Esaminare i registri di controllo

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-119/audit/index.html on December 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Esaminare i registri di controllo

Messaggi e registri di controllo

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di controllo e dei registri di controllo StorageGRID . È possibile utilizzare queste informazioni per leggere e analizzare la traccia di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli amministratori responsabili della produzione di report sull'attività e l'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID .

Per utilizzare il file di registro di testo, è necessario avere accesso alla condivisione di controllo configurata sul nodo di amministrazione.

Per informazioni sulla configurazione dei livelli dei messaggi di controllo e sull'utilizzo di un server syslog esterno, vedere"Configurare i messaggi di controllo e le destinazioni dei registri" .

Flusso e conservazione dei messaggi di audit

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. Dovresti capire come questi messaggi di controllo si spostano attraverso il sistema StorageGRID verso `audit.log` file.

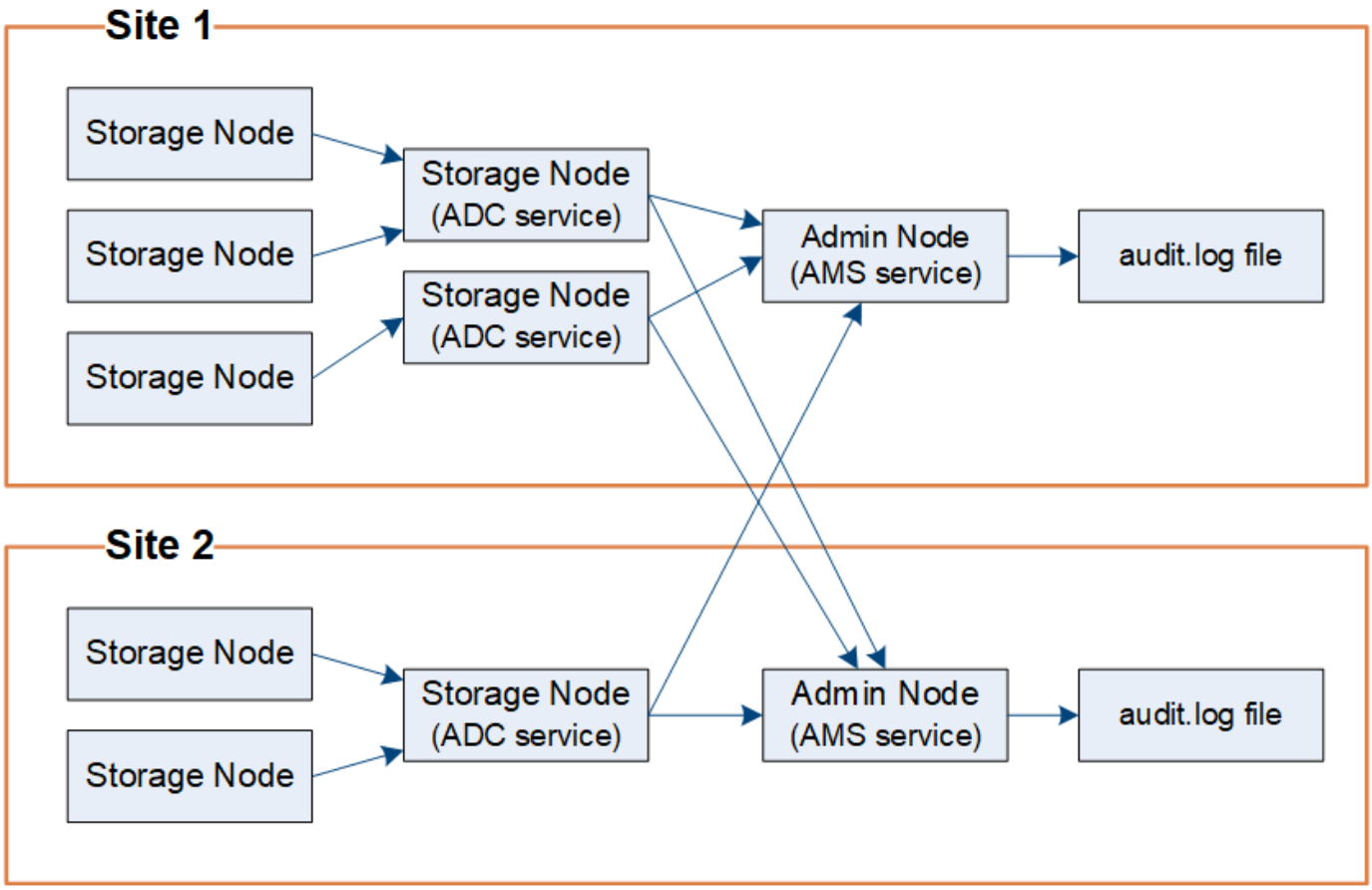
Flusso dei messaggi di audit

I messaggi di controllo vengono elaborati dai nodi di amministrazione e dai nodi di archiviazione che dispongono di un servizio di controller di dominio amministrativo (ADC).

Come mostrato nel diagramma del flusso dei messaggi di controllo, ogni nodo StorageGRID invia i propri messaggi di controllo a uno dei servizi ADC presso il sito del data center. Il servizio ADC viene abilitato automaticamente per i primi tre nodi di archiviazione installati in ciascun sito.

A sua volta, ogni servizio ADC funge da relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID , il che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

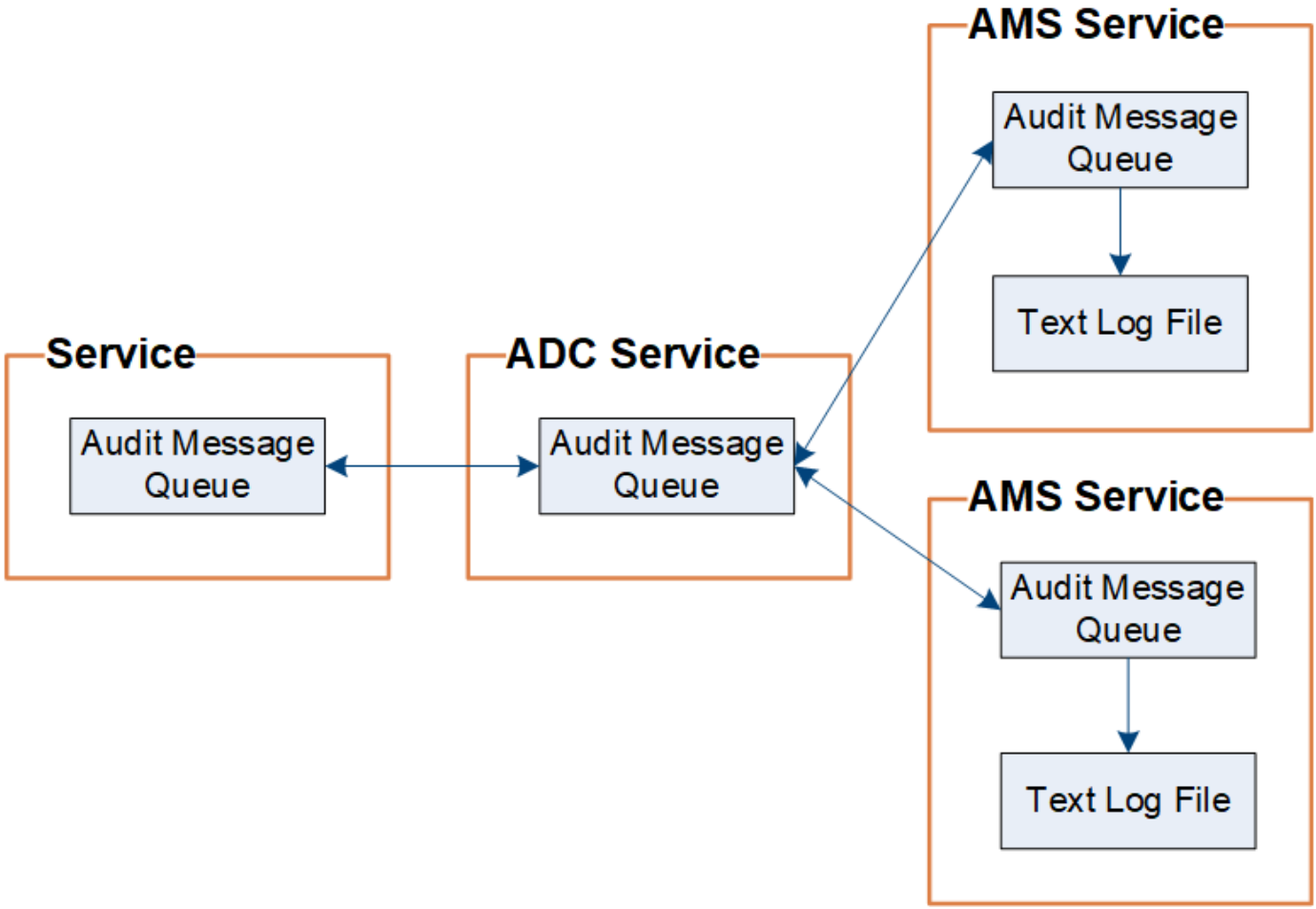
Ogni nodo di amministrazione memorizza i messaggi di controllo in file di registro di testo; il file di registro attivo è denominato `audit.log` .



