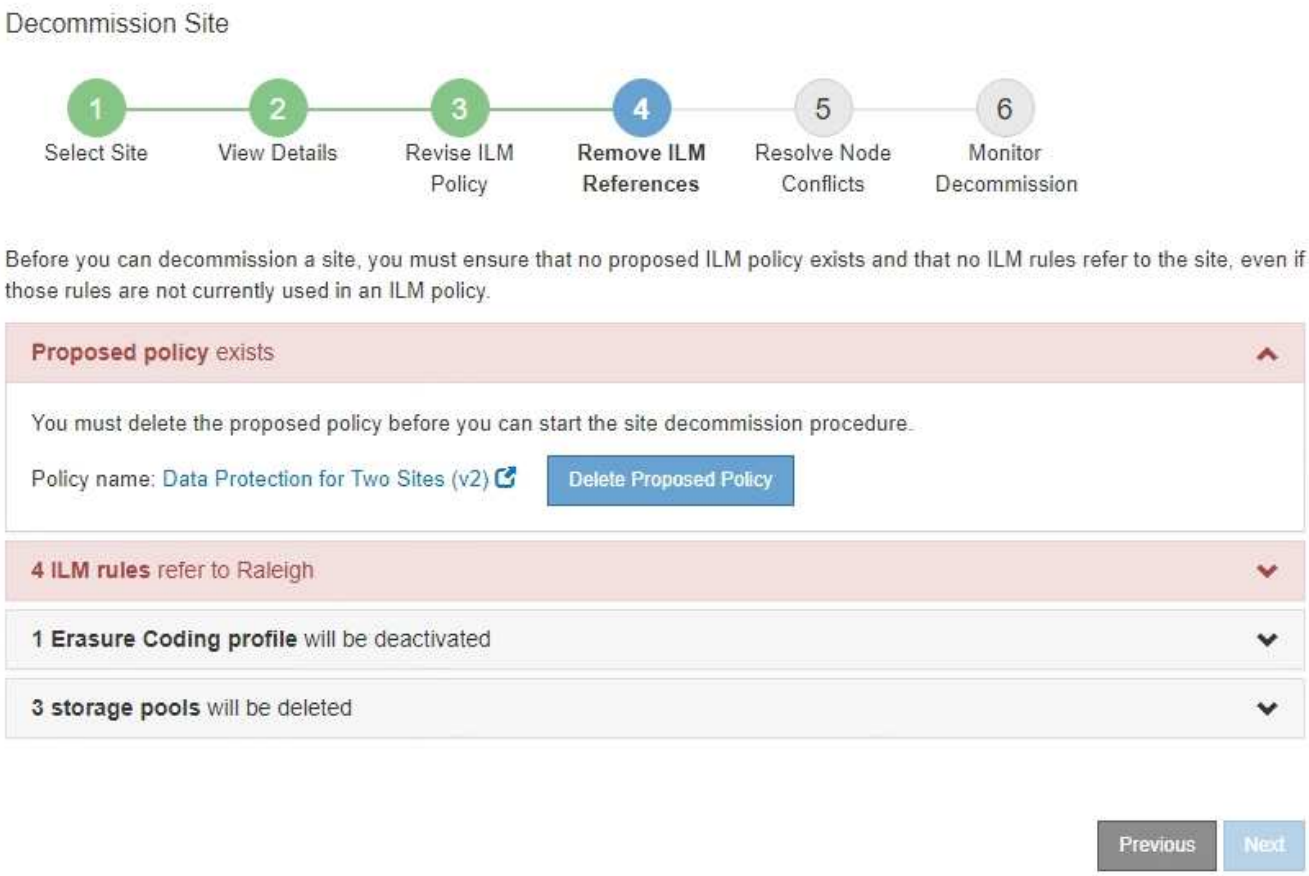
A proposito di questa attività

Non è possibile avviare la procedura di decommissionamento del sito nei seguenti casi:

- Esiste una policy ILM proposta. Se si dispone di una policy proposta, è necessario eliminarla.
- Qualsiasi regola ILM si riferisce al sito, anche se tale regola non viene utilizzata in alcun criterio ILM. È necessario eliminare o modificare tutte le regole che fanno riferimento al sito.

Fasi

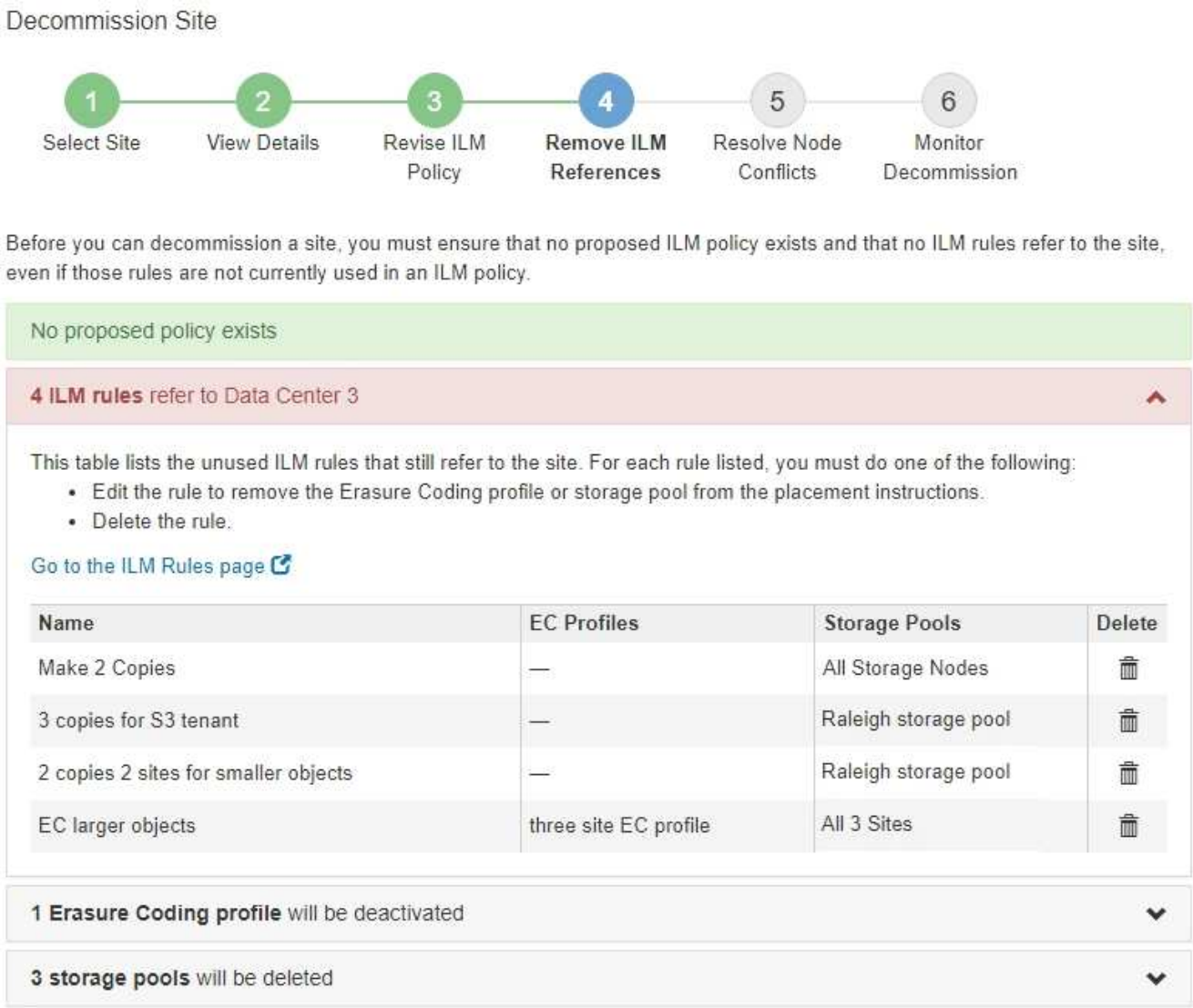
1. Se viene elencato un criterio proposto, rimuoverlo.



a. Selezionare **Delete Proposed Policy** (Elimina policy proposte).

b. Selezionare **OK** nella finestra di dialogo di conferma.

2. Determinare se eventuali regole ILM inutilizzate fanno riferimento al sito.



Tutte le regole ILM elencate fanno ancora riferimento al sito ma non vengono utilizzate in alcuna policy. Nell'esempio:

- La regola **Crea 2 copie** utilizza il pool di storage predefinito di sistema **tutti i nodi di storage**, che utilizza il sito All Sites.
- La regola **3 copie inutilizzate per il tenant S3** si riferisce al pool di storage **Raleigh**.
- La regola **2 copy 2 siti non utilizzati per oggetti di piccole dimensioni** si riferisce al pool di storage **Raleigh**.
- Le regole **EC larger objects** inutilizzate utilizzano il sito Raleigh nel profilo di codifica Erasure di **All 3 Sites**.
- Se non sono elencate regole ILM, selezionare **Avanti** per passare al **Passo 5 (Risolvi conflitti di nodi)**.

Fase 5: Risolvere i conflitti dei nodi (e avviare la decommissionazione)

> Quando StorageGRID decommissiona il sito, disattiva automaticamente i profili di codifica di cancellazione non utilizzati che fanno riferimento al sito e elimina automaticamente i pool di storage inutilizzati che fanno riferimento al sito. Il pool di storage di tutti i nodi di storage predefinito del sistema viene rimosso perché utilizza il sito All Sites.

- Se sono elencate una o più regole ILM, passare alla fase successiva.

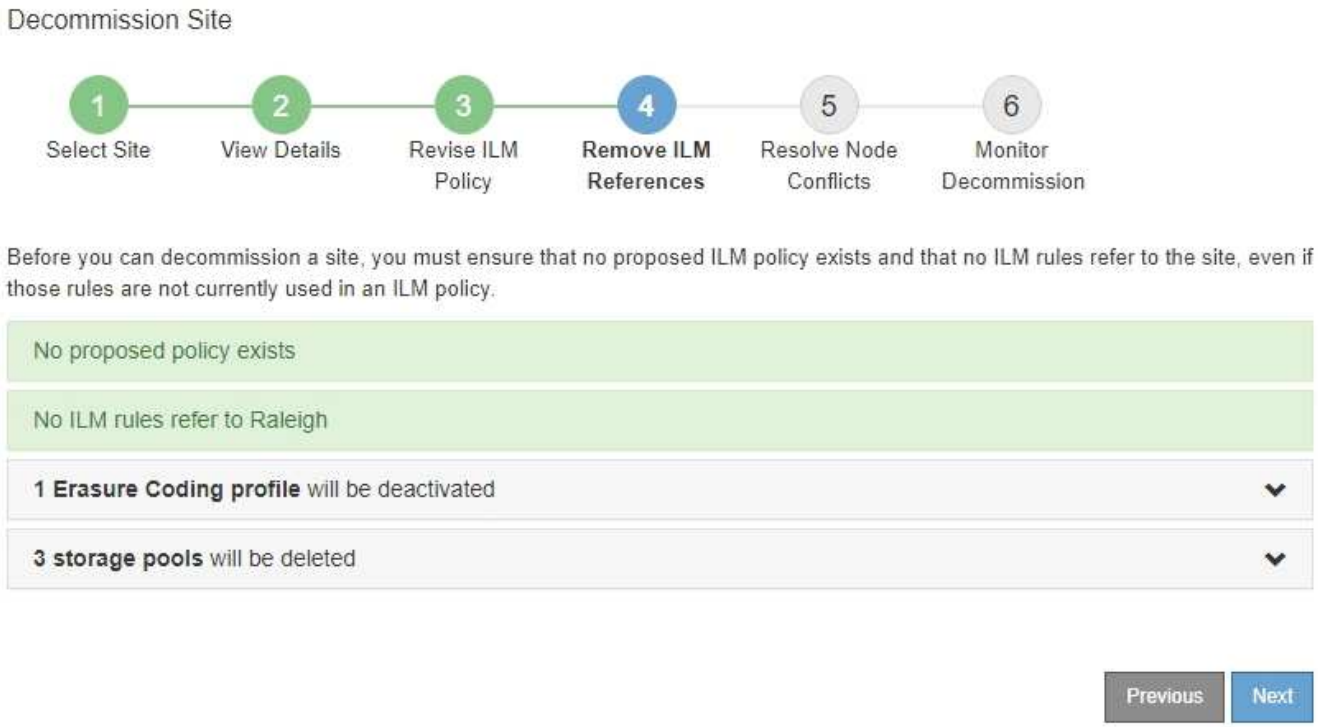
3. Modificare o eliminare ogni regola inutilizzata:
   - Per modificare una regola, accedere alla pagina ILM Rules (regole ILM) e aggiornare tutte le posizioni che utilizzano un profilo di codifica Erasure o un pool di storage che fa riferimento al sito. Quindi, tornare al **Passo 4 (Rimozione dei riferimenti ILM)**.

     > Per ulteriori informazioni, consulta le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

   - Per eliminare una regola, selezionare l'icona del cestino E selezionare **OK**.

     > Prima di poter decommissionare un sito, è necessario eliminare la regola **Make 2 copies**.

4. Verificare che non esista alcun criterio ILM proposto, che non vi siano regole ILM inutilizzate relative al sito e che il pulsante **Avanti** sia attivato.



5. Selezionare **Avanti**.

   > Gli eventuali pool di storage rimanenti e i profili di codifica Erasure che fanno riferimento al sito diventeranno invalidi quando il sito viene rimosso. Quando StorageGRID decommissiona il sito, disattiva automaticamente i profili di codifica di cancellazione non utilizzati che fanno riferimento al sito e elimina automaticamente i pool di storage inutilizzati che fanno riferimento al sito. Il pool di storage di tutti i nodi di storage predefinito del sistema viene rimosso perché utilizza il sito All Sites.

   Viene visualizzato il punto 5 (Risolvi conflitti di nodi).

Fase 5: Risolvere i conflitti dei nodi (e avviare la decommissionazione)

Dalla fase 5 (Risolvi conflitti di nodi) della procedura guidata Smantella sito, è possibile determinare se i nodi nel sistema StorageGRID sono disconnessi o se i nodi nel sito selezionato appartengono a un gruppo ad alta disponibilità (ha). Una volta risolti i conflitti di nodo, avviare la procedura di decommissionamento da questa pagina.

È necessario assicurarsi che tutti i nodi nel sistema StorageGRID siano nello stato corretto, come indicato di seguito:

- Tutti i nodi nel sistema StorageGRID devono essere connessi ( ).

  > Se si sta eseguendo una decommissionazione del sito disconnesso, tutti i nodi del sito che si sta rimuovendo devono essere disconnessi e tutti i nodi di tutti gli altri siti devono essere connessi.

- Nessun nodo del sito che si sta rimuovendo può avere un'interfaccia che appartiene a un gruppo ad alta disponibilità (ha).

Se un nodo è elencato per la fase 5 (Risolvi conflitti di nodi), è necessario correggere il problema prima di poter avviare la decommissionazione.

Prima di iniziare la procedura di decommissionamento del sito da questa pagina, fare riferimento alle seguenti considerazioni:

- Per completare la procedura di decommissionamento, è necessario attendere il tempo necessario.

  > Lo spostamento o l'eliminazione dei dati degli oggetti da un sito potrebbe richiedere giorni, settimane o persino mesi, a seconda della quantità di dati nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

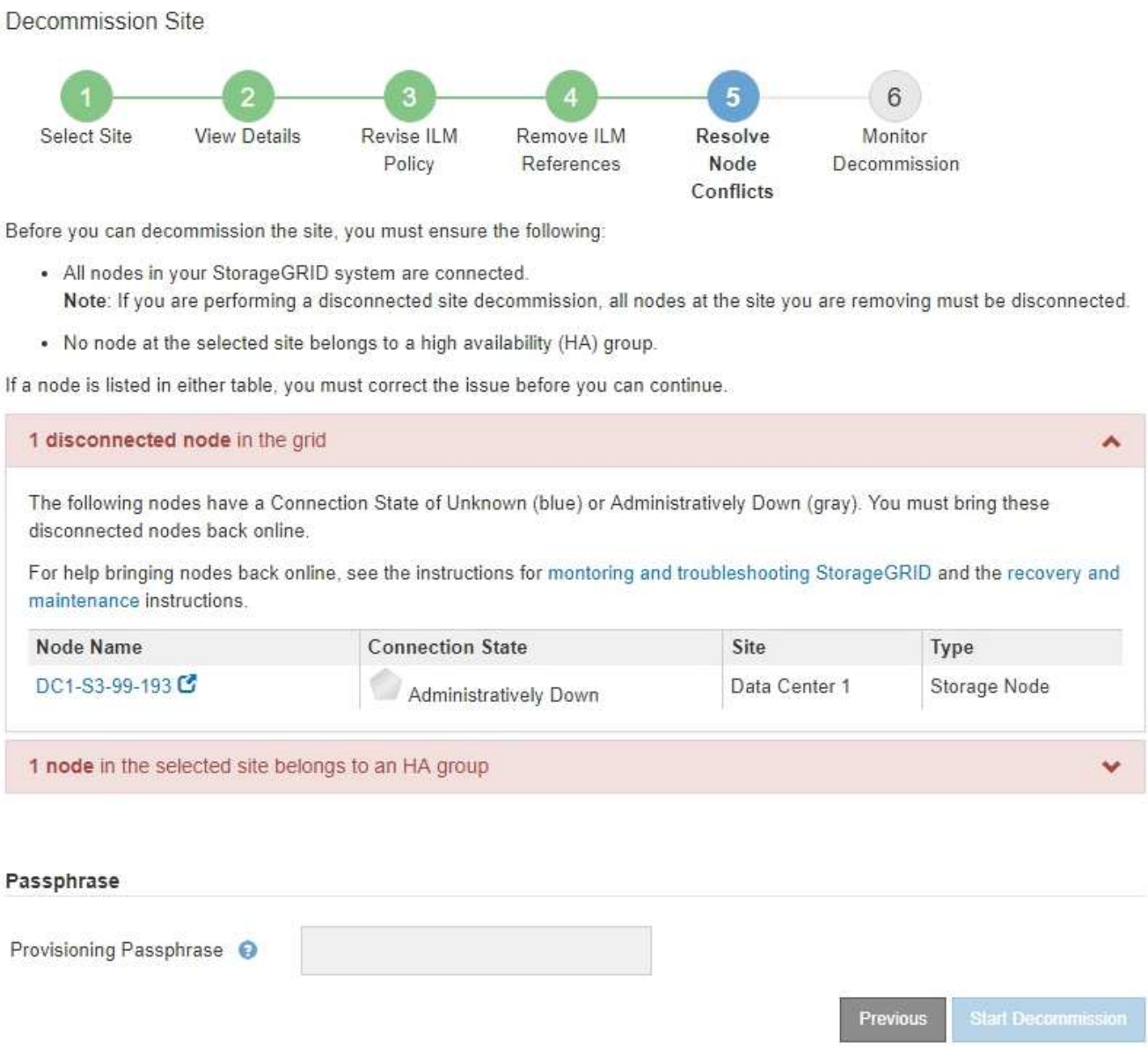
- Durante l'esecuzione della procedura di decommissionamento del sito:
  - Non è possibile creare regole ILM che si riferiscono al sito da smantellare. Non è inoltre possibile modificare una regola ILM esistente per fare riferimento al sito.
  - Non è possibile eseguire altre procedure di manutenzione, ad esempio l'espansione o l'aggiornamento.

    > Se è necessario eseguire un'altra procedura di manutenzione durante la decommissionazione di un sito connesso, è possibile sospendere la procedura durante la rimozione dei nodi di storage. Il pulsante **Pause** viene attivato durante la fase "Deommissioning Replicated and Erasure Coded Data".

  - Se è necessario ripristinare un nodo dopo aver avviato la procedura di decommissionamento del sito, contattare il supporto.

Fasi

1. Consultare la sezione nodi disconnessi del passaggio 5 (Risolvi conflitti di nodi) per determinare se uno stato di connessione dei nodi nel sistema StorageGRID è sconosciuto ( ) O dal punto di vista amministrativo ( ).

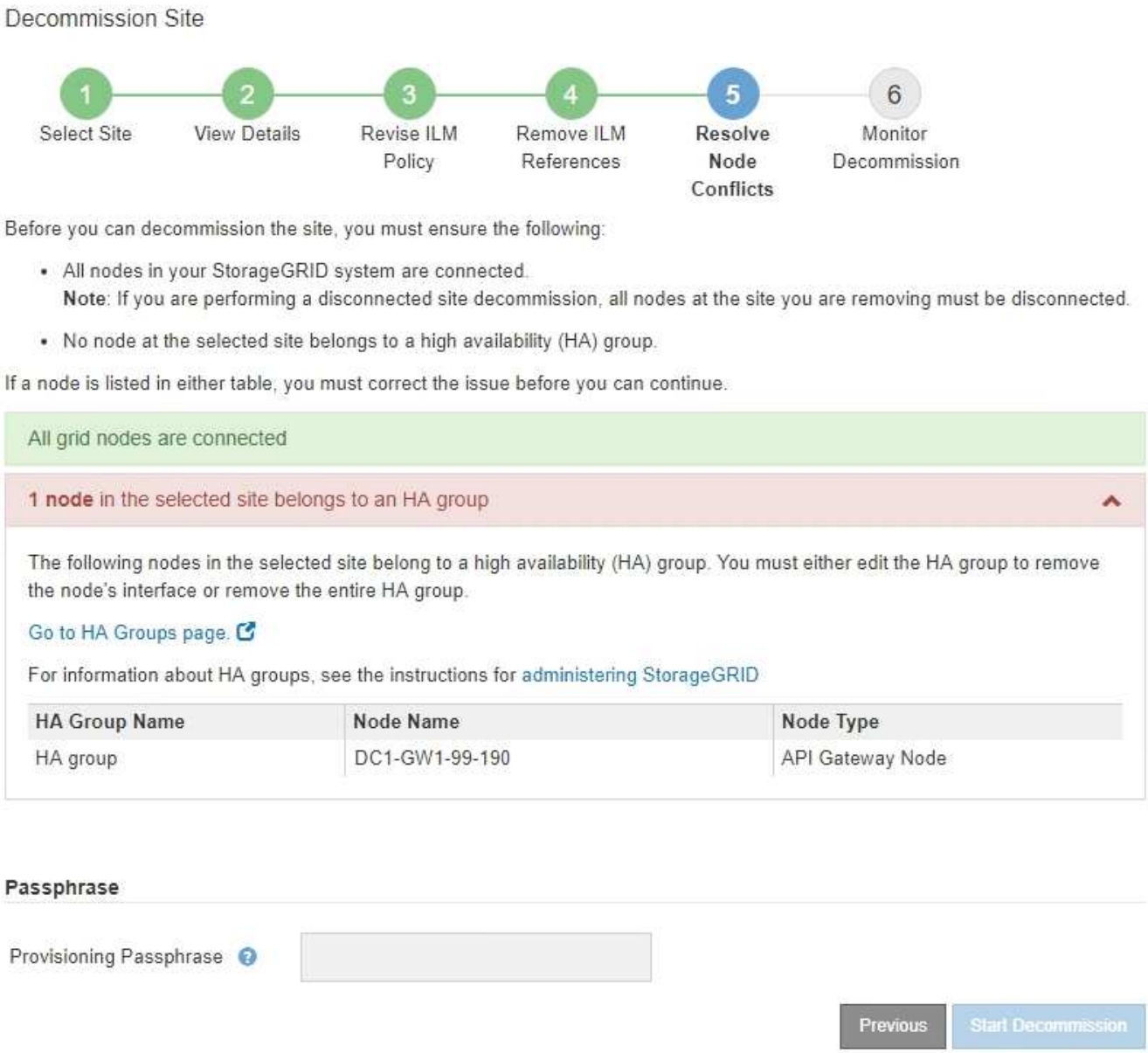


2. Se alcuni nodi sono disconnessi, riportarli in linea.

   Consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID e delle procedure del nodo di rete. Se hai bisogno di assistenza, contatta il supporto tecnico.

3. Quando tutti i nodi disconnessi sono stati riportati online, consultare la sezione gruppi ha del passaggio 5 (Risolvi i conflitti dei nodi).

   Questa tabella elenca tutti i nodi del sito selezionato che appartengono a un gruppo ad alta disponibilità (ha).

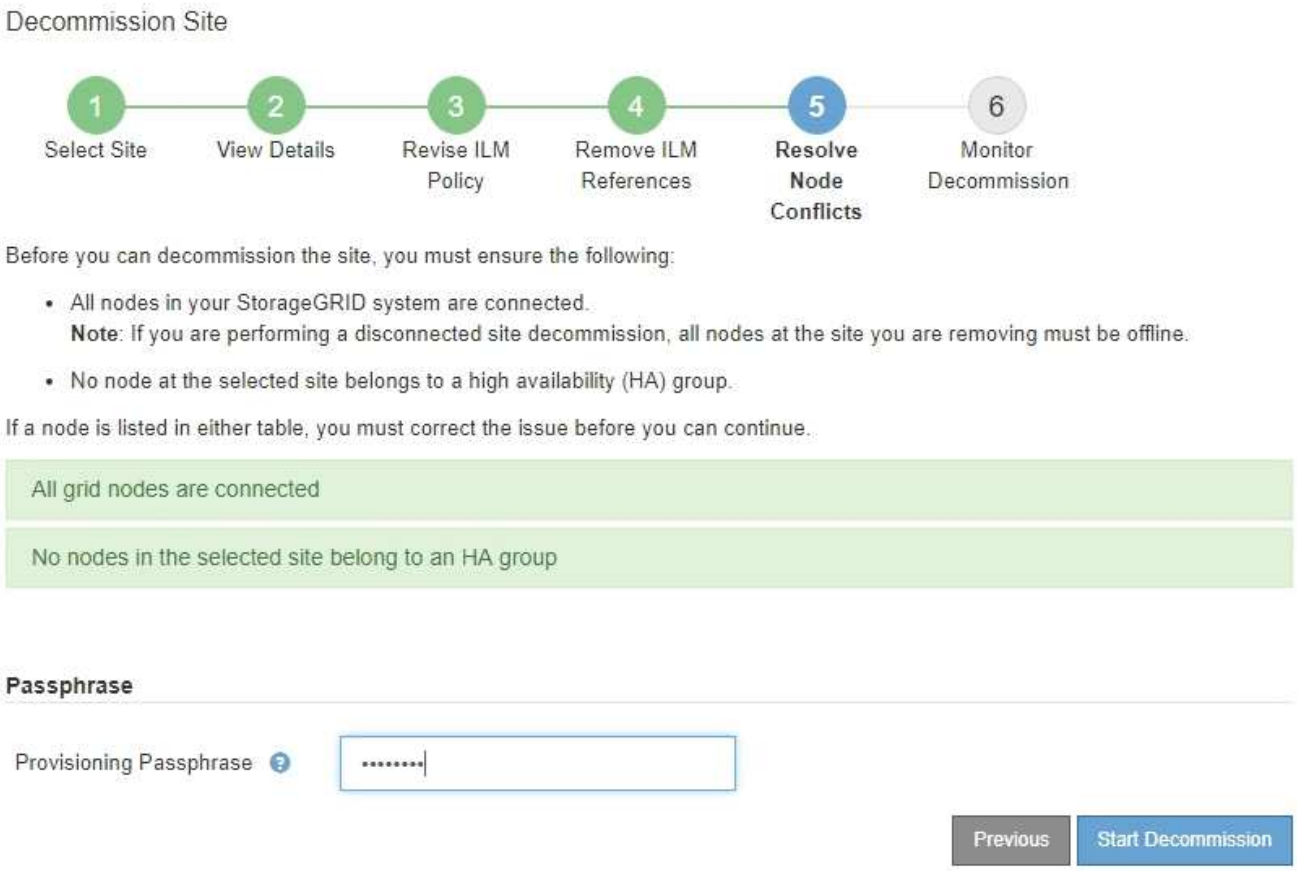


4. Se nell'elenco sono presenti nodi, eseguire una delle seguenti operazioni:
   - Modificare ciascun gruppo ha interessato per rimuovere l'interfaccia del nodo.
   - Rimuovere un gruppo ha che include solo i nodi da questo sito. Consultare le istruzioni per l'amministrazione di StorageGRID.

   Se tutti i nodi sono connessi e nessun nodo nel sito selezionato viene utilizzato in un gruppo ha, viene attivato il campo **Provisioning Passphrase**.

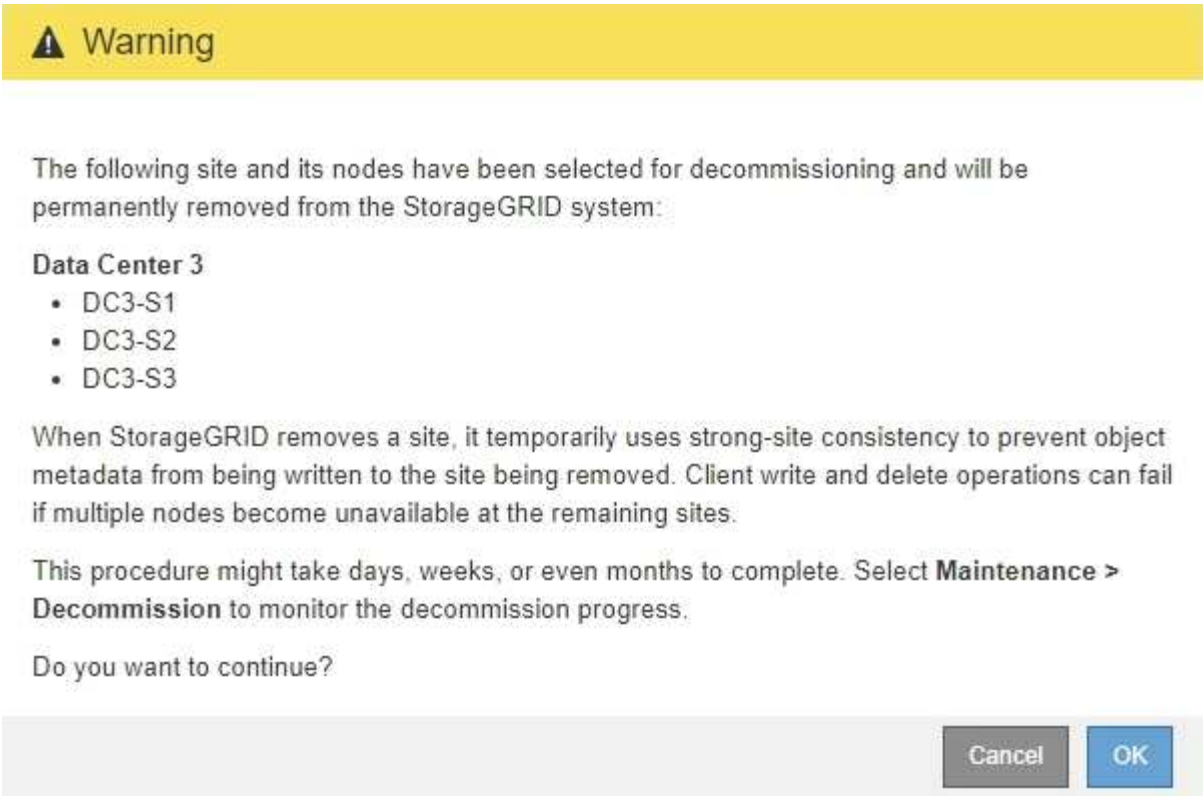
5. Inserire la passphrase di provisioning.

   Il pulsante **Avvia decommissionazione** viene attivato.



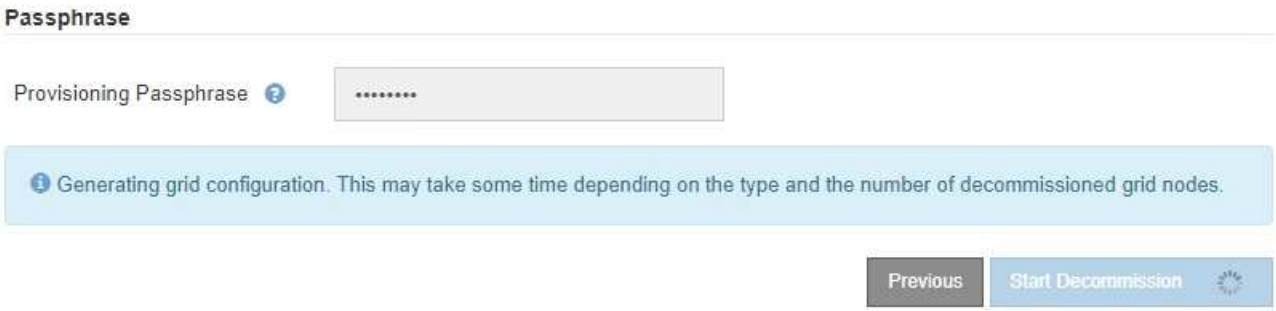
6. Se si è pronti per avviare la procedura di decommissionamento del sito, selezionare **Avvia decommissionazione**.

   Un avviso elenca il sito e i nodi che verranno rimossi. Ti ricordiamo che potrebbero essere necessari giorni, settimane o mesi per rimuovere completamente il sito.



7. Esaminare l'avviso. Se si è pronti per iniziare, selezionare **OK**.

   Quando viene generata la nuova configurazione della griglia, viene visualizzato un messaggio. Questo processo potrebbe richiedere del tempo, a seconda del tipo e del numero di nodi di rete decommissionati.



   Una volta generata la nuova configurazione della griglia, viene visualizzato il punto 6 (Monitor Decommission).

   Il pulsante **precedente** rimane disattivato fino al completamento della decommissionazione.

Informazioni correlate

Monitorare e risolvere i problemi

Procedure del nodo di rete

Amministrare StorageGRID

Fase 6: Rimozione del monitor

Dalla fase 6 (Monitor Decommission) della procedura guidata della pagina Decommission Site (Smantella sito), è possibile monitorare l'avanzamento della procedura di rimozione del sito.

A proposito di questa attività

Quando StorageGRID rimuove un sito connesso, rimuove i nodi nel seguente ordine:

1. Nodi gateway
2. Nodi di amministrazione
3. Nodi di storage

Quando StorageGRID rimuove un sito disconnesso, rimuove i nodi nel seguente ordine:

1. Nodi gateway
2. Nodi di storage
3. Nodi di amministrazione

Ogni nodo gateway o nodo amministratore potrebbe richiedere solo pochi minuti o un'ora per la rimozione; tuttavia, i nodi storage potrebbero richiedere giorni o settimane.

Fasi

1. Non appena viene generato un nuovo pacchetto di ripristino, scaricare il file.

> Scarica il pacchetto di ripristino il prima possibile per assicurarti di ripristinare la griglia in caso di problemi durante la procedura di decommissionamento.

a. Selezionare il collegamento nel messaggio o selezionare **MANUTENZIONE sistema pacchetto di ripristino**.

b. Scaricare il `.zip` file.