Conservazione dei messaggi di controllo

StorageGRID utilizza un processo di copia ed eliminazione per garantire che nessun messaggio di controllo venga perso prima che possa essere scritto nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di controllo, il messaggio viene memorizzato in una coda di messaggi di controllo sul disco di sistema del nodo della griglia. Una copia del messaggio viene sempre conservata in una coda di messaggi di controllo finché il messaggio non viene scritto nel file di registro di controllo nel nodo di amministrazione `/var/local/log` elenco. Ciò aiuta a prevenire la perdita di un messaggio di controllo durante il trasporto.



La coda dei messaggi di controllo può aumentare temporaneamente a causa di problemi di connettività di rete o di capacità di controllo insufficiente. Man mano che le code aumentano, consumano più spazio disponibile in ciascun nodo `/var/local/` elenco. Se il problema persiste e la directory dei messaggi di controllo di un nodo diventa troppo piena, i singoli nodi daranno priorità all'elaborazione del loro arretrato e diventeranno temporaneamente non disponibili per nuovi messaggi.

Nello specifico, potresti riscontrare i seguenti comportamenti:

- Se il `/var/local/log` Se la directory utilizzata da un nodo di amministrazione diventa piena, il nodo di amministrazione verrà contrassegnato come non disponibile per nuovi messaggi di controllo finché la directory non sarà più piena. Le richieste del client S3 non sono interessate. L'allarme XAMS (Unreachable Audit Repositories) viene attivato quando un repository di audit non è raggiungibile.
- Se il `/var/local/` Quando la directory utilizzata da un nodo di archiviazione con il servizio ADC è piena al 92%, il nodo verrà contrassegnato come non disponibile per i messaggi di controllo finché la directory non sarà piena solo all'87%. Le richieste del client S3 ad altri nodi non sono interessate. L'allarme NRLY (Available Audit Relays) viene attivato quando i relay di audit non sono raggiungibili.

> Se non sono disponibili nodi di archiviazione con il servizio ADC, i nodi di archiviazione archiviano i messaggi di controllo localmente nel `/var/local/log/localaudit.log` file.

- Se il `/var/local/` la directory utilizzata da un nodo di archiviazione diventa piena all'85%, il nodo inizierà a rifiutare le richieste del client S3 con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare un aumento notevole delle dimensioni delle code dei messaggi di controllo:

- Interruzione di un nodo di amministrazione o di un nodo di archiviazione con il servizio ADC. Se uno dei nodi del sistema è inattivo, i nodi rimanenti potrebbero accumulare arretrati.
- Un tasso di attività sostenuto che supera la capacità di audit del sistema.
- IL `/var/local/` spazio su un nodo di archiviazione ADC che si riempie per motivi non correlati ai messaggi di controllo. Quando ciò accade, il nodo smette di accettare nuovi messaggi di audit e dà priorità al suo arretrato attuale, il che può causare arretrati su altri nodi.

Avviso di coda di controllo di grandi dimensioni e allarme di messaggi di controllo in coda (AMQS)

Per aiutarti a monitorare le dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Coda di controllo di grandi dimensioni** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda del nodo di archiviazione o in una coda del nodo di amministrazione raggiunge determinate soglie.

Se viene attivato l'avviso **Coda di controllo di grandi dimensioni** o l'allarme AMQS legacy, iniziare controllando il carico sul sistema: se si è verificato un numero significativo di transazioni recenti, l'avviso e l'allarme dovrebbero risolversi nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di gravità, visualizza un grafico delle dimensioni della coda. Se il numero aumenta costantemente nel corso di ore o giorni, è probabile che il carico di controllo abbia superato la capacità di controllo del sistema. Ridurre la frequenza operativa del client o diminuire il numero di messaggi di controllo registrati modificando il livello di controllo per Scritture client e Letture client su Errore o Disattivato. Vedere "Configurare i messaggi di controllo e le destinazioni dei registri" .

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto della rete o del nodo. Per questo motivo potrebbero esserci messaggi duplicati nel registro di controllo.

Accedi al file di registro di controllo

La condivisione di controllo contiene l'attivo `audit.log` file e tutti i file di registro di controllo compressi. È possibile accedere ai file di registro di controllo direttamente dalla riga di comando del nodo di amministrazione.

Prima di iniziare

- Hai"autorizzazioni di accesso specifiche" .
- Devi avere il `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo di amministrazione.

Passi

1. Accedi a un nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Inserisci la password elencata nel `Passwords.txt` file.
   c. Immettere il seguente comando per passare alla root: `su -`
   d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` A `#` .

2. Andare alla directory contenente i file di registro di controllo:

```
cd /var/local/log
```

3. Visualizzare il file di registro di controllo corrente o salvato, a seconda delle necessità.

Rotazione del file di registro di controllo

I file dei registri di controllo vengono salvati nel nodo di amministrazione `/var/local/log` elenco. I file di registro di controllo attivi sono denominati `audit.log` .

> Facoltativamente, è possibile modificare la destinazione dei log di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e archiviati quando viene configurato un server syslog esterno. Vedere "Configurare i messaggi di controllo e le destinazioni dei registri" .

Una volta al giorno, l'attivo `audit.log` il file viene salvato e ne viene creato uno nuovo `audit.log` il file è avviato. Il nome del file salvato indica quando è stato salvato, nel formato *`yyyy-mm-dd.txt`* . Se in un singolo giorno viene creato più di un registro di controllo, i nomi dei file utilizzano la data di salvataggio del file, seguita da un numero, nel formato *`yyyy-mm-dd.txt.n`* . Per esempio, `2018-04-15.txt` E `2018-04-15.txt.1` sono il primo e il secondo file di registro creati e salvati il 15 aprile 2018.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato *`yyyy-mm-dd.txt.gz`* , che conserva la data originale. Nel tempo, ciò si traduce nel consumo dello spazio di archiviazione allocato per i log di controllo sul nodo di amministrazione. Uno script monitora il consumo di spazio del registro di controllo ed elimina i file di registro se necessario per liberare spazio nel `/var/local/log` elenco. I registri di controllo vengono eliminati in base alla data di creazione, partendo da quelli più vecchi. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log` .

Questo esempio mostra l'attivo `audit.log` file, il file del giorno precedente(`2018-04-15.txt`), e il file compresso del giorno precedente(`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato del file di registro di controllo

Formato del file di registro di controllo

I file di registro di controllo si trovano su ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di controllo.

Ogni messaggio di controllo contiene quanto segue:

- Il tempo coordinato universale (UTC) dell'evento che ha attivato il messaggio di controllo (ATIM) nel formato ISO 8601, seguito da uno spazio:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, Dove *UUUUUU* sono microsecondi.

- Il messaggio di controllo stesso, racchiuso tra parentesi quadre e che inizia con `AUDT` .

L'esempio seguente mostra tre messaggi di controllo in un file di registro di controllo (interruzioni di riga aggiunte per migliorare la leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e ha aggiunto due oggetti a tale bucket.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
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::17530064241597054
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::17530064241597054
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 controllo nei file di registro di controllo non sono facili da leggere o interpretare. Puoi usare il"strumento di verifica e spiegazione" per ottenere riepiloghi semplificati dei messaggi di controllo nel registro di controllo. Puoi usare il"strumento di somma di controllo" per riepilogare quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto queste operazioni.

Utilizzare lo strumento di verifica e spiegazione

Puoi usare il `audit-explain` strumento per tradurre i messaggi di controllo nel registro

di controllo in un formato di facile lettura.

Prima di iniziare

- Hai"autorizzazioni di accesso specifiche" .
- Devi avere il `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

Informazioni su questo compito

IL `audit-explain` strumento, disponibile sul nodo di amministrazione principale, fornisce riepiloghi semplificati dei messaggi di controllo in un registro di controllo.

> IL `audit-explain` Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Elaborazione `audit-explain` le query possono consumare una grande quantità di potenza della CPU, il che potrebbe avere un impatto sulle operazioni StorageGRID .

Questo esempio mostra l'output tipico del `audit-explain` attrezzo. Questi quattro"SPUT" sono stati generati messaggi di controllo quando il tenant S3 con ID account 92484777680322627870 ha utilizzato richieste PUT S3 per creare un bucket denominato "bucket1" e aggiungere tre oggetti a tale bucket.

```
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` lo strumento può fare quanto segue:

- Elaborare registri di controllo semplici o compressi. Per esempio:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Elaborare più file contemporaneamente. Per esempio:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- Accetta input da una pipe, che consente di filtrare e preelaborare l'input utilizzando `grep` comando o altri mezzi. Per esempio:

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Poiché i registri di controllo possono essere molto grandi e lenti da analizzare, è possibile risparmiare tempo filtrando le parti che si desidera esaminare ed eseguendo `audit-explain` sulle parti, anziché sull'intero file.

> IL `audit-explain` lo strumento non accetta file compressi come input inoltrato. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` strumento per decomprimere prima i file. Per esempio:
>
> `zcat audit.log.gz | audit-explain`

Utilizzare il `help (-h)` opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-explain -h
```

Passi

1. Accedi al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Inserisci la password elencata nel `Passwords.txt` file.
   c. Immettere il seguente comando per passare alla root: `su -`
   d. Inserisci la password elencata nel `Passwords.txt` file.

   Quando si accede come root, il prompt cambia da `$` A `#` .
2. Immettere il seguente comando, dove `/var/local/log/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   IL `audit-explain` Lo strumento stampa interpretazioni leggibili dall'uomo di tutti i messaggi nel file o nei file specificati.

   > Per ridurre la lunghezza delle righe e migliorare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se vuoi vedere i timestamp, usa il timestamp(`-t`) opzione.

Utilizzare lo strumento audit-sum

Puoi usare il `audit-sum` strumento per contare i messaggi di controllo di scrittura, lettura, intestazione ed eliminazione e per visualizzare il tempo minimo, massimo e medio (o dimensione) per ciascun tipo di operazione.

Prima di iniziare

- Hai"autorizzazioni di accesso specifiche" .
- Devi avere il `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

Informazioni su questo compito

IL `audit-sum` strumento, disponibile sul nodo di amministrazione primario, riepiloga quante operazioni di

scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto tali operazioni.

> IL `audit-sum` Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Elaborazione `audit-sum` le query possono consumare una grande quantità di potenza della CPU, il che potrebbe avere un impatto sulle operazioni StorageGRID .

Questo esempio mostra l'output tipico del `audit-sum` attrezzo. Questo esempio mostra quanto tempo hanno richiesto le operazioni del protocollo.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

IL `audit-sum` Lo strumento fornisce conteggi e orari per i seguenti messaggi di controllo S3, Swift e ILM in un registro di controllo.

> I codici di controllo vengono rimossi dal prodotto e dalla documentazione quando le funzionalità diventano obsolete. Se riscontri un codice di controllo non elencato qui, controlla le versioni precedenti di questo argomento per le versioni SG più vecchie. Ad esempio, "StorageGRID 11.8 Utilizzo della documentazione dello strumento di somma di controllo" .

Codice	Descrizione	Fare riferimento a
IDEL	Eliminazione avviata da ILM: registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: ILM ha avviato l'eliminazione"
SDEL	S3 DELETE: registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: S3 ELIMINA"
SGET	S3 GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	"SGET: S3 GET"
KARITÉ	S3 HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	"SHEA: TESTA S3"
SPUT	S3 PUT: registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"

Codice	Descrizione	Fare riferimento a
WDEL	Swift DELETE: registra una transazione riuscita per eliminare un oggetto o un contenitore.	"WDEL: CANCELLA rapida"
WGET	Swift GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un contenitore.	"WGET: GET rapido"
WHEA	Swift HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un contenitore.	"WHEA: TESTA Veloce"
WPUT	Swift PUT: registra una transazione riuscita per creare un nuovo oggetto o contenitore.	"WPUT: PUT rapido"

IL `audit-sum` lo strumento può fare quanto segue:

- Elaborare registri di controllo semplici o compressi. Per esempio:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Elaborare più file contemporaneamente. Per esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- Accetta input da una pipe, che consente di filtrare e preelaborare l'input utilizzando `grep` comando o altri mezzi. Per esempio:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> Questo strumento non accetta file compressi come input inoltrato. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` strumento per decomprimere prima i file. Per esempio:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

È possibile utilizzare le opzioni della riga di comando per riepilogare le operazioni sui bucket separatamente dalle operazioni sugli oggetti oppure per raggruppare i riepiloghi dei messaggi in base al nome del bucket, al periodo di tempo o al tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di funzionamento minimo, massimo e medio, ma è possibile utilizzare `size (-s)` opzione per guardare invece le dimensioni dell'oggetto.

Utilizzare il `help (-h)` opzione per vedere le opzioni disponibili. Per esempio:

```
$ audit-sum -h
```

Passi

1. Accedi al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Inserisci la password elencata nel `Passwords.txt` file.
   c. Immettere il seguente comando per passare alla root: `su -`
   d. Inserisci la password elencata nel `Passwords.txt` file.

      Quando si accede come root, il prompt cambia da `$` A `#` .

2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, intestazione ed eliminazione, seguire questi passaggi:
   a. Immettere il seguente comando, dove `/var/local/log/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Questo esempio mostra l'output tipico del `audit-sum` attrezzo. Questo esempio mostra quanto tempo hanno richiesto le operazioni del protocollo.

      ```
        message group           count     min(sec)        max(sec)
      average(sec)
        =============           =====     ========        ========
      ============
        IDEL                      274
        SDEL                   213371        0.004          20.934
      0.352
        SGET                   201906        0.010        1740.290
      1.132
        SHEA                    22716        0.005           2.349
      0.272
        SPUT                 1771398        0.011        1770.563
      0.487
      ```

      In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media, con 1,13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano entrambe tempi molto lunghi nel caso peggiore, pari a circa 1.770 secondi.

   b. Per mostrare le 10 operazioni di recupero più lente, utilizzare il comando grep per selezionare solo i messaggi SGET e aggiungere l'opzione di output lunga(`-l`) per includere i percorsi degli oggetti:

      ```
      grep SGET audit.log | audit-sum -l
      ```

      I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di cercare nel registro di

controllo altri messaggi relativi a questi oggetti specifici.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/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 output di esempio, è possibile vedere che le tre richieste S3 GET più lente riguardavano oggetti di circa 5 GB di dimensione, ovvero molto più grandi degli altri oggetti. Le grandi dimensioni spiegano i lenti tempi di recupero nel caso peggiore.