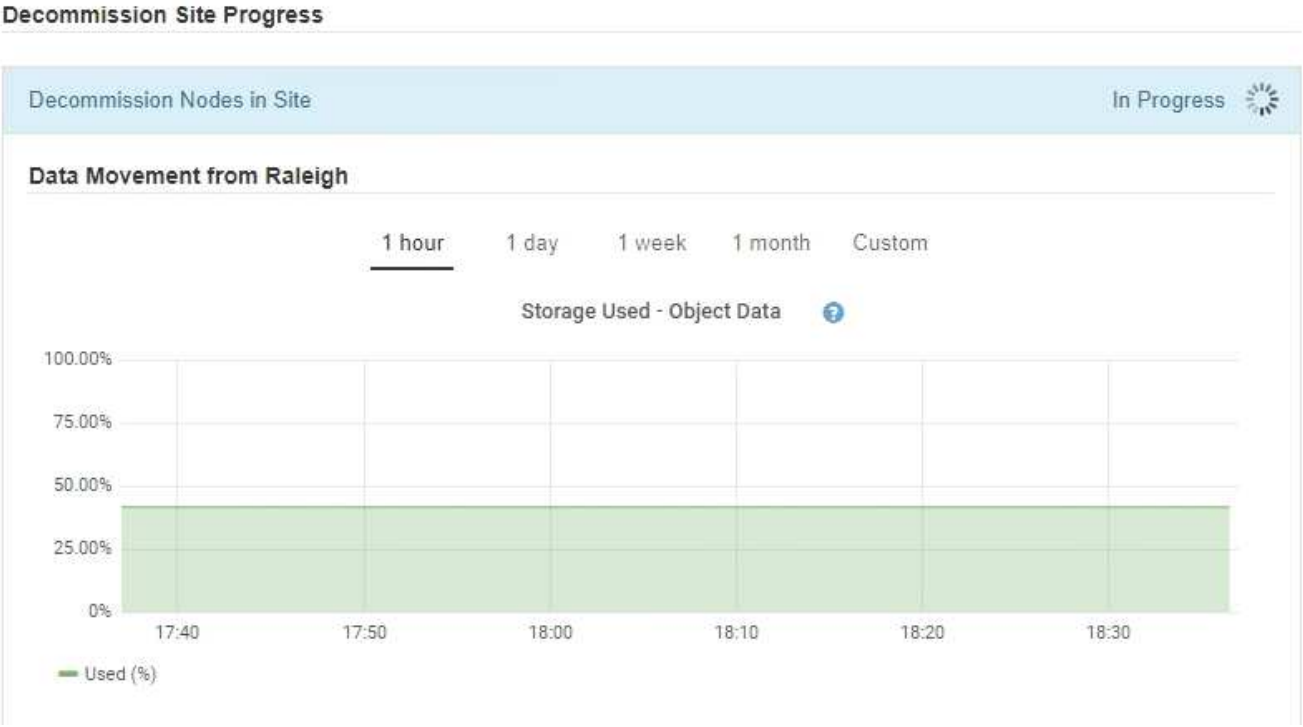
   Consultare le istruzioni per Download del pacchetto di ripristino.

> Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

2. Utilizzando il grafico spostamento dati, monitorare lo spostamento dei dati oggetto da questo sito ad altri

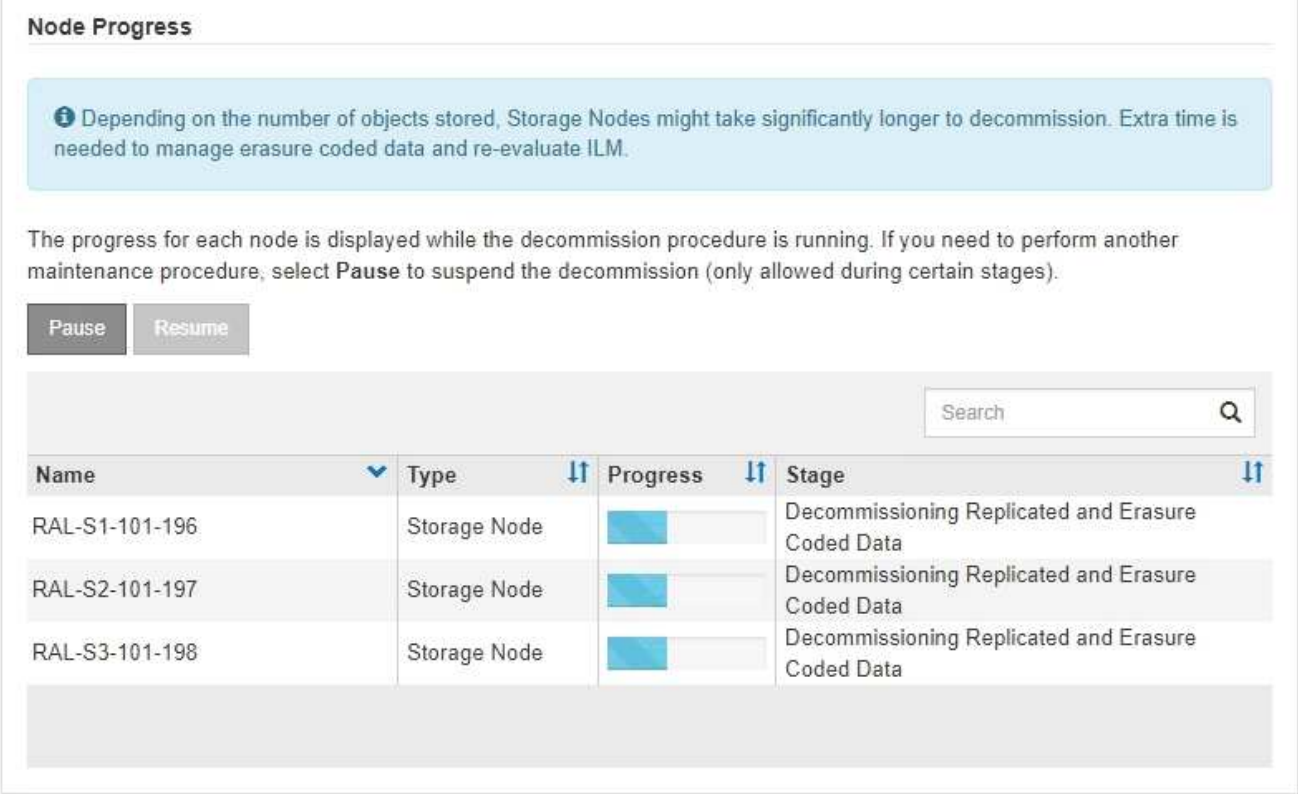
siti.

Lo spostamento dei dati ha avuto inizio quando è stata attivata la nuova policy ILM nella fase 3 (revisione policy ILM). Lo spostamento dei dati avviene durante l'intera procedura di decommissionamento.



3. Nella sezione Node Progress della pagina, monitorare l'avanzamento della procedura di decommissionamento man mano che i nodi vengono rimossi.

   Quando un nodo di storage viene rimosso, ciascun nodo passa attraverso una serie di fasi. Sebbene la maggior parte di queste fasi si verifichi rapidamente o anche in modo impercettibile, potrebbe essere necessario attendere giorni o addirittura settimane per il completamento di altre fasi, in base alla quantità di dati da spostare. Per gestire i dati con codifica di cancellazione e rivalutare ILM è necessario un tempo aggiuntivo.



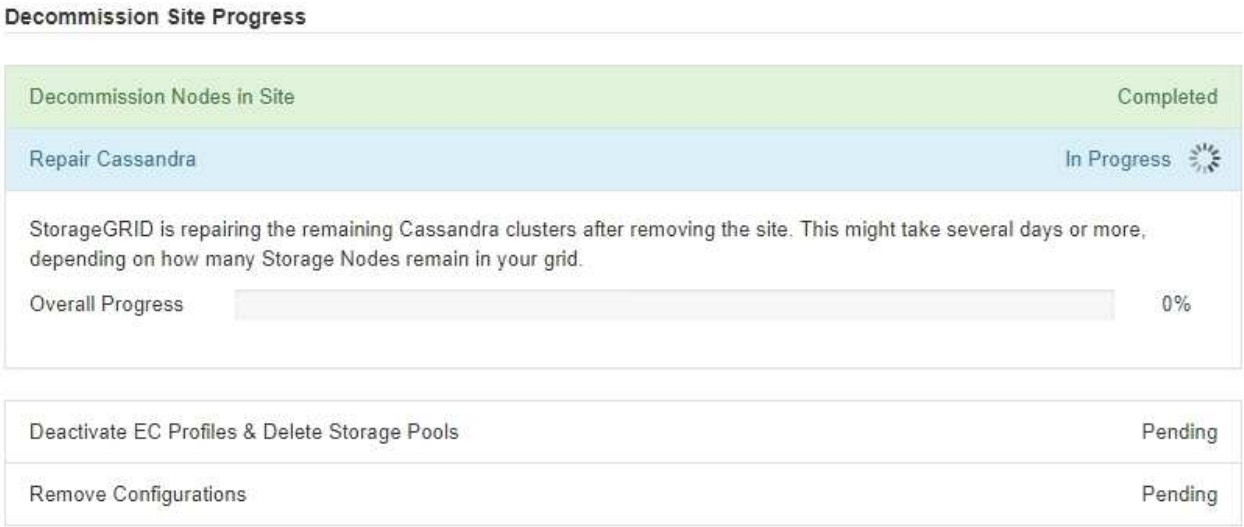
Se si sta monitorando l'avanzamento della decommissionazione di un sito connesso, fare riferimento a questa tabella per comprendere le fasi di decommissionamento di un nodo di storage:

Fase	Durata stimata
In sospeso	Minuti o meno
Attendere i blocchi	Minuti
Preparare l'attività	Minuti o meno
Contrassegno LDR disattivato	Minuti
Decommissionamento dei dati replicati ed Erasure Coded	Ore, giorni o settimane in base alla quantità di dati **Nota**: Se è necessario eseguire altre attività di manutenzione, è possibile sospendere la decommissionazione del sito in questa fase.
Stato impostato LDR	Minuti
Svuotare le code di audit	Da minuti a ore, in base al numero di messaggi e alla latenza di rete.
Completo	Minuti

Se si sta monitorando l'avanzamento di una decommissionazione di un sito disconnesso, fare riferimento a questa tabella per comprendere le fasi di decommissionamento di un nodo di storage:

Fase	Durata stimata
In sospeso	Minuti o meno
Attendere i blocchi	Minuti
Preparare l'attività	Minuti o meno
Disattiva servizi esterni	Minuti
Revoca del certificato	Minuti
Annulla registrazione nodo	Minuti
Livello di storage Annulla registrazione	Minuti
Rimozione del gruppo di storage	Minuti
Rimozione entità	Minuti
Completo	Minuti

4. Una volta che tutti i nodi hanno raggiunto la fase completa, attendere il completamento delle restanti operazioni di decommissionamento del sito.
   - Durante la fase **Riparazione Cassandra**, StorageGRID effettua le riparazioni necessarie ai cluster Cassandra che rimangono nella vostra griglia. Queste riparazioni potrebbero richiedere diversi giorni o più, a seconda del numero di nodi di storage rimasti nel vostro grid.

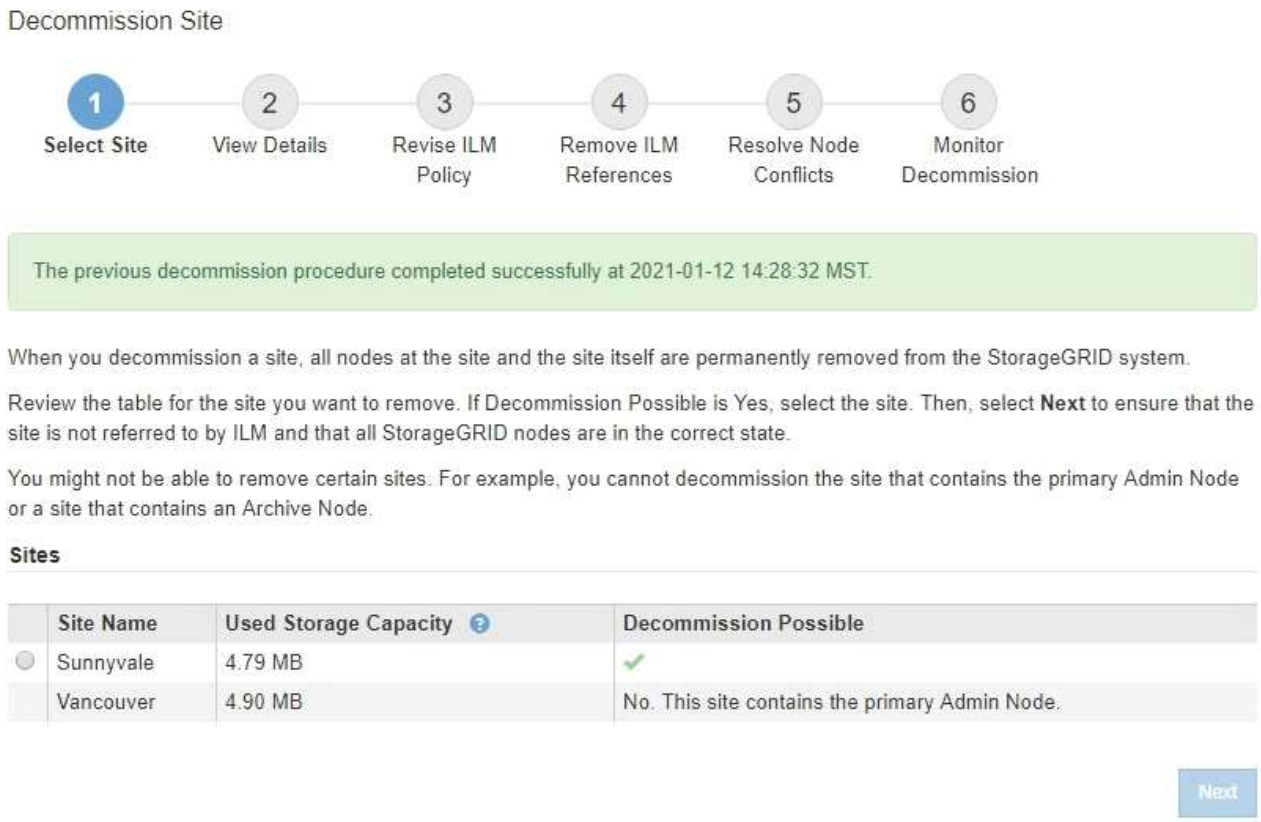


   - Durante la fase **Disattiva profili EC Elimina pool di storage**, vengono apportate le seguenti modifiche ILM:
     - Tutti i profili di codifica Erasure che fanno riferimento al sito vengono disattivati.
     - Tutti i pool di storage che fanno riferimento al sito vengono eliminati.

> Il pool di storage di tutti i nodi di storage predefinito del sistema viene rimosso anche perché utilizza il sito All Sites.

- Infine, durante la fase **Remove Configuration**, tutti i riferimenti rimanenti al sito e ai relativi nodi vengono rimossi dal resto della griglia.

5. Una volta completata la procedura di decommissionamento, la pagina Decommission Site (Sito di decommissionamento) mostra un messaggio di esito positivo e il sito rimosso non viene più visualizzato.



Al termine

Completare queste attività dopo aver completato la procedura di decommissionamento del sito:

- Assicurarsi che i dischi di tutti i nodi di storage nel sito decommissionato siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo

permanente e sicuro i dati dai dischi.

- Se il sito includeva uno o più nodi di amministrazione e l'SSO (Single Sign-on) è attivato per il sistema StorageGRID, rimuovere tutti i trust delle parti che si affidano al sito dai servizi di federazione di Active Directory (ad FS).
- Una volta spenti automaticamente i nodi durante la procedura di decommissionamento del sito connesso, rimuovere le macchine virtuali associate.

Procedure di manutenzione della rete

Aggiornare le subnet per Grid Network

StorageGRID mantiene un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete (eth0). Queste voci includono le subnet utilizzate per la rete griglia da ciascun sito nel sistema StorageGRID, nonché le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della rete griglia. Quando si aggiungono nodi griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere sottoreti alla rete Grid.

Di cosa hai bisogno

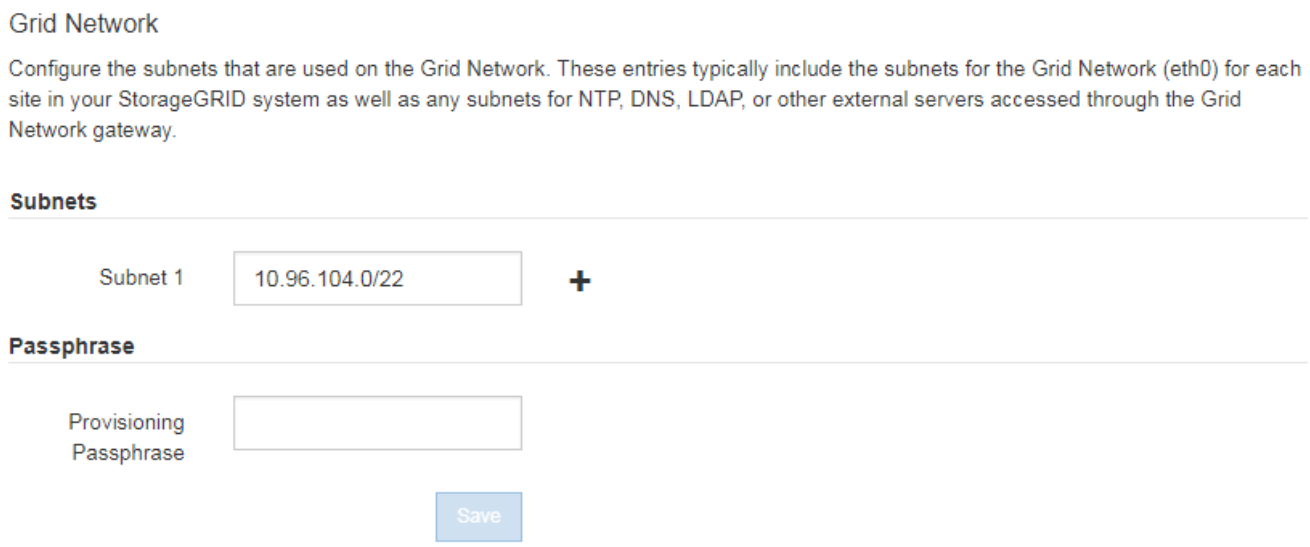
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre dell'autorizzazione Maintenance (manutenzione) o Root Access (accesso root).
- È necessario disporre della passphrase di provisioning.
- È necessario disporre degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

A proposito di questa attività

Se si sta eseguendo un'attività di espansione che include l'aggiunta di una nuova subnet, è necessario aggiungere la nuova subnet della griglia prima di avviare la procedura di espansione.

Fasi

1. Selezionare **MANUTENZIONE** > **rete** > **rete griglia**.



2. Nell'elenco delle subnet, fare clic sul segno più per aggiungere una nuova subnet nella notazione CIDR.

Ad esempio, immettere `10.96.104.0/22`.

3. Inserire la passphrase di provisioning e fare clic su **Save** (Salva).

   Le subnet specificate vengono configurate automaticamente per il sistema StorageGRID.

4. Scarica un nuovo pacchetto di ripristino da Grid Manager.
   a. Selezionare **MANUTENZIONE sistema pacchetto di ripristino**.
   b. Inserire la passphrase di provisioning.

Configurare gli indirizzi IP

È possibile eseguire la configurazione di rete configurando gli indirizzi IP per i nodi della griglia utilizzando lo strumento Change IP (Modifica IP).

È necessario utilizzare lo strumento Change IP per apportare la maggior parte delle modifiche alla configurazione di rete impostata inizialmente durante l'implementazione della griglia. Le modifiche manuali che utilizzano i comandi e i file di rete Linux standard potrebbero non propagarsi a tutti i servizi StorageGRID e non persistere tra gli aggiornamenti, i riavvii o le procedure di ripristino dei nodi.

> Se si desidera modificare l'indirizzo IP Grid Network per tutti i nodi della griglia, utilizzare procedura speciale per le modifiche a livello di griglia.

> Se si apportano modifiche solo all'elenco subnet di rete griglia, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Change IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si stanno eseguendo contemporaneamente modifiche al routing Grid Network e altre modifiche di rete.

> La procedura di modifica dell'IP può essere una procedura di interruzione. Alcune parti della griglia potrebbero non essere disponibili fino a quando non viene applicata la nuova configurazione.

Interfacce Ethernet

L'indirizzo IP assegnato a eth0 è sempre l'indirizzo IP Grid Network del nodo Grid. L'indirizzo IP assegnato a eth1 è sempre l'indirizzo IP Admin Network del nodo della griglia. L'indirizzo IP assegnato a eth2 è sempre l'indirizzo IP della rete client del nodo della griglia.

Si noti che su alcune piattaforme, come le appliance StorageGRID, eth0, eth1 ed eth2 potrebbero essere interfacce aggregate composte da bridge o legami subordinati di interfacce fisiche o VLAN. Su queste piattaforme, la scheda **SSM** > **Resources** potrebbe visualizzare l'indirizzo IP Grid, Admin e Client Network assegnato ad altre interfacce oltre a eth0, eth1 o eth2.

DHCP

È possibile configurare DHCP solo durante la fase di implementazione. Non è possibile impostare DHCP durante la configurazione. Se si desidera modificare gli indirizzi IP, le subnet mask e i gateway predefiniti per un nodo griglia, è necessario utilizzare le procedure di modifica dell'indirizzo IP. Utilizzando lo strumento Change IP, gli indirizzi DHCP diventano statici.

Gruppi ad alta disponibilità (ha)

- Se un'interfaccia di rete del client è contenuta in un gruppo ha, non è possibile modificare l'indirizzo IP di rete del client per tale interfaccia con un indirizzo esterno alla subnet configurata per il gruppo ha.
- Non è possibile modificare l'indirizzo IP della rete client con il valore di un indirizzo IP virtuale esistente assegnato a un gruppo ha configurato sull'interfaccia di rete client.
- Se un'interfaccia di rete Grid è contenuta in un gruppo ha, non è possibile modificare l'indirizzo IP della rete Grid per tale interfaccia con un indirizzo esterno alla subnet configurata per il gruppo ha.
- Non è possibile modificare l'indirizzo IP Grid Network con il valore di un indirizzo IP virtuale esistente assegnato a un gruppo ha configurato sull'interfaccia Grid Network.

Modificare la configurazione di rete del nodo

È possibile modificare la configurazione di rete di uno o più nodi utilizzando lo strumento Change IP. È possibile modificare la configurazione di Grid Network o aggiungere, modificare o rimuovere le reti Admin o Client.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

Linux: se si aggiunge un nodo Grid alla rete di amministrazione o alla rete client per la prima volta e non si è precedentemente configurato ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET nel file di configurazione del nodo, è necessario farlo ora.

Consultare le istruzioni per l'installazione di StorageGRID relative al sistema operativo in uso.

Appliance: sulle appliance StorageGRID, se il client o la rete amministrativa non sono stati configurati nel programma di installazione dell'appliance StorageGRID durante l'installazione iniziale, la rete non può essere aggiunta utilizzando solo il tool Cambia IP. Innanzitutto, è necessario impostare l'apparecchio in modalità di manutenzione, Configurare i collegamenti, ripristinare la normale modalità operativa dell'appliance, quindi utilizzare lo strumento Change IP per modificare la configurazione di rete. Consultare la procedura per la configurazione dei collegamenti di rete nelle istruzioni di installazione e manutenzione dell'appliance.

È possibile modificare l'indirizzo IP, la subnet mask, il gateway o il valore MTU per uno o più nodi su qualsiasi rete.

È inoltre possibile aggiungere o rimuovere un nodo da una rete client o da una rete amministrativa:

- È possibile aggiungere un nodo a una rete client o a una rete amministrativa aggiungendo un indirizzo IP/subnet mask su tale rete al nodo.
- È possibile rimuovere un nodo da una rete client o da una rete amministrativa eliminando l'indirizzo IP/subnet mask del nodo sulla rete.

  I nodi non possono essere rimossi dalla rete griglia.

> Gli swap degli indirizzi IP non sono consentiti. Se è necessario scambiare indirizzi IP tra nodi di rete, è necessario utilizzare un indirizzo IP intermedio temporaneo.

Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e si sta modificando l'indirizzo IP di un nodo di amministrazione, tenere presente che qualsiasi trust della parte che si basa configurato utilizzando l'indirizzo IP del nodo di amministrazione (invece del nome di dominio completo, come consigliato) non sarà valido. Non sarà più possibile accedere al nodo. Subito dopo aver modificato l'indirizzo IP, è necessario aggiornare o riconfigurare il trust della parte di supporto del nodo in Active Directory Federation Services (ad FS) con il nuovo indirizzo IP. Consultare le istruzioni per l'amministrazione di StorageGRID.

Le modifiche apportate alla rete utilizzando lo strumento Cambia IP vengono propagate al firmware del programma di installazione delle appliance StorageGRID. In questo modo, se il software StorageGRID viene reinstallato su un'appliance o se un'appliance viene messa in modalità di manutenzione, la configurazione di rete sarà corretta.

Fasi

1. 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. `#`.
2. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`
3. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. Se si desidera, selezionare **1** per scegliere i nodi da aggiornare. Quindi selezionare una delle seguenti opzioni:
   - **1**: Nodo singolo — selezionare per nome
   - **2**: Nodo singolo — selezionare per sito, quindi per nome
   - **3**: Nodo singolo — selezionare in base all'IP corrente
   - **4**: Tutti i nodi di un sito

- **5**: Tutti i nodi della griglia

  Nota: se si desidera aggiornare tutti i nodi, lasciare selezionato "tutti".

Una volta effettuata la selezione, viene visualizzato il menu principale, con il campo **Selected Nodes** (nodi selezionati) aggiornato per riflettere la scelta. Tutte le azioni successive vengono eseguite solo sui nodi visualizzati.

5. Nel menu principale, selezionare l'opzione **2** per modificare le informazioni relative a IP/mask, gateway e MTU per i nodi selezionati.
   a. Selezionare la rete in cui si desidera apportare le modifiche:
      - **1**: Rete di rete
      - **2**: Rete amministrativa
      - **3**: Rete client
      - **4**: Tutte le reti dopo aver effettuato la selezione, il prompt visualizza il nome del nodo, il nome della rete (griglia, Amministratore o Client), il tipo di dati (IP/mask, Gateway o MTU) e il valore corrente.

        Se si modificano l'indirizzo IP, la lunghezza del prefisso, il gateway o la MTU di un'interfaccia configurata con DHCP, l'interfaccia diventa statica. Quando si sceglie di modificare un'interfaccia configurata da DHCP, viene visualizzato un avviso per informare l'utente che l'interfaccia passerà a static (statica).

      Interfacce configurate come `fixed` impossibile modificare.

   b. Per impostare un nuovo valore, immetterlo nel formato indicato per il valore corrente.
   c. Per lasciare invariato il valore corrente, premere **Invio**.
   d. Se il tipo di dati è `IP/mask`, È possibile eliminare la rete Admin o Client dal nodo immettendo **d** o **0.0.0.0/0**.
   e. Dopo aver modificato tutti i nodi che si desidera modificare, immettere **q** per tornare al menu principale.

      Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

6. Per rivedere le modifiche, selezionare una delle seguenti opzioni:
   - **5**: Mostra le modifiche nell'output isolato per mostrare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'output di esempio:

```
==========================================================================
Site: RTP
==========================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

- **6**: Mostra le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).

> Alcune interfacce della riga di comando potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough. La corretta visualizzazione dipende dal client terminale che supporta le sequenze di escape VT100 necessarie.

7. Selezionare l'opzione **7** per convalidare tutte le modifiche.

   Questa convalida garantisce che le regole per le reti Grid, Admin e Client, come ad esempio il mancato utilizzo di sottoreti sovrapposte, non vengano violate.

   In questo esempio, la convalida ha restituito errori.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   In questo esempio, la convalida è stata superata.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. Una volta superata la convalida, scegliere una delle seguenti opzioni:
   - **8**: Salva le modifiche non applicate.

     Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

   - **10**: Applicare la nuova configurazione di rete.
9. Se è stata selezionata l'opzione **10**, scegliere una delle seguenti opzioni:
   - **Apply**: Applica le modifiche immediatamente e riavvia automaticamente ogni nodo, se necessario.

     Se la nuova configurazione di rete non richiede modifiche fisiche, selezionare **Apply** (Applica) per applicare le modifiche immediatamente. I nodi verranno riavviati automaticamente, se necessario. Verranno visualizzati i nodi che devono essere riavviati.

   - **Fase**: Applicare le modifiche al successivo riavvio manuale dei nodi.

     Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale per il funzionamento della nuova configurazione di rete, utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le necessarie modifiche fisiche di rete e riavviare i nodi interessati. Se si seleziona **Apply** (Applica) senza apportare prima queste modifiche alla rete, le modifiche non vengono eseguite correttamente.

     > Se si utilizza l'opzione **stage**, è necessario riavviare il nodo il prima possibile dopo lo staging per ridurre al minimo le interruzioni.

   - **CANCEL** (Annulla): Non apportare modifiche alla rete in questo momento.

     Se non si è a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, è possibile posticipare le modifiche per ridurre al minimo l'impatto sull'utente. Selezionando **CANCEL** si torna al menu principale e si conservano le modifiche in modo da poterle applicare in un secondo momento.

     Quando si seleziona **Apply** o **Stage**, viene generato un nuovo file di configurazione di rete, viene eseguito il provisioning e i nodi vengono aggiornati con nuove informazioni di lavoro.

     Durante il provisioning, l'output visualizza lo stato man mano che vengono applicati gli aggiornamenti.

     ```
     Generating new grid networking description file...

     Running provisioning...

     Updating grid network configuration on Name
     ```

   Dopo l'applicazione o lo staging delle modifiche, viene generato un nuovo pacchetto di ripristino in seguito alla modifica della configurazione della griglia.

10. Se si seleziona **fase**, seguire questi passaggi al termine del provisioning:

    a. Apportare le modifiche di rete fisiche o virtuali richieste.

       Modifiche fisiche alla rete: Apportare le modifiche fisiche necessarie alla rete, spegnendo il nodo in modo sicuro, se necessario.

Linux: Se si aggiunge il nodo a una rete amministrativa o a una rete client per la prima volta, assicurarsi di aver aggiunto l'interfaccia come descritto in "aggiunta di interfacce a un nodo esistente".

   a. Riavviare i nodi interessati.

11. Selezionare **0** per uscire dallo strumento Change IP una volta completate le modifiche.
12. Scarica un nuovo pacchetto di ripristino da Grid Manager.
    a. Selezionare **MANUTENZIONE sistema pacchetto di ripristino**.
    b. Inserire la passphrase di provisioning.

Informazioni correlate

Linux: Aggiunta di interfacce al nodo esistente

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Appliance di servizi SG100 e SG1000

Appliance di storage SG6000

Appliance di storage SG5700

Amministrare StorageGRID

Configurare gli indirizzi IP

Aggiungere o modificare gli elenchi di subnet nella rete amministrativa

È possibile aggiungere, eliminare o modificare le subnet nell'elenco subnet di rete amministrativa di uno o più nodi.

Di cosa hai bisogno

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

È possibile aggiungere, eliminare o modificare le subnet in tutti i nodi dell'elenco subnet di rete amministrativa.

Fasi

1. 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. `#`.

2. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`
3. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. Facoltativamente, limitare le reti/nodi su cui vengono eseguite le operazioni. Scegliere una delle seguenti opzioni:
   - Selezionare i nodi da modificare scegliendo **1**, se si desidera filtrare su nodi specifici su cui eseguire l'operazione. Selezionare una delle seguenti opzioni:
     - **1**: Nodo singolo (selezionare per nome)
     - **2**: Nodo singolo (selezionare per sito, quindi per nome)
     - **3**: Nodo singolo (selezionato in base all'IP corrente)
     - **4**: Tutti i nodi di un sito
     - **5**: Tutti i nodi della griglia
     - **0**: Torna indietro
   - Consenti a "tutti" di rimanere selezionato. Una volta effettuata la selezione, viene visualizzata la schermata del menu principale. Il campo Selected Nodes (nodi selezionati) riflette la nuova selezione e ora tutte le operazioni selezionate verranno eseguite solo su questo elemento.
5. Nel menu principale, selezionare l'opzione per modificare le subnet per la rete amministrativa (opzione **3**).
6. Scegliere una delle seguenti opzioni:
   - Per aggiungere una subnet, immettere il seguente comando: `add CIDR`
   - Per eliminare una subnet, immettere il seguente comando: `del CIDR`
   - Impostare l'elenco delle subnet immettendo questo comando: `set CIDR`

     > Per tutti i comandi, è possibile inserire più indirizzi utilizzando questo formato: `add CIDR, CIDR`

     Esempio: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

     > È possibile ridurre la quantità di digitazione richiesta utilizzando "freccia verso l'alto" per richiamare i valori precedentemente digitati al prompt di immissione corrente e, se necessario, modificarli.

     L'esempio riportato di seguito mostra l'aggiunta di subnet all'elenco subnet di rete amministrativa:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. Una volta pronti, inserire **q** per tornare alla schermata del menu principale. Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

> Se è stata selezionata una delle modalità di selezione del nodo "all" nel passaggio 2, premere **Invio** (senza **q**) per passare al nodo successivo nell'elenco.

8. Scegliere una delle seguenti opzioni:

   - Selezionare l'opzione **5** per visualizzare le modifiche nell'output isolato in modo da visualizzare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio riportato di seguito:

```
==============================================================================
Site: Data Center 1
==============================================================================
DC1-ADM1-105-154 Admin  Subnets                        add 172.17.0.0/16
                                                       del 172.16.0.0/16
                              [      172.14.0.0/16 ]
                              [      172.15.0.0/16 ]
                              [      172.17.0.0/16 ]
                              [      172.19.0.0/16 ]
                              [      172.20.0.0/16 ]
                              [      172.21.0.0/16 ]
Press Enter to continue
```

   - Selezionare l'opzione **6** per visualizzare le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni). **Nota:** alcuni emulatori di terminali potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough.

     Quando si tenta di modificare l'elenco delle subnet, viene visualizzato il seguente messaggio:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not reachable using default StorageGRID routing, but are
reachable using a different interface and gateway. Making and
applying changes to the subnet list will make all automatically
applied subnets persistent. If you do not want that to happen, delete
the unwanted subnets before applying changes. If you know that all
/32 subnets in the list were added intentionally, you can ignore this
caution.
```

Se non sono state assegnate in modo specifico le subnet NTP e DNS dei server a una rete, StorageGRID crea automaticamente un percorso host (/32) per la connessione. Se, ad esempio, si preferisce un percorso /16 o /24 per la connessione in uscita a un server DNS o NTP, eliminare il percorso /32 creato automaticamente e aggiungere i percorsi desiderati. Se non si elimina la route host creata automaticamente, questa verrà persistente dopo aver apportato eventuali modifiche all'elenco delle subnet.

> Sebbene sia possibile utilizzare questi percorsi host rilevati automaticamente, in generale è necessario configurare manualmente i percorsi DNS e NTP per garantire la connettività.

9. Selezionare l'opzione **7** per convalidare tutte le modifiche in fasi.

   Questa convalida garantisce il rispetto delle regole per le reti Grid, Admin e Client, ad esempio l'utilizzo di sottoreti sovrapposte.

10. Se si desidera, selezionare l'opzione **8** per salvare tutte le modifiche in più fasi e tornare in seguito per continuare ad apportare le modifiche.

    Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

11. Effettuare una delle seguenti operazioni:
    - Selezionare l'opzione **9** se si desidera annullare tutte le modifiche senza salvare o applicare la nuova configurazione di rete.
    - Selezionare l'opzione **10** se si desidera applicare le modifiche e fornire la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato man mano che gli aggiornamenti vengono applicati, come mostrato nell'output di esempio seguente:

    ```
    Generating new grid networking description file...

    Running provisioning...

    Updating grid network configuration on Name
    ```

12. Scarica un nuovo pacchetto di ripristino da Grid Manager.

a. Selezionare **MANUTENZIONE sistema pacchetto di ripristino**.

b. Inserire la passphrase di provisioning.