3. Se vuoi determinare quali dimensioni degli oggetti vengono acquisiti e recuperati dalla tua griglia, usa l'opzione dimensione(`-s`):

   ```
   audit-sum -s audit.log
   ```

```
  message group           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 dell'oggetto per SPUT è inferiore a 2,5 MB, ma la dimensione media per SGET è molto più grande. Il numero di messaggi SPUT è molto più elevato del numero di messaggi SGET, il che indica che la maggior parte degli oggetti non viene mai recuperata.

4. Se vuoi determinare se i recuperi sono stati lenti ieri:

   a. Emettere il comando sul registro di controllo appropriato e utilizzare l'opzione di raggruppamento per ora(`-gt`), seguito dal periodo di tempo (ad esempio, 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           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 il traffico S3 GET ha registrato un picco tra le 06:00 e le 07:00. Anche i tempi massimi e medi sono considerevolmente più alti in questi momenti e non aumentano gradualmente con l'aumentare del conteggio. Ciò suggerisce che da qualche parte è stata superata la capacità, forse nella rete o nella capacità della griglia di elaborare le richieste.

b. Per determinare la dimensione degli oggetti recuperati ogni ora ieri, aggiungi l'opzione dimensione(`-s`) al comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           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 alcuni recuperi molto grandi si sono verificati quando il traffico di recupero complessivo era al massimo.

c. Per vedere più dettagli, usa il"strumento di verifica e spiegazione" per rivedere tutte le operazioni SGET durante quell'ora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se si prevede che l'output del comando grep sia composto da molte righe, aggiungere `less` comando per mostrare il contenuto del file di registro di controllo una pagina (una schermata) alla volta.

5. Se si desidera determinare se le operazioni SPUT sui bucket sono più lente delle operazioni SPUT sugli oggetti:

a. Inizia utilizzando il `-go` opzione, che raggruppa separatamente i messaggi per le operazioni su oggetti e bucket:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

I risultati mostrano che le operazioni SPUT per i bucket presentano caratteristiche prestazionali diverse rispetto alle operazioni SPUT per gli oggetti.

b. Per determinare quali bucket hanno le operazioni SPUT più lente, utilizzare `-gb` opzione, che raggruppa i messaggi per bucket:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Per determinare quali bucket hanno la dimensione dell'oggetto SPUT più grande, utilizzare entrambi `-gb` e il `-s` opzioni:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          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
```

Formato del messaggio di controllo

Formato del messaggio di controllo

I messaggi di controllo scambiati all'interno del sistema StorageGRID includono informazioni standard comuni a tutti i messaggi e contenuti specifici che descrivono l'evento o l'attività segnalata.

Se le informazioni riassuntive fornite dal"audit-spiegazione" E"somma di controllo" strumenti non è sufficiente, fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di audit.

Di seguito è riportato un esempio di messaggio di controllo, così come potrebbe apparire nel file di registro di controllo:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Ogni messaggio di controllo contiene una stringa di elementi di attributo. L'intera stringa è racchiusa tra parentesi(`[ ]`), e ogni elemento attributo nella stringa ha le seguenti caratteristiche:

- Racchiuso tra parentesi `[ ]`
- Introdotto dalla stringa `AUDT` , che indica un messaggio di controllo
- Senza delimitatori (senza virgole o spazi) prima o dopo
- Terminato da un carattere di avanzamento riga `\n`

Ogni elemento include un codice attributo, un tipo di dati e un valore che vengono riportati nel seguente formato:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Il numero di elementi attributo nel messaggio dipende dal tipo di evento del messaggio. Gli elementi attributo non sono elencati in un ordine particolare.

L'elenco seguente descrive gli elementi dell'attributo:

- `ATTR`è un codice di quattro caratteri per l'attributo segnalato. Alcuni attributi sono comuni a tutti i messaggi di controllo, mentre altri sono specifici dell'evento.
- `type`è un identificatore di quattro caratteri del tipo di dati di programmazione del valore, ad esempio UI64, FC32 e così via. Il tipo è racchiuso tra parentesi `( ) .
- `value`è il contenuto dell'attributo, in genere un valore numerico o di testo. I valori seguono sempre i due punti(:`). I valori del tipo di dati CSTR sono racchiusi tra virgolette doppie " ".

Tipi di dati

Per memorizzare le informazioni nei messaggi di controllo vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero lungo senza segno (32 bit); può memorizzare i numeri da 0 a 4.294.967.295.
UI64	Numero intero doppio lungo senza segno (64 bit); può memorizzare i numeri da 0 a 18.446.744.073.709.551.615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32 bit rappresentato da quattro caratteri ASCII, ad esempio "ABCD".
iPad	Utilizzato per gli indirizzi IP.
CSTR	Un array di lunghezza variabile di caratteri UTF-8. I caratteri possono essere sottoposti a escape con le seguenti convenzioni: • La barra rovesciata è \\. • Il ritorno a capo è \r. • Le virgolette doppie sono \". • L'avanzamento di riga (nuova riga) è \n. • I caratteri possono essere sostituiti dai loro equivalenti esadecimali (nel formato \xHH, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento

Ogni messaggio di controllo nel registro di controllo registra dati specifici di un evento di sistema.

Dopo l'apertura `[AUDT:` contenitore che identifica il messaggio stesso, il set successivo di attributi fornisce informazioni sull'evento o sull'azione descritta dal messaggio di controllo. Questi attributi sono evidenziati nel seguente esempio:

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRs
KJA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(CSTR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\] \[UUID\(CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

IL `ATYP` elemento (sottolineato nell'esempio) identifica quale evento ha generato il messaggio. Questo messaggio di esempio include il"KARITÉ" codice messaggio ([ATYP(FC32):SHEA]), che indica che è stato generato da una richiesta S3 HEAD riuscita.

Elementi comuni nei messaggi di audit

Tutti i messaggi di audit contengono elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	ID modulo: identificatore di quattro caratteri dell'ID modulo che ha generato il messaggio. Indica il segmento di codice all'interno del quale è stato generato il messaggio di controllo.
ANID	UI32	ID nodo: ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID . Questo ID non può essere modificato.
ASES	UI64	Identificatore della sessione di audit: nelle versioni precedenti, questo elemento indicava l'ora in cui il sistema di audit veniva inizializzato dopo l'avvio del servizio. Questo valore temporale è stato misurato in microsecondi a partire dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). **Nota:** questo elemento è obsoleto e non compare più nei messaggi di controllo.

Codice	Tipo	Descrizione
ASQN	UI64	Conteggio sequenza: nelle versioni precedenti, questo contatore veniva incrementato per ogni messaggio di controllo generato sul nodo della griglia (ANID) e reimpostato a zero al riavvio del servizio. **Nota:** questo elemento è obsoleto e non compare più nei messaggi di controllo.
ATID	UI64	ID traccia: identificatore condiviso dall'insieme dei messaggi attivati da un singolo evento.
ATIM	UI64	Timestamp: ora in cui è stato generato l'evento che ha attivato il messaggio di controllo, misurata in microsecondi a partire dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per convertire il timestamp in data e ora locali si basano sui millisecondi. Potrebbe essere necessario arrotondare o troncare il timestamp registrato. L'ora leggibile dall'uomo che appare all'inizio del messaggio di controllo nel `audit.log` il file è l'attributo ATIM nel formato ISO 8601. La data e l'ora sono rappresentate come *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , dove il `T` è un carattere stringa letterale che indica l'inizio del segmento temporale della data. *`UUUUUU`* sono microsecondi.
ATYP	FC32	Tipo di evento: identificatore di quattro caratteri dell'evento registrato. Questo regola il contenuto del "payload" del messaggio: gli attributi che sono inclusi.
AVERE	UI32	Versione: la versione del messaggio di controllo. Con l'evoluzione del software StorageGRID , le nuove versioni dei servizi potrebbero incorporare nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti del servizio AMS per elaborare messaggi provenienti da versioni precedenti dei servizi.
RSLT	FC32	Risultato: il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, viene utilizzato NONE anziché SUCS, in modo che il messaggio non venga filtrato accidentalmente.

Esempi di messaggi di audit

Puoi trovare informazioni dettagliate in ogni messaggio di controllo. Tutti i messaggi di controllo utilizzano lo stesso formato.

Di seguito è riportato un esempio di messaggio di controllo come potrebbe apparire nel `audit.log` file:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Il messaggio di controllo contiene informazioni sull'evento registrato, nonché informazioni sul messaggio di controllo stesso.

Per identificare quale evento viene registrato dal messaggio di controllo, cercare l'attributo ATYP (evidenziato di seguito):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Il valore dell'attributo ATYP è SPUT. "SPUT" rappresenta una transazione S3 PUT, che registra l'inserimento di un oggetto in un bucket.

Il seguente messaggio di controllo mostra anche il bucket a cui è associato l'oggetto:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Per scoprire quando si è verificato l'evento PUT, annotare il timestamp UTC (Universal Coordinated Time) all'inizio del messaggio di controllo. Questo valore è una versione leggibile dall'uomo dell'attributo ATIM del messaggio di controllo stesso:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"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, trascorso dall'inizio dell'epoca UNIX. Nell'esempio, il valore `1405631878959669` si traduce in giovedì 17-lug-2014 21:17:59 UTC.

Messaggi di audit e ciclo di vita degli oggetti

Quando vengono generati i messaggi di audit?

I messaggi di controllo vengono generati ogni volta che un oggetto viene acquisito, recuperato o eliminato. È possibile identificare queste transazioni nel registro di controllo individuando i messaggi di controllo specifici dell'API S3.

I messaggi di controllo sono collegati tramite identificatori specifici per ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (secchio), S3KY (chiave) o entrambi
Collegamento delle operazioni Swift	WCON (contenitore), WOBJ (oggetto) o entrambi
Collegamento delle operazioni interne	CBID (identificatore interno dell'oggetto)

Tempistica dei messaggi di audit

A causa di fattori quali le differenze di temporizzazione tra i nodi della griglia, le dimensioni degli oggetti e i ritardi di rete, l'ordine dei messaggi di controllo generati dai diversi servizi può variare da quello mostrato negli esempi di questa sezione.

Transazioni di acquisizione di oggetti

È possibile identificare le transazioni di acquisizione del client nel registro di controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di acquisizione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

Messaggi di controllo di acquisizione S3

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione di acquisizione S3 PUT è stata completata correttamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regole dell'oggetto soddisfatte	Per questo oggetto è stata soddisfatta la politica ILM.	CBID	"ORLM: Regole dell'oggetto soddisfatte"

Messaggi di controllo di acquisizione rapida

Codice	Nome	Descrizione	Traccia	Vedere
WPUT	Transazione PUT rapida	Una transazione di acquisizione Swift PUT è stata completata con successo.	CBID, WCON, WOBJ	"WPUT: PUT rapido"
ORLM	Regole dell'oggetto soddisfatte	Per questo oggetto è stata soddisfatta la politica ILM.	CBID	"ORLM: Regole dell'oggetto soddisfatte"

Esempio: acquisizione di oggetti S3

La serie di messaggi di controllo riportata di seguito è un esempio dei messaggi di controllo generati e salvati nel registro di controllo quando un client S3 acquisisce un oggetto in un nodo di archiviazione (servizio LDR).

In questo esempio, la policy ILM attiva include la regola ILM Crea 2 copie.

> Non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione di acquisizione S3 (SPUT).

In questo esempio si presuppone che sia stato precedentemente creato un bucket S3.

SPUT: S3 PUT

Il messaggio SPUT viene generato per indicare che è stata emessa una transazione S3 PUT per creare un oggetto in un bucket specifico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_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 dell'oggetto soddisfatte

Il messaggio ORLM indica che la policy ILM è stata soddisfatta per questo oggetto. Il messaggio include il CBID dell'oggetto e il nome della regola ILM applicata.

Per gli oggetti replicati, il campo LOCS include l'ID del nodo LDR e l'ID del volume delle posizioni degli oggetti.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Per gli oggetti con codice di cancellazione, il campo LOCS include l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Il campo PATH include informazioni sul bucket S3 e sulla chiave oppure informazioni sul contenitore Swift e sull'oggetto, a seconda dell'API utilizzata.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
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 controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

S3 elimina i messaggi di controllo

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta effettuata per eliminare l'oggetto da un bucket.	CBID, S3KY	"SDEL: S3 ELIMINA"

Eliminazione rapida dei messaggi di controllo

Codice	Nome	Descrizione	Traccia	Vedere
WDEL	Eliminazione rapida	Richiesta effettuata per eliminare l'oggetto da un contenitore o il contenitore stesso.	CBID, WOBJ	"WDEL: CANCELLA rapida"

Esempio: eliminazione dell'oggetto S3

Quando un client S3 elimina un oggetto da un nodo di archiviazione (servizio LDR), viene generato un messaggio di controllo che viene salvato nel registro di controllo.

> Nell'esempio seguente non sono elencati tutti i messaggi di controllo generati durante una transazione di eliminazione. Sono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: Elimina S3

L'eliminazione dell'oggetto inizia quando il client invia una richiesta DeleteObject a un servizio LDR. Il messaggio contiene il bucket da cui eliminare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificarlo.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(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 controllo individuando i messaggi di controllo specifici dell'API S3.

Non tutti i messaggi di controllo generati durante una transazione di recupero sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di recupero.

Messaggi di controllo del recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta effettuata per recuperare un oggetto da un bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Messaggi di controllo di recupero rapido

Codice	Nome	Descrizione	Traccia	Vedere
WGET	GET rapido	Richiesta effettuata per recuperare un oggetto da un contenitore.	CBID, WCON, WOBJ	"WGET: GET rapido"

Esempio: recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di archiviazione (servizio LDR), viene generato un messaggio di controllo che viene salvato nel registro di controllo.

Si noti che non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti inizia quando il client invia una richiesta GetObject a un servizio LDR. Il messaggio contiene il bucket da cui recuperare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificarlo.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):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 del bucket lo consente, un client può recuperare oggetti in modo anonimo oppure può recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di controllo contiene informazioni sull'account tenant del proprietario del bucket, in modo da poter monitorare queste richieste anonime e tra account.

Nel seguente messaggio di esempio, il client invia una richiesta GetObject per un oggetto archiviato in un bucket di cui non è proprietario. I valori per SBAI e SBAC registrano l'ID e il nome dell'account tenant del proprietario del bucket, che differiscono dall'ID e dal nome dell'account tenant del client registrati in S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):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 Seleziona su un oggetto

Quando un client S3 emette una query S3 Select su un oggetto, vengono generati messaggi di controllo che vengono salvati nel registro di controllo.

Si noti che non tutti i messaggi di controllo generati durante una transazione sono elencati nell'esempio seguente. Sono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

Ogni query genera due messaggi di controllo: uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "select") e una successiva operazione GET standard che recupera i dati dall'archivio durante l'elaborazione.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messaggi di aggiornamento dei metadati

I messaggi di controllo vengono generati quando un client S3 aggiorna i metadati di un oggetto.

Messaggi di controllo dell'aggiornamento dei metadati S3

Codice	Nome	Descrizione	Traccia	Vedere
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati per un oggetto acquisito.	CBID, S3KY, HTRH	"SUPD: Metadati S3 aggiornati"

Esempio: aggiornamento dei metadati S3

L'esempio mostra una transazione riuscita per aggiornare i metadati di un oggetto S3 esistente.

SUPD: Aggiornamento metadati S3

Il client S3 effettua una richiesta (SUPD) per aggiornare i metadati specificati(`x-amz-meta-\*`) per l'oggetto S3 (S3KY). In questo esempio, le intestazioni delle richieste sono incluse nel campo HTRH perché è stato configurato come intestazione del protocollo di controllo (**CONFIGURAZIONE** > **Monitoraggio** > **Server di controllo e syslog**). Vedere "Configurare i messaggi di controllo e le destinazioni dei registri" .