Informazioni correlate

Configurare gli indirizzi IP

Aggiungere o modificare gli elenchi di subnet su Grid Network

È possibile utilizzare lo strumento Change IP per aggiungere o modificare le subnet nella rete griglia.

Di cosa hai bisogno

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

È possibile aggiungere, eliminare o modificare le subnet nell'elenco subnet di rete griglia. Le modifiche influiscono sul routing su tutti i nodi della griglia.

> Se si apportano modifiche solo all'elenco subnet di rete griglia, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Change IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si stanno eseguendo contemporaneamente modifiche al routing Grid Network e altre modifiche di rete.

Fasi

1. 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. `#`.

2. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`

3. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. Nel menu principale, selezionare l'opzione per modificare le subnet per Grid Network (opzione **4**).

> Le modifiche apportate all'elenco di subnet di rete griglia sono a livello di griglia.

5. Scegliere una delle seguenti opzioni:
   - Per aggiungere una subnet, immettere il seguente comando: `add CIDR`
   - Per eliminare una subnet, immettere il seguente comando: `del CIDR`
   - Impostare l'elenco delle subnet immettendo questo comando: `set CIDR`

> Per tutti i comandi, è possibile inserire più indirizzi utilizzando questo formato: `add CIDR, CIDR`

Esempio: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

> È possibile ridurre la quantità di digitazione richiesta utilizzando "freccia verso l'alto" per richiamare i valori precedentemente digitati al prompt di immissione corrente e, se necessario, modificarli.

L'input di esempio riportato di seguito mostra l'impostazione delle subnet per l'elenco di subnet di rete griglia:

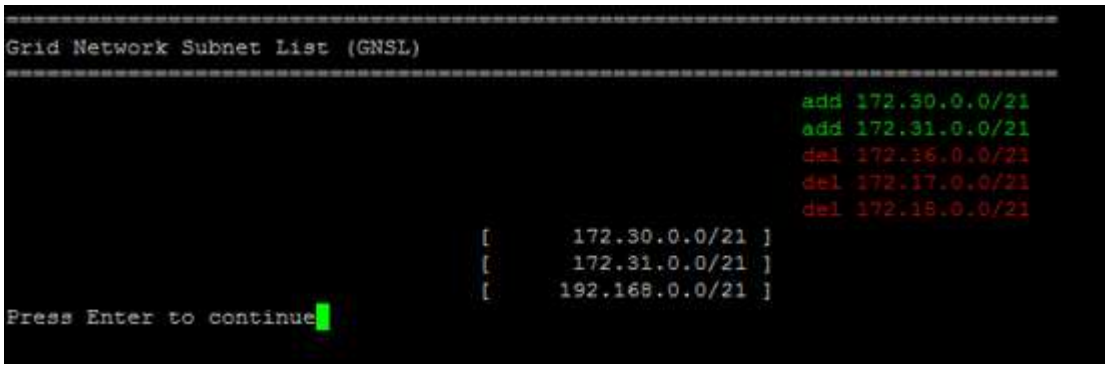
```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. Una volta pronti, inserire **q** per tornare alla schermata del menu principale. Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.
7. Scegliere una delle seguenti opzioni:
   - Selezionare l'opzione **5** per visualizzare le modifiche nell'output isolato in modo da visualizzare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio riportato di seguito:



   - Selezionare l'opzione **6** per visualizzare le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).

> Alcune interfacce della riga di comando potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough.

8. Selezionare l'opzione **7** per convalidare tutte le modifiche in fasi.

   Questa convalida garantisce il rispetto delle regole per le reti Grid, Admin e Client, ad esempio l'utilizzo di sottoreti sovrapposte.

9. Se si desidera, selezionare l'opzione **8** per salvare tutte le modifiche in più fasi e tornare in seguito per continuare ad apportare le modifiche.

   Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

10. Effettuare una delle seguenti operazioni:
    - Selezionare l'opzione **9** se si desidera annullare tutte le modifiche senza salvare o applicare la nuova configurazione di rete.
    - Selezionare l'opzione **10** se si desidera applicare le modifiche e fornire la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato man mano che gli aggiornamenti vengono applicati, come mostrato nell'output di esempio seguente:

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

11. Se è stata selezionata l'opzione **10** quando si apportano modifiche alla rete griglia, selezionare una delle seguenti opzioni:

- **Apply**: Applica le modifiche immediatamente e riavvia automaticamente ogni nodo, se necessario.

  Se la nuova configurazione di rete funziona contemporaneamente alla vecchia configurazione di rete senza modifiche esterne, è possibile utilizzare l'opzione **Apply** per una modifica della configurazione completamente automatica.

- **Fase**: Applicare le modifiche al successivo riavvio dei nodi.

  Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale per il funzionamento della nuova configurazione di rete, utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le necessarie modifiche fisiche di rete e riavviare i nodi interessati.

  > Se si utilizza l'opzione **stage**, è necessario riavviare il nodo il prima possibile dopo lo staging per ridurre al minimo le interruzioni.

- **CANCEL** (Annulla): Non apportare modifiche alla rete in questo momento.

  Se non si è a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, è possibile posticipare le modifiche per ridurre al minimo l'impatto sull'utente. Selezionando **CANCEL** si torna al menu principale e si conservano le modifiche in modo da poterle applicare in un secondo momento.

Dopo l'applicazione o lo staging delle modifiche, viene generato un nuovo pacchetto di ripristino in seguito alla modifica della configurazione della griglia.

12. Se la configurazione viene interrotta a causa di errori, sono disponibili le seguenti opzioni:
    - Per interrompere la procedura di modifica dell'indirizzo IP e tornare al menu principale, immettere **a**.
    - Per riprovare l'operazione non riuscita, immettere **r**.
    - Per passare all'operazione successiva, immettere **c**.

      L'operazione non riuscita può essere rieseguita in un secondo momento selezionando l'opzione **10** (Applica modifiche) dal menu principale. La procedura di modifica dell'IP non sarà completa fino a quando tutte le operazioni non saranno state completate correttamente.

    - Se è stato necessario intervenire manualmente (ad esempio per riavviare un nodo) e si è certi che l'azione che lo strumento ritiene non sia riuscita sia stata completata correttamente, immettere **f** per contrassegnarla come riuscita e passare all'operazione successiva.
13. Scarica un nuovo pacchetto di ripristino da Grid Manager.
    a. Selezionare **MANUTENZIONE sistema pacchetto di ripristino**.
    b. Inserire la passphrase di provisioning.

    > Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

Informazioni correlate

Configurare gli indirizzi IP

Modificare gli indirizzi IP per tutti i nodi nella griglia

Se è necessario modificare l'indirizzo IP Grid Network per tutti i nodi della griglia, seguire questa procedura speciale. Non è possibile eseguire una modifica dell'IP Grid-wide

Network utilizzando la procedura per modificare i singoli nodi.

Di cosa hai bisogno

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

Per garantire che la griglia venga avviata correttamente, è necessario apportare tutte le modifiche contemporaneamente.

> Questa procedura si applica solo alla rete di rete. Non è possibile utilizzare questa procedura per modificare gli indirizzi IP nelle reti Admin o Client.

Se si desidera modificare gli indirizzi IP e la MTU per i nodi di un solo sito, seguire la Modificare la configurazione di rete del nodo istruzioni.

Fasi

1. Pianificare in anticipo le modifiche da apportare al di fuori dello strumento Change IP, ad esempio le modifiche a DNS o NTP, e le modifiche alla configurazione SSO (Single Sign-on), se utilizzata.

   > Se i server NTP esistenti non sono accessibili alla griglia dei nuovi indirizzi IP, aggiungere i nuovi server NTP prima di eseguire la procedura di modifica dell'ip.

   > Se i server DNS esistenti non sono accessibili alla griglia dei nuovi indirizzi IP, aggiungere i nuovi server DNS prima di eseguire la procedura di modifica dell'ip.

   > Se SSO è attivato per il sistema StorageGRID e i trust di qualsiasi parte che si basa sono configurati utilizzando gli indirizzi IP del nodo di amministrazione (invece di nomi di dominio completi, come consigliato), è necessario essere pronti ad aggiornare o riconfigurare i trust di tali parti in Active Directory Federation Services (ad FS) Subito dopo aver modificato gli indirizzi IP. Consultare le istruzioni per l'amministrazione di StorageGRID.

   > Se necessario, aggiungere la nuova subnet per i nuovi indirizzi IP.

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. Avviare lo strumento Change IP immettendo il seguente comando: `change-ip`
4. Inserire la passphrase di provisioning quando richiesto.

   Viene visualizzato il menu principale. Per impostazione predefinita, il `Selected nodes` il campo è impostato su `all`.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

5. Nel menu principale, selezionare **2** per modificare le informazioni relative a IP/subnet mask, gateway e MTU per tutti i nodi.

   a. Selezionare **1** per apportare modifiche alla rete griglia.

      Una volta effettuata la selezione, il prompt visualizza i nomi dei nodi, il nome della rete di griglia, il tipo di dati (IP/mask, Gateway o MTU), e valori correnti.

      Se si modificano l'indirizzo IP, la lunghezza del prefisso, il gateway o la MTU di un'interfaccia configurata con DHCP, l'interfaccia diventa statica. Viene visualizzato un avviso prima di ogni interfaccia configurata da DHCP.

   Interfacce configurate come `fixed` impossibile modificare.

   a. Per impostare un nuovo valore, immetterlo nel formato indicato per il valore corrente.
   b. Dopo aver modificato tutti i nodi che si desidera modificare, immettere **q** per tornare al menu principale.

      Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

6. Per rivedere le modifiche, selezionare una delle seguenti opzioni:
   - **5**: Mostra le modifiche nell'output isolato per mostrare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'output di esempio:

```
==========================================================================
Site: RTP
==========================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

- **6**: Mostra le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).

> Alcune interfacce della riga di comando potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough. La corretta visualizzazione dipende dal client terminale che supporta le sequenze di escape VT100 necessarie.

7. Selezionare l'opzione **7** per convalidare tutte le modifiche.

   Questa convalida garantisce che le regole per la rete grid, come ad esempio il non utilizzo di sottoreti sovrapposte, non vengano violate.

   In questo esempio, la convalida ha restituito errori.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   In questo esempio, la convalida è stata superata.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. Una volta superata la convalida, selezionare **10** per applicare la nuova configurazione di rete.
9. Selezionare **stage** per applicare le modifiche al successivo riavvio dei nodi.

> Selezionare **stage**. Non eseguire un rolling restart, manualmente o selezionando **Apply** invece di **stage**; la griglia non si avvierà correttamente.

10. Una volta completate le modifiche, selezionare **0** per uscire dallo strumento Change IP.
11. Arrestare tutti i nodi contemporaneamente.

> L'intera griglia deve essere chiusa contemporaneamente, in modo che tutti i nodi siano spenti contemporaneamente.

12. Apportare le modifiche di rete fisiche o virtuali richieste.
13. Verificare che tutti i nodi della griglia non siano attivi.
14. Accendere tutti i nodi.
15. Una volta che la griglia si avvia correttamente:
    a. Se sono stati aggiunti nuovi server NTP, eliminare i vecchi valori del server NTP.
    b. Se sono stati aggiunti nuovi server DNS, eliminare i vecchi valori del server DNS.
16. Scarica il nuovo pacchetto di ripristino da Grid Manager.
    a. Selezionare **MANUTENZIONE sistema pacchetto di ripristino**.
    b. Inserire la passphrase di provisioning.

Informazioni correlate

Amministrare StorageGRID

Aggiungere o modificare gli elenchi di subnet su Grid Network

Chiudere il nodo della griglia

Aggiungere interfacce al nodo esistente

Linux: Aggiunta di interfacce Admin o Client a un nodo esistente

Seguire questa procedura per aggiungere un'interfaccia sulla rete di amministrazione o sulla rete client a un nodo Linux dopo l'installazione.

Se NON sono stati configurati ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET nel file di configurazione del nodo sull'host Linux durante l'installazione, utilizzare questa procedura per aggiungere l'interfaccia. Per ulteriori informazioni sul file di configurazione del nodo, consultare le istruzioni relative al sistema operativo Linux in uso:

- Installare Red Hat Enterprise Linux o CentOS
- Installare Ubuntu o Debian

Questa procedura viene eseguita sul server Linux che ospita il nodo che richiede la nuova assegnazione di rete, non all'interno del nodo. Questa procedura aggiunge l'interfaccia solo al nodo; si verifica un errore di convalida se si tenta di specificare altri parametri di rete.

Per fornire le informazioni di indirizzamento, è necessario utilizzare lo strumento Change IP (Modifica IP). Vedere Modificare la configurazione di rete del nodo.

Fasi

1. Accedere al server Linux che ospita il nodo.
2. Modificare il file di configurazione del nodo: `/etc/storagegrid/nodes/node-name.conf`.

   Non specificare altri parametri di rete, altrimenti si verificherà un errore di convalida.

   a. Aggiungere una voce per la nuova destinazione di rete. Ad esempio:

   ```
   CLIENT_NETWORK_TARGET = bond0.3206
   ```

   b. Facoltativo: Aggiungere una voce per l'indirizzo MAC. Ad esempio:

   ```
   CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
   ```

3. Eseguire il comando node validate:

   ```
   sudo storagegrid node validate node-name
   ```

4. Risolvere tutti gli errori di convalida.
5. Eseguire il comando node reload:

   ```
   sudo storagegrid node reload node-name
   ```

Linux: Aggiunta di interfacce di accesso o trunk a un nodo

È possibile aggiungere trunk o interfacce di accesso supplementari a un nodo Linux dopo averlo installato. Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

Di cosa hai bisogno

- Hai accesso alle istruzioni per l'installazione di StorageGRID sulla tua piattaforma Linux.
  - Installare Red Hat Enterprise Linux o CentOS
  - Installare Ubuntu o Debian
- Hai il `Passwords.txt` file.
- Si dispone di autorizzazioni di accesso specifiche.

Non tentare di aggiungere interfacce a un nodo mentre è attiva una procedura di aggiornamento, ripristino o espansione del software.

A proposito di questa attività

Seguire questa procedura per aggiungere una o più interfacce aggiuntive a un nodo Linux dopo l'installazione del nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si

aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.

Il nodo non è disponibile per un breve periodo di tempo quando si aggiungono interfacce. Eseguire questa procedura su un nodo alla volta.

Fasi

1. Accedere al server Linux che ospita il nodo.
2. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo:

   ```
   /etc/storagegrid/nodes/node-name.conf
   ```

3. Aggiungere una voce al file per specificare il nome e, facoltativamente, la descrizione di ogni interfaccia aggiuntiva che si desidera aggiungere al nodo. USA questo formato.

   ```
   INTERFACES_TARGET_nnnn=value
   ```

   Per *nnnn*, specificare un numero univoco per ciascuno di essi `INTERFACES_TARGET` voce da aggiungere.

   Per *valore*, specificare il nome dell'interfaccia fisica sull'host bare-metal. Quindi, facoltativamente, aggiungere una virgola e fornire una descrizione dell'interfaccia, che viene visualizzata nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

   Ad esempio:

   ```
   INTERFACES_TARGET_01=ens256, Trunk
   ```

   > Non specificare altri parametri di rete, altrimenti si verificherà un errore di convalida.

4. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo:

   ```
   sudo storagegrid node validate node-name
   ```

   Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

5. Eseguire il seguente comando per aggiornare la configurazione del nodo:

   ```
   sudo storagegrid node reload node-name
   ```

Al termine

- Se sono state aggiunte una o più interfacce di linea, passare a. Configurare le interfacce VLAN Per configurare una o più interfacce VLAN per ogni nuova interfaccia principale.
- Se sono state aggiunte una o più interfacce di accesso, visitare il sito configurare i gruppi ad alta disponibilità Per aggiungere le nuove interfacce direttamente ai gruppi ha.

VMware: Aggiunta di interfacce di accesso o trunk a un nodo

Una volta installato il nodo, è possibile aggiungere un trunk o un'interfaccia di accesso a un nodo VM. Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

Di cosa hai bisogno

- È possibile accedere alle istruzioni per l'installazione di StorageGRID sulla piattaforma VMware.

Installare VMware

- StorageGRID 11.6 è stato configurato.
- Si dispone di macchine virtuali VMware con nodo di amministrazione e nodo di gateway.
- Si dispone di una subnet di rete che non viene utilizzata come rete Grid, Admin o Client.
- Hai il `Passwords.txt` file.
- Si dispone di autorizzazioni di accesso specifiche.

> Non tentare di aggiungere interfacce a un nodo mentre è attiva una procedura di aggiornamento, ripristino o espansione del software.

A proposito di questa attività

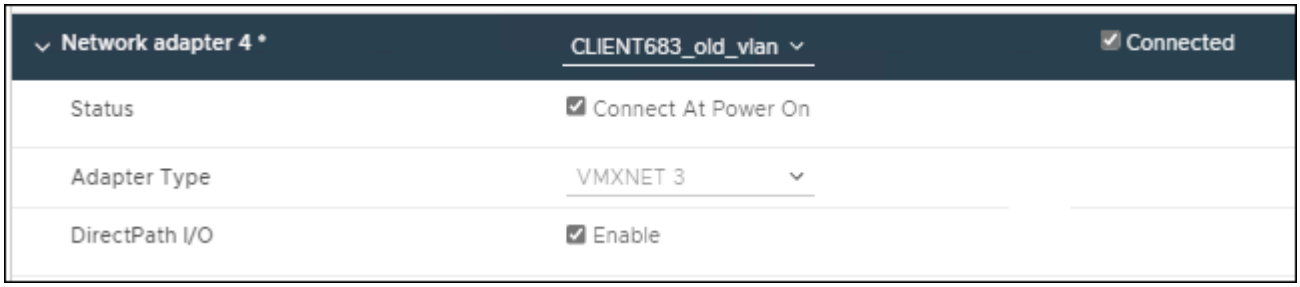
Seguire questa procedura per aggiungere una o più interfacce aggiuntive a un nodo VMware dopo l'installazione del nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.

Il nodo potrebbe non essere disponibile per un breve periodo di tempo quando si aggiungono interfacce.

Fasi

1. In vCenter, aggiungere una nuova scheda di rete (tipo VMXNET3) a un nodo di amministrazione e a una macchina virtuale del nodo gateway. Selezionare le caselle di controllo **connesso** e **Connetti all'accensione**.



2. Utilizzare SSH per accedere al nodo di amministrazione o al nodo gateway.
3. Utilizzare `ip link show` per confermare il rilevamento della nuova interfaccia di rete ens256.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Al termine

- Se sono state aggiunte una o più interfacce di linea, passare a. Configurare le interfacce VLAN Per configurare una o più interfacce VLAN per ogni nuova interfaccia principale.
- Se sono state aggiunte una o più interfacce di accesso, visitare il sito configurare i gruppi ad alta disponibilità Per aggiungere le nuove interfacce direttamente ai gruppi ha.

Configurare i server DNS

È possibile aggiungere, rimuovere e aggiornare i server DNS (Domain Name System), in modo da poter utilizzare i nomi host FQDN (Fully Qualified Domain Name) anziché gli indirizzi IP.

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).
- Per eseguire la configurazione, è necessario disporre degli indirizzi IP dei server DNS.

La specifica delle informazioni sul server DNS consente di utilizzare i nomi host FQDN (Fully Qualified Domain Name) anziché gli indirizzi IP per le notifiche e-mail o SNMP e AutoSupport. Si consiglia di specificare almeno due server DNS.

> Fornire da due a sei indirizzi IP per i server DNS. In generale, selezionare i server DNS ai quali ciascun sito può accedere localmente in caso di rete. In questo modo si garantisce che un sito islanded continui ad avere accesso al servizio DNS. Dopo aver configurato l'elenco dei server DNS a livello di griglia, è possibile Personalizzare ulteriormente l'elenco dei server DNS per ciascun nodo.

Se le informazioni del server DNS vengono omesse o configurate in modo errato, viene attivato un allarme DNST sul servizio SSM di ciascun nodo della rete. L'allarme viene cancellato quando il DNS è configurato correttamente e le nuove informazioni sul server hanno raggiunto tutti i nodi della griglia.

Fasi

1. Selezionare **MANUTENZIONE rete Server DNS**.
2. Nella sezione Server, aggiungere o rimuovere le voci del server DNS, se necessario.

   Si consiglia di specificare almeno due server DNS per sito. È possibile specificare fino a sei server DNS.

3. Fare clic su **Save** (Salva).

Modificare la configurazione DNS per un nodo griglia singolo

Invece di configurare il DNS (Domain Name System) a livello globale per l'intera implementazione, è possibile eseguire uno script per configurare il DNS in modo diverso per ciascun nodo della griglia.

In generale, utilizzare l'opzione **MANUTENZIONE** > **rete** > **server DNS** in Grid Manager per configurare i server DNS. Utilizzare il seguente script solo se è necessario utilizzare server DNS diversi per nodi griglia diversi.

1. 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. `#`.

   e. Aggiungere la chiave privata SSH all'agente SSH. Inserire: `ssh-add`
   f. Inserire la password di accesso SSH elencata in `Passwords.txt` file.
2. Accedi al nodo che desideri aggiornare con una configurazione DNS personalizzata: `ssh node_IP_address`
3. Eseguire lo script di installazione del DNS: `setup_resolv.rb.`

   Lo script risponde con l'elenco dei comandi supportati.

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. Aggiungere l'indirizzo IPv4 di un server che fornisce il servizio dei nomi di dominio per la rete: `add <nameserver IP_address>`
5. Ripetere il `add nameserver` comando per aggiungere i server dei nomi.
6. Seguire le istruzioni richieste per altri comandi.
7. Salvare le modifiche e uscire dall'applicazione: `save`
8. chiudere la shell dei comandi sul server: `exit`
9. Per ciascun nodo della griglia, ripetere i passi da accesso al nodo attraverso chiudere la shell dei comandi.
10. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente

SSH. Inserire: `ssh-add -D`

Configurare i server NTP

È possibile aggiungere, aggiornare o rimuovere server NTP (Network Time Protocol) per garantire che i dati siano sincronizzati in modo accurato tra i nodi della griglia nel sistema StorageGRID.

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).
- È necessario disporre della passphrase di provisioning.
- Per eseguire la configurazione, è necessario disporre degli indirizzi IPv4 dei server NTP.

A proposito di questa attività

Il sistema StorageGRID utilizza il protocollo NTP (Network Time Protocol) per sincronizzare l'ora tra tutti i nodi della griglia.

In ogni sito, ad almeno due nodi nel sistema StorageGRID viene assegnato il ruolo NTP primario. Si sincronizzano con un minimo consigliato di quattro e un massimo di sei sorgenti di tempo esterne e tra loro. Ogni nodo del sistema StorageGRID che non è un nodo NTP primario agisce come client NTP e si sincronizza con questi nodi NTP primari.

I server NTP esterni si connettono ai nodi ai quali sono stati precedentemente assegnati ruoli NTP primari. Per questo motivo, si consiglia di specificare almeno due nodi con ruoli NTP primari.

> Assicurarsi che almeno due nodi di ciascun sito possano accedere ad almeno quattro origini NTP esterne. Se solo un nodo di un sito può raggiungere le origini NTP, si verificheranno problemi di tempistica se tale nodo non funziona. Inoltre, la designazione di due nodi per sito come origini NTP primarie garantisce tempi precisi se un sito viene isolato dal resto della rete.

I server NTP esterni specificati devono utilizzare il protocollo NTP. È necessario specificare i riferimenti al server NTP di strato 3 o superiore per evitare problemi di deriva del tempo.

> 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.

"Supportare il limite per configurare il servizio Time di Windows per ambienti ad alta precisione"

In caso di problemi con la stabilità o la disponibilità dei server NTP originariamente specificati durante l'installazione, è possibile aggiornare l'elenco delle origini NTP esterne utilizzate dal sistema StorageGRID aggiungendo server aggiuntivi o aggiornando o rimuovendo i server esistenti.

Fasi

1. Selezionare **MANUTENZIONE rete Server NTP**.
2. Nella sezione Server, aggiungere o rimuovere le voci del server NTP, secondo necessità.

   È necessario includere almeno 4 server NTP ed è possibile specificare fino a 6 server.

3. Nella casella di testo **Passphrase di provisioning**, immettere la passphrase di provisioning per il sistema StorageGRID e fare clic su **Salva**.

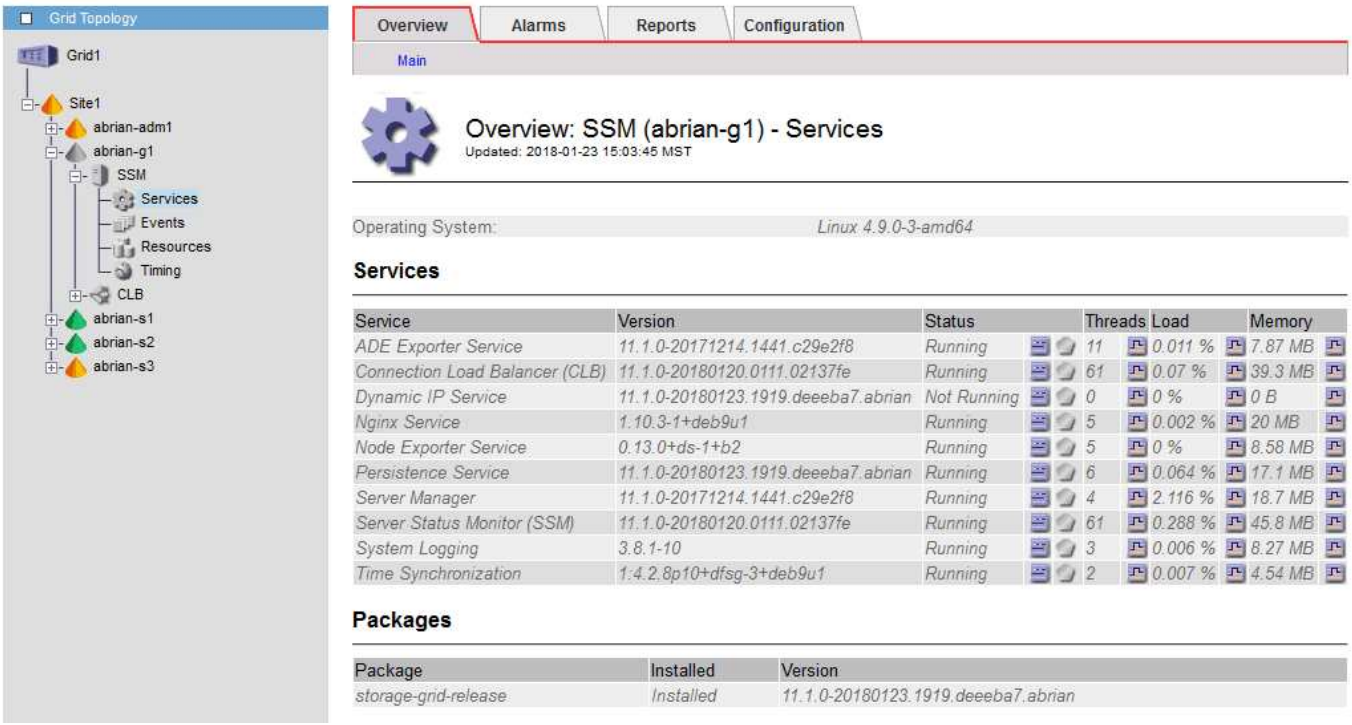
   Lo stato della procedura viene visualizzato nella parte superiore della pagina. La pagina viene disattivata fino al completamento degli aggiornamenti della configurazione.

> Se tutti i server NTP non superano il test di connessione dopo aver salvato i nuovi server NTP, non procedere. Contattare il supporto tecnico.

Ripristinare la connettività di rete per i nodi isolati

In alcuni casi, ad esempio in caso di modifica dell'indirizzo IP a livello di sito o di griglia, uno o più gruppi di nodi potrebbero non essere in grado di contattare il resto della griglia.

In Grid Manager (**SUPPORT Tools Grid topology**), se un nodo è grigio o se un nodo è blu con molti dei suoi servizi che mostrano uno stato diverso da quello in esecuzione, è necessario verificare l'isolamento del nodo.



Di seguito sono riportate alcune delle conseguenze derivanti dall'utilizzo di nodi isolati:

- Se sono isolati più nodi, potrebbe non essere possibile accedere a Grid Manager o accedervi.
- Se si isolano più nodi, i valori di utilizzo dello storage e di quota mostrati nella dashboard per il tenant Manager potrebbero essere obsoleti. I totali verranno aggiornati al ripristino della connettività di rete.

Per risolvere il problema di isolamento, eseguire un'utilità della riga di comando su ciascun nodo isolato o su un nodo di un gruppo (tutti i nodi di una subnet che non contiene il nodo di amministrazione primario) isolato dalla griglia. L'utility fornisce ai nodi l'indirizzo IP di un nodo non isolato nella griglia, che consente al nodo isolato o al gruppo di nodi di contattare nuovamente l'intera griglia.

> Se il multicast Domain Name System (mDNS) è disattivato nelle reti, potrebbe essere necessario eseguire l'utility della riga di comando su ciascun nodo isolato.

1. Accedere al nodo e controllare `/var/local/log/dynip.log` per i messaggi di isolamento.

   Ad esempio:

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action may be required.
   ```

   Se si utilizza la console VMware, viene visualizzato un messaggio che indica che il nodo potrebbe essere isolato.

   Nelle implementazioni Linux, i messaggi di isolamento vengono visualizzati in `/var/log/storagegrid/node/<nodename>.log` file.

2. Se i messaggi di isolamento sono ricorrenti e persistenti, eseguire il seguente comando:

   `add_node_ip.py <address>`

   dove `<address>` È l'indirizzo IP di un nodo remoto connesso alla rete.

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. Verificare quanto segue per ciascun nodo precedentemente isolato:
   - I servizi del nodo sono stati avviati.
   - Lo stato del servizio IP dinamico è "running" (in esecuzione) dopo aver eseguito `storagegrid-status` comando.
   - Nell'albero topologia griglia, il nodo non appare più disconnesso dal resto della griglia.

> Se si esegue `add_node_ip.py` il comando non risolve il problema, potrebbero essere presenti altri problemi di rete che devono essere risolti.

Procedure middleware e a livello di host

Alcune procedure di manutenzione sono specifiche per le implementazioni Linux o VMware di StorageGRID o sono specifiche di altri componenti della soluzione StorageGRID.

Linux: Migrazione del nodo grid al nuovo host

È possibile migrare i nodi StorageGRID da un host Linux a un altro per eseguire la manutenzione dell'host (ad esempio, l'installazione di patch e il riavvio del sistema

operativo) senza influire sulle funzionalità o sulla disponibilità del grid.

Si esegue la migrazione di uno o più nodi da un host Linux ("host di origine`") a un altro host Linux (“host di destinazione `s”). L’host di destinazione deve essere stato precedentemente preparato per l’utilizzo di StorageGRID.

> È possibile utilizzare questa procedura solo se l’implementazione di StorageGRID è stata pianificata per includere il supporto per la migrazione.

Per eseguire la migrazione di un nodo Grid a un nuovo host, devono essere soddisfatte entrambe le seguenti condizioni:

- Lo storage condiviso viene utilizzato per tutti i volumi di storage per nodo
- Le interfacce di rete hanno nomi coerenti tra gli host

> In un’implementazione in produzione, non eseguire più di un nodo di storage su un singolo host. L’utilizzo di un host dedicato per ciascun nodo di storage fornisce un dominio di errore isolato.

Sullo stesso host è possibile implementare altri tipi di nodi, come ad esempio i nodi Admin o Gateway. Tuttavia, se si dispone di più nodi dello stesso tipo (ad esempio due nodi gateway), non installare tutte le istanze sullo stesso host.

Per ulteriori informazioni, consultare “requisiti di migrazione dei nodi” nelle istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso.

Informazioni correlate

Implementare nuovi host Linux

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Linux: Nodo di esportazione dall’host di origine

Chiudere il nodo grid ed esportarlo dall’host Linux di origine.

Eseguire il seguente comando sull’host Linux di origine.

1. Ottenere lo stato di tutti i nodi attualmente in esecuzione sull’host di origine.

```
sudo storagegrid node status all
```

```
Name Config-State Run-State

DC1-ADM1 Configured Running

DC1-ARC1 Configured Running

DC1-GW1 Configured Running

DC1-S1 Configured Running
```

```
DC1-S2 Configured Running

DC1-S3 Configured Running
```

2. Identificare il nome del nodo che si desidera migrare e interromperlo se si trova nello stato di esecuzione `Running`.

```
sudo storagegrid node stop DC1-S3
```

```
Stopping node DC1-S3

Waiting up to 630 seconds for node shutdown
```

3. Esportare il nodo dall'host di origine.

```
sudo storagegrid node export DC1-S3
```

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.

Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you

want to import it again.
```

4. Prendere nota di `import command suggested in the output of the `export` comando.

   Questo comando verrà eseguito sull'host di destinazione nel passaggio successivo.

Linux: Nodo di importazione sull'host di destinazione

Dopo aver esportato il nodo dall'host di origine, importare e convalidare il nodo sull'host Linux di destinazione. La convalida conferma che il nodo ha accesso agli stessi dispositivi di storage a blocchi e di interfaccia di rete dell'host di origine.

Eseguire il seguente comando sull'host Linux di destinazione.

1. Importare il nodo sull'host di destinazione.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.

You should run 'storagegrid node validate DC1-S3'
```

2. Convalidare la configurazione del nodo sul nuovo host.