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):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]]
```

Messaggi di controllo

Descrizioni dei messaggi di audit

Nelle sezioni seguenti sono elencate descrizioni dettagliate dei messaggi di controllo restituiti dal sistema. Ogni messaggio di controllo viene prima elencato in una tabella che raggruppa i messaggi correlati in base alla classe di attività che il messaggio rappresenta. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit, sia per selezionare il tipo desiderato di filtraggio dei messaggi di audit.

I messaggi di controllo sono inoltre elencati in ordine alfabetico in base ai rispettivi codici di quattro caratteri. Questo elenco alfabetico consente di trovare informazioni su messaggi specifici.

I codici a quattro caratteri utilizzati in questo capitolo sono i valori ATYP presenti nei messaggi di controllo, come mostrato nel seguente messaggio di esempio:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Per informazioni sull'impostazione dei livelli dei messaggi di controllo, sulla modifica delle destinazioni dei registri e sull'utilizzo di un server syslog esterno per le informazioni di controllo, vedere"Configurare i messaggi di controllo e le destinazioni dei registri"

Categorie di messaggi di audit

Messaggi di controllo del sistema

I messaggi di audit appartenenti alla categoria di audit del sistema vengono utilizzati per eventi correlati al sistema di audit stesso, agli stati dei nodi della griglia, alle attività delle attività a livello di sistema (attività della griglia) e alle operazioni di backup del servizio.

Codice	Titolo e descrizione del messaggio	Vedere
ECMC	Frammento di dati con codice di cancellazione mancante: indica che è stato rilevato un frammento di dati con codice di cancellazione mancante.	"ECMC: frammento di dati codificato in modo cancellabile mancante"
ECOC	Frammento di dati con codice di cancellazione danneggiato: indica che è stato rilevato un frammento di dati con codice di cancellazione danneggiato.	"ECOC: Frammento di dati corrotti con codice di cancellazione"
ETAF	Autenticazione di sicurezza non riuscita: un tentativo di connessione tramite Transport Layer Security (TLS) non è riuscito.	"ETAF: Autenticazione di sicurezza non riuscita"
GNRG	Registrazione GNDS: un servizio che aggiorna o registra informazioni su se stesso nel sistema StorageGRID .	"GNRG: Registrazione GNDS"
GNUR	Annullamento della registrazione GNDS: un servizio ha annullato la registrazione dal sistema StorageGRID .	"GNUR: Annullamento della registrazione GNDS"
GTED	Attività di griglia terminata: il servizio CMN ha terminato l'elaborazione dell'attività di griglia.	"GTED: attività di griglia terminata"
GTST	Attività di griglia avviata: il servizio CMN ha iniziato a elaborare l'attività di griglia.	"GTST: Attività di griglia avviata"
GTSU	Attività di griglia inviata: un'attività di griglia è stata inviata al servizio CMN.	"GTSU: compito di griglia inviato"

Codice	Titolo e descrizione del messaggio	Vedere
LLST	Posizione persa: questo messaggio di controllo viene generato quando una posizione viene persa.	"LLST: Posizione persa"
OLST	Oggetto perso: l'oggetto richiesto non può essere individuato nel sistema StorageGRID .	"OLST: il sistema ha rilevato un oggetto smarrito"
SADD	Disattivazione controllo di sicurezza: la registrazione dei messaggi di controllo è stata disattivata.	"SADD: Disabilitazione controllo sicurezza"
SADE	Abilitazione controllo di sicurezza: la registrazione dei messaggi di controllo è stata ripristinata.	"SADE: Abilitazione controllo sicurezza"
SVRF	Verifica fallita dell'archivio oggetti: un blocco di contenuto non ha superato i controlli di verifica.	"SVRF: Errore di verifica dell'archivio oggetti"
SVRU	Verifica archivio oggetti sconosciuta: rilevati dati oggetto inattesi nell'archivio oggetti.	"SVRU: Verifica archivio oggetti sconosciuto"
SYSD	Arresto del nodo: è stato richiesto un arresto.	"SYSD: arresto del nodo"
SISTEMA	Arresto del nodo: un servizio ha avviato un arresto regolare.	"SYST: Arresto del nodo"
SIST	Avvio nodo: un servizio avviato; la natura dell'arresto precedente è indicata nel messaggio.	"SYSU: Avvio del nodo"

Messaggi di controllo dell'archiviazione degli oggetti

I messaggi di controllo appartenenti alla categoria di controllo dell'archiviazione degli oggetti vengono utilizzati per gli eventi correlati all'archiviazione e alla gestione degli oggetti all'interno del sistema StorageGRID . Tra questi rientrano l'archiviazione e il recupero di oggetti, i trasferimenti da nodo griglia a nodo griglia e le verifiche.

> I codici di controllo vengono rimossi dal prodotto e dalla documentazione quando le funzionalità diventano obsolete. Se riscontri un codice di controllo non elencato qui, controlla le versioni precedenti di questo argomento per le versioni SG più vecchie. Ad esempio, "Messaggi di controllo dell'archiviazione degli oggetti StorageGRID 11.8" .

Codice	Descrizione	Vedere
FRATELLO	Richiesta di sola lettura del bucket: un bucket è entrato o uscito dalla modalità di sola lettura.	"BROR: Richiesta di sola lettura del bucket"

Codice	Descrizione	Vedere
CBSE	Fine invio oggetto: l'entità sorgente ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	"CBSE: Fine invio oggetto"
CBRE	Fine ricezione oggetto: l'entità di destinazione ha completato un'operazione di trasferimento dati da nodo griglia a nodo griglia.	"CBRE: Oggetto Ricevente Fine"
CGRR	Richiesta di replica tra griglie: StorageGRID ha tentato un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglia.	"CGRR: richiesta di replicazione tra griglie"
EBDL	Eliminazione bucket vuoto: lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione di bucket vuoto).	"EBDL: Eliminazione bucket vuoto"
EBKR	Richiesta di bucket vuoto: un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).	"EBKR: Richiesta bucket vuoto"
SCMT	Commit dell'archivio oggetti: un blocco di contenuto è stato completamente archiviato e verificato e ora può essere richiesto.	"SCMT: richiesta di commit dell'archivio oggetti"
SREM	Rimozione archivio oggetti: un blocco di contenuto è stato eliminato da un nodo della griglia e non può più essere richiesto direttamente.	"SREM: Rimozione dell'archivio oggetti"

Il cliente ha letto i messaggi di controllo

I messaggi di controllo di lettura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
S3SL	Richiesta S3 Select: registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.	Cliente S3	"S3SL: Richiesta di selezione S3"

Codice	Descrizione	Utilizzato da	Vedere
SGET	S3 GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	Cliente S3	"SGET: S3 GET"
KARITÉ	S3 HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Cliente S3	"SHEA: TESTA S3"
WGET	Swift GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un contenitore.	Cliente Swift	"WGET: GET rapido"
WHEA	Swift HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un contenitore.	Cliente Swift	"WHEA: TESTA Veloce"

Il cliente scrive messaggi di audit

I messaggi di controllo di scrittura del client vengono registrati quando un'applicazione client S3 effettua una richiesta per creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Sovrascrittura oggetto: registra una transazione per sovrascrivere un oggetto con un altro oggetto.	Client S3 e Swift	"OVWR: sovrascrittura oggetto"
SDEL	S3 DELETE: registra una transazione riuscita per eliminare un oggetto o un bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	Cliente S3	"SDEL: S3 ELIMINA"
SPOS	S3 POST: registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Cliente S3	"SPOS: S3 POST"
SPUT	S3 PUT: registra una transazione riuscita per creare un nuovo oggetto o bucket. **Nota:** se la transazione opera su una sottorisorsa, il messaggio di controllo includerà il campo S3SR.	Cliente S3	"SPUT: S3 PUT"
SUPD	Metadati S3 aggiornati: registra una transazione riuscita per aggiornare i metadati per un oggetto o un bucket esistente.	Cliente S3	"SUPD: Metadati S3 aggiornati"

Codice	Descrizione	Utilizzato da	Vedere
WDEL	Swift DELETE: registra una transazione riuscita per eliminare un oggetto o un contenitore.	Cliente Swift	"WDEL: CANCELLA rapida"
WPUT	Swift PUT: registra una transazione riuscita per creare un nuovo oggetto o contenitore.	Cliente Swift	"WPUT: PUT rapido"

Messaggio di controllo di gestione

La categoria Gestione registra le richieste degli utenti nell'API di gestione.

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di controllo dell'API di gestione: un registro delle richieste degli utenti.	"MGAU: Messaggio di audit di gestione"

Messaggi di controllo ILM

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per eventi correlati alle operazioni di gestione del ciclo di vita delle informazioni (ILM).

Codice	Titolo e descrizione del messaggio	Vedere
IDEL	Eliminazione avviata da ILM: questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: ILM ha avviato l'eliminazione"
LKCU	Pulizia degli oggetti sovrascritti. Questo messaggio di controllo viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di archiviazione.	"LKCU: Pulizia degli oggetti sovrascritti"
ORLM	Regole oggetto soddisfatte: questo messaggio di controllo viene generato quando i dati dell'oggetto vengono archiviati come specificato dalle regole ILM.	"ORLM: Regole dell'oggetto soddisfatte"

Riferimento al messaggio di audit

BROR: Richiesta di sola lettura del bucket