```
sudo storagegrid node validate DC1-S3
```

```
Confirming existence of node DC1-S3... PASSED

Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node DC1-
S3... PASSED

Checking for duplication of unique values... PASSED
```

3. Se si verificano errori di convalida, risolverli prima di avviare il nodo migrato.

   Per informazioni sulla risoluzione dei problemi, consultare le istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso.

Informazioni correlate

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Linux: Avviare il nodo migrato

Dopo aver convalidato il nodo migrato, avviare il nodo eseguendo un comando sull'host Linux di destinazione.

Fasi

1. Avviare il nodo sul nuovo host.

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. In Grid Manager, verificare che lo stato del nodo sia verde e che non vengano generati allarmi.

   > Verificare che lo stato del nodo sia verde per garantire che il nodo migrato sia stato riavviato completamente e ricongiungesso alla griglia. Se lo stato non è verde, non migrare nodi aggiuntivi in modo da non avere più di un nodo fuori servizio.

   Se non si riesce ad accedere a Grid Manager, attendere 10 minuti, quindi eseguire il seguente comando:

   `sudo storagegrid node status` ***`node-name`***

   Verificare che il nodo migrato abbia uno stato di esecuzione di `Running`.

Manutenzione del nodo di archiviazione per il middleware TSM

I nodi di archiviazione possono essere configurati per essere utilizzati come destinazione su nastro tramite un server middleware TSM o il cloud tramite l'API S3. Una volta configurata, la destinazione di un nodo di archiviazione non può essere modificata.

Se il server che ospita il nodo di archiviazione non funziona, sostituire il server e seguire la procedura di ripristino appropriata.

Guasto ai dispositivi storage di archiviazione

Se si determina la presenza di un guasto nel dispositivo di storage di archiviazione a cui il nodo di archiviazione sta accedendo tramite TSM, impostare il nodo di archiviazione offline per limitare il numero di allarmi visualizzati nel sistema StorageGRID. È quindi possibile utilizzare gli strumenti di amministrazione del server TSM o del dispositivo di storage, o entrambi, per diagnosticare e risolvere ulteriormente il problema.

Portare il componente di destinazione offline

Prima di eseguire qualsiasi manutenzione del server middleware TSM che potrebbe rendere il server non disponibile per il nodo di archiviazione, portare il componente di destinazione offline per limitare il numero di allarmi che vengono attivati se il server middleware TSM diventa non disponibile.

Di cosa hai bisogno

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

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare **nodo archivio** > **ARC** > **destinazione** > **Configurazione** > **principale**.
3. Impostare il valore di Tivoli Storage Manager state su **Offline** e fare clic su **Apply Changes** (Applica modifiche).
4. Una volta completata la manutenzione, modificare il valore di Tivoli Storage Manager state (Stato di Tivoli Storage Manager) su **Online** e fare clic su **Apply Changes** (Applica modifiche).

Strumenti di amministrazione di Tivoli Storage Manager

Lo strumento dsmadmc è la console amministrativa per il server middleware TSM installato sul nodo di archiviazione. È possibile accedere allo strumento digitando `dsmadmc` nella riga di comando del server. Accedere alla console di amministrazione utilizzando lo stesso nome utente e la stessa password configurati per il servizio ARC.

Il `tsmquery.rb` lo script è stato creato per generare informazioni sullo stato da dsmacmc in un formato più leggibile. È possibile eseguire questo script immettendo il seguente comando nella riga di comando del nodo di archiviazione: `/usr/local/arc/tsmquery.rb status`

Per ulteriori informazioni sulla console di amministrazione di TSM dsmadmc, consultare *Tivoli Storage Manager for Linux: Administrator's Reference*.

Oggetto permanentemente non disponibile

Quando il nodo di archiviazione richiede un oggetto dal server Tivoli Storage Manager (TSM) e il recupero non riesce, il nodo di archiviazione riprova la richiesta dopo un intervallo di 10 secondi. Se l'oggetto non è permanentemente disponibile (ad esempio, perché l'oggetto è corrotto su nastro), l'API TSM non può indicare questo al nodo di archiviazione, quindi il nodo di archiviazione continua a riprovare la richiesta.

Quando si verifica questa situazione, viene attivato un allarme e il valore continua ad aumentare. Per visualizzare l'allarme, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare **Archive Node** > **ARC** > **Retrieve** > **Request Failures**.

Se l'oggetto non è permanentemente disponibile, è necessario identificarlo e quindi annullare manualmente la

richiesta del nodo di archiviazione come descritto nella procedura, Determinare se gli oggetti non sono permanentemente disponibili.

Il recupero può anche avere esito negativo se l'oggetto non è temporaneamente disponibile. In questo caso, le richieste di recupero successive dovrebbero avere successo.

Se il sistema StorageGRID è configurato per utilizzare una regola ILM che crea una singola copia a oggetti e tale copia non può essere recuperata, l'oggetto viene perso e non può essere recuperato. Tuttavia, è comunque necessario seguire la procedura per determinare se l'oggetto non è permanentemente disponibile per "ripulire" il sistema StorageGRID, per annullare la richiesta del nodo di archiviazione e per eliminare i metadati per l'oggetto perso.

Determinare se gli oggetti non sono permanentemente disponibili

È possibile determinare se gli oggetti non sono permanentemente disponibili effettuando una richiesta utilizzando la console di amministrazione di TSM.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

A proposito di questa attività

Questo esempio viene fornito solo a scopo informativo; questa procedura non può aiutare a identificare tutte le condizioni di errore che potrebbero causare oggetti o volumi su nastro non disponibili. Per informazioni sull'amministrazione di TSM, consultare la documentazione di TSM Server.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
2. Identificare l'oggetto o gli oggetti che non possono essere recuperati dal nodo di archiviazione:
   a. Accedere alla directory contenente i file di log di controllo: `cd /var/local/audit/export`

      Il file di log di audit attivo è denominato audit.log. Una volta al giorno, il attivo `audit.log` il file viene salvato e viene visualizzato un nuovo `audit.log` il file viene avviato. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`. Dopo un giorno, il file salvato viene compresso e rinominato, nel formato `yyyy-mm-dd.txt.gz`, che conserva la data originale.

   b. Cercare nel file di log di audit pertinente i messaggi che indicano che non è stato possibile recuperare un oggetto archiviato. Ad esempio, immettere: `grep ARCE audit.log | less -n`

      Quando un oggetto non può essere recuperato da un nodo di archiviazione, il messaggio di audit ARCE (fine recupero oggetto archivio) visualizza ARUN (middleware di archiviazione non disponibile) o GERR (errore generale) nel campo dei risultati. La seguente riga di esempio del registro di controllo mostra che il messaggio ARCE è terminato con il risultato ARUN per CBID 498D8A1F681F05B3.

```
[AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
):ARUN][AVER(UI32):7]
[ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
MID(FC32):ARCI]
[ATID(UI64):4560349751312520631]]
```

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

c. Registrare il CBID di ciascun oggetto che ha avuto un errore di richiesta.

È inoltre possibile registrare le seguenti informazioni aggiuntive utilizzate dal TSM per identificare gli oggetti salvati dal nodo di archiviazione:

- **Nome spazio file**: Equivalente all'ID nodo archivio. Per trovare l'ID nodo archivio, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare **nodo archivio** > **ARC** > **destinazione** > **Panoramica**.
- **High Level Name**: Equivalente all'ID del volume assegnato all'oggetto dal nodo di archiviazione. L'ID del volume assume la forma di una data (ad esempio, `20091127`), e viene registrato come VLID dell'oggetto nei messaggi di audit dell'archivio.
- **Nome livello basso**: Equivalente al CBID assegnato a un oggetto dal sistema StorageGRID.

d. Disconnettersi dalla shell dei comandi: `exit`

3. Controllare il server TSM per verificare se gli oggetti identificati al punto 2 non sono permanentemente disponibili:

a. Accedere alla console di amministrazione del server TSM: `dsmadmc`

Utilizzare il nome utente amministrativo e la password configurati per il servizio ARC. Immettere il nome utente e la password in Grid Manager. Per visualizzare il nome utente, selezionare **SUPPORT** > **Tools** > **Grid topology**. Quindi, selezionare **Archive Node** > **ARC** > **Target** > **Configuration**.)

b. Determinare se l'oggetto non è permanentemente disponibile.

Ad esempio, è possibile cercare nel registro attività TSM un errore di integrità dei dati per quell'oggetto. Nell'esempio seguente viene illustrata una ricerca nel registro delle attività per il giorno precedente di un oggetto con CBID `498D8A1F681F05B3`.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

A seconda della natura dell'errore, il CBID potrebbe non essere registrato nel log delle attività del TSM. Potrebbe essere necessario cercare altri errori TSM nel registro durante il periodo di errore della richiesta.

c. Se un intero nastro non è disponibile in modo permanente, identificare i CBID per tutti gli oggetti memorizzati su quel volume: `query content TSM_Volume_Name`

   dove `TSM_Volume_Name` È il nome TSM del nastro non disponibile. Di seguito viene riportato un esempio dell'output di questo comando:

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- ----------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

   Il `Client's Name for File Name` È uguale all'ID del volume del nodo di archiviazione (o TSM "high level name") seguito dal CBID dell'oggetto (o TSM "low level name"). Ovvero, il `Client's Name for File Name` prende la forma `/Archive Node volume ID /CBID`. Nella prima riga dell'output di esempio, il `Client's Name for File Name` è `/20081201/ C1D172940E6C7E12`.

   Ricordate anche che il `Filespace` È l'ID del nodo del nodo di archiviazione.

Per annullare la richiesta di recupero, sono necessari il CBID di ciascun oggetto memorizzato nel volume e l'ID del nodo del nodo di archiviazione.

4. Per ogni oggetto non disponibile in modo permanente, annullare la richiesta di recupero ed emettere un comando per informare il sistema StorageGRID che la copia dell'oggetto è stata persa:

   > Utilizzare la console ADE con cautela. Se la console non viene utilizzata correttamente, è possibile interrompere le operazioni di sistema e danneggiare i dati. Immettere i comandi con attenzione e utilizzare solo i comandi descritti in questa procedura.

   a. Se non si è già connessi al nodo di archiviazione, effettuare l'accesso come segue:
      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.
   b. Accedere alla console ADE del servizio ARC: `telnet localhost 1409`
   c. Annullare la richiesta per l'oggetto: `/proc/BRTR/cancel -c CBID`

      dove `CBID` È l'identificativo dell'oggetto che non può essere recuperato dal TSM.

      Se le sole copie dell'oggetto sono su nastro, la richiesta "recupero in blocco" viene annullata con un messaggio "1 Requests Cancelled". Se nel sistema sono presenti copie dell'oggetto, il recupero dell'oggetto viene elaborato da un modulo diverso, in modo che la risposta al messaggio sia "0 requests Cancelled" (0 richieste annullate).

   d. Eseguire un comando per notificare al sistema StorageGRID che una copia dell'oggetto è stata persa e che è necessario eseguire un'altra copia: `/proc/CMSI/Object_Lost CBID node_ID`

dove `CBID` È l'identificatore dell'oggetto che non può essere recuperato dal server TSM, e. `node_ID` È l'ID nodo del nodo di archiviazione in cui il recupero non è riuscito.

Immettere un comando separato per ogni copia di oggetto persa: L'immissione di un intervallo di CBID non è supportata.

Nella maggior parte dei casi, il sistema StorageGRID inizia immediatamente a creare copie aggiuntive dei dati degli oggetti per garantire che venga rispettato il criterio ILM del sistema.

Tuttavia, se la regola ILM dell'oggetto specifica che è stata eseguita una sola copia e che tale copia è stata persa, l'oggetto non può essere recuperato. In questo caso, eseguire il `Object_Lost` Il comando rimuove i metadati dell'oggetto perso dal sistema StorageGRID.

Quando il `Object_Lost` il comando viene completato correttamente e viene visualizzato il seguente messaggio:

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

> Il `/proc/CMSI/Object_Lost` Il comando è valido solo per gli oggetti persi memorizzati nei nodi di archiviazione.

a. Uscire dalla console ADE: `exit`

b. Disconnettersi dal nodo di archiviazione: `exit`

5. Reimpostare il valore di Request Failures (errori richiesta) nel sistema StorageGRID:

   a. Accedere a **nodo archivio** > **ARC** > **Recupera** > **Configurazione** e selezionare **Reset Request Failure Count**.

   b. Fare clic su **Applica modifiche**.

Informazioni correlate

Amministrare StorageGRID

Esaminare i registri di audit

VMware: Configurare la macchina virtuale per il riavvio automatico

Se la macchina virtuale non si riavvia dopo il riavvio di VMware vSphere Hypervisor, potrebbe essere necessario configurare la macchina virtuale per il riavvio automatico.

Eseguire questa procedura se si nota che una macchina virtuale non si riavvia durante il ripristino di un nodo di griglia o l'esecuzione di un'altra procedura di manutenzione.

Fasi

1. Nell'albero di VMware vSphere Client, selezionare la macchina virtuale non avviata.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Power on** (accensione).
3. Configurare VMware vSphere Hypervisor per riavviare automaticamente la macchina virtuale in futuro.

Procedure del nodo di rete

Potrebbe essere necessario eseguire procedure su un nodo di griglia specifico. Sebbene sia possibile eseguire alcune di queste procedure da Grid Manager, la maggior parte delle procedure richiede l'accesso a Server Manager dalla riga di comando del nodo.

Server Manager viene eseguito su ogni nodo grid per supervisionare l'avvio e l'arresto dei servizi e per garantire che i servizi si uniscano e abbandonino correttamente il sistema StorageGRID. Server Manager monitora inoltre i servizi su ogni nodo grid e tenta automaticamente di riavviare tutti i servizi che segnalano gli errori.

> L'accesso a Server Manager deve essere effettuato solo se il supporto tecnico lo ha richiesto.

> Al termine dell'operazione con Server Manager, chiudere la sessione corrente della shell dei comandi e disconnettersi. Inserire: `exit`

Visualizzare lo stato e la versione di Server Manager

Per ciascun nodo Grid, è possibile visualizzare lo stato e la versione correnti di Server Manager in esecuzione su tale nodo Grid. È inoltre possibile ottenere lo stato corrente di tutti i servizi in esecuzione su quel nodo della griglia.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Visualizzare lo stato corrente di Server Manager in esecuzione sul nodo grid: **`service servermanager status`**

   Viene riportato lo stato corrente di Server Manager in esecuzione sul nodo grid (in esecuzione o meno). Se lo stato di Server Manager è `running`, l'ora in cui è stato eseguito dall'ultimo avvio. Ad esempio:

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

3. Visualizzare la versione corrente di Server Manager in esecuzione su un nodo Grid: **`service servermanager version`**

   Viene visualizzata la versione corrente. Ad esempio:

```
11.1.0-20180425.1905.39c9493
```

4. Disconnettersi dalla shell dei comandi: **`exit`**

Visualizzare lo stato corrente di tutti i servizi

È possibile visualizzare lo stato corrente di tutti i servizi in esecuzione su un nodo Grid in qualsiasi momento.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo grid: `storagegrid-status`

   Ad esempio, l'output per il nodo di amministrazione primario mostra lo stato corrente dei servizi AMS, CMN e NMS in esecuzione. Questo output viene aggiornato immediatamente se lo stato di un servizio cambia.

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

3. Tornare alla riga di comando, premere **Ctrl+C**.
4. Se si desidera, visualizzare un report statico per tutti i servizi in esecuzione sul nodo Grid: `/usr/local/servermanager/reader.rb`

   Questo report include le stesse informazioni del report continuamente aggiornato, ma non viene aggiornato se lo stato di un servizio cambia.

5. Disconnettersi dalla shell dei comandi: `exit`

Avviare Server Manager e tutti i servizi

Potrebbe essere necessario avviare Server Manager, che avvia anche tutti i servizi sul nodo Grid.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

L'avvio di Server Manager su un nodo grid in cui è già in esecuzione comporta il riavvio di Server Manager e di tutti i servizi sul nodo grid.

Fasi

1. 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. `#`.

2. Avviare Server Manager: `service servermanager start`
3. Disconnettersi dalla shell dei comandi: `exit`

Riavviare Server Manager e tutti i servizi

Potrebbe essere necessario riavviare il server manager e tutti i servizi in esecuzione su un nodo grid.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Riavviare Server Manager e tutti i servizi sul nodo grid: `service servermanager restart`

   Server Manager e tutti i servizi sul nodo grid vengono arrestati e quindi riavviati.

   > Utilizzando il `restart` il comando è identico a quello utilizzato da `stop` seguito dal comando `start` comando.

3. Disconnettersi dalla shell dei comandi: `exit`

Arrestare Server Manager e tutti i servizi

Server Manager è progettato per essere eseguito in qualsiasi momento, ma potrebbe essere necessario interrompere Server Manager e tutti i servizi in esecuzione su un nodo grid.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Arrestare Server Manager e tutti i servizi in esecuzione sul nodo grid: `service servermanager stop`

   Server Manager e tutti i servizi in esecuzione sul nodo grid vengono terminati senza problemi. L'arresto dei servizi può richiedere fino a 15 minuti.

3. Disconnettersi dalla shell dei comandi: `exit`

Visualizzare lo stato corrente del servizio

È possibile visualizzare lo stato corrente di un servizio in esecuzione su un nodo Grid in qualsiasi momento.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Visualizzare lo stato corrente di un servizio in esecuzione su un nodo grid: `**service *servicename* status** lo stato corrente del servizio richiesto in esecuzione sul nodo grid viene segnalato (in esecuzione o meno). Ad esempio:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Disconnettersi dalla shell dei comandi: **`exit`**

Interrompere il servizio

Alcune procedure di manutenzione richiedono l'interruzione di un singolo servizio mantenendo in esecuzione altri servizi sul nodo grid. Interrompere i singoli servizi solo quando richiesto da una procedura di manutenzione.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

Quando si utilizza questa procedura per "arrestare amministrativamente" un servizio, Server Manager non riavvierà automaticamente il servizio. È necessario avviare il servizio singolo manualmente o riavviare Server Manager.

Se è necessario arrestare il servizio LDR su un nodo di storage, tenere presente che potrebbe essere necessario un po' di tempo per arrestare il servizio in presenza di connessioni attive.

Fasi

1. 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. `#`.

2. Interruzione di un singolo servizio: `service servicename stop`

   Ad esempio:

```
service ldr stop
```

L'interruzione dei servizi può richiedere fino a 11 minuti.

3. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

Forzare l'interruzione del servizio

Impostare l'apparecchio in modalità di manutenzione

Prima di eseguire specifiche procedure di manutenzione, è necessario attivare la modalità di manutenzione dell'apparecchio.

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. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

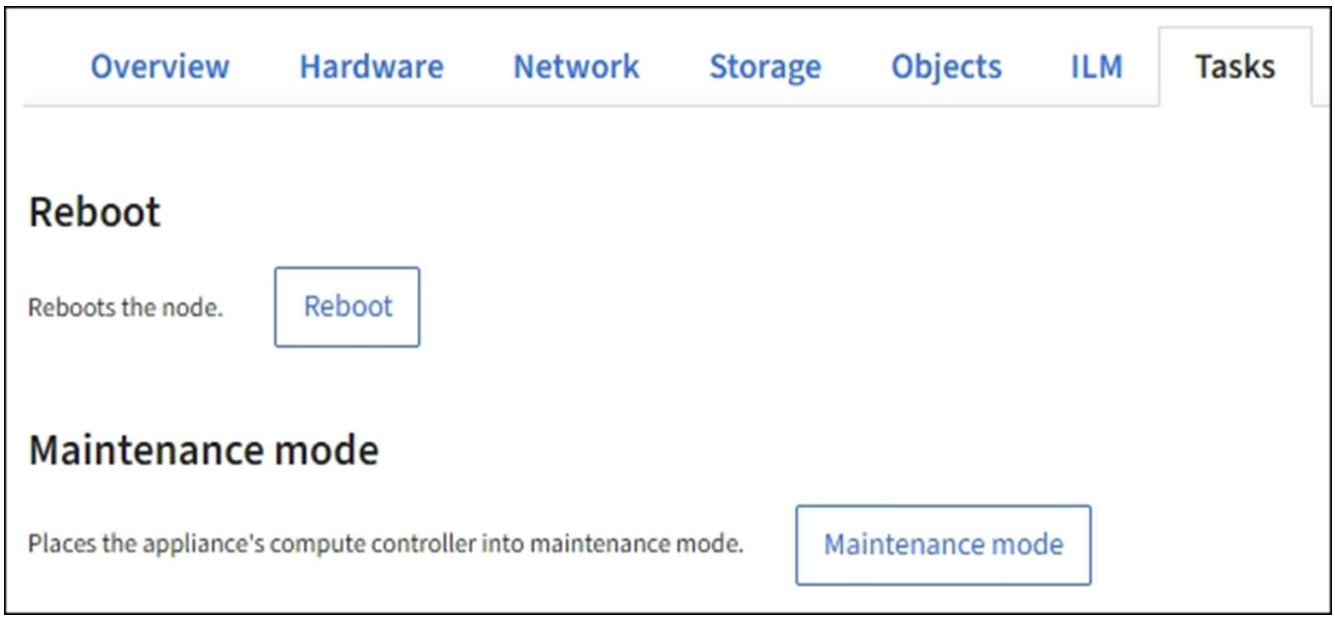
A proposito di questa attività

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

La password dell'account admin e le chiavi host SSH per un'appliance StorageGRID in modalità di manutenzione rimangono le stesse di quando l'appliance era in servizio.

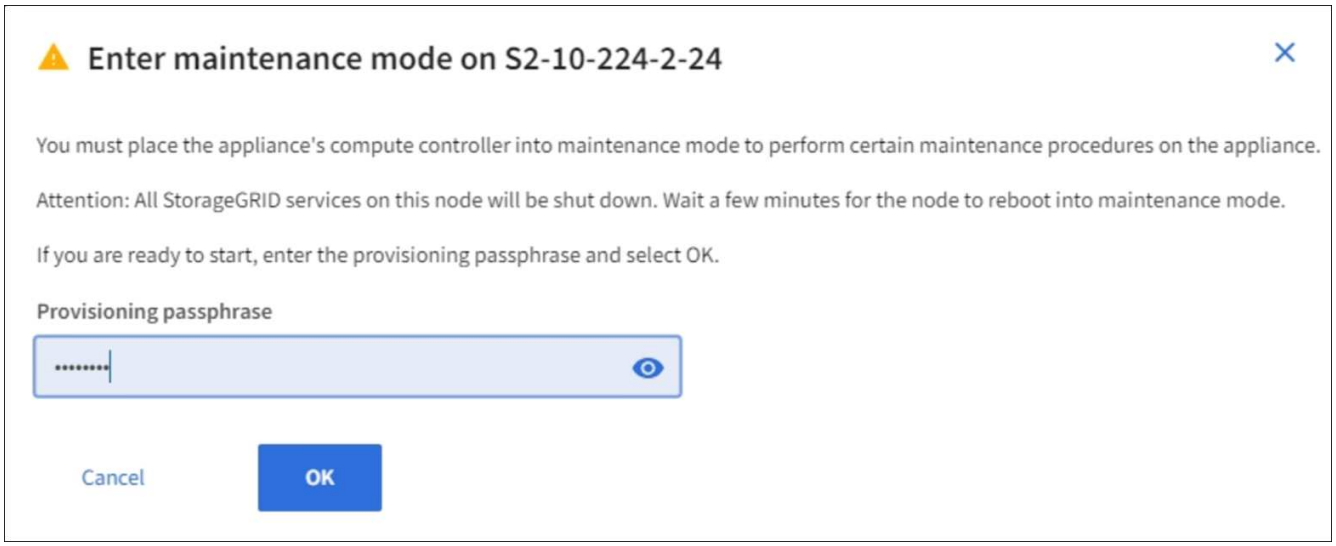
Fasi

1. Da Grid Manager, selezionare **NODES**.
2. Dalla vista ad albero della pagina Nodes (nodi), selezionare il nodo di storage dell'appliance.
3. Selezionare **Tasks**.



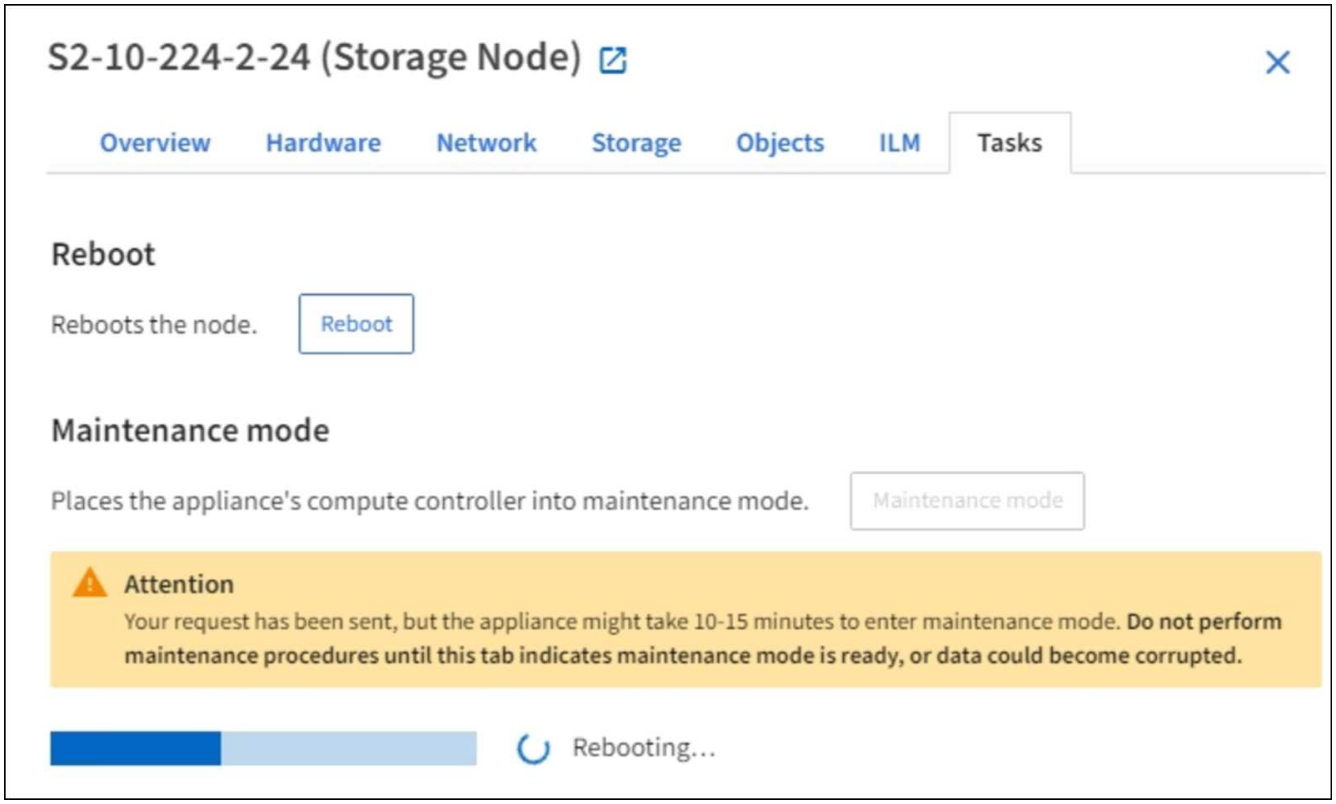
4. Selezionare **modalità di manutenzione**.

   Viene visualizzata una finestra di dialogo di conferma.

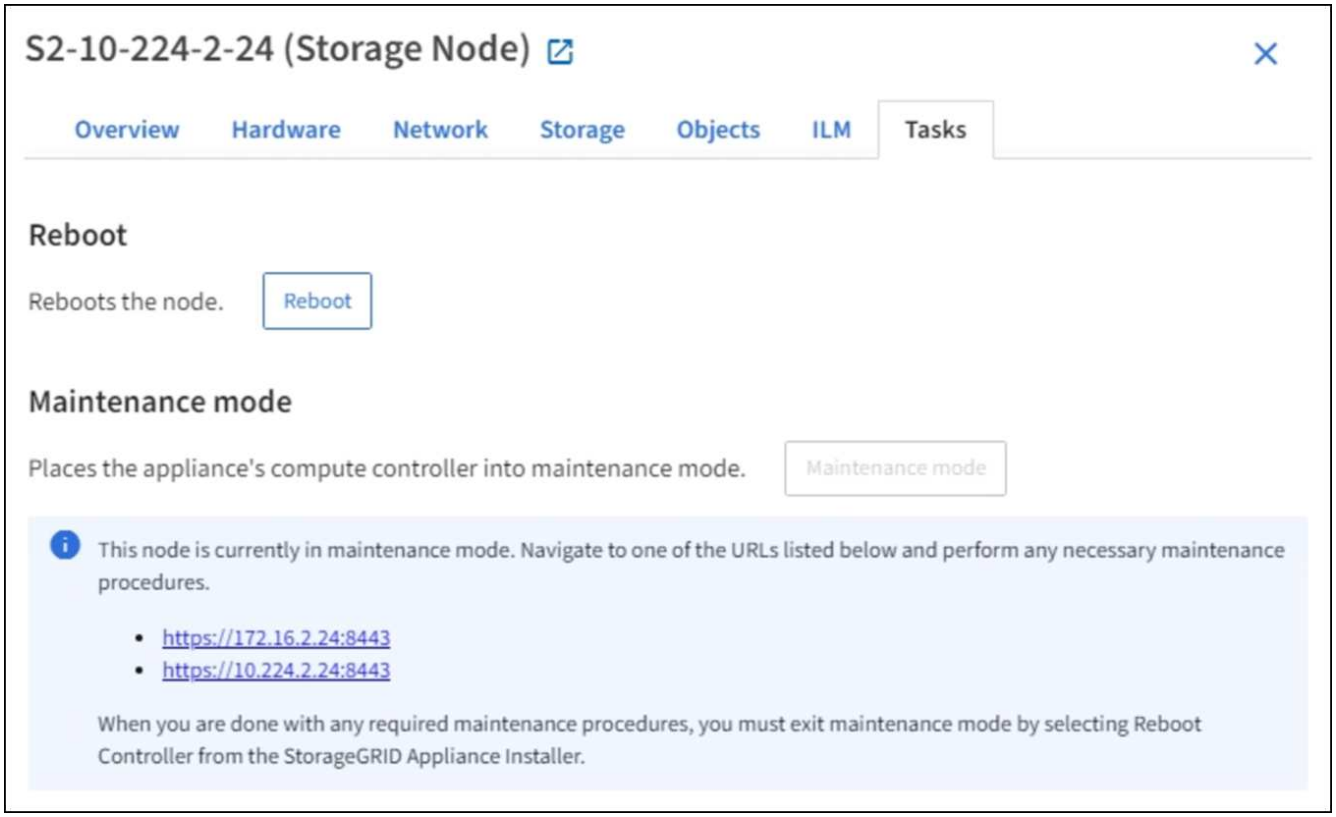


5. Inserire la passphrase di provisioning e selezionare **OK**.

   Una barra di avanzamento e una serie di messaggi, tra cui "richiesta inviata", "interruzione StorageGRID" e "riavvio", indicano che l'appliance sta completando la procedura per accedere alla modalità di manutenzione.



   Quando l'appliance è in modalità di manutenzione, un messaggio di conferma elenca gli URL che è possibile utilizzare per accedere al programma di installazione dell'appliance StorageGRID.



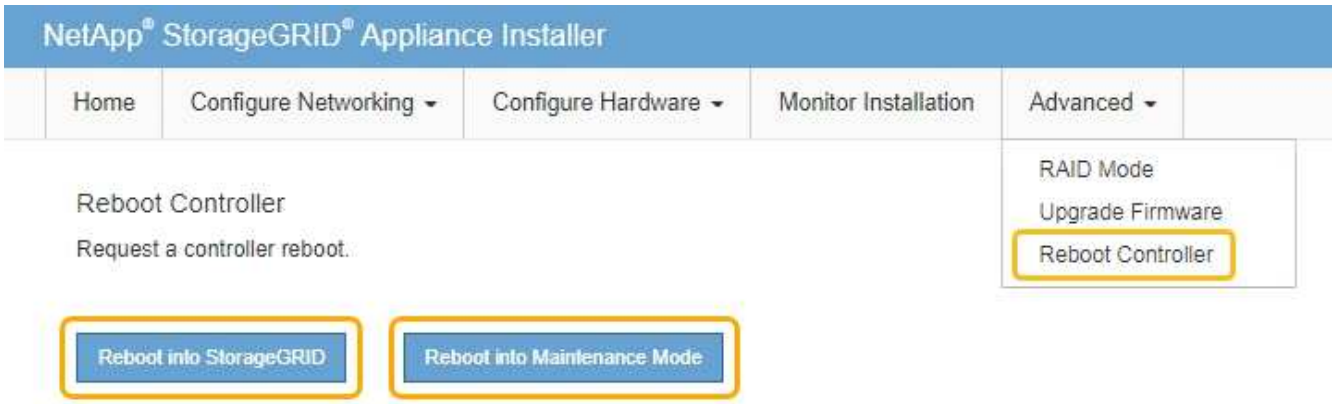
6. Per accedere al programma di installazione dell'appliance StorageGRID, selezionare uno degli URL visualizzati.

   Se possibile, utilizzare l'URL contenente l'indirizzo IP della porta Admin Network dell'appliance.

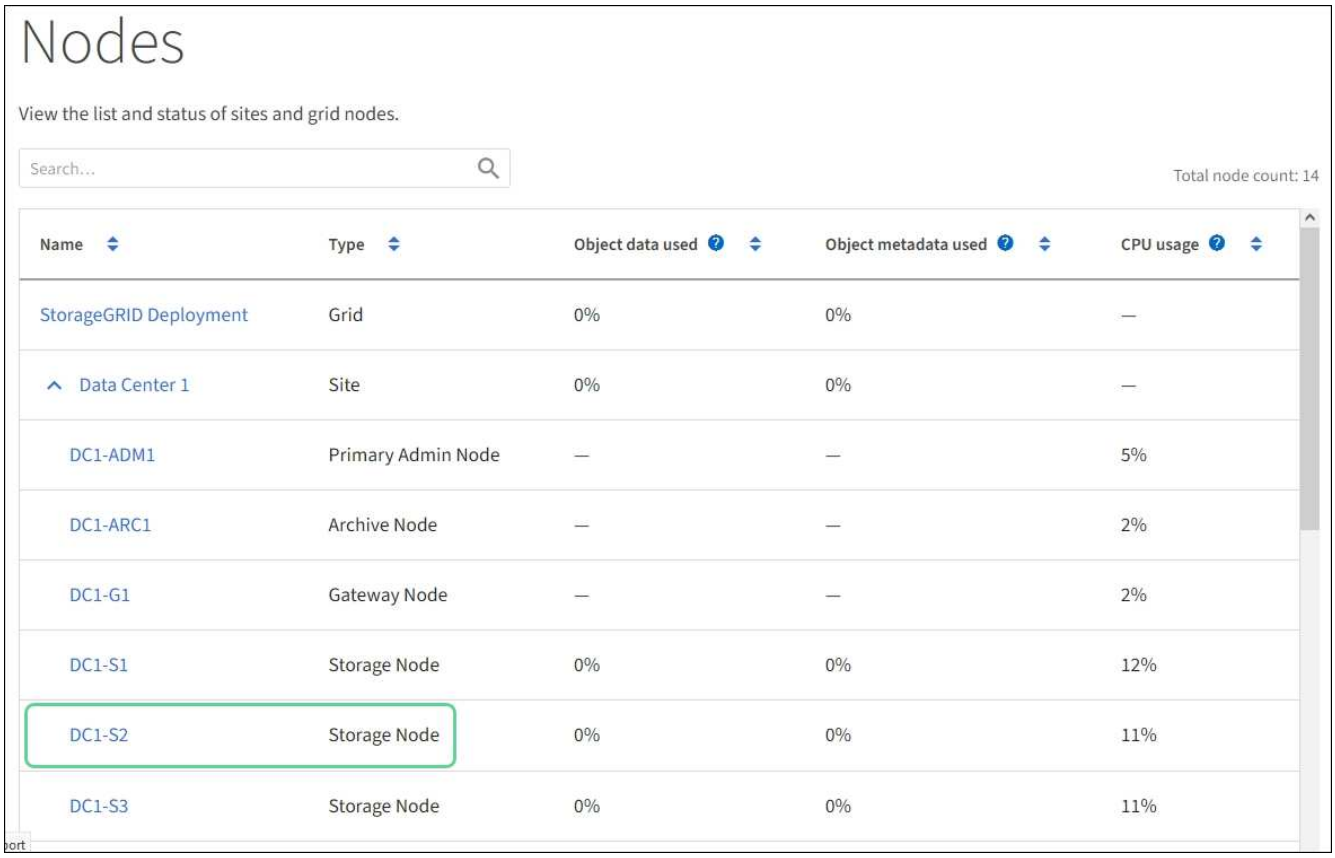
   > Accesso `https://169.254.0.1:8443` richiede una connessione diretta alla porta di gestione locale.

7. Dal programma di installazione dell'appliance StorageGRID, verificare che l'appliance sia in modalità di manutenzione.

8. Eseguire le attività di manutenzione richieste.
9. Dopo aver completato le attività di manutenzione, uscire dalla modalità di manutenzione e riprendere il normale funzionamento del nodo. Dal programma di installazione dell'appliance StorageGRID, selezionare **Avanzate** > **Riavvia controller**, quindi selezionare **Riavvia in StorageGRID**.



Il riavvio dell'appliance e il ricongiungersi alla griglia possono richiedere fino a 20 minuti. Per confermare che il riavvio è stato completato e che il nodo ha ricongiungersi alla griglia, tornare a Grid Manager. La pagina **Nodes** dovrebbe visualizzare uno stato normale (nessuna icona a sinistra del nome del nodo) per il nodo appliance, a indicare che non sono attivi avvisi e che il nodo è connesso alla griglia.



Forzare l'interruzione del servizio

Se è necessario interrompere immediatamente un servizio, è possibile utilizzare `force-stop` comando.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Forzare manualmente l'interruzione del servizio: `service servicename force-stop`

   Ad esempio:

   ```
   service ldr force-stop
   ```

   Il sistema attende 30 secondi prima di terminare il servizio.

3. Disconnettersi dalla shell dei comandi: `exit`

Avviare o riavviare il servizio

Potrebbe essere necessario avviare un servizio che è stato arrestato oppure arrestare e riavviare un servizio.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Decidere quale comando emettere, in base al fatto che il servizio sia attualmente in esecuzione o interrotto.

   - Se il servizio è attualmente arrestato, utilizzare `start` comando per avviare il servizio manualmente: `service servicename start`

     Ad esempio:

```
service ldr start
```

- Se il servizio è in esecuzione, utilizzare `restart` comando per arrestare e riavviare il servizio: `service servicename restart`

  Ad esempio:

```
service ldr restart
```

+

> Utilizzando il `restart` il comando è identico a quello utilizzato da `stop` seguito dal comando `start` comando. È possibile che si verifici problemi `restart` anche se il servizio è attualmente arrestato.

3. Disconnettersi dalla shell dei comandi: `exit`

Rimuovere i rimap delle porte

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta che è già stata configurata come porta mappata di un remap di porta, è necessario prima rimuovere il remap di porta esistente, altrimenti l'endpoint non sarà efficace. È necessario eseguire uno script su ciascun nodo Admin e nodo gateway che dispone di porte remapped in conflitto per rimuovere tutti i remap delle porte del nodo.

> **A proposito di questa attività**
>
> Questa procedura rimuove tutti i rimap delle porte. Se hai bisogno di conservare alcuni rimaps, contatta il supporto tecnico.

Per informazioni sulla configurazione degli endpoint del bilanciamento del carico, vedere le istruzioni per l'amministrazione di StorageGRID.

> Se il remap della porta fornisce l'accesso al client, il client deve essere riconfigurato in modo da utilizzare una porta diversa configurata come endpoint del bilanciamento del carico, se possibile, per evitare la perdita di servizio, altrimenti la rimozione del mapping delle porte causerà la perdita dell'accesso al client e dovrebbe essere pianificata in modo appropriato.

> Questa procedura non funziona per un sistema StorageGRID implementato come container su host bare metal. Consultare le istruzioni per rimozione dei rimaps delle porte sugli host bare metal.

Fasi

1. Accedere al nodo.
   a. Immettere il seguente comando: `ssh -p 8022 admin@node_IP`

      La porta 8022 è la porta SSH del sistema operativo di base, mentre la porta 22 è la porta SSH del

motore dei container che esegue StorageGRID.

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. `#`.

2. Eseguire il seguente script: `remove-port-remap.sh`
3. Riavviare il nodo.

   Seguire le istruzioni per riavvio di un nodo grid.

4. Ripetere questi passaggi su ogni nodo Admin e nodo gateway con porte remapped in conflitto.

Informazioni correlate

Amministrare StorageGRID

Rimuovere i rimaps delle porte sugli host bare metal

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta che è già stata configurata come porta mappata di un remap di porta, è necessario prima rimuovere il remap di porta esistente, altrimenti l'endpoint non sarà efficace. Se si esegue StorageGRID su host bare metal, seguire questa procedura invece della procedura generale per rimuovere i rimaps delle porte. È necessario modificare il file di configurazione del nodo per ogni nodo Admin e nodo gateway che ha porte remapped in conflitto per rimuovere tutti i remap delle porte del nodo e riavviare il nodo.

A proposito di questa attività

Questa procedura rimuove tutti i rimap delle porte. Se hai bisogno di conservare alcuni rimaps, contatta il supporto tecnico.

Per informazioni sulla configurazione degli endpoint del bilanciamento del carico, vedere le istruzioni per l'amministrazione di StorageGRID.

Questa procedura può causare una perdita temporanea del servizio quando i nodi vengono riavviati.

Fasi

1. Accedere all'host che supporta il nodo. Accedere come root o con un account che dispone dell'autorizzazione sudo.
2. Eseguire il seguente comando per disattivare temporaneamente il nodo: `sudo storagegrid node stop node-name`
3. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo per il nodo.

   Il file di configurazione del nodo è disponibile all'indirizzo `/etc/storagegrid/nodes/node-name.conf`.

4. Individuare la sezione del file di configurazione del nodo che contiene i rimap delle porte.

   Vedere le ultime due righe nell'esempio seguente.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. Modificare LE voci PORT_REMAP e PORT_REMAP_INBOUND per rimuovere i rimap delle porte.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo per il nodo: `sudo storagegrid node validate node-name`

   Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

7. Eseguire il seguente comando per riavviare il nodo senza i rimaps delle porte: `sudo storagegrid node start node-name`
8. Accedere al nodo come admin utilizzando la password elencata in `Passwords.txt` file.
9. Verificare che i servizi vengano avviati correttamente.

a. Visualizzare un elenco degli stati di tutti i servizi sul server:`sudo storagegrid-status`

   Lo stato viene aggiornato automaticamente.

b. Attendere che tutti i servizi abbiano lo stato di in esecuzione o verificato.

c. Uscire dalla schermata di stato:`Ctrl+C`

10. Ripetere questi passaggi su ogni nodo Admin e nodo gateway con porte remapped in conflitto.

Nodo di reboot grid

È possibile riavviare un nodo Grid da Grid Manager o dalla shell dei comandi del nodo.

A proposito di questa attività

Quando si riavvia un nodo Grid, il nodo si spegne e si riavvia. Tutti i servizi vengono riavviati automaticamente.

Se si prevede di riavviare i nodi 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.

Informazioni correlate

Amministrare StorageGRID

Riavviare il nodo Grid da Grid Manager

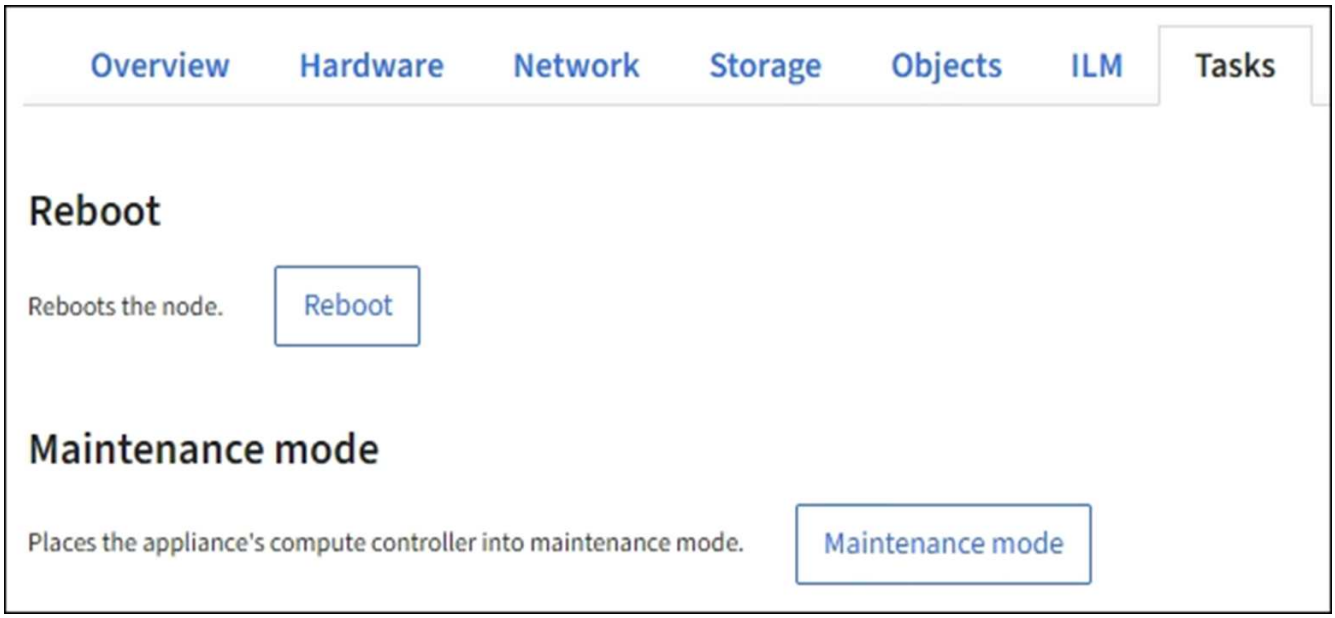
Il riavvio di un nodo Grid da Grid Manager genera il `reboot` sul nodo di destinazione.

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.

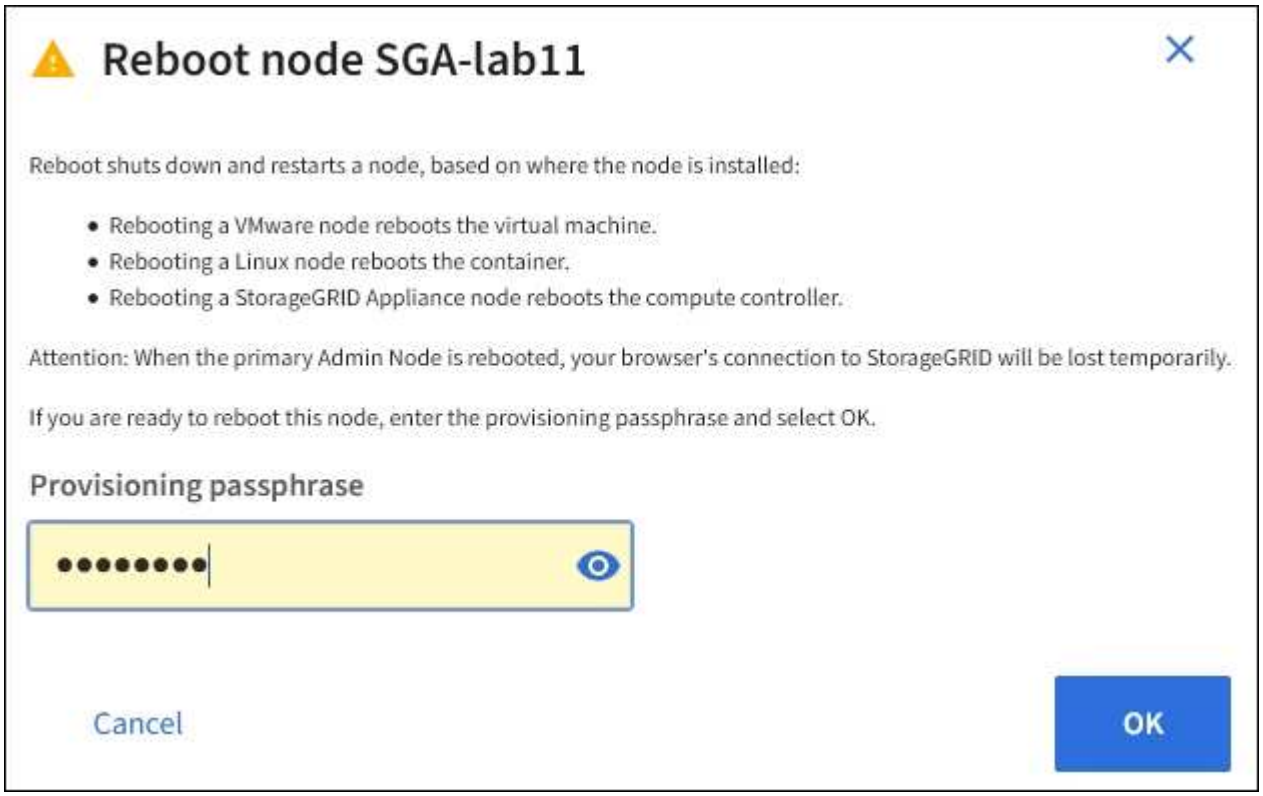
Fasi

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.

Riavviare il nodo Grid dalla shell dei comandi

Se è necessario monitorare più da vicino l'operazione di riavvio o se non si riesce ad accedere a Grid Manager, è possibile accedere al nodo Grid ed eseguire il comando di riavvio di Server Manager dalla shell dei comandi.

È necessario disporre di `Passwords.txt` file.

1. 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. `#`.

2. Facoltativamente, interrompere i servizi: `service servermanager stop`

   L'interruzione dei servizi è un passaggio facoltativo, ma consigliato. L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto prima di riavviare il nodo nella fase successiva.

3. Riavviare il nodo Grid: `reboot`

4. Disconnettersi dalla shell dei comandi: `exit`

Chiudere il nodo della griglia

È possibile chiudere un nodo Grid dalla shell dei comandi del nodo.

Di cosa hai bisogno

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

A proposito di questa attività

Prima di eseguire questa procedura, esaminare le seguenti considerazioni:

- In generale, non è necessario spegnere più di un nodo alla volta per evitare interruzioni.
- Non spegnere un nodo durante una procedura di manutenzione, a meno che non venga espressamente richiesto dalla documentazione o dal supporto tecnico.
- Il processo di shutdown si basa sulla posizione in cui è installato il nodo, come segue:
  - L'arresto di un nodo VMware arresta la macchina virtuale.

- L'arresto di un nodo Linux arresta il container.
- L'arresto di un nodo appliance StorageGRID arresta il controller di calcolo.

- Se si prevede di chiudere più di un nodo di storage in un sito, interrompere l'acquisizione di oggetti in quel sito per circa un'ora prima di spegnere i nodi.

  Se una regola ILM utilizza l'opzione di acquisizione **doppio commit** (o se una regola utilizza l'opzione **bilanciato** e non è possibile creare immediatamente tutte le copie richieste), StorageGRID commuta immediatamente gli oggetti appena acquisiti a due nodi di storage sullo stesso sito e valuta ILM in un secondo momento. Se più di un nodo di storage in un sito viene arrestato, potrebbe non essere possibile accedere agli oggetti appena acquisiti per la durata della chiusura. Anche le operazioni di scrittura potrebbero non riuscire se nel sito rimangono disponibili troppi nodi di storage.

Fasi

1. 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. `#`.

2. Arrestare tutti i servizi: `service servermanager stop`

   L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

3. Se il nodo è in esecuzione su una macchina virtuale VMware o si tratta di un nodo appliance, eseguire il comando shutdown: `shutdown -h now`

   Eseguire questa operazione indipendentemente dal risultato dell' `service servermanager stop` comando.

   > Dopo aver eseguito il `shutdown -h now` su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

   Per l'appliance, questo comando spegne il controller, ma l'appliance è ancora accesa. Completare la fase successiva.

4. Se si sta spegnendo un nodo appliance:
   - Per l'appliance di servizi SG100 o SG1000
     i. Spegnere l'apparecchio.
     ii. Attendere che il LED di alimentazione blu si spenga.
   - Per l'appliance SG6000
     i. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

     Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi.

Prima di spegnere il prodotto, attendere che il LED si spenga.

ii. Spegnere l'apparecchio e attendere che il LED di alimentazione blu si spenga.

- Per l'appliance SG5700

  i. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

  Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

  ii. Spegnere l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.

Informazioni correlate

Amministrare StorageGRID

Spegnere l'host

Prima di spegnere un host, è necessario interrompere i servizi su tutti i nodi della rete su tale host.

Fasi

1. 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. `#`.

2. Arrestare tutti i servizi in esecuzione sul nodo: `service servermanager stop`

   L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

3. Ripetere i passaggi 1 e 2 per ciascun nodo dell'host.
4. Se si dispone di un host Linux:

   a. Accedere al sistema operativo host.

   b. Arrestare il nodo: `storagegrid node stop`

   c. Arrestare il sistema operativo host.

5. Se il nodo è in esecuzione su una macchina virtuale VMware o si tratta di un nodo appliance, eseguire il comando shutdown: `shutdown -h now`

   Eseguire questa operazione indipendentemente dal risultato dell' `service servermanager stop` comando.

   > Dopo aver eseguito il `shutdown -h now` su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

Per l'appliance, questo comando spegne il controller, ma l'appliance è ancora accesa. Completare la fase successiva.

6. Se si sta spegnendo un nodo appliance:
   - Per l'appliance di servizi SG100 o SG1000
     i. Spegnere l'apparecchio.
     ii. Attendere che il LED di alimentazione blu si spenga.
   - Per l'appliance SG6000
     i. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

        Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

     ii. Spegnere l'apparecchio e attendere che il LED di alimentazione blu si spenga.
   - Per l'appliance SG5700
     i. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

        Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

     ii. Spegnere l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.
7. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

Appliance di servizi SG100 e SG1000

Appliance di storage SG6000

Appliance di storage SG5700

Spegnere e riaccendere tutti i nodi della rete

Potrebbe essere necessario spegnere l'intero sistema StorageGRID, ad esempio, se si sta spostando un data center. Questi passaggi forniscono una panoramica di alto livello della sequenza consigliata per l'esecuzione di uno shutdown e di un startup controllati.

Quando si spengono tutti i nodi di un sito o di una griglia, non sarà possibile accedere agli oggetti acquisiti mentre i nodi di storage sono offline.

Arrestare i servizi e chiudere i nodi di rete

Prima di spegnere un sistema StorageGRID, è necessario arrestare tutti i servizi in esecuzione su ciascun nodo di rete e quindi arrestare tutte le macchine virtuali VMware, i motori di container e le appliance StorageGRID.

A proposito di questa attività

Arrestare prima i servizi sui nodi Admin e sui nodi API Gateway, quindi arrestare i servizi sui nodi Storage.

Questo approccio consente di utilizzare l'Admin Node primario per monitorare lo stato degli altri nodi della griglia il più a lungo possibile.

> Se un singolo host include più di un nodo di griglia, non spegnere l'host fino a quando non sono stati arrestati tutti i nodi su tale host. Se l'host include il nodo di amministrazione primario, arrestare l'host per ultimo.

> Se necessario, è possibile Migrare i nodi da un host Linux a un altro per eseguire la manutenzione degli host senza influire sulle funzionalità o sulla disponibilità del grid.

Fasi

1. Impedire a tutte le applicazioni client di accedere alla griglia.
2. Accedi a ciascun nodo gateway:
   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. Arresta tutti i servizi in esecuzione sul nodo: `service servermanager stop`

   L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.
4. Ripetere i due passaggi precedenti per arrestare i servizi su tutti i nodi di storage, i nodi di archivio e i nodi di amministrazione non primari.

   È possibile interrompere i servizi su questi nodi in qualsiasi ordine.

   > Se si esegue il `service servermanager stop` Per arrestare i servizi su un nodo di storage dell'appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.
5. Per il nodo di amministrazione principale, ripetere i passaggi per accesso al nodo e. interruzione di tutti i servizi sul nodo.
6. Per i nodi in esecuzione su host Linux:
   a. Accedere al sistema operativo host.
   b. Arrestare il nodo: `storagegrid node stop`
   c. Arrestare il sistema operativo host.
7. Per i nodi in esecuzione sulle macchine virtuali VMware e per i nodi di storage dell'appliance, eseguire il comando shutdown: `shutdown -h now`

   Eseguire questa operazione indipendentemente dal risultato dell' `service servermanager stop` comando.

   Per l'appliance, questo comando arresta il controller di calcolo, ma l'appliance è ancora accesa.

Completare la fase successiva.

8. Se si dispone di nodi appliance:
   - Per l'appliance di servizi SG100 o SG1000
     i. Spegnere l'apparecchio.
     ii. Attendere che il LED di alimentazione blu si spenga.
   - Per l'appliance SG6000
     i. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

        Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

     ii. Spegnere l'apparecchio e attendere che il LED di alimentazione blu si spenga.
   - Per l'appliance SG5700
     i. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

        Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

     ii. Spegnere l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.
9. Se necessario, disconnettersi dalla shell dei comandi: `exit`

   La griglia StorageGRID è stata chiusa.

Informazioni correlate

Appliance di servizi SG100 e SG1000

Appliance di storage SG6000

Appliance di storage SG5700

Avviare i nodi della griglia

Seguire questa sequenza per avviare i nodi della griglia dopo un arresto completo.

> **Quello di cui hai bisogno 8217**
>
> Se l'intero grid è stato spento per più di 15 giorni, è necessario contattare il supporto tecnico prima di avviare qualsiasi grid node. Non tentare di eseguire le procedure di ripristino che ricostruiscono i dati Cassandra. Ciò potrebbe causare la perdita di dati.

A proposito di questa attività

Se possibile, accendere i nodi della rete in questo ordine:

- Prima di tutto, alimentare i nodi di amministrazione.
- Alimentare per ultimo i nodi gateway.

Se un host include più nodi di rete, i nodi torneranno automaticamente in linea all'accensione dell'host.

Fasi

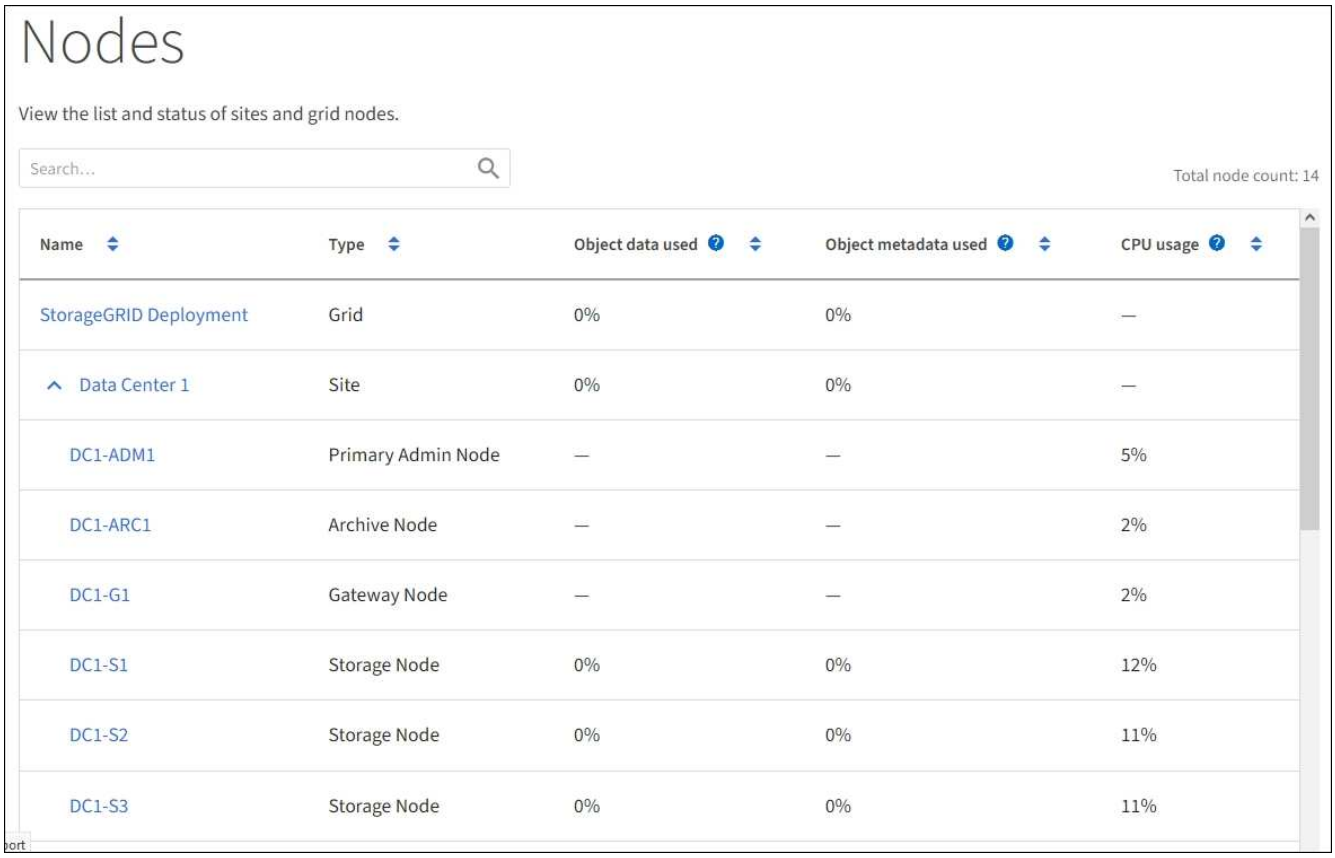
1. Accendere gli host per il nodo di amministrazione primario e tutti i nodi di amministrazione non primari.

   Non sarà possibile accedere ai nodi di amministrazione fino a quando i nodi di storage non saranno stati riavviati.

2. Accendere gli host per tutti i nodi di archiviazione e i nodi di storage.

   È possibile accendere questi nodi in qualsiasi ordine.

3. Accendere gli host per tutti i nodi gateway.
4. Accedi a Grid Manager.
5. Selezionare **NODI** e monitorare lo stato dei nodi della griglia. Verificare che non siano presenti icone di avviso accanto ai nomi dei nodi.



Utilizzare un file DoNotStart

Se si eseguono diverse procedure di manutenzione o configurazione sotto la direzione del supporto tecnico, potrebbe essere richiesto di utilizzare un file DoNotStart per impedire l'avvio dei servizi all'avvio o al riavvio di Server Manager.

Aggiungere o rimuovere un file DoNotStart solo se richiesto dal supporto tecnico.

Per impedire l'avvio di un servizio, inserire un file DoNotStart nella directory del servizio che si desidera impedire l'avvio. All'avvio, Server Manager cerca il file DoNotStart. Se il file è presente, non è possibile avviare il servizio (e i servizi da esso dipendenti). Quando il file DoNotStart viene rimosso, il servizio precedentemente interrotto viene avviato al successivo avvio o riavvio di Server Manager. I servizi non vengono avviati automaticamente quando il file DoNotStart viene rimosso.

Il modo più efficiente per impedire il riavvio di tutti i servizi consiste nell'impedire l'avvio del servizio NTP. Tutti i servizi dipendono dal servizio NTP e non possono essere eseguiti se il servizio NTP non è in esecuzione.

Aggiungere il file DoNotStart per il servizio

È possibile impedire l'avvio di un singolo servizio aggiungendo un file DoNotStart alla directory del servizio su un nodo Grid.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Aggiunta di un file DoNotStart: `touch /etc/sv/`*`service`*`/DoNotStart`

   dove `service` indica il nome del servizio che non può essere avviato. Ad esempio,

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   Viene creato un file DoNotStart. Non è necessario alcun contenuto di file.

   Al riavvio di Server Manager o del nodo grid, Server Manager viene riavviato, ma il servizio non viene attivato.

3. Disconnettersi dalla shell dei comandi: `exit`

Rimuovere il file DoNotStart per l'assistenza

Quando si rimuove un file DoNotStart che impedisce l'avvio di un servizio, è necessario avviarlo.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

Fasi

1. 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. `#`.

2. Rimuovere il file DoNotStart dalla directory di servizio: `rm /etc/sv/service/DoNotStart`

   dove `service` è il nome del servizio. Ad esempio,

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. Avviare il servizio: `service servicename start`

4. Disconnettersi dalla shell dei comandi: `exit`

Risolvere i problemi di Server Manager

Accedere al file di log di Server Manager

Se si verifica un problema durante l'utilizzo di Server Manager, controllare il file di log.

I messaggi di errore relativi a Server Manager vengono acquisiti nel file di log di Server Manager, che si trova all'indirizzo: `/var/local/log/servermanager.log`

Controllare questo file per i messaggi di errore relativi agli errori. Se necessario, inoltrare il problema al supporto tecnico. Potrebbe essere richiesto di inoltrare i file di registro al supporto tecnico.

Servizio con stato di errore

Se si rileva che un servizio è entrato in uno stato di errore, tentare di riavviare il servizio.

Di cosa hai bisogno

È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

Server Manager monitora i servizi e riavvia quelli che si sono arrestati inaspettatamente. Se un servizio non riesce, Server Manager tenta di riavviarlo. Se si verificano tre tentativi non riusciti di avvio di un servizio entro cinque minuti, il servizio entra in uno stato di errore. Server Manager non tenta un altro riavvio.

Fasi

1. 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. `#`.

2. Confermare lo stato di errore del servizio: `service *servicename* status`

   Ad esempio:

   ```
   service ldr status
   ```

   Se il servizio si trova in uno stato di errore, viene visualizzato il seguente messaggio: `*servicename* in error state`. Ad esempio:

   ```
   ldr in error state
   ```

   > Se lo stato del servizio è `disabled`, consultare le istruzioni per Rimozione di un file DoNotStart per un servizio.

3. Tentare di rimuovere lo stato di errore riavviando il servizio: `service *servicename* restart`

   Se il servizio non viene riavviato, contattare il supporto tecnico.

4. Disconnettersi dalla shell dei comandi: `exit`

Cloning del nodo dell'appliance

È possibile clonare un nodo appliance in StorageGRID per utilizzare un'appliance di progettazione più recente o con funzionalità avanzate. La clonazione trasferisce tutte le informazioni sul nodo esistente alla nuova appliance, fornisce un processo di aggiornamento dell'hardware semplice da eseguire e fornisce un'alternativa alla disattivazione e all'espansione per la sostituzione delle appliance.

Come funziona la clonazione dei nodi dell'appliance

La clonazione dei nodi dell'appliance consente di sostituire facilmente un nodo (origine) dell'appliance esistente nella griglia con un'appliance compatibile (destinazione) che fa parte dello stesso sito StorageGRID logico. Il processo trasferisce tutti i dati alla nuova appliance, mettendola in servizio per sostituire il nodo della vecchia appliance e lasciandola in uno stato pre-installato.

Perché clonare un nodo appliance?

È possibile clonare un nodo appliance se è necessario:

- Sostituire le appliance che stanno per terminare il ciclo di vita.
- Aggiorna i nodi esistenti per sfruttare la tecnologia delle appliance migliorata.

- Aumenta la capacità dello storage grid senza modificare il numero di nodi di storage nel sistema StorageGRID.
- Migliorare l'efficienza dello storage, ad esempio cambiando la modalità RAID da DDP-8 a DDP-16 o RAID-6.
- Implementare in modo efficiente la crittografia dei nodi per consentire l'utilizzo di server di gestione delle chiavi (KMS) esterni.

Quale rete StorageGRID viene utilizzata?

La clonazione trasferisce i dati dal nodo di origine direttamente all'appliance di destinazione su una qualsiasi delle tre reti StorageGRID. In genere viene utilizzata la rete Grid, ma è anche possibile utilizzare la rete Admin o la rete Client se l'appliance di origine è collegata a queste reti. Scegliere la rete da utilizzare per clonare il traffico che offre le migliori prestazioni di trasferimento dei dati senza compromettere le prestazioni della rete StorageGRID o la disponibilità dei dati.

Quando si installa l'appliance sostitutiva, è necessario specificare gli indirizzi IP temporanei per la connessione StorageGRID e il trasferimento dei dati. Poiché l'appliance sostitutiva fa parte delle stesse reti del nodo dell'appliance che sostituisce, è necessario specificare gli indirizzi IP temporanei per ciascuna di queste reti sull'appliance sostitutiva.

Compatibilità con le appliance di destinazione

Le appliance sostitutive devono essere dello stesso tipo del nodo di origine che stanno sostituendo ed entrambe devono far parte dello stesso sito logico StorageGRID.