Il servizio LDR genera questo messaggio di controllo quando un bucket entra o esce dalla modalità di sola lettura. Ad esempio, un bucket entra in modalità di sola lettura mentre tutti gli oggetti vengono eliminati.

Codice	Campo	Descrizione
BKHD	UUID del bucket	L'ID del bucket.

Codice	Campo	Descrizione
BROV	Valore della richiesta di sola lettura del bucket	Se il bucket viene reso di sola lettura o sta abbandonando lo stato di sola lettura (1 = di sola lettura, 0 = non di sola lettura).
FRATELLI	Motivo di sola lettura del bucket	Il motivo per cui il bucket viene reso di sola lettura o abbandona lo stato di sola lettura. Ad esempio, emptyBucket.
S3AI	ID account tenant S3	ID dell'account tenant che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.

CBRB: Oggetto Ricevi Inizio

Durante il normale funzionamento del sistema, i blocchi di contenuto vengono trasferiti continuamente tra diversi nodi man mano che i dati vengono consultati, replicati e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo a un altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo conteggio sequenziale richiesto. Se l'operazione ha esito positivo, il trasferimento inizia da questo conteggio sequenziale.
CTES	Conteggio previsto della sequenza finale	Indica l'ultimo conteggio sequenziale richiesto. In caso di esito positivo, il trasferimento è considerato completato quando è stato ricevuto questo conteggio sequenziale.

Codice	Campo	Descrizione
RSLT	Stato di inizio del trasferimento	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato con successo.

Questo messaggio di controllo indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo contenuto, come identificato dal suo identificatore del blocco di contenuto. L'operazione richiede i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale previsto". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e, se combinate con i messaggi di controllo dell'archiviazione, per verificare i conteggi delle repliche.

CBRE: Oggetto Ricevente Fine

Quando il trasferimento di un blocco di contenuto da un nodo a un altro è completato, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il conteggio della sequenza in cui è iniziato il trasferimento.
CTAS	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio sequenziale trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è andato a buon fine, non è stato scambiato alcun dato.

Codice	Campo	Descrizione
RSLT	Risultato del trasferimento	Il risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: trasferimento completato con successo; tutti i conteggi delle sequenze richiesti sono stati inviati. CONL: connessione persa durante il trasferimento CTMO: timeout della connessione durante l'avvio o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di controllo indica che è stata completata un'operazione di trasferimento dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale effettivo". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se abbinato ai messaggi di controllo dell'archiviazione, può essere utilizzato anche per verificare i conteggi delle repliche.

CBSB: Inizio invio oggetto

Durante il normale funzionamento del sistema, i blocchi di contenuto vengono trasferiti continuamente tra diversi nodi man mano che i dati vengono consultati, replicati e conservati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo a un altro, questo messaggio viene emesso dall'entità sorgente.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.

Codice	Campo	Descrizione
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo conteggio sequenziale richiesto. Se l'operazione ha esito positivo, il trasferimento inizia da questo conteggio sequenziale.
CTES	Conteggio previsto della sequenza finale	Indica l'ultimo conteggio sequenziale richiesto. In caso di esito positivo, il trasferimento è considerato completato quando è stato ricevuto questo conteggio sequenziale.
RSLT	Stato di inizio del trasferimento	Stato al momento dell'avvio del trasferimento: SUCS: trasferimento avviato con successo.

Questo messaggio di controllo indica che è stata avviata un'operazione di trasferimento dati da nodo a nodo su un singolo contenuto, come identificato dal suo identificatore del blocco di contenuto. L'operazione richiede i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale previsto". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e, se combinate con i messaggi di controllo dell'archiviazione, per verificare i conteggi delle repliche.

CBSE: Fine invio oggetto

Quando il trasferimento di un blocco di contenuto da un nodo a un altro è completato, questo messaggio viene emesso dall'entità sorgente.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione da nodo a nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità sorgente	ID nodo dell'origine (mittente) del trasferimento CBID.
CTDS	Entità di destinazione	ID del nodo di destinazione (ricevitore) del trasferimento CBID.

Codice	Campo	Descrizione
CTSS	Avvia conteggio sequenza	Indica il conteggio della sequenza in cui è iniziato il trasferimento.
CTAS	Conteggio effettivo della sequenza finale	Indica l'ultimo conteggio sequenziale trasferito correttamente. Se il conteggio effettivo della sequenza finale è uguale al conteggio della sequenza iniziale e il risultato del trasferimento non è andato a buon fine, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Il risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato con successo; tutti i conteggi delle sequenze richiesti sono stati inviati. CONL: connessione persa durante il trasferimento CTMO: timeout della connessione durante l'avvio o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di controllo indica che è stata completata un'operazione di trasferimento dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Conteggio sequenza iniziale" a "Conteggio sequenza finale effettivo". I nodi di invio e ricezione sono identificati dai rispettivi ID nodo. Queste informazioni possono essere utilizzate per monitorare il flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se abbinato ai messaggi di controllo dell'archiviazione, può essere utilizzato anche per verificare i conteggi delle repliche.

CGRR: richiesta di replicazione tra griglie

Questo messaggio viene generato quando StorageGRID tenta un'operazione di replica tra griglie per replicare oggetti tra bucket in una connessione di federazione di griglie.

Codice	Campo	Descrizione
CSIZ	Dimensione dell'oggetto	La dimensione dell'oggetto in byte. L'attributo CSIZ è stato introdotto in StorageGRID 11.8. Di conseguenza, le richieste di replica tra griglie che coprono un aggiornamento StorageGRID dalla versione 11.7 alla 11.8 potrebbero avere una dimensione totale degli oggetti non accurata.
S3AI	ID account tenant S3	ID dell'account tenant proprietario del bucket da cui viene replicato l'oggetto.

Codice	Campo	Descrizione
GFID	ID di connessione della federazione di rete	ID della connessione di federazione della griglia utilizzata per la replica tra griglie.
OPER	operazione CGR	Tipo di operazione di replicazione tra griglie tentata: • 0 = Replica oggetto • 1 = Replica oggetto multiparte • 2 = Replica elimina marcatore
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket.
VSID	ID versione	ID della versione specifica di un oggetto che è stato replicato.
RSLT	Codice risultato	Restituisce un errore riuscito (SUCS) o generale (GERR).

EBDL: Eliminazione bucket vuoto

Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione di svuotamento del bucket).

Codice	Campo	Descrizione
CSIZ	Dimensione dell'oggetto	La dimensione dell'oggetto in byte.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
RSLT	Risultato dell'operazione di eliminazione	Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, viene utilizzato NONE anziché SUCS, in modo che il messaggio non venga filtrato accidentalmente.

EBKR: Richiesta bucket vuoto

Questo messaggio indica che un utente ha inviato una richiesta per attivare o disattivare un bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).

Codice	Campo	Descrizione
COSTRUIRE	UUID del bucket	L'ID del bucket.
EBJS	Configurazione JSON del bucket vuoto	Contiene il JSON che rappresenta la configurazione corrente del bucket vuoto.
S3AI	ID account tenant S3	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.

ECMC: frammento di dati codificato in modo cancellabile mancante

Questo messaggio di controllo indica che il sistema ha rilevato un frammento di dati mancante con codice di cancellazione.

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il blocco mancante.
MCID	ID del blocco	L'identificatore del frammento mancante con codice di cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo specifico messaggio. Viene utilizzato 'NONE' anziché 'SUCS' in modo che il messaggio non venga filtrato.

ECOC: Frammento di dati corrotti con codice di cancellazione

Questo messaggio di controllo indica che il sistema ha rilevato un frammento di dati con codice di cancellazione corrotto.

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco danneggiato.
VLID	ID volume	Il volume RangeDB che contiene il frammento con codice di cancellazione danneggiato.

Codice	Campo	Descrizione
CCID	ID del blocco	L'identificatore del frammento corrotto con codice di cancellazione.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo specifico messaggio. Viene utilizzato 'NONE' anziché 'SUCS' in modo che il messaggio non venga filtrato.