- Un'appliance di servizi sostitutiva può essere diversa dal nodo di amministrazione o dal nodo gateway che sta sostituendo.
  - È possibile clonare un'appliance del nodo di origine SG100 su un'appliance di destinazione dei servizi SG1000 per offrire maggiori funzionalità al nodo di amministrazione o al nodo gateway.
  - È possibile clonare un'appliance del nodo di origine SG1000 su un'appliance di destinazione dei servizi SG100 per ridistribuire SG1000 per un'applicazione più impegnativa.

    Ad esempio, se un'appliance SG1000 di nodi di origine viene utilizzata come nodo di amministrazione e si desidera utilizzarla come nodo di bilanciamento del carico dedicato.

  - La sostituzione di un'appliance di nodo di origine SG1000 con un'appliance di destinazione dei servizi SG100 riduce la velocità massima delle porte di rete da 100 GbE a 25 GbE.
  - Le appliance SG100 e SG1000 dispongono di diversi connettori di rete. La modifica del tipo di appliance potrebbe richiedere la sostituzione dei cavi o dei moduli SFP.
- Un'appliance di storage sostitutiva deve avere una capacità uguale o superiore a quella del nodo di storage che sta sostituendo.
  - Se l'appliance di storage di destinazione ha lo stesso numero di dischi del nodo di origine, i dischi dell'appliance di destinazione devono avere una capacità maggiore (in TB).
  - Se si intende utilizzare la stessa modalità RAID sul nodo di destinazione utilizzata sul nodo di origine, In caso di una modalità RAID meno efficiente in termini di storage (ad esempio, passando da RAID6 a DDP), i dischi dell'appliance di destinazione devono essere più grandi (in TB) rispetto ai dischi dell'appliance di origine.
  - Se il numero di dischi standard installati in un'appliance di storage di destinazione è inferiore al numero di dischi nel nodo di origine, a causa dell'installazione di dischi a stato solido (SSD), la capacità di storage complessiva dei dischi standard nell'appliance di destinazione (in TB) Deve soddisfare o

superare la capacità totale delle unità funzionali di tutti i dischi nel nodo di storage di origine.

Ad esempio, quando si clonano un'appliance SG5660 Storage Node di origine con 60 unità su un'appliance di destinazione SG6060 o SG6060X con 58 unità standard, è necessario installare unità più grandi nell'appliance di destinazione SG6060 o SG6060X prima di eseguire la clonazione per mantenere la capacità dello storage. (I due slot per dischi contenenti SSD nell'appliance di destinazione non sono inclusi nella capacità di storage dell'appliance totale).

Tuttavia, se un'appliance di nodi di origine SG5660 a 60 dischi è configurata con i pool di dischi dinamici SANtricity DDP-8, la configurazione di un'appliance di destinazione SG6060 o SG6060X a 58 dischi con le stesse dimensioni con DDP-16 potrebbe rendere l'appliance SG6060 o SG6060X una destinazione clona valida grazie alla maggiore efficienza dello storage.

È possibile visualizzare le informazioni sulla modalità RAID corrente del nodo dell'appliance di origine nella pagina **NODES** in Grid Manager. Selezionare la scheda **Storage** dell'appliance.

Quali informazioni non vengono clonate?

Le seguenti configurazioni dell'appliance non vengono trasferite all'appliance sostitutiva durante la clonazione. È necessario configurarli durante la configurazione iniziale dell'appliance sostitutiva.

- Interfaccia BMC
- Collegamenti di rete
- Stato di crittografia del nodo
- Gestore di sistema SANtricity (per nodi di storage)
- Modalità RAID (per nodi di storage)

Quali problemi impediscono la clonazione?

Se durante la clonazione si verifica uno dei seguenti problemi, il processo di clonazione si interrompe e viene generato un messaggio di errore:

- Configurazione di rete errata
- Mancanza di connettività tra le appliance di origine e di destinazione
- Incompatibilità tra appliance di origine e di destinazione
- Per i nodi di storage, un'appliance sostitutiva con capacità insufficiente

Per continuare, è necessario risolvere ciascun problema.

Considerazioni e requisiti per la clonazione del nodo dell'appliance

Prima di clonare un nodo appliance, è necessario comprendere le considerazioni e i requisiti.

Requisiti hardware per l'appliance sostitutiva

Assicurarsi che l'apparecchio sostitutivo soddisfi i seguenti criteri:

- Il nodo di origine (appliance da sostituire) e l'appliance di destinazione (nuova) devono essere dello stesso tipo di appliance:

    - È possibile clonare solo un'appliance Admin Node o un'appliance Gateway Node su una nuova appliance di servizi.
    - È possibile clonare un'appliance Storage Node solo su una nuova appliance di storage.
- Per le appliance Admin Node o Gateway Node, l'appliance del nodo di origine e l'appliance di destinazione non devono necessariamente essere dello stesso tipo di appliance; tuttavia, la modifica del tipo di appliance potrebbe richiedere la sostituzione dei cavi o dei moduli SFP.

  Ad esempio, è possibile sostituire un'appliance a nodi SG1000 con un SG100 o un'appliance SG100 con un'appliance SG1000.

- Per le appliance Storage Node, l'appliance del nodo di origine e l'appliance di destinazione non devono necessariamente essere dello stesso tipo di appliance; tuttavia, l'appliance di destinazione deve avere una capacità di storage superiore a quella dell'appliance di origine.

  Ad esempio, è possibile sostituire un'appliance a nodi SG5600 con un'appliance SG5700 o SG6000.

Contatta il tuo rappresentante commerciale StorageGRID per assistenza nella scelta di appliance sostitutive compatibili per clonare nodi di appliance specifici nella tua installazione StorageGRID.

Preparare la clonazione di un nodo appliance

Prima di clonare un nodo appliance, è necessario disporre delle seguenti informazioni:

- Richiedere all'amministratore di rete un indirizzo IP temporaneo per Grid Network da utilizzare con l'appliance di destinazione durante l'installazione iniziale. Se il nodo di origine appartiene a una rete Admin Network o Client Network, ottenere indirizzi IP temporanei per queste reti.

  Gli indirizzi IP temporanei si trovano normalmente sulla stessa subnet dell'appliance del nodo di origine clonata e non sono necessari al termine della clonazione. Per stabilire una connessione di clonazione, le appliance di origine e di destinazione devono essere collegate al nodo di amministrazione principale di StorageGRID.

- Determinare quale rete utilizzare per clonare il traffico di trasferimento dei dati in grado di fornire le migliori prestazioni di trasferimento dei dati senza compromettere le prestazioni della rete StorageGRID o la disponibilità dei dati.

  > L'utilizzo della rete di amministrazione 1-GbE per il trasferimento dei dati dei cloni comporta un rallentamento della clonazione.

- Determinare se la crittografia del nodo utilizzando un server di gestione delle chiavi (KMS) verrà utilizzata sull'appliance di destinazione, in modo da poter attivare la crittografia del nodo durante l'installazione iniziale dell'appliance di destinazione prima della clonazione. È possibile verificare se la crittografia del nodo è attivata sul nodo dell'appliance di origine, come descritto in Installazione dell'appliance.

  Il nodo di origine e l'appliance di destinazione possono avere diverse impostazioni di crittografia del nodo. La decrittografia e la crittografia dei dati vengono eseguite automaticamente durante il trasferimento dei dati e quando il nodo di destinazione viene riavviato e si unisce alla griglia.

    - Appliance di servizi SG100 e SG1000
    - Appliance di storage SG5600
    - Appliance di storage SG5700
    - Appliance di storage SG6000

- Determinare se la modalità RAID sull'appliance di destinazione deve essere modificata rispetto all'impostazione predefinita, in modo da poter specificare queste informazioni durante l'installazione iniziale dell'appliance di destinazione prima della clonazione. È possibile visualizzare le informazioni sulla modalità RAID corrente del nodo dell'appliance di origine nella pagina **NODES** in Grid Manager. Selezionare la scheda **Storage** dell'appliance.

  Il nodo di origine e l'appliance di destinazione possono avere impostazioni RAID diverse.

- Pianificare un tempo sufficiente per completare il processo di clonazione del nodo. Potrebbero essere necessari diversi giorni per trasferire i dati da un nodo di storage operativo a un'appliance di destinazione. Pianifica la clonazione in un momento che minimizza l'impatto sul tuo business.
- È necessario clonare un solo nodo appliance alla volta. La clonazione può impedire l'esecuzione contemporanea di altre funzioni di manutenzione di StorageGRID.
- Dopo aver clonato un nodo appliance, è possibile utilizzare l'appliance di origine che è stata restituita in uno stato pre-installazione come destinazione per clonare un'altra appliance di nodi compatibile.

Nodo appliance clone

Il processo di clonazione potrebbe richiedere diversi giorni per trasferire i dati tra il nodo di origine (appliance da sostituire) e l'appliance di destinazione (nuova).

Di cosa hai bisogno

- L'appliance di destinazione compatibile è stata installata in un cabinet o rack, sono stati collegati tutti i cavi e l'alimentazione è stata applicata.
- È stato verificato che la versione del programma di installazione dell'appliance StorageGRID installata sull'appliance sostitutiva corrisponde alla versione software del sistema StorageGRID, aggiornando il firmware del programma di installazione dell'appliance StorageGRID, se necessario.
- L'appliance di destinazione è stata configurata, inclusa la configurazione delle connessioni StorageGRID, di Gestore di sistema SANtricity (solo appliance di storage) e dell'interfaccia BMC.
  - Quando si configurano le connessioni StorageGRID, utilizzare gli indirizzi IP temporanei.
  - Quando si configurano i collegamenti di rete, utilizzare la configurazione finale del collegamento.

> Lasciare aperto il programma di installazione dell'appliance StorageGRID dopo aver completato la configurazione iniziale dell'appliance di destinazione. Una volta avviato il processo di clonazione del nodo, viene visualizzata nuovamente la pagina del programma di installazione dell'appliance di destinazione.

- Se si desidera, è stata attivata la crittografia dei nodi per l'appliance di destinazione.
- Se si desidera, è stata impostata la modalità RAID per l'appliance di destinazione (solo per le appliance di storage).
- Considerazioni e requisiti per la clonazione del nodo dell'appliance

  Appliance di servizi SG100 e SG1000

  Appliance di storage SG5600

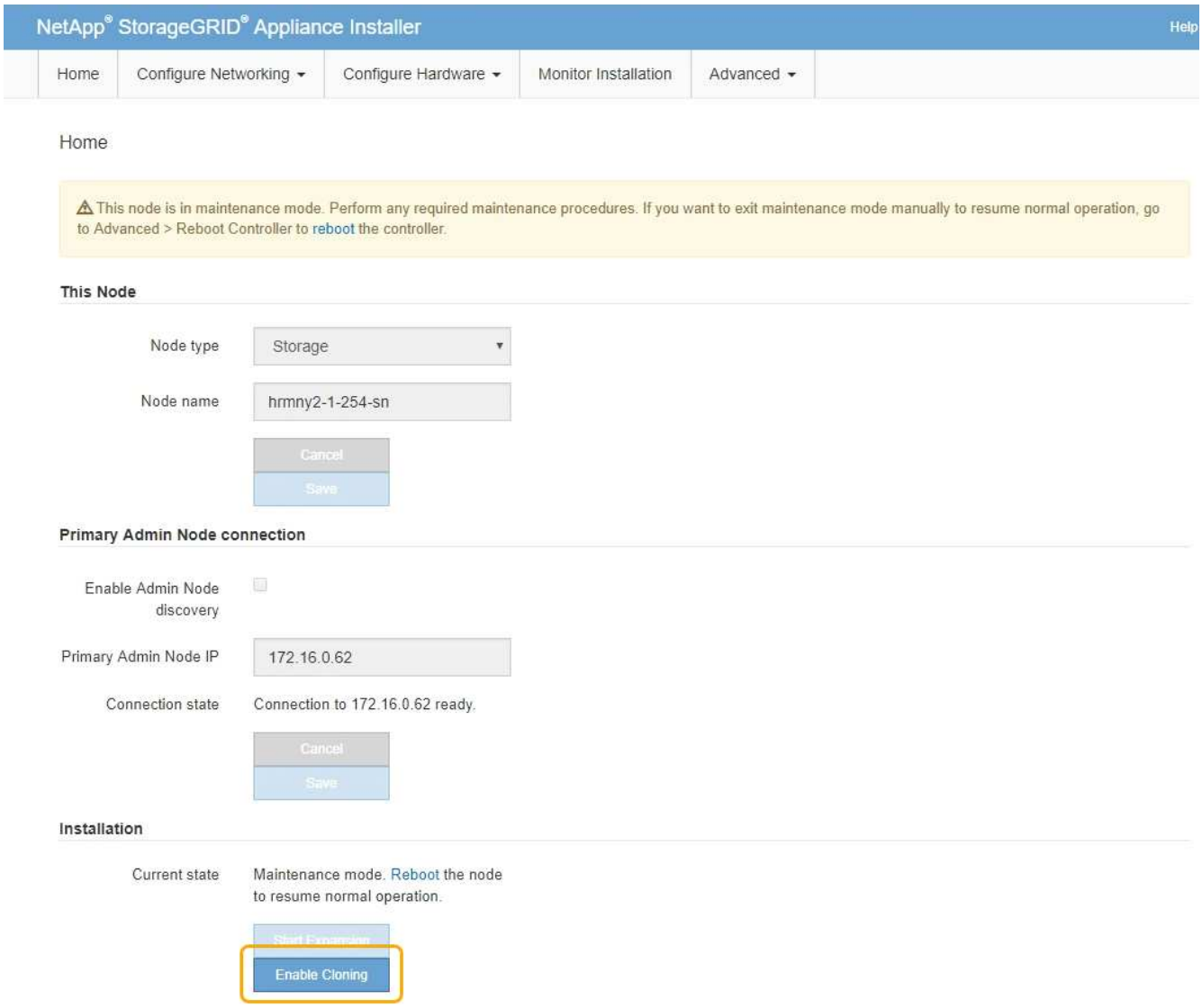
  Appliance di storage SG5700

  Appliance di storage SG6000

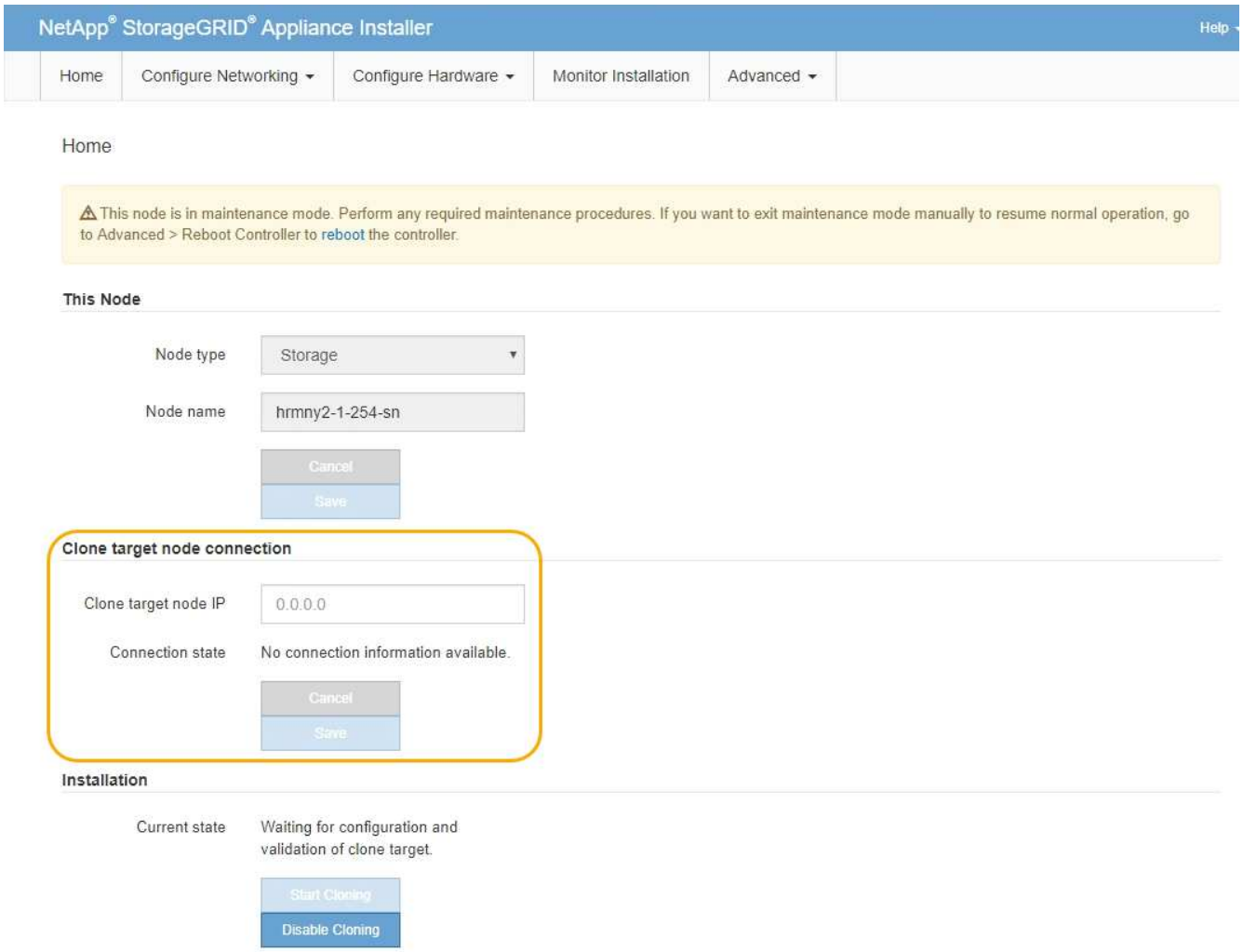
Per mantenere le performance di rete e la disponibilità dei dati di StorageGRID, è necessario clonare un solo nodo appliance alla volta.

Fasi

1. Impostare il nodo di origine che si desidera clonare in modalità di manutenzione.
2. Dal programma di installazione dell'appliance StorageGRID nel nodo di origine, nella sezione Installazione della home page, selezionare **attiva clonazione**.



La sezione Primary Admin Node Connection viene sostituita con la sezione Clone target node Connection.

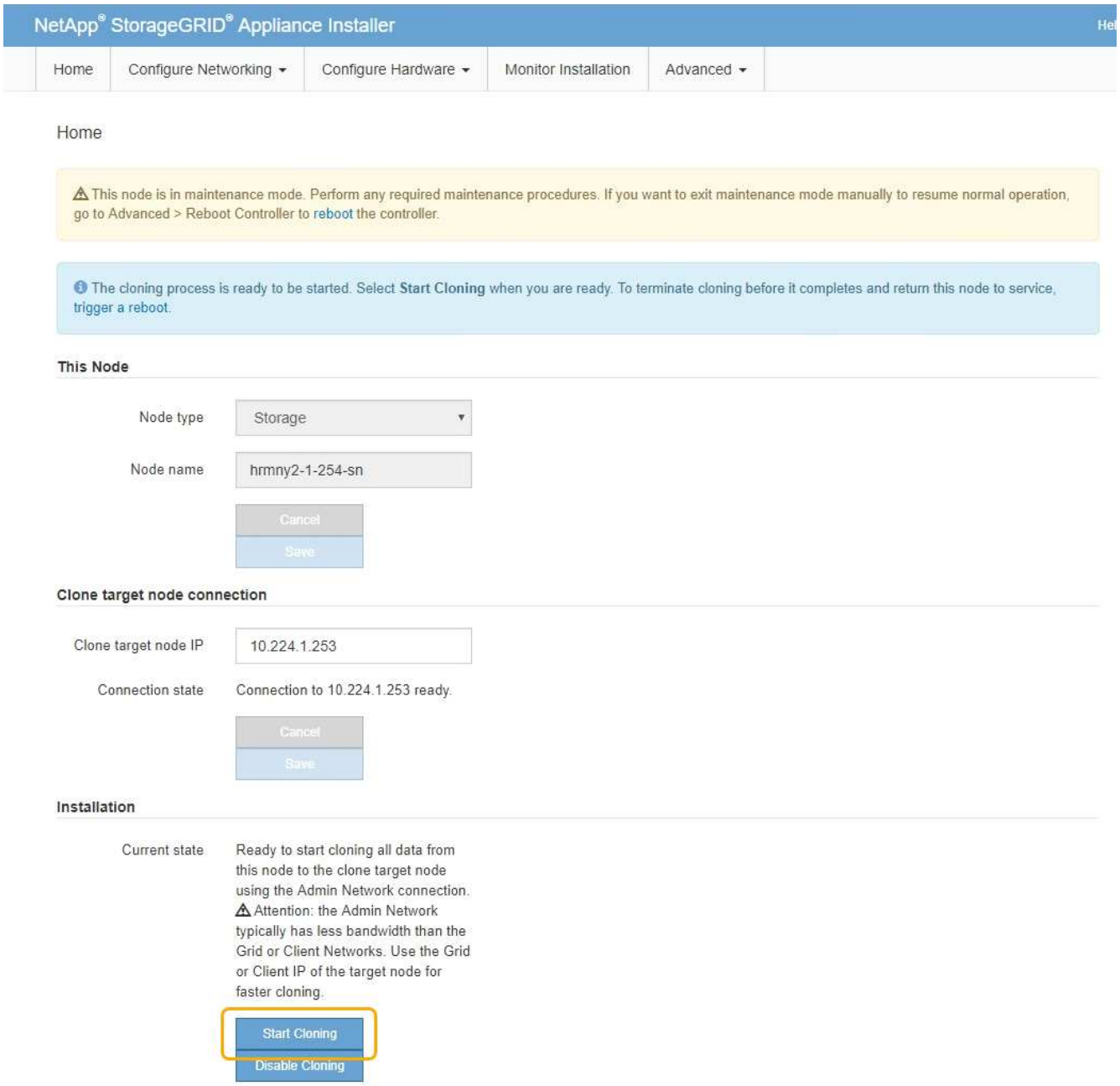


3. Per **Clone target node IP**, immettere l'indirizzo IP temporaneo assegnato al nodo di destinazione per la rete da utilizzare per il traffico di trasferimento dati clone, quindi selezionare **Save** (Salva).

   In genere, si inserisce l'indirizzo IP per Grid Network, ma se si desidera utilizzare una rete diversa per il traffico di trasferimento dati clone, immettere l'indirizzo IP del nodo di destinazione su tale rete.

   > L'utilizzo della rete di amministrazione 1-GbE per il trasferimento dei dati dei cloni comporta un rallentamento della clonazione.

   Dopo aver configurato e validato l'appliance di destinazione, nella sezione Installazione, sul nodo di origine viene attivato **Avvia clonazione**.



Se si verificano problemi che impediscono la clonazione, **Avvia clonazione** non è abilitato e i problemi da risolvere vengono elencati come **Stato connessione**. Questi problemi sono elencati nella home page del programma di installazione dell'appliance StorageGRID del nodo di origine e dell'appliance di destinazione. Viene visualizzato un solo problema alla volta e lo stato si aggiorna automaticamente quando cambiano le condizioni. Risolvi tutti i problemi di clonazione per attivare **Avvia clonazione**.

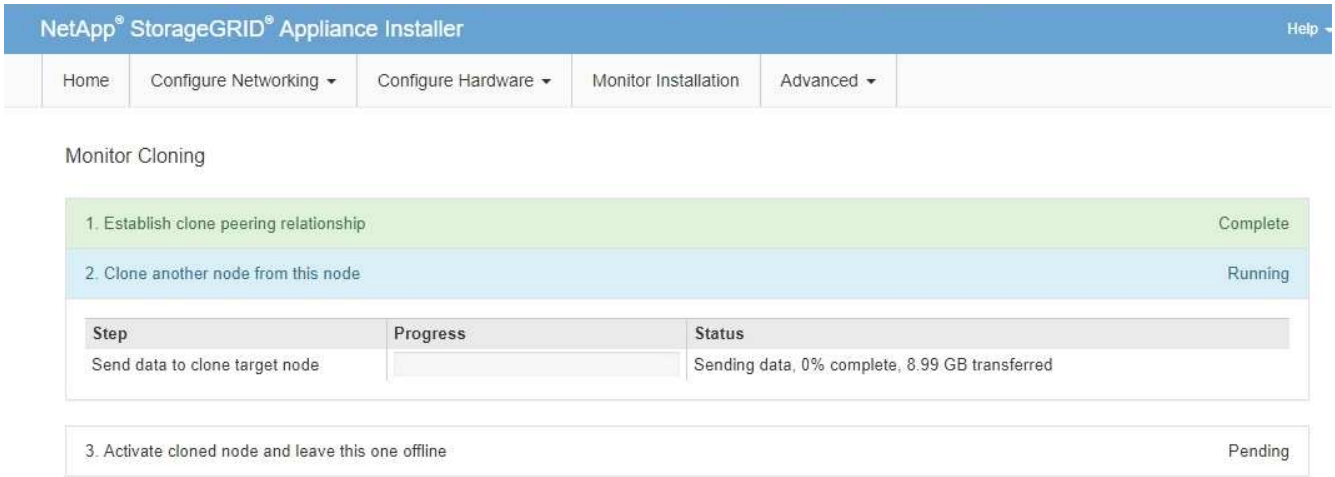
Quando l'opzione **Avvia clonazione** è attivata, lo stato **corrente** indica la rete StorageGRID selezionata per la clonazione del traffico, insieme alle informazioni sull'utilizzo della connessione di rete.

Considerazioni e requisiti per la clonazione del nodo dell'appliance

4. Selezionare **Avvia clonazione** sul nodo di origine.
5. Monitorare l'avanzamento della clonazione utilizzando il programma di installazione dell'appliance StorageGRID sul nodo di origine o di destinazione.

   Il programma di installazione dell'appliance StorageGRID sui nodi di origine e di destinazione indica lo

stesso stato.



La pagina Monitor Cloning fornisce informazioni dettagliate sui progressi di ciascuna fase del processo di cloning:

- **Stabilire una relazione di peering dei cloni** mostra l'avanzamento dell'impostazione e della configurazione della clonazione.
- **Clone another node from this node** (Clona un altro nodo da questo nodo) mostra lo stato di avanzamento del trasferimento dei dati. (Questa parte del processo di cloning può richiedere diversi giorni).
- **Attivare il nodo clonato e lasciarlo offline** indica l'avanzamento del trasferimento del controllo al nodo di destinazione e il posizionamento del nodo di origine in uno stato pre-installazione, una volta completato il trasferimento dei dati.

6. Se è necessario terminare il processo di cloning e ripristinare il nodo di origine prima del completamento della clonazione, sul nodo di origine accedere alla home page del programma di installazione dell'appliance StorageGRID e selezionare **Avanzate Riavvia controller**, quindi selezionare **Riavvia in StorageGRID**.

   Se il processo di cloning viene terminato:

   - Il nodo di origine esce dalla modalità di manutenzione e si ricongiunge a StorageGRID.
   - Il nodo di destinazione rimane in stato pre-installazione. Per riavviare la clonazione del nodo di origine, riavviare il processo di clonazione dal passaggio 1.

Al termine della clonazione:

- I nodi di origine e di destinazione scambiano gli indirizzi IP:
  - Il nodo di destinazione ora utilizza gli indirizzi IP originariamente assegnati al nodo di origine per le reti Grid, Admin e Client.
  - Il nodo di origine ora utilizza l'indirizzo IP temporaneo inizialmente assegnato al nodo di destinazione.
- Il nodo di destinazione esce dalla modalità di manutenzione e si unisce a StorageGRID, sostituendo il nodo di origine.
- L'appliance di origine si trova in uno stato preinstallato, come se fosse già stato installato preparato per la reinstallazione.

> Se l'appliance non si riconnette alla griglia, accedere alla home page del programma di installazione dell'appliance StorageGRID relativa al nodo di origine, selezionare **Avanzate Riavvia controller**, quindi selezionare **Riavvia in modalità manutenzione**. Dopo il riavvio del nodo di origine in modalità di manutenzione, ripetere la procedura di cloning del nodo.

I dati dell'utente rimangono sull'appliance di origine come opzione di ripristino se si verifica un problema imprevisto con il nodo di destinazione. Una volta che il nodo di destinazione ha raggiunto StorageGRID, i dati dell'utente sull'appliance di origine sono obsoleti e non sono più necessari. Se lo si desidera, chiedere al supporto StorageGRID di cancellare l'appliance di origine per distruggere questi dati.

È possibile:

- Utilizzare l'appliance di origine come destinazione per ulteriori operazioni di cloning: Non è richiesta alcuna configurazione aggiuntiva. A questo dispositivo è già stato assegnato l'indirizzo IP temporaneo specificato originariamente per la destinazione del primo clone.
- Installare e configurare l'appliance di origine come nuovo nodo dell'appliance.
- Smaltire l'apparecchio di origine se non viene più utilizzato con StorageGRID.

Esaminare i registri di audit

Esaminare i registri di audit: Panoramica

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di audit e dei registri di audit di StorageGRID. È possibile utilizzare queste informazioni per leggere e analizzare il registro di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli amministratori responsabili della produzione di report sull'attività e sull'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID.

Per utilizzare il file di log di testo, è necessario disporre dell'accesso alla condivisione di audit configurata nel nodo di amministrazione.

Per informazioni sulla configurazione dei livelli dei messaggi di controllo e sull'utilizzo di un server syslog esterno, vedere Configurare i messaggi di audit e le destinazioni dei log.

Informazioni correlate

- Amministrare StorageGRID

Controllare il flusso e la conservazione dei messaggi

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. È necessario comprendere in che modo questi messaggi di audit vengono spostati nel sistema StorageGRID `audit.log` file.

Controllare il flusso dei messaggi

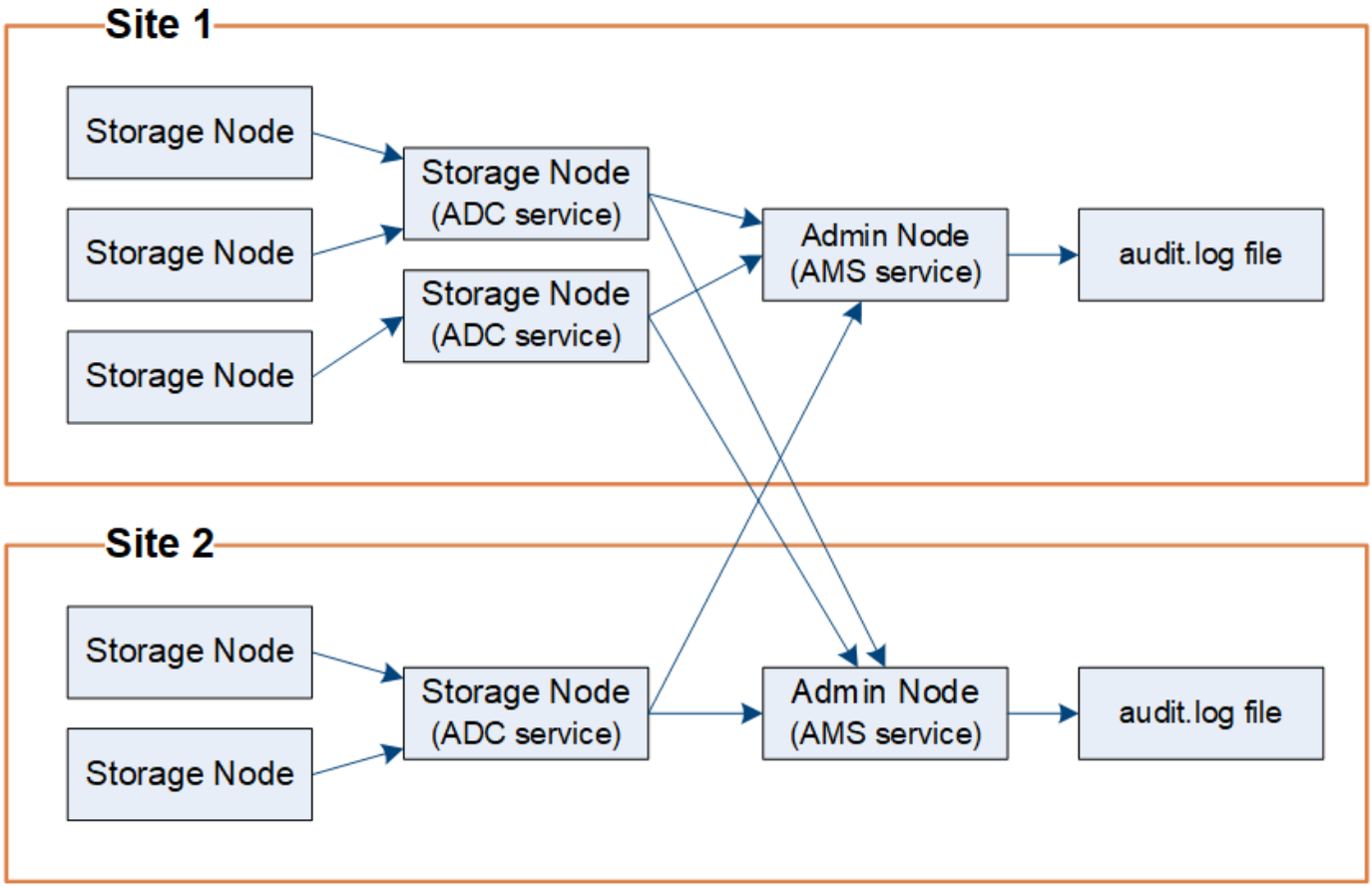
I messaggi di audit vengono elaborati dai nodi di amministrazione e dai nodi di storage che dispongono di un servizio ADC (Administrative Domain Controller).

Come mostrato nel diagramma di flusso dei messaggi di audit, ciascun nodo StorageGRID invia i propri messaggi di audit a uno dei servizi ADC nel sito del data center. Il servizio ADC viene attivato

automaticamente per i primi tre nodi di storage installati in ogni sito.

A sua volta, ogni servizio ADC agisce come un relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID, che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

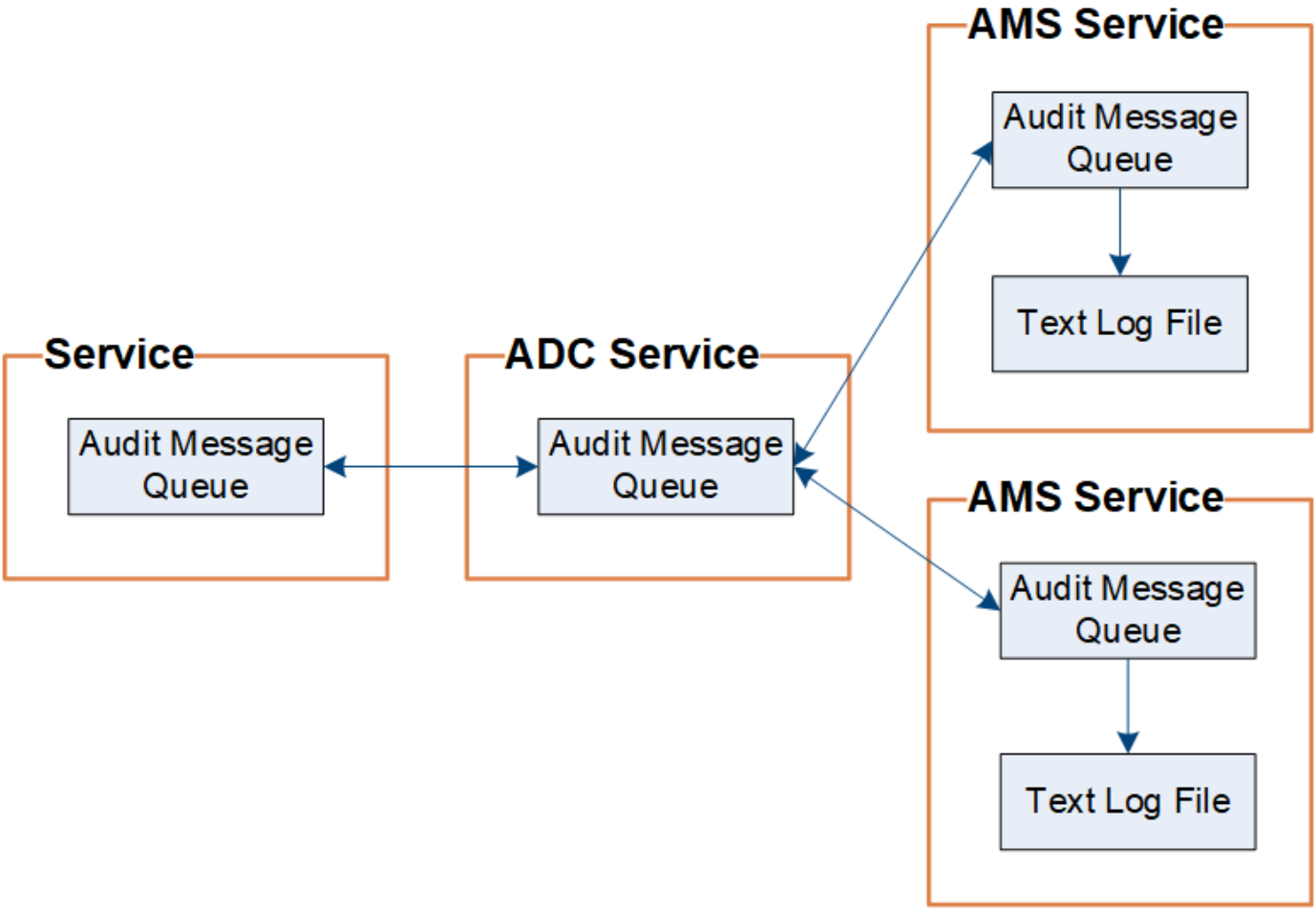
Ogni nodo amministrativo memorizza i messaggi di audit in file di log di testo; il file di log attivo viene denominato `audit.log`.



Controllare la conservazione dei messaggi

StorageGRID utilizza un processo di copia e cancellazione per garantire che non vengano persi messaggi di controllo prima di poter essere scritti nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di audit, il messaggio viene memorizzato in una coda di messaggi di audit sul disco di sistema del nodo Grid. Una copia del messaggio viene sempre mantenuta in una coda di messaggi di audit fino a quando il messaggio non viene scritto nel file di log di audit nel nodo di amministrazione `/var/local/audit/export` directory. In questo modo si evita la perdita di un messaggio di audit durante il trasporto.



La coda dei messaggi di audit può aumentare temporaneamente a causa di problemi di connettività di rete o di capacità di audit insufficiente. Man mano che le code aumentano, consumano più spazio disponibile in ogni nodo `/var/local/` directory. Se il problema persiste e la directory dei messaggi di controllo di un nodo diventa troppo piena, i singoli nodi assegneranno la priorità all'elaborazione del proprio backlog e diventeranno temporaneamente non disponibili per i nuovi messaggi.

In particolare, potrebbero verificarsi i seguenti comportamenti:

- Se il `/var/local/audit/export` La directory utilizzata da un nodo amministratore diventa piena, il nodo amministratore viene contrassegnato come non disponibile per i nuovi messaggi di audit fino a quando la directory non è più piena. Le richieste dei client S3 e Swift non sono interessate. L'allarme XAMS (Unreachable Audit Repository) viene attivato quando un repository di audit non è raggiungibile.
- Se il `/var/local/` La directory utilizzata da un nodo di storage con il servizio ADC diventa piena al 92%, il nodo viene contrassegnato come non disponibile per i messaggi di controllo fino a quando la directory non è piena al 87%. Le richieste dei client S3 e Swift ad altri nodi non sono interessate. L'allarme NRLY (Available Audit Relay) viene attivato quando i relè di audit non sono raggiungibili.

  > Se non sono disponibili nodi di storage con il servizio ADC, i nodi di storage memorizzano i messaggi di audit in locale in `/var/local/log/localaudit.log` file.

- Se il `/var/local/` La directory utilizzata da un nodo di storage diventa piena al 85%, il nodo inizia a rifiutare le richieste dei client S3 e Swift con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare un aumento delle code dei messaggi di audit:

- Interruzione di un nodo amministrativo o di un nodo di storage con il servizio ADC. Se uno dei nodi del sistema non è attivo, i nodi rimanenti potrebbero diventare backlogged.
- Tasso di attività sostenuta che supera la capacità di audit del sistema.
- Il `/var/local/` Lo spazio su un nodo di storage ADC diventa pieno per motivi non correlati ai messaggi di audit. In questo caso, il nodo smette di accettare nuovi messaggi di audit e assegna la priorità al backlog corrente, che può causare backlog su altri nodi.

Avviso di coda di audit estesa e allarme di messaggi di audit in coda (AMQS)

Per facilitare il monitoraggio delle dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Large audit queue** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda Storage Node o Admin Node raggiunge determinate soglie.

Se viene attivato l'avviso **Large audit queue** o l'allarme AMQS legacy, iniziare controllando il carico sul sistema. Se si è verificato un numero significativo di transazioni recenti, l'avviso e l'allarme devono essere risolti nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di severità, visualizzare un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, il carico di audit ha probabilmente superato la capacità di audit del sistema. Ridurre la velocità di funzionamento del client o diminuire il numero di messaggi di audit registrati modificando il livello di audit per le scritture del client e le letture del client su Error (errore) o Off. Vedere "Configurare i messaggi di audit e le destinazioni dei log."

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto di rete o nodo. Per questo motivo, nel registro di controllo potrebbero essere presenti messaggi duplicati.

Accedere al file di log di audit

La condivisione di audit contiene il attivo `audit.log` file ed eventuali file di log di audit compressi. Per un facile accesso ai log di audit, è possibile configurare l'accesso client per le condivisioni di audit per NFS e CIFS (CIFS è obsoleto). È inoltre possibile accedere ai file di log di audit direttamente dalla riga di comando del nodo di amministrazione.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
2. Accedere alla directory contenente i file di log di controllo:

```
cd /var/local/audit/export
```

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

Informazioni correlate

Amministrare StorageGRID

Controllo della rotazione del file di log

I file di log di audit vengono salvati in un nodo di amministrazione `/var/local/audit/export` directory. I file di log di audit attivi sono denominati `audit.log`.

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

Una volta al giorno, il attivo `audit.log` il file viene salvato e viene visualizzato un nuovo `audit.log` il file viene avviato. Il nome del file salvato indica quando è stato salvato, nel formato *`yyyy-mm-dd.txt`*. Se in un singolo giorno vengono creati più log di audit, i nomi dei file utilizzano la data in cui il file è stato salvato, aggiunto da un numero, nel formato *`yyyy-mm-dd.txt.n`*. Ad esempio, `2018-04-15.txt` e. `2018-04-15.txt.1` Sono il primo e il secondo file di log creati e salvati il 15 aprile 2018.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato *`yyyy-mm-dd.txt.gz`*, che conserva la data originale. Con il passare del tempo, ciò comporta un consumo di storage allocato per i registri di controllo sul nodo di amministrazione. Uno script monitora il consumo di spazio nel registro di controllo ed elimina i file di registro in base alle necessità per liberare spazio in `/var/local/audit/export` directory. I registri di audit vengono cancellati in base alla data di creazione, con la data in cui sono stati cancellati per prima. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

In questo esempio viene visualizzato il valore attivo `audit.log` file del giorno precedente (`2018-04-15.txt`) e il file compresso per il giorno precedente (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

File di log di audit e formati dei messaggi

È possibile utilizzare i registri di controllo per raccogliere informazioni sul sistema e risolvere i problemi. È necessario conoscere il formato del file di log di audit e il formato generale utilizzato per i messaggi di audit.

Formato del file di log di audit

I file di log di audit si trovano in ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di audit.

Ogni messaggio di audit contiene quanto segue:

- Il tempo universale coordinato (UTC) dell'evento che ha attivato il messaggio di audit (ATIM) in formato ISO 8601, seguito da uno spazio:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, dove *UUUUUU* sono microsecondi.

- Il messaggio di audit, racchiuso tra parentesi quadre e che inizia con `AUDT`.

L'esempio seguente mostra tre messaggi di audit in un file di log di audit (interruzioni di riga aggiunte per la leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e aggiunto due oggetti a tale bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Nel loro formato predefinito, i messaggi di audit nei file di log di audit non sono facili da leggere o interpretare. È possibile utilizzare `audit-explain` tool per ottenere riepiloghi semplificati dei messaggi di audit nel log di audit. È possibile utilizzare `audit-sum` tool per riepilogare il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.

Informazioni correlate

Utilizzare lo strumento di verifica e spiegazione

Utilizzare lo strumento audit-sum

È possibile utilizzare `audit-explain` strumento per tradurre i messaggi di audit nel log di audit in un formato di facile lettura.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

Il `audit-explain` Tool, disponibile nel nodo di amministrazione principale, fornisce riepiloghi semplificati dei messaggi di audit in un registro di audit.

> Il `audit-explain` lo strumento è destinato principalmente all'utilizzo da parte del supporto tecnico durante le operazioni di troubleshooting. Elaborazione in corso `audit-explain` Le query possono consumare una grande quantità di potenza della CPU, con un conseguente impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico di `audit-explain` tool. Questi quattro messaggi di audit SPUT sono stati generati quando il tenant S3 con ID account 92484777680322627870 utilizzava S3 PUT Requests per creare un bucket denominato "bucket1" e aggiungere tre oggetti a quel bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Il `audit-explain` può elaborare registri di audit semplici o compressi. Ad esempio:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

Il `audit-explain` può anche elaborare più file contemporaneamente. Ad esempio:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Infine, il `audit-explain` lo strumento può accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando `grep` comando o altro mezzo. Ad esempio:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Poiché i log di audit possono essere molto grandi e lenti da analizzare, è possibile risparmiare tempo filtrando le parti che si desidera esaminare ed eseguire `audit-explain` sulle parti, invece dell'intero file.

> Il `audit-explain` lo strumento non accetta i file compressi come input di tipo pipped. Per elaborare i file compressi, specificare i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` per decomprimere prima i file. Ad esempio:

```
zcat audit.log.gz | audit-explain
```

Utilizzare `help (-h)` per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-explain -h
```

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
2. Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   Il `audit-explain` consente di stampare interpretazioni leggibili di tutti i messaggi contenuti nel file o nei file specificati.

   > Per ridurre le lunghezze delle linee e agevolare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se si desidera visualizzare gli indicatori di data e ora, utilizzare l'indicatore di data e ora (`-t`).

Informazioni correlate

SPUT: S3 PUT

Utilizzare lo strumento audit-sum

È possibile utilizzare `audit-sum` strumento per contare i messaggi di audit di scrittura,

lettura, testa ed eliminazione e per visualizzare il tempo (o la dimensione) minimo, massimo e medio per ciascun tipo di operazione.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

Il `audit-sum` Tool, disponibile sul nodo di amministrazione primario, riepiloga il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.

> Il `audit-sum` lo strumento è destinato principalmente all'utilizzo da parte del supporto tecnico durante le operazioni di troubleshooting. Elaborazione in corso `audit-sum` Le query possono consumare una grande quantità di potenza della CPU, con un conseguente impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico di `audit-sum` tool. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                    213371        0.004          20.934
0.352
  SGET                    201906        0.010        1740.290
1.132
  SHEA                     22716        0.005           2.349
0.272
  SPUT                  1771398        0.011        1770.563
0.487
```

Il `audit-sum` Lo strumento fornisce conteggi e tempi per i seguenti messaggi di audit S3, Swift e ILM in un registro di audit:

Codice	Descrizione	Fare riferimento a.
ARCT	Recupero archivio da Cloud-Tier	ARCT: Recupero archivio da Cloud-Tier
ASTT	Archivio Store Cloud-Tier	ASCT: Archivio Store Cloud-Tier
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Registra quando ILM avvia il processo di eliminazione di un oggetto.	IDEL: Eliminazione avviata da ILM

Codice	Descrizione	Fare riferimento a.
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket.	SDEL: ELIMINAZIONE S3
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	SGET: S3 GET
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	SHEA: TESTA S3
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	SPUT: S3 PUT
WDEL	Eliminazione rapida: Registra una transazione riuscita per eliminare un oggetto o un container.	WDEL: ELIMINAZIONE rapida
WGET	Swift GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un container.	WGET: Swift GET
WHEA	Swift HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un container.	WHEA: TESTA veloce
WPUT	Swift PUT: Registra una transazione riuscita per creare un nuovo oggetto o container.	WPUT: MESSA rapida

Il `audit-sum` può elaborare registri di audit semplici o compressi. Ad esempio:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

Il `audit-sum` può anche elaborare più file contemporaneamente. Ad esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Infine, il `audit-sum` lo strumento può anche accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando `grep` comando o altro mezzo. Ad esempio:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

> Questo strumento non accetta i file compressi come input di tipo pipped. Per elaborare i file compressi, specificare i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` per decomprimere prima i file. Ad esempio:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

È possibile utilizzare le opzioni della riga di comando per riepilogare le operazioni sui bucket separatamente dalle operazioni sugli oggetti o per raggruppare i riepiloghi dei messaggi in base al nome del bucket, al periodo di tempo o al tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di funzionamento minimo, massimo e medio, ma è possibile utilizzare `size (-s)` opzione per esaminare invece la dimensione dell'oggetto.

Utilizzare `help (-h)` per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-sum -h
```

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, testa ed eliminazione, attenersi alla seguente procedura:
   a. Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

Questo esempio mostra l'output tipico di `audit-sum` tool. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                    213371        0.004          20.934
0.352
  SGET                    201906        0.010        1740.290
1.132
  SHEA                     22716        0.005           2.349
0.272
  SPUT                   1771398        0.011        1770.563
0.487
```

In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media a 1.13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano tempi lunghi nel caso peggiore di circa 1,770 secondi.

b. Per visualizzare le 10 operazioni di recupero più lente, utilizzare il comando grep per selezionare solo i messaggi SGET e aggiungere l'opzione di output lungo (`-l`) per includere i percorsi degli oggetti: `grep SGET audit.log | audit-sum -l`

   I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di eseguire il grep del log di audit per altri messaggi relativi a questi oggetti specifici.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+ Da questo esempio di output, è possibile notare che le tre richieste S3 GET più lente erano per oggetti di dimensioni pari a circa 5 GB, che sono molto più grandi degli altri oggetti. Le grandi dimensioni rappresentano i tempi di recupero lenti dei casi peggiori.

3. Se si desidera determinare le dimensioni degli oggetti da acquisire e recuperare dalla griglia, utilizzare l'opzione size (dimensione) (`-s`):

```
audit-sum -s audit.log
```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

In questo esempio, la dimensione media degli oggetti per SPUT è inferiore a 2.5 MB, ma la dimensione media per SGET è molto maggiore. Il numero di messaggi SPUT è molto superiore al numero di messaggi SGET, a indicare che la maggior parte degli oggetti non viene mai recuperata.

4. Se si desidera determinare se i recuperi sono stati lenti ieri:

   a. Eseguire il comando sul registro di controllo appropriato e utilizzare l'opzione group-by-time (`-gt`), seguito dal periodo di tempo (ad esempio, 15M, 1H, 10S):

   ```
   grep SGET audit.log | audit-sum -gt 1H
   ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Questi risultati mostrano che S3 OTTIENE un incremento del traffico tra le 06:00 e le 07:00. Anche in questi casi, i tempi massimi e medi sono notevolmente più elevati e non sono aumentati gradualmente con l'aumentare del numero. Ciò suggerisce che la capacità è stata superata da qualche parte, ad esempio nella rete o nella capacità della rete di elaborare le richieste.

b. Per determinare le dimensioni degli oggetti recuperati ogni ora di ieri, aggiungere l'opzione size (dimensione) (`-s`) al comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Questi risultati indicano che si sono verificati alcuni recuperi molto grandi quando il traffico di recupero complessivo era al massimo.

c. Per ulteriori dettagli, utilizzare `audit-explain` Tool per esaminare tutte le operazioni SGET durante quell'ora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se si prevede che l'output del comando grep sia costituito da molte righe, aggiungere `less` comando per visualizzare il contenuto del file di log di audit una pagina (una schermata) alla volta.

5. Se si desidera determinare se le operazioni SPUT sui bucket sono più lente delle operazioni SPUT per gli oggetti:

a. Iniziare utilizzando `-go` opzione, che raggruppa i messaggi per le operazioni a oggetti e a bucket separatamente:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

I risultati mostrano che le operazioni SPUT per i bucket hanno caratteristiche di performance diverse rispetto alle operazioni SPUT per gli oggetti.

b. Per determinare quali bucket hanno le operazioni SPUT più lente, utilizzare `-gb` opzione, che raggruppa i messaggi per bucket:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Per determinare quali bucket hanno la dimensione maggiore dell'oggetto SPUT, utilizzare entrambi i campi `-gb` e a. `-s` opzioni:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Informazioni correlate

Utilizzare lo strumento di verifica e spiegazione

Formato del messaggio di audit

I messaggi di audit scambiati all'interno del sistema StorageGRID includono informazioni standard comuni a tutti i messaggi e contenuti specifici che descrivono l'evento o l'attività da segnalare.

Se le informazioni di riepilogo fornite da `audit-explain` e. `audit-sum` gli strumenti non sono sufficienti. fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di audit.

Di seguito viene riportato un esempio di messaggio di audit che potrebbe essere visualizzato nel file di log dell'audit:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Ogni messaggio di audit contiene una stringa di elementi di attributo. L'intera stringa è racchiusa tra parentesi (`[ ]`), e ogni elemento di attributo nella stringa ha le seguenti caratteristiche:

- Racchiuso tra parentesi `[ ]`
- Introdotto dalla stringa `AUDT`, che indica un messaggio di audit
- Senza delimitatori (senza virgole o spazi) prima o dopo
- Terminato da un carattere di avanzamento riga `\n`

Ogni elemento include un codice di attributo, un tipo di dati e un valore che vengono riportati in questo formato:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Il numero di elementi di attributo nel messaggio dipende dal tipo di evento del messaggio. Gli elementi dell'attributo non sono elencati in un ordine specifico.

L'elenco seguente descrive gli elementi degli attributi:

- `ATTR` è un codice di quattro caratteri per l'attributo da segnalare. Esistono alcuni attributi comuni a tutti i messaggi di audit e ad altri specifici degli eventi.
- `type` È un identificatore di quattro caratteri del tipo di dati di programmazione del valore, ad esempio UI64, FC32 e così via. Il tipo è racchiuso tra parentesi `( )`.
- `value` è il contenuto dell'attributo, in genere un valore numerico o di testo. I valori seguono sempre i due punti (`:`). I valori del tipo di dati CSTR sono racchiuse tra virgolette doppie `" "`.

Informazioni correlate

Utilizzare lo strumento di verifica e spiegazione

Utilizzare lo strumento audit-sum

Messaggi di audit

Elementi comuni nei messaggi di audit

Tipi di dati

Esempi di messaggi di audit

Tipi di dati

Per memorizzare le informazioni nei messaggi di audit vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero senza segno (32 bit); può memorizzare i numeri da 0 a 4,294,967,295.
UI64	Numero intero doppio senza segno (64 bit); può memorizzare i numeri da 0 a 18,446,744,073,709,551,615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32-bit rappresentato da quattro caratteri ASCII, ad esempio "ABCD".
IPAD	Utilizzato per gli indirizzi IP.

Tipo	Descrizione
CSTR	Matrice a lunghezza variabile di UTF-8 caratteri. È possibile eseguire l'escape dei caratteri con le seguenti convenzioni: • La barra rovesciata è • Il ritorno a capo è • Le virgolette doppie sono ". • L'avanzamento riga (nuova riga) è il n. • I caratteri possono essere sostituiti dai rispettivi equivalenti esadecimali (nel formato HH, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento

Ogni messaggio di audit nel registro di audit registra i dati specifici di un evento di sistema.

Dopo l'apertura `[AUDT:` container che identifica il messaggio stesso, il successivo set di attributi fornisce informazioni sull'evento o sull'azione descritti dal messaggio di audit. Questi attributi sono evidenziati nel seguente esempio:

```
2018-12-05T08:24:45.921845 [AUDT:*[RSLT:"60025621595611246499"] *[TIME(UI64):11454][SAIP](IPAD
BUCKET):"10.224.0 60025621595611246499.100 60025621595611246499"]
*[S3AI(CSTGSTR):[S3CSTGSTR] *[S3CSTGK]: *[S3CSTGSTGSTR] *[S3CSTGSTR]:
*[S3CSTGSTGSTGSTGSTR]: *[S3GSTGSTGSTGSTR]: *[S3GSTGSTGSTGSTR] *] *[S3K]:
*[S3CSTGSTGSTGSTGSTGSTGSTGSTGSTGSTR]: *[S3K] *: * *: * *: * * *: * *
S3CSTGSTGSTGSTGSTGSTGSTGSTGSTGSTGSTGSTGSTGSTGSTGSTGSTG 15552417629170647261
12281045 1543998285921845 10 30720
```

Il `ATYP` element (sottolineato nell'esempio) identifica l'evento che ha generato il messaggio. Questo messaggio di esempio include il codice del messaggio SHEA ([ATYP(FC32):SHEA]), che indica che è stato generato da una richiesta S3 HEAD riuscita.

Informazioni correlate

Elementi comuni nei messaggi di audit

Messaggi di audit

Elementi comuni nei messaggi di audit

Tutti i messaggi di audit contengono gli elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	Module ID (ID modulo): Identificatore di quattro-caratteri dell'ID modulo che ha generato il messaggio. Indica il segmento di codice all'interno del quale è stato generato il messaggio di audit.
ANID	UI32	Node ID (ID nodo): L'ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID. Questo ID non può essere modificato.
ASE	UI64	Audit Session Identifier (identificatore sessione di audit): Nelle release precedenti, questo elemento indica l'ora in cui il sistema di audit è stato inizializzato dopo l'avvio del servizio. Questo valore di tempo è stato misurato in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). **Nota:** questo elemento è obsoleto e non compare più nei messaggi di audit.
ASQN	UI64	Sequence Count (Conteggio sequenze): Nelle release precedenti, questo contatore è stato incrementato per ogni messaggio di audit generato sul nodo della griglia (ANID) e azzerato al riavvio del servizio. **Nota:** questo elemento è obsoleto e non compare più nei messaggi di audit.
ATID	UI64	Trace ID (ID traccia): Identificatore condiviso dalla serie di messaggi attivati da un singolo evento.
ATIM	UI64	Timestamp: L'ora in cui è stato generato l'evento che ha attivato il messaggio di audit, misurata in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per la conversione dell'indicatore data e ora in data e ora locali si basano su millisecondi. Potrebbe essere richiesto l'arrotondamento o il troncamento dell'indicatore data e ora registrato. Il tempo di lettura-umano visualizzato all'inizio del messaggio di audit in `audit.log` File è l'attributo ATIM nel formato ISO 8601. La data e l'ora sono rappresentate come *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, dove il `T` è un carattere di stringa letterale che indica l'inizio del segmento temporale della data. *`UUUUUU`* sono microsecondi.
ATYP	FC32	Event Type (tipo di evento): Identificatore di quattro-caratteri dell'evento registrato. Questo regola il contenuto "payload" del messaggio: Gli attributi che sono inclusi.
MEDIA	UI32	Version (versione): La versione del messaggio di audit. Man mano che il software StorageGRID si evolve, le nuove versioni dei servizi potrebbero incorporare nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti del servizio AMS per l'elaborazione dei messaggi provenienti da versioni precedenti dei servizi.

Codice	Tipo	Descrizione
RSLT	FC32	Risultato: Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

Esempi di messaggi di audit

È possibile trovare informazioni dettagliate in ciascun messaggio di audit. Tutti i messaggi di audit utilizzano lo stesso formato.

Di seguito viene riportato un esempio di messaggio di audit come potrebbe essere visualizzato in `audit.log` file:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Il messaggio di audit contiene informazioni sull'evento registrato, nonché informazioni sul messaggio di audit stesso.

Per identificare l'evento registrato dal messaggio di audit, cercare l'attributo ATYP (evidenziato di seguito):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP\(FC32\):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Il valore dell'attributo ATYP è SPUT. SPUT rappresenta una transazione S3 PUT, che registra l'acquisizione di un oggetto in un bucket.

Il seguente messaggio di audit mostra anche il bucket a cui è associato l'oggetto:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Per scoprire quando si è verificato l'evento PUT, prendere nota dell'indicatore orario UTC (Universal Coordinated Time) all'inizio del messaggio di audit. Questo valore è una versione leggibile-umana dell'attributo ATIM del messaggio di audit stesso:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM registra il tempo, in microsecondi, dall'inizio dell'epoca UNIX. Nell'esempio, il valore `1405631878959669` Tradotto a Giovedì, 17-lug-2014 21:17:59 UTC.

Informazioni correlate

SPUT: S3 PUT

Elementi comuni nei messaggi di audit

Messaggi di audit e ciclo di vita degli oggetti

I messaggi di audit vengono generati ogni volta che un oggetto viene acquisito, recuperato o eliminato. È possibile identificare queste transazioni nel registro di controllo individuando i messaggi di audit specifici dell'API (S3 o Swift).

I messaggi di audit sono collegati tramite identificatori specifici di ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (S3 bucket) e/o S3KY (S3 Key)
Collegamento delle operazioni Swift	WCON (Swift container) e/o WOBJ (Swift Object)
Collegamento delle operazioni interne	CBID (identificativo interno dell'oggetto)

Tempistiche dei messaggi di audit

A causa di fattori come le differenze di tempo tra i nodi della griglia, le dimensioni degli oggetti e i ritardi di rete, l'ordine dei messaggi di controllo generati dai diversi servizi può variare rispetto a quello mostrato negli esempi di questa sezione.

Configurazione delle policy per la gestione del ciclo di vita delle informazioni

Con il criterio ILM predefinito (copia Baseline 2), i dati dell'oggetto vengono copiati una volta per un totale di due copie. Se la policy ILM richiede più di due copie, sarà disponibile un set aggiuntivo di messaggi CBRE, CBSE e SCMT per ogni copia extra. Per ulteriori informazioni sui criteri ILM, vedere informazioni sulla gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Nodi di archiviazione

La serie di messaggi di audit generati quando un nodo di archiviazione invia dati a oggetti a un sistema di storage di archiviazione esterno è simile a quella dei nodi di storage, ad eccezione del fatto che non esiste alcun messaggio SCMT (Store Object Commit), Inoltre, vengono generati i messaggi ATCE (Archive Object Store Begin) e ASCE (Archive Object Store End) per ogni copia archiviata dei dati dell'oggetto.

La serie di messaggi di controllo generati quando un nodo di archiviazione recupera i dati degli oggetti da un sistema di storage di archiviazione esterno è simile a quella dei nodi di storage, ad eccezione del fatto che i messaggi ARCB (Archive Object Retrieve Begin) e ARCE (Archive Object Retrieve End) vengono generati per ogni copia recuperata dei dati degli oggetti.

La serie di messaggi di controllo generati quando un nodo di archiviazione elimina i dati degli oggetti da un sistema di storage di archiviazione esterno è simile a quella dei nodi di storage, ad eccezione del fatto che non è presente alcun messaggio SREM (Object Store Remove) e che è presente un messaggio AREM (Archive Object Remove) per ogni richiesta di eliminazione.

Informazioni correlate

Gestire gli oggetti con ILM

Transazioni di acquisizione degli oggetti

È possibile identificare le transazioni di acquisizione dei client nel registro di audit individuando i messaggi di audit specifici dell'API (S3 o Swift).

Non tutti i messaggi di audit generati durante una transazione di acquisizione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

S3: Acquisizione di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione S3 PUT ingest è stata completata correttamente.	CBID, S3BK, S3KY	SPUT: S3 PUT
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	ORLM: Regole oggetto soddisfatte

Acquisizione rapida di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
WPUT	Transazione SWIFT PUT	Una transazione Swift PUT Ingest è stata completata correttamente.	CBID, WCON, WOBJ	WPUT: MESSA rapida
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	ORLM: Regole oggetto soddisfatte

Esempio: Acquisizione di oggetti S3

La serie di messaggi di controllo riportata di seguito è un esempio dei messaggi di controllo generati e salvati nel registro di controllo quando un client S3 acquisisce un oggetto in un nodo di storage (servizio LDR).

In questo esempio, il criterio ILM attivo include la regola ILM di stock, eseguire 2 copie.

> Non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di acquisizione S3 (SPUT).

Questo esempio presuppone che sia stato precedentemente creato un bucket S3.

SPUT: S3 PUT

Il messaggio SPUT viene generato per indicare che è stata emessa una transazione S3 PUT per creare un oggetto in un bucket specifico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Regole oggetto soddisfatte

Il messaggio ORLM indica che il criterio ILM è stato soddisfatto per questo oggetto. Il messaggio include il CBID dell'oggetto e il nome della regola ILM applicata.

Per gli oggetti replicati, il campo LOCS include l'ID del nodo LDR e l'ID del volume delle posizioni degli oggetti.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Per gli oggetti con codifica erasure, il campo LOCS include l'ID del profilo Erasure coding e l'ID del gruppo Erasure coding

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Il campo PATH include informazioni sul bucket S3 e sulla chiave o informazioni sul container Swift e sull'oggetto, a seconda dell'API utilizzata.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Transazioni di eliminazione degli oggetti

È possibile identificare le transazioni di eliminazione degli oggetti nel registro di audit individuando i messaggi di audit specifici dell'API (S3 e Swift).

Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

S3 eliminare i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta di eliminazione dell'oggetto da un bucket.	CBID, S3KY	SDEL: ELIMINAZIONE S3

Eliminazione rapida dei messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
WDEL	Eliminazione rapida	Richiesta di eliminazione dell'oggetto da un container o dal container.	CBID, WOBJ	WDEL: ELIMINAZIONE rapida

Esempio: Eliminazione di oggetti S3

Quando un client S3 elimina un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.

> Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: S3 Elimina

L'eliminazione degli oggetti inizia quando il client invia una richiesta DI ELIMINAZIONE degli oggetti a un servizio LDR. Il messaggio contiene il bucket da cui eliminare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificare l'oggetto.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Transazioni di recupero degli oggetti

È possibile identificare le transazioni di recupero degli oggetti nel registro di audit individuando i messaggi di audit specifici dell'API (S3 e Swift).

Non tutti i messaggi di audit generati durante una transazione di recupero sono elencati nelle tabelle seguenti.

Sono inclusi solo i messaggi necessari per tracciare la transazione di recupero.

Messaggi di controllo per il recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta di recupero di un oggetto da un bucket.	CBID, S3BK, S3KY	SGET: S3 GET

Messaggi di audit per il recupero rapido

Codice	Nome	Descrizione	Traccia	Vedere
WGET	OTTENERE rapidamente	Richiesta di recupero di un oggetto da un container.	CBID, WCON, WOBJ	WGET: Swift GET

Esempio: Recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti inizia quando il client invia una richiesta GET Object a un servizio LDR. Il messaggio contiene il bucket da cui recuperare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificare l'oggetto.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se la policy bucket lo consente, un client può recuperare in modo anonimo oggetti o recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di audit contiene informazioni sull'account tenant del proprietario del bucket, in modo da poter tenere traccia di queste richieste anonime e multiaccount.

Nel seguente messaggio di esempio, il client invia una richiesta DI oggetto GET per un oggetto memorizzato in un bucket che non possiede. I valori di SBAI e SBAC registrano l'ID e il nome dell'account tenant del bucket Owner, che differiscono dall'ID dell'account tenant e dal nome del client registrati in S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Esempio: S3 selezionare su un oggetto

Quando un client S3 esegue una query S3 Select su un oggetto, i messaggi di audit vengono generati e salvati nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

Ogni query genera due messaggi di audit: Uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "Select") e un'operazione GET standard successiva che recupera i dati dallo storage durante l'elaborazione.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):13630097093968959 85]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messaggi di aggiornamento dei metadati

I messaggi di audit vengono generati quando un client S3 aggiorna i metadati di un oggetto.

I metadati S3 aggiornano i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati di un oggetto acquisito.	CBID, S3KY, HTRH	SUPD: Metadati S3 aggiornati

Esempio: Aggiornamento dei metadati S3

L'esempio mostra una transazione riuscita per aggiornare i metadati di un oggetto S3 esistente.

SUPD: Aggiornamento dei metadati S3

Il client S3 effettua una richiesta (SUPD) per aggiornare i metadati specificati (`x-amz-meta-\*`) Per l'oggetto S3 (S3KY). In questo esempio, le intestazioni delle richieste sono incluse nel campo HTRH perché è stato configurato come intestazione del protocollo di audit (**CONFIGURAZIONE** > **monitoraggio** > **server di audit e syslog**).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Informazioni correlate

Configurare i messaggi di audit e le destinazioni dei log

Messaggi di audit

Le descrizioni dettagliate dei messaggi di controllo restituiti dal sistema sono elencate nelle sezioni seguenti. Ciascun messaggio di audit viene elencato per primo in una tabella che raggruppa i messaggi correlati in base alla classe di attività rappresentata dal messaggio. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit che per selezionare il tipo di filtro dei messaggi di audit desiderato.

I messaggi di audit sono anche elencati in ordine alfabetico in base ai codici a quattro caratteri. Questo elenco alfabetico consente di trovare informazioni su messaggi specifici.

I codici a quattro caratteri utilizzati in questo capitolo sono i valori ATYP presenti nei messaggi di audit, come mostrato nel seguente messaggio di esempio:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Per informazioni sull'impostazione dei livelli dei messaggi di controllo, sulla modifica delle destinazioni dei log e sull'utilizzo di un server syslog esterno per le informazioni di controllo, vedere Configurare i messaggi di audit e

Controllare le categorie dei messaggi

È necessario conoscere le varie categorie all'interno delle quali sono raggruppati i messaggi di audit. Questi gruppi sono organizzati in base alla classe di attività rappresentata dal messaggio.

Messaggi di audit del sistema

Si consiglia di acquisire familiarità con i messaggi di audit appartenenti alla categoria di audit del sistema. Si tratta di eventi correlati al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema (attività della griglia) e alle operazioni di backup del servizio, in modo da poter risolvere potenziali problemi.

Codice	Titolo e descrizione del messaggio	Vedere
ECMC	Missing Erasure Coded Data Fragment (frammento di dati codificato con cancellazione mancante): Indica che è stato rilevato un frammento di dati codificato con cancellazione mancante.	ECMC: Frammento di dati codificato Erasure mancante
ECOC	Corrotto Erasure Coded Data Fragment: Indica che è stato rilevato un frammento di dati corrotto con codifica di cancellazione.	ECOC: Corrotto Erasure Coded Data Fragment
ETAF	Autenticazione di sicurezza non riuscita: Tentativo di connessione con Transport Layer Security (TLS) non riuscito.	ETAF: Autenticazione di sicurezza non riuscita
GNRG	Registrazione GNDS: Un servizio aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.	GNRG: Registrazione GNDS
NUR	Annullamento registrazione GNDS: Un servizio non si è registrato dal sistema StorageGRID.	GNUR: Annullamento registrazione GNDS
GTED	Grid Task Ended (attività griglia terminata): Il servizio CMN ha terminato l'elaborazione dell'attività Grid.	GTED: Task Grid terminato

Codice	Titolo e descrizione del messaggio	Vedere
GTST	Grid Task Started (attività griglia avviata): Il servizio CMN ha avviato l'elaborazione dell'attività Grid.	GTST: Task Grid avviato
GTSU	Grid Task Submitted (attività griglia inviata): È stata inviata un'attività Grid al servizio CMN.	GTSU: Task Grid inviato
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	IDEL: Eliminazione avviata da ILM
LKCU	Pulitura oggetto sovrascritto. Questo messaggio di audit viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di storage.	LKCU: Pulitura oggetto sovrascritta
LLST	Location Lost (posizione persa): Questo messaggio di audit viene generato quando una posizione viene persa.	LLST: Località persa
OLST	Object Lost (oggetti persi): Non è possibile individuare un oggetto richiesto all'interno del sistema StorageGRID.	OLST: Il sistema ha rilevato un oggetto perso
ORLM	Regole oggetto soddisfatte: I dati dell'oggetto vengono memorizzati come specificato dalle regole ILM.	ORLM: Regole oggetto soddisfatte
SADD	Security Audit Disable (Disattiva controllo protezione): La registrazione del messaggio di controllo è stata disattivata.	SADD: Disattivazione dell'audit di sicurezza
SADE	Security Audit Enable (attiva controllo di sicurezza): La registrazione del messaggio di controllo è stata ripristinata.	SADE: Abilitazione controllo di sicurezza

Codice	Titolo e descrizione del messaggio	Vedere
SVRF	Verifica archivio oggetti non riuscita: Un blocco di contenuto non ha superato i controlli di verifica.	SVRF: Verifica archivio oggetti non riuscita
SVRU	Object Store Verify Unknown (verifica archivio oggetti sconosciuto): Dati di oggetti imprevisti rilevati nell'archivio oggetti.	SVRU: Verifica archivio oggetti sconosciuta
SYSD	Node Stop (arresto nodo): È stato richiesto lo spegnimento.	SYSD: Interruzione nodo
SIST	Node stopping (interruzione nodo): Un servizio ha avviato un'interruzione senza interruzioni.	SYST: Interruzione del nodo
SISU	Node Start (Avvio nodo): Un servizio avviato; la natura dello shutdown precedente viene indicata nel messaggio.	SYSU: Avvio nodo
VLST	Volume avviato dall'utente perso: Il `/proc/CMSI/Volume_Lost` comando eseguito.	VLST: Perdita del volume avviata dall'utente

Informazioni correlate

LKCU: Pulitura oggetto sovrascritta

Messaggi di audit dello storage a oggetti

Si consiglia di acquisire familiarità con i messaggi di audit appartenenti alla categoria di audit dello storage a oggetti. Si tratta di eventi correlati allo storage e alla gestione di oggetti all'interno del sistema StorageGRID. Tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.

Codice	Descrizione	Vedere
APCT	Eliminazione dell'archivio dal livello cloud: I dati degli oggetti archiviati vengono cancellati da un sistema storage di archiviazione esterno, che si connette a StorageGRID tramite l'API S3.	APCT: Eliminazione dell'archivio dal Cloud-Tier

Codice	Descrizione	Vedere
ARCB	Archive Object Retrieve Begin (inizio recupero oggetto archivio): Il servizio ARC avvia il recupero dei dati oggetto dal sistema di storage di archiviazione esterno.	ARCB: Inizio recupero oggetto archivio
ARCE	Archive Object Retrieve End (fine recupero oggetto archivio): I dati dell'oggetto sono stati recuperati da un sistema di storage di archiviazione esterno e il servizio ARC segnala lo stato dell'operazione di recupero.	ARCE: Fine recupero oggetto archivio
ARCT	Recupero archivio dal livello cloud: I dati degli oggetti archiviati vengono recuperati da un sistema storage di archiviazione esterno, che si connette a StorageGRID tramite l'API S3.	ARCT: Recupero archivio da Cloud-Tier
AREM	Archive Object Remove (Rimozione oggetto archivio): Un blocco di contenuto è stato eliminato correttamente o senza successo dal sistema di storage di archiviazione esterno.	AREM: Rimozione dell'oggetto di archiviazione
ASCE	Archive Object Store End (fine archivio oggetti): Un blocco di contenuto è stato scritto nel sistema di storage di archiviazione esterno e il servizio ARC segnala lo stato dell'operazione di scrittura.	ASCE: Fine archivio oggetti
ASTT	Livello cloud archivio: I dati degli oggetti vengono memorizzati in un sistema storage di archiviazione esterno, che si connette a StorageGRID tramite l'API S3.	ASCT: Archivio Store Cloud-Tier
ATCE	Archive Object Store Begin (inizio archivio: Scrittura di un blocco di contenuto in uno storage di archiviazione esterno).	ATCE: Inizio archivio oggetti

Codice	Descrizione	Vedere
AVCC	Archive Validate Cloud-Tier Configuration (convalida archivio configurazione livello cloud): Le impostazioni dell'account e del bucket fornite sono state validate correttamente o senza successo.	AVCC: Convalida archivio configurazione Cloud-Tier
CBSE	Object Send End (fine invio oggetto): L'entità di origine ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	CBSE: Fine invio oggetto
CBRE	Object Receive End (fine ricezione oggetto): L'entità di destinazione ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	CBRE: Fine ricezione oggetto
SCMT	Commit dell'archivio oggetti: Un blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto.	SCMT: Commit dell'archivio di oggetti
SREM	Rimozione archivio oggetti: Un blocco di contenuto è stato cancellato da un nodo griglia e non può più essere richiesto direttamente.	SREM: Rimozione dell'archivio di oggetti

Messaggi di audit in lettura del client

I messaggi di audit in lettura del client vengono registrati quando un'applicazione client S3 o Swift richiede di recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	SGET: S3 GET

Codice	Descrizione	Utilizzato da	Vedere
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Client S3	SHEA: TESTA S3
WGET	Swift GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un container.	Client Swift	WGET: Swift GET
WHEA	Swift HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un container.	Client Swift	WHEA: TESTA veloce

Messaggi di audit di scrittura del client

I messaggi di audit di scrittura del client vengono registrati quando un'applicazione client S3 o Swift richiede di creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Object Overwrite: Registra una transazione per sovrascrivere un oggetto con un altro oggetto.	Client S3 Client Swift	OVWR: Sovrascrittura degli oggetti
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	SDEL: ELIMINAZIONE S3
SPOS	S3 POST: Registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Client S3	SPOS: POST S3

Codice	Descrizione	Utilizzato da	Vedere
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	SPUT: S3 PUT
SUPD	S3 Metadata Updated: Registra una transazione riuscita per aggiornare i metadati di un oggetto o bucket esistente.	Client S3	SUPD: Metadati S3 aggiornati
WDEL	Eliminazione rapida: Registra una transazione riuscita per eliminare un oggetto o un container.	Client Swift	WDEL: ELIMINAZIONE rapida
WPUT	Swift PUT: Registra una transazione riuscita per creare un nuovo oggetto o container.	Client Swift	WPUT: MESSA rapida

Messaggio di audit della gestione

La categoria Gestione registra le richieste degli utenti all'API di gestione.

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di audit API di gestione: Un registro delle richieste degli utenti.	MGAU: Messaggio di audit della gestione

Riferimento del messaggio di audit

APCT: Eliminazione dell'archivio dal Cloud-Tier

Questo messaggio viene generato quando i dati degli oggetti archiviati vengono cancellati da un sistema di storage di archiviazione esterno, che si connette a StorageGRID attraverso l'API S3.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto eliminato.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto in byte. Restituisce sempre 0.
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.
SUID	Identificatore univoco dello storage	Identificatore univoco (UUID) del cloud-Tier da cui l'oggetto è stato cancellato.

ARCB: Inizio recupero oggetto archivio

Questo messaggio viene generato quando viene effettuata una richiesta di recupero dei dati dell'oggetto archiviato e inizia il processo di recupero. Le richieste di recupero vengono elaborate immediatamente, ma possono essere riordinate per migliorare l'efficienza del recupero da supporti lineari come il nastro.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto da recuperare dal sistema di storage di archiviazione esterno.
RSLT	Risultato	Indica il risultato dell'avvio del processo di recupero dell'archivio. Il valore attualmente definito è:SUCS: La richiesta di contenuto è stata ricevuta e messa in coda per il recupero.

Questo messaggio di audit indica l'ora del recupero di un archivio. Consente di associare il messaggio a un corrispondente messaggio ARCE End per determinare la durata del recupero dell'archivio e se l'operazione è stata eseguita correttamente.

ARCE: Fine recupero oggetto archivio

Questo messaggio viene generato quando viene completato un tentativo da parte del nodo di archiviazione di recuperare i dati dell'oggetto da un sistema di storage di archiviazione esterno. Se l'esito è positivo, il messaggio indica che i dati dell'oggetto richiesti sono stati letti completamente dalla posizione di archiviazione ed è stato verificato correttamente. Una volta recuperati e verificati i dati dell'oggetto, questi vengono consegnati al servizio richiedente.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto da recuperare dal sistema di storage di archiviazione esterno.
VLID	Identificatore del volume	L'identificatore del volume su cui sono stati archiviati i dati.se non viene trovata una posizione di archiviazione per il contenuto, viene restituito un ID volume pari a 0.
RSLT	Risultato del recupero	Lo stato di completamento del processo di recupero dell'archivio: • SUC: Riuscito • VRFL: Non riuscito (errore di verifica dell'oggetto) • ARUN: Errore (sistema storage di archiviazione esterno non disponibile) • CANC: Non riuscito (operazione di recupero annullata) • GERR: Failed (errore generale)

La corrispondenza di questo messaggio con il corrispondente messaggio ARCB può indicare il tempo necessario per eseguire il recupero dell'archivio. Questo messaggio indica se il recupero è riuscito e, in caso di errore, la causa del mancato recupero del blocco di contenuto.

ARCT: Recupero archivio da Cloud-Tier

Questo messaggio viene generato quando i dati degli oggetti archiviati vengono recuperati da un sistema di storage di archiviazione esterno, che si connette a StorageGRID attraverso l'API S3.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto recuperato.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto in byte. Il valore è preciso solo per i recuperi riusciti.
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.

Codice	Campo	Descrizione
SUID	Identificatore univoco dello storage	Identificatore univoco (UUID) del sistema di storage di archiviazione esterno.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.

AREM: Rimozione dell'oggetto di archiviazione

Il messaggio di controllo Archive Object Remove (Rimozione oggetto archivio) indica che un blocco di contenuto è stato eliminato correttamente o senza successo da un nodo di archivio. Se il risultato è positivo, il nodo di archiviazione ha informato correttamente il sistema di storage di archiviazione esterno che StorageGRID ha rilasciato una posizione dell'oggetto. La rimozione dell'oggetto dal sistema di storage di archiviazione esterno dipende dal tipo di sistema e dalla relativa configurazione.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuti da recuperare dal sistema di supporti di archiviazione esterno.
VLID	Identificatore del volume	L'identificativo del volume su cui sono stati archiviati i dati dell'oggetto.
RSLT	Risultato	Lo stato di completamento del processo di rimozione dell'archivio: • SUC: Riuscito • ARUN: Errore (sistema storage di archiviazione esterno non disponibile) • GERR: Failed (errore generale)

ASCE: Fine archivio oggetti

Questo messaggio indica che la scrittura di un blocco di contenuto in un sistema di storage di archiviazione esterno è terminata.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore del blocco di contenuto memorizzato nel sistema di storage di archiviazione esterno.

Codice	Campo	Descrizione
VLID	Identificatore del volume	L'identificatore univoco del volume di archivio in cui vengono scritti i dati dell'oggetto.
VREN	Verifica abilitata	Indica se viene eseguita la verifica per i blocchi di contenuto. I valori attualmente definiti sono: • VENA: La verifica è attivata • VDSA: Verifica disattivata
MCLS	Classe di gestione	Stringa che identifica la classe di gestione TSM a cui viene assegnato il blocco di contenuto, se applicabile.
RSLT	Risultato	Indica il risultato del processo di archiviazione. I valori attualmente definiti sono: • SUC: Riuscito (processo di archiviazione riuscito) • OFFL: Non riuscito (archiviazione offline) • VRFL: Non riuscito (verifica oggetto non riuscita) • ARUN: Errore (sistema storage di archiviazione esterno non disponibile) • GERR: Failed (errore generale)

Questo messaggio di audit indica che il blocco di contenuto specificato è stato scritto nel sistema di storage di archiviazione esterno. Se la scrittura non riesce, il risultato fornisce informazioni di base sulla risoluzione dei problemi relativi alla posizione in cui si è verificato l'errore. Informazioni più dettagliate sugli errori di archiviazione sono disponibili esaminando gli attributi del nodo di archiviazione nel sistema StorageGRID.

ASCT: Archivio Store Cloud-Tier

Questo messaggio viene generato quando i dati degli oggetti archiviati vengono memorizzati in un sistema storage di archiviazione esterno, che si connette a StorageGRID attraverso l'API S3.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto recuperato.

Codice	Campo	Descrizione
CSIZ	Dimensione contenuto	La dimensione dell'oggetto in byte.
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.
SUID	Identificatore univoco dello storage	Identificatore univoco (UUID) del livello cloud in cui è stato memorizzato il contenuto.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.

ATCE: Inizio archivio oggetti

Questo messaggio indica che è stata avviata la scrittura di un blocco di contenuto in uno storage di archiviazione esterno.

Codice	Campo	Descrizione
CBID	ID blocco di contenuto	Identificatore univoco del blocco di contenuto da archiviare.
VLID	Identificatore del volume	Identificatore univoco del volume in cui viene scritto il blocco di contenuto. Se l'operazione non riesce, viene restituito un ID volume pari a 0.
RSLT	Risultato	Indica il risultato del trasferimento del blocco di contenuto. I valori attualmente definiti sono: • SUC: Riuscito (blocco di contenuto memorizzato correttamente) • EXIS: Ignorato (blocco di contenuto già memorizzato) • ISFD: Errore (spazio su disco insufficiente) • STER: Failed (errore durante la memorizzazione del CBID) • OFFL: Non riuscito (archiviazione offline) • GERR: Failed (errore generale)

AVCC: Convalida archivio configurazione Cloud-Tier

Questo messaggio viene generato quando le impostazioni di configurazione vengono validate per un tipo di destinazione Cloud Tiering - Simple Storage Service (S3).

Codice	Campo	Descrizione
RSLT	Codice risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.
SUID	Identificatore univoco dello storage	UUID associato al sistema di storage di archiviazione esterno da validare.

CBRB: Inizio ricezione oggetto

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.

Codice	Campo	Descrizione
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

CBRE: Fine ricezione oggetto

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.

Codice	Campo	Descrizione
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati. CONL: Connessione persa durante il trasferimento CTMO: Timeout della connessione durante la creazione o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi (potrebbe indicare manomissione)

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

CBSB: Inizio invio oggetto

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

CBSE: Fine invio oggetto

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.

Codice	Campo	Descrizione
RSLT	Risultato del trasferimento	Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati. CONL: Connessione persa durante il trasferimento CTMO: Timeout della connessione durante la creazione o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi (potrebbe indicare manomissione)

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

ECMC: Frammento di dati codificato Erasure mancante

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati con codifica di cancellazione mancante.

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il blocco mancante.
MCID	ID chunk	L'identificatore del frammento con codifica di cancellazione mancante.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

ECOC: Corrotto Erasure Coded Data Fragment

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati corrotto con codifica di cancellazione.

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco corrotto.
VLID	ID volume	Volume RangeDB contenente il frammento corrotto con codifica di cancellazione.
CCID	ID chunk	L'identificatore del frammento corrotto con codifica in cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

ETAF: Autenticazione di sicurezza non riuscita

Questo messaggio viene generato quando un tentativo di connessione con Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP su cui l'autenticazione non è riuscita.

Codice	Campo	Descrizione
MALEDUCATO	Identità dell'utente	Identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.
RSLT	Codice di motivazione	Il motivo del guasto: SCNI: Connessione sicura non riuscita. CERM: Certificato mancante. CERT: Certificato non valido. CERE: Certificato scaduto. CER: Certificato revocato. CSGN: Firma del certificato non valida. CSGU: Il firmatario del certificato non era noto. UCRM: Credenziali utente mancanti. UCRI: Credenziali utente non valide. UCRU: Le credenziali dell'utente non sono consentite. TOUT: Timeout dell'autenticazione.

Quando viene stabilita una connessione a un servizio sicuro che utilizza TLS, le credenziali dell'entità remota vengono verificate utilizzando il profilo TLS e la logica aggiuntiva integrata nel servizio. Se l'autenticazione non riesce a causa di certificati o credenziali non validi, imprevisti o non consentiti, viene registrato un messaggio di audit. Ciò consente di eseguire query per tentativi di accesso non autorizzati e altri problemi di connessione correlati alla sicurezza.

Il messaggio potrebbe derivare da un'entità remota con una configurazione errata o da tentativi di presentare credenziali non valide o non consentite al sistema. Questo messaggio di audit deve essere monitorato per rilevare i tentativi di accesso non autorizzato al sistema.

GNRG: Registrazione GNDS

Il servizio CMN genera questo messaggio di audit quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUC: Riuscito • SUNV: Servizio non disponibile • GERR: Altro guasto
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.
GNTP	Tipo di dispositivo	Il tipo di dispositivo del nodo Grid (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello di dispositivo del nodo Grid nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo grid (nel contesto dei costi di collegamento e della classificazione delle query di servizio).
GNIA	Indirizzo IP	L'indirizzo IP del nodo della griglia.

Questo messaggio viene generato ogni volta che un nodo della griglia aggiorna la propria voce nel bundle dei nodi della griglia.

GNUR: Annullamento registrazione GNDS

Il servizio CMN genera questo messaggio di audit quando un servizio ha informazioni non registrate su se stesso dal sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUC: Riuscito • SUNV: Servizio non disponibile • GERR: Altro guasto

Codice	Campo	Descrizione
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.

GTED: Task Grid terminato

Questo messaggio di audit indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e che l'attività è stata spostata nella tabella Cronologia. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato un messaggio di audit Grid Task Started (attività griglia avviata) corrispondente. Gli altri risultati indicano che l'elaborazione di questa attività della griglia non è mai stata avviata.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in modo univoco un'attività Grid generata e consente di gestire l'attività Grid nel suo ciclo di vita. **Nota:** l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato finale dello stato dell'attività Grid: • SUCS: L'attività Grid è stata completata correttamente. • ABRT: L'attività Grid è stata interrotta senza un errore di rollback. • ROLF: L'attività Grid è stata interrotta e non è stato possibile completare il processo di rollback. • CANC: L'attività della griglia è stata annullata dall'utente prima dell'avvio. • EXPR: L'attività Grid è scaduta prima dell'avvio. • IVLD: L'attività della griglia non era valida. • AUTH: L'attività della rete non è stata autorizzata. • DUPL: L'attività Grid è stata rifiutata come duplicata.

GTST: Task Grid avviato

Questo messaggio di audit indica che il servizio CMN ha avviato l'elaborazione dell'attività Grid specificata. Il messaggio di audit segue immediatamente il messaggio Grid Task Submitted per le attività Grid avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inoltrate nella tabella Pending (in sospeso), questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in maniera univoca un'attività grid generata e consente di gestirne l'intero ciclo di vita. **Nota:** l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: • SUCS: L'attività Grid è stata avviata correttamente.

GTSU: Task Grid inviato

Questo messaggio di audit indica che un'attività Grid è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	Identifica in modo univoco un'attività grid generata e consente di gestarla per l'intero ciclo di vita. **Nota:** l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
TTIP	Tipo di attività	Il tipo di attività della griglia.
VER	Versione attività	Un numero che indica la versione dell'attività Grid.

Codice	Campo	Descrizione
TDSC	Descrizione dell'attività	Una descrizione leggibile dell'attività Grid.
VAT	Valido dopo l'indicatore di data e ora	Il primo tempo (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui l'attività grid è valida.
VBTS	Valido prima dell'indicatore di data e ora	L'ultima ora (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui è valida l'attività grid.
TSRC	Origine	L'origine dell'attività: • TXTB: L'attività Grid è stata inviata tramite il sistema StorageGRID come blocco di testo firmato. • GRID: L'attività Grid è stata inviata tramite il Grid Task Submission Service interno.
ACTV	Tipo di attivazione	Il tipo di attivazione: • AUTO: L'attività della griglia è stata inviata per l'attivazione automatica. • PEND: L'attività Grid è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per l'origine TXTB.
RSLT	Risultato	Risultato dell'invio: • SUCS: L'attività Grid è stata inviata correttamente. • ERRORE: L'attività è stata spostata direttamente nella tabella storica.

IDEL: Eliminazione avviata da ILM

Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto.

Il messaggio IDEL viene generato in una delle seguenti situazioni:

- **Per gli oggetti nei bucket S3 conformi**: Questo messaggio viene generato quando ILM avvia il processo di eliminazione automatica di un oggetto perché il relativo periodo di conservazione è scaduto

(supponendo che l'impostazione di eliminazione automatica sia attivata e che la sospensione legale sia disattivata).

- **Per oggetti in bucket S3 o container Swift non conformi**. Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto perché nessuna istruzione di posizionamento nel criterio ILM attivo è attualmente applicabile all'oggetto.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Compliance: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (false) o 1 (true), che indica se un oggetto conforme deve essere cancellato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a una conservazione legale.
CMPL	Compliance: Conservazione a fini legali	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), che indica se il bucket è attualmente in stato di conservazione legale.
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. La durata del periodo di conservazione dell'oggetto in minuti.
CTME	Compliance: Tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Il tempo di acquisizione dell'oggetto. È possibile aggiungere il periodo di conservazione in minuti a questo valore per determinare quando l'oggetto può essere cancellato dal bucket.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato). CLEC: Per gli oggetti con codifica erasure, l'ID del profilo erasure coding e l'ID del gruppo erasure coding applicato ai dati dell'oggetto. CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.

Codice	Campo	Descrizione
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.
RSLT	Risultato	Risultato dell'operazione ILM. SUCS: Operazione ILM riuscita.
REGOLA	Etichetta regole	• Se un oggetto in un bucket S3 conforme viene cancellato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. • Se l'oggetto viene eliminato perché non sono presenti ulteriori istruzioni di posizionamento attualmente applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM applicata all'oggetto.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

LKCU: Pulitura oggetto sovrascritta

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza richiedeva la pulizia per liberare spazio di storage. Un oggetto viene sovrascritto quando un client S3 o Swift scrive un oggetto in un percorso che già contiene un oggetto. Il processo di rimozione avviene automaticamente e in background.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LTYP	Tipo di pulizia	*Solo per uso interno.*
LUID	UUID oggetto rimosso	L'identificativo dell'oggetto rimosso.
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.

Codice	Campo	Descrizione
SGC	UUID container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificativo dell'oggetto ancora esistente. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

LLST: Località persa

Questo messaggio viene generato ogni volta che non è possibile trovare una posizione per una copia di oggetto (replicata o codificata per la cancellazione).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.
NOID. (NOIDE	ID nodo di origine	L'ID del nodo in cui sono state perse le posizioni.
UUID	ID universalamente univoco	L'identificativo dell'oggetto interessato nel sistema StorageGRID.
ECPR	Erasure Coding Profile (erasure Coding Profile	Per i dati degli oggetti con codifica erasure. L'ID del profilo di codifica Erasure utilizzato.
LTYP	Tipo di ubicazione	CLDI (online): Per i dati degli oggetti replicati CLEC (Online): Per i dati degli oggetti con codifica erasure CLNL (Nearline): Per i dati degli oggetti replicati archiviati
PCLD	Percorso dell'oggetto replicato	Il percorso completo alla posizione del disco dei dati dell'oggetto perso. Viene restituito solo quando LTYP ha un valore di CLDI (vale a dire, per gli oggetti replicati). Prende la forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`

Codice	Campo	Descrizione
RSLT	Risultato	SEMPRE NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
TSRC	Fonte di attivazione	UTENTE: Attivato dall'utente SYST: Attivato dal sistema

MGAU: Messaggio di audit della gestione

La categoria Gestione registra le richieste degli utenti all'API di gestione. Ogni richiesta che non è UNA richiesta GET o HEAD all'API registra una risposta con il nome utente, l'IP e il tipo di richiesta all'API.

Codice	Campo	Descrizione
MDIP	Indirizzo IP di destinazione	L'indirizzo IP del server (destinazione).
MDNA	Nome di dominio	Il nome del dominio host.
MPAT	PERCORSO di richiesta	Il percorso della richiesta.
MPQP	Parametri di query della richiesta	I parametri di query per la richiesta.

Codice	Campo	Descrizione
MRBD	Corpo della richiesta	Il contenuto dell'organismo di richiesta. Mentre il corpo della risposta viene registrato per impostazione predefinita, il corpo della richiesta viene registrato in alcuni casi quando il corpo della risposta è vuoto. Poiché le seguenti informazioni non sono disponibili nel corpo della risposta, vengono prese dal corpo della richiesta per i seguenti metodi POST: • Nome utente e ID account in **POST authorize** • Nuova configurazione delle subnet in **POST /grid/grid-networks/update** • Nuovi server NTP in **POST /grid/ntp-servers/update** • ID server decommissionati in **POST /grid/servers/decommissionation** **Nota:** le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).
MRMD	Metodo di richiesta	Il metodo di richiesta HTTP: • POST • IN PRIMO PIANO • ELIMINARE • PATCH
MRSC	Codice di risposta	Il codice di risposta.
MRSP	Corpo di risposta	Il contenuto della risposta (il corpo della risposta) viene registrato per impostazione predefinita. **Nota:** le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).

Codice	Campo	Descrizione
MSIP	Indirizzo IP di origine	L'indirizzo IP (di origine) del client.
MUN	URN utente	L'URN (Uniform resource name) dell'utente che ha inviato la richiesta.
RSLT	Risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.

OLST: Il sistema ha rilevato un oggetto perso

Questo messaggio viene generato quando il servizio DDS non riesce a individuare alcuna copia di un oggetto all'interno del sistema StorageGRID.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto perso.
NOID. (NOIDE	ID nodo	Se disponibile, l'ultima posizione nota diretta o nearline dell'oggetto perso. Se le informazioni sul volume non sono disponibili, è possibile avere solo l'ID nodo senza un ID volume.
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Se disponibili, il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
UUID	ID universalamente univoco	L'identificativo dell'oggetto perso nel sistema StorageGRID.
VOLO	ID volume	Se disponibile, l'ID del volume del nodo di storage o del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

ORLM: Regole oggetto soddisfatte

Questo messaggio viene generato quando l'oggetto viene memorizzato e copiato correttamente come specificato dalle regole ILM.

> Il messaggio ORLM non viene generato quando un oggetto viene memorizzato correttamente dalla regola predefinita Make 2 Copies se un'altra regola del criterio utilizza il filtro avanzato dimensione oggetto.

Codice	Campo	Descrizione
BUID (BUID)	Testata benna	Campo ID bucket. Utilizzato per operazioni interne. Viene visualizzato solo se STAT è PRGD.
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato). CLEC: Per gli oggetti con codifica erasure, l'ID del profilo erasure coding e l'ID del gruppo erasure coding applicato ai dati dell'oggetto. CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
PERCORSO	ID bucket/chiave S3 o container/oggetto Swift	Il nome del bucket S3 e il nome della chiave S3 oppure il nome del container Swift e l'identificatore dell'oggetto Swift.
RSLT	Risultato	Risultato dell'operazione ILM. SUCS: Operazione ILM riuscita.
REGOLA	Etichetta regole	Etichetta leggibile assegnata alla regola ILM applicata a questo oggetto.
SGC	UUID container	UUID del container per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.

Codice	Campo	Descrizione
SGCB	CBID container	CBID del container per l'oggetto segmentato. Questo valore è disponibile solo per gli oggetti segmentati e multiparte.
URGENZA	Stato	Lo stato del funzionamento di ILM. FATTO: Operazioni ILM rispetto all'oggetto completate. DFER: L'oggetto è stato contrassegnato per la futura rivalutazione ILM. PRGD: L'oggetto è stato cancellato dal sistema StorageGRID. NLOC: I dati dell'oggetto non possono più essere trovati nel sistema StorageGRID. Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.

Il messaggio di audit ORLM può essere emesso più volte per un singolo oggetto. Ad esempio, viene emesso ogni volta che si verifica uno dei seguenti eventi:

- Le regole ILM per l'oggetto sono soddisfatte per sempre.
- Le regole ILM per l'oggetto sono soddisfatte per questa epoca.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati degli oggetti replicati è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto corrotto.

Informazioni correlate

- Transazioni di acquisizione degli oggetti
- Transazioni di eliminazione degli oggetti

OVWR: Sovrascrittura degli oggetti

Questo messaggio viene generato quando un'operazione esterna (richiesta dal client) causa la sovrascrittura di un oggetto da parte di un altro oggetto.

Codice	Campo	Descrizione
CBID	Content Block Identifier (nuovo)	Il CBID per il nuovo oggetto.

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto da sovrascrivere.
OCBD	Content Block Identifier (precedente)	Il CBID dell'oggetto precedente.
UUID	ID universally Unique (nuovo)	L'identificativo del nuovo oggetto all'interno del sistema StorageGRID.
ID OUID	ID universally Unique (precedente)	L'identificativo dell'oggetto precedente all'interno del sistema StorageGRID.
PERCORSO	S3 o Swift Object Path	Il percorso di oggetti S3 o Swift utilizzato sia per l'oggetto precedente che per quello nuovo
RSLT	Codice risultato	Risultato della transazione Object Overwrite. Il risultato è sempre: SUC: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato cancellato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto sovrascritto.

SADD: Disattivazione dell'audit di sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di audit; i messaggi di audit non vengono più raccolti o consegnati.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per disattivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione era stata precedentemente attivata, ma ora è stata disattivata. Questo viene generalmente utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato (SADE) e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

SADE: Abilitazione controllo di sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione del messaggio di audit; i messaggi di audit vengono nuovamente raccolti e consegnati.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Il metodo utilizzato per attivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per attivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione è stata precedentemente disattivata (SADD), ma ora è stata ripristinata. In genere viene utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

SCMT: Commit dell'archivio di oggetti

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato fino a quando non viene assegnato (ovvero viene memorizzato in modo persistente). Il contenuto memorizzato in maniera persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene emesso quando un blocco di contenuto viene assegnato allo storage.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto impegnato nello storage permanente.

Codice	Campo	Descrizione
RSLT	Codice risultato	Stato al momento in cui l'oggetto è stato memorizzato sul disco: SUCS: Oggetto memorizzato correttamente.

Questo messaggio indica che un dato blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto. Può essere utilizzato per tenere traccia del flusso di dati all'interno del sistema.

SDEL: ELIMINAZIONE S3

Quando un client S3 esegue una transazione DI ELIMINAZIONE, viene inviata una richiesta per rimuovere l'oggetto o il bucket specificato. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.

Codice	Campo	Descrizione
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SGET: S3 GET

Quando un client S3 esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RANG	Range Read (lettura intervallo)	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) mostra la dimensione dell'intero oggetto.
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.

Codice	Campo	Descrizione
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SHEA: TESTA S3

Quando un client S3 esegue una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un oggetto o bucket e recuperare i metadati relativi a un oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto controllato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SPOS: POST S3

Quando un client S3 invia una richiesta di oggetto POST, questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della richiesta DI ripristino dell'oggetto POST. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

Codice	Campo	Descrizione
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile. Impostare su “select” (Seleziona) per un’operazione S3 Select.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell’account tenant per l’utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L’indirizzo IP dell’applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell’account tenant per il proprietario del bucket. Utilizzato per identificare l’accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L’ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l’accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	S3 User URN (richiesta mittente)	L’ID account tenant e il nome utente dell’utente che effettua la richiesta. L’utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l’indirizzo IP del bilanciamento del carico.

Codice	Campo	Descrizione
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SPUT: S3 PUT

Quando un client S3 esegue una transazione PUT, viene inviata una richiesta per creare un nuovo oggetto o bucket. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di compliance	Le impostazioni di compliance utilizzate durante la creazione del bucket, se presenti nella richiesta PUT bucket (troncate ai primi 1024 caratteri)
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
LKEN	Blocco oggetto attivato	Valore dell'intestazione della richiesta `x-amz-bucket-object-lock-enabled`, Se presente nella richiesta PUT bucket.
LKSX	Blocco oggetto Legal Hold	Valore dell'intestazione della richiesta `x-amz-object-lock-legal-hold`, Se presente nella richiesta DI oggetto PUT.
LKMD	Modalità di conservazione del blocco degli oggetti	Valore dell'intestazione della richiesta `x-amz-object-lock-mode`, Se presente nella richiesta DI oggetto PUT.
LKRU	Blocco oggetto conserva fino alla data	Valore dell'intestazione della richiesta `x-amz-object-lock-retain-until-date`, Se presente nella richiesta DI oggetto PUT.
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.

Codice	Campo	Descrizione
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	S3KY	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.

Codice	Campo	Descrizione
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
ULID	ID upload	Incluso solo nei messaggi SPUT per operazioni complete di caricamento multiparte. Indica che tutte le parti sono state caricate e assemblate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.
VSST	Stato di versione	Il nuovo stato di versione di un bucket. Vengono utilizzati due stati: "Enabled" (attivato) o "Suspended" (sospeso). Le operazioni sugli oggetti non includono questo campo.

SREM: Rimozione dell'archivio di oggetti

Questo messaggio viene inviato quando il contenuto viene rimosso dallo storage persistente e non è più accessibile tramite API regolari.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto cancellato dallo storage permanente.
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è: SUC: Contenuto rimosso dallo storage persistente

Questo messaggio di audit indica che un dato blocco di contenuto è stato cancellato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tenere traccia del flusso di contenuti cancellati all'interno del sistema.

SUPD: Metadati S3 aggiornati

Questo messaggio viene generato dall'API S3 quando un client S3 aggiorna i metadati per un oggetto acquisito. Il messaggio viene emesso dal server se l'aggiornamento dei metadati ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, quando si aggiornano le impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito

Codice	Campo	Descrizione
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.

Codice	Campo	Descrizione
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

SVRF: Verifica archivio oggetti non riuscita

Questo messaggio viene emesso ogni volta che un blocco di contenuto non supera il processo di verifica. Ogni volta che i dati degli oggetti replicati vengono letti o scritti su disco, vengono eseguiti diversi controlli di verifica e integrità per garantire che i dati inviati all'utente richiedente siano identici ai dati originariamente acquisiti nel sistema. Se uno di questi controlli non riesce, il sistema mette automaticamente in quarantena i dati dell'oggetto replicato corrotto per impedirne il recupero.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto che non ha superato la verifica.

Codice	Campo	Descrizione
RSLT	Codice risultato	Tipo di errore di verifica: CRCF: Controllo di ridondanza ciclico (CRC) non riuscito. HMAC: Controllo HMAC (hash-based message Authentication code) non riuscito. EHSH: Hash di contenuto crittografato inatteso. PHSH: Hash di contenuto originale inaspettato. SEQC: Sequenza di dati errata sul disco. PERR: Struttura del file di disco non valida. DERR: Errore del disco. FNAM: Nome file non valido.

Nota: questo messaggio deve essere monitorato attentamente. Gli errori di verifica del contenuto possono indicare tentativi di manomissione del contenuto o guasti hardware imminenti.

Per determinare quale operazione ha attivato il messaggio, vedere il valore del campo AMID (Module ID) (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, ovvero la verifica in background e STOR indica che il messaggio è stato attivato dal recupero del contenuto.

SVRU: Verifica archivio oggetti sconosciuta

Il componente Storage del servizio LDR esegue una scansione continua di tutte le copie dei dati degli oggetti replicati nell'archivio di oggetti. Questo messaggio viene visualizzato quando viene rilevata una copia sconosciuta o imprevista dei dati degli oggetti replicati nell'archivio di oggetti e spostata nella directory di quarantena.

Codice	Campo	Descrizione
FPTH	Percorso del file	Il percorso del file della copia imprevista dell'oggetto.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

Nota: il messaggio di audit SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie impreviste dei dati dell'oggetto nell'archivio di oggetti. Questa situazione deve essere esaminata immediatamente per determinare come sono state create queste copie, in quanto può indicare tentativi di manomissione del contenuto o guasti hardware imminenti.

SYSD: Interruzione nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto lo shutdown. In genere, questo messaggio viene inviato solo dopo un riavvio successivo, in quanto la coda dei messaggi di controllo non viene cancellata prima dell'arresto. Se il servizio non è stato riavviato, cercare il messaggio SYST inviato all'inizio della sequenza di arresto.

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno shutdown "dirty", perché il messaggio viene generato solo dagli shutdown "clean".

SYST: Interruzione del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto lo shutdown e che il servizio ha avviato la sequenza di shutdown. SYST può essere utilizzato per determinare se è stato richiesto lo shutdown, prima che il servizio venga riavviato (a differenza di SYSD, che in genere viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. Il codice RSLT di un

messaggio SYST non può indicare uno shutdown "dirty", perché il messaggio viene generato solo dagli shutdown "clean".

SYSU: Avvio nodo

Quando un servizio viene riavviato, questo messaggio viene generato per indicare se l'arresto precedente era pulito (comandato) o disordinato (imprevisto).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito. DSDN: Il sistema non è stato spento correttamente. VRGN: Il sistema è stato avviato per la prima volta dopo l'installazione (o la reinstallazione) del server.

Il messaggio non indica se il server host è stato avviato, ma solo il servizio di reporting. Questo messaggio può essere utilizzato per:

- Rilevare la discontinuità nel registro di controllo.
- Determinare se un servizio si guasta durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio guasto.

VLST: Perdita del volume avviata dall'utente

Questo messaggio viene visualizzato ogni volta che `/proc/CMSI/Volume_Lost` viene eseguito il comando.

Codice	Campo	Descrizione
VOL	Identificatore del volume inferiore	L'estremità inferiore dell'intervallo di volume interessato o di un singolo volume.
VOLU	Identificatore del volume superiore	L'estremità superiore dell'intervallo di volume interessato. Uguale a VOLL se si tratta di un singolo volume.
NOID. (NOIDE	ID nodo di origine	L'ID del nodo in cui sono state perse le posizioni.

Codice	Campo	Descrizione
LTYP	Tipo di ubicazione	'CLDI' (online) o 'CLNL' (Nearline). Se non specificato, l'impostazione predefinita è 'CLDI'.
RSLT	Risultato	Sempre 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

WDEL: ELIMINAZIONE rapida

Quando un client Swift esegue una transazione DI ELIMINAZIONE, viene inviata una richiesta per rimuovere l'oggetto o il container specificato. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre: SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.

Codice	Campo	Descrizione
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni sui container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WGET: Swift GET

Quando un client Swift esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto, elencare gli oggetti in un container o elencare i container in un account. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni su account e container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e container non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni su account e container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WHEA: TESTA veloce

Quando un client Swift esegue una transazione HEAD, viene inviata una richiesta per verificare l'esistenza di un account, un container o un oggetto e recuperare eventuali metadati pertinenti. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni su account e container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e container non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
RSLT	Codice risultato	Risultato della transazione HEAD. Il risultato è sempre: SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.

Codice	Campo	Descrizione
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni su account e container non includono questo campo.
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

WPUT: MESSA rapida

Quando un client Swift esegue una transazione PUT, viene inviata una richiesta per creare un nuovo oggetto o container. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui container non includono questo campo.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui container non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. **Nota:** `X-Forwarded-For` viene automaticamente incluso se è presente nella richiesta e se `X-Forwarded-For` Il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di audit SAIP).
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUC: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
WACC	ID account Swift	L'ID account univoco specificato dal sistema StorageGRID.
WCON	Container Swift	Il nome del container Swift.
WOBJ	Oggetto Swift	L'identificatore dell'oggetto Swift. Le operazioni sui container non includono questo campo.

Codice	Campo	Descrizione
WUSR	Utente Swift account	Il nome utente dell'account Swift che identifica in modo univoco il client che esegue la transazione.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI 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.