ETAF: Autenticazione di sicurezza non riuscita

Questo messaggio viene generato quando un tentativo di connessione tramite Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP su cui l'autenticazione non è riuscita.
RUID	Identità utente	Un identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.
RSLT	Codice motivo	Motivo del fallimento: SCNI: Impossibile stabilire una connessione sicura. CERM: Certificato mancante. CERT: Il certificato non è valido. CERE: Il certificato è scaduto. CERR: Il certificato è stato revocato. CSGN: la firma del certificato non è valida. CSGU: Il firmatario del certificato era sconosciuto. UCRM: le credenziali utente erano mancanti. UCRI: Le credenziali utente non erano valide. UCRU: Le credenziali utente non erano consentite. TOUT: Autenticazione scaduta.

Quando viene stabilita una connessione a un servizio sicuro che utilizza TLS, le credenziali dell'entità remota vengono verificate utilizzando il profilo TLS e la logica aggiuntiva integrata nel servizio. Se l'autenticazione fallisce a causa di certificati o credenziali non validi, inattesi o non consentiti, viene registrato un messaggio di controllo. Ciò consente di effettuare query su tentativi di accesso non autorizzati e altri problemi di connessione correlati alla sicurezza.

Il messaggio potrebbe essere causato da un'entità remota con una configurazione errata o da tentativi di presentare al sistema credenziali non valide o non consentite. Questo messaggio di controllo deve essere monitorato per rilevare tentativi di accesso non autorizzato al sistema.

GNRG: Registrazione GNDS

Il servizio CMN genera questo messaggio di controllo quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID .

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUCS: Riuscito • SUNV: Servizio non disponibile • GERR: Altro fallimento
GNID	Nodo ID	ID nodo del servizio che ha avviato la richiesta di aggiornamento.
GNTP	Tipo di dispositivo	Il tipo di dispositivo del nodo della griglia (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello del dispositivo del nodo della griglia nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo della griglia (nel contesto dei costi dei collegamenti e della classificazione delle query di servizio).
GNIA	Indirizzo IP	L'indirizzo IP del nodo della griglia.

Questo messaggio viene generato ogni volta che un nodo della griglia aggiorna la propria voce nel Grid Nodes Bundle.

GNUR: Annullamento della registrazione GNDS

Il servizio CMN genera questo messaggio di controllo quando un servizio dispone di informazioni non registrate su se stesso dal sistema StorageGRID .

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUCS: Riuscito • SUNV: Servizio non disponibile • GERR: Altro fallimento
GNID	Nodo ID	ID nodo del servizio che ha avviato la richiesta di aggiornamento.

GTED: attività di griglia terminata

Questo messaggio di controllo indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e ha spostato l'attività nella tabella Cronologica. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato il messaggio di controllo corrispondente Grid Task Started. Gli altri risultati indicano che l'elaborazione di questa attività di griglia non è mai iniziata.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita. **Nota:** l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.
RSLT	Risultato	Il risultato finale dello stato dell'attività della griglia: • SUCS: L'attività della griglia è stata completata con successo. • ABRT: L'attività della griglia è stata terminata senza un errore di rollback. • ROLF: L'attività di griglia è stata terminata e non è stato possibile completare il processo di rollback. • CANC: l'attività della griglia è stata annullata dall'utente prima di essere avviata. • EXPR: L'attività della griglia è scaduta prima di essere avviata. • IVLD: L'attività della griglia non era valida. • AUTH: L'attività di griglia non era autorizzata. • DUPL: l'attività della griglia è stata rifiutata come duplicata.

GTST: Attività di griglia avviata

Questo messaggio di controllo indica che il servizio CMN ha iniziato a elaborare l'attività di griglia specificata. Il messaggio di controllo segue immediatamente il messaggio Grid Task Submitted per le attività della griglia avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inviate alla tabella In sospeso, questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita. **Nota:** l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: • SUCS: L'attività della griglia è stata avviata correttamente.

GTSU: compito di griglia inviato

Questo messaggio di controllo indica che un'attività di griglia è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	Identifica in modo univoco un'attività di griglia generata e consente di gestirla durante il suo ciclo di vita. **Nota:** l'ID attività viene assegnato al momento della generazione di un'attività della griglia, non al momento dell'invio. È possibile che una determinata attività della griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di controllo Inviato, Iniziato e Terminato.
TTYP	Tipo di attività	Il tipo di attività della griglia.
TVER	Versione dell'attività	Un numero che indica la versione dell'attività della griglia.
TDSC	Descrizione dell'attività	Una descrizione leggibile dall'uomo dell'attività della griglia.
IVA	Valido dopo il timestamp	Il momento più remoto (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui l'attività della griglia è valida.
VBTS	Valido prima del timestamp	L'ultima ora (UINT64 microsecondi dal 1° gennaio 1970 - ora UNIX) in cui l'attività della griglia è valida.

Codice	Campo	Descrizione
TSRC	Fonte	La fonte del compito: • TXTB: l'attività della griglia è stata inviata tramite il sistema StorageGRID come blocco di testo firmato. • GRIGLIA: l'attività della griglia è stata inviata tramite il servizio interno di invio delle attività della griglia.
ACTV	Tipo di attivazione	Il tipo di attivazione: • AUTO: l'attività della griglia è stata inviata per l'attivazione automatica. • PEND: l'attività della griglia è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per la sorgente TXTB.
RSLT	Risultato	Il risultato dell'invio: • SUCS: L'attività della griglia è stata inviata correttamente. • FAIL: l'attività è stata spostata direttamente nella tabella storica.

IDEL: ILM ha avviato l'eliminazione

Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto.

Il messaggio IDEL viene generato in una di queste situazioni:

- **Per gli oggetti nei bucket S3 conformi**: questo messaggio viene generato quando ILM avvia il processo di eliminazione automatica di un oggetto perché il suo periodo di conservazione è scaduto (presupponendo che l'impostazione di eliminazione automatica sia abilitata e la conservazione legale sia disattivata).
- **Per gli oggetti nei bucket S3 non conformi**. Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto perché nessuna istruzione di posizionamento nei criteri ILM attivi è attualmente applicabile all'oggetto.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Conformità: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), indica se un oggetto conforme deve essere eliminato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale.
CMPL	Conformità: Conservazione legale	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), indica se il bucket è attualmente sottoposto a un blocco legale.

Codice	Campo	Descrizione
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. Durata del periodo di conservazione dell'oggetto in minuti.
CTME	Conformità: tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Tempo di ingestione dell'oggetto. È possibile aggiungere a questo valore il periodo di conservazione in minuti per determinare quando l'oggetto può essere eliminato dal bucket.
DMRK	Elimina ID versione marcatore	ID versione del marcatore di eliminazione creato durante l'eliminazione di 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.
LOCATION	Posizioni	Posizione di archiviazione dei dati degli oggetti all'interno del sistema StorageGRID . Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato eliminato). CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione applicati ai dati dell'oggetto. CLDI: per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID del nodo ARC della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
RSLT	Risultato	Il risultato dell'operazione ILM. SUCS: L'operazione ILM ha avuto successo.
REGOLA	Etichetta delle regole	• Se un oggetto in un bucket S3 conforme viene eliminato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. • Se l'oggetto viene eliminato perché non ci sono più istruzioni di posizionamento applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM applicata all'oggetto.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.

Codice	Campo	Descrizione
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto che è stato eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

LKCU: Pulizia degli oggetti sovrascritti

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza necessitava di essere ripulito per liberare spazio di archiviazione. Un oggetto viene sovrascritto quando un client S3 scrive un oggetto in un percorso che contiene già un oggetto. Il processo di rimozione avviene automaticamente e in background.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LTYP	Tipo di pulizia	*Solo per uso interno.*
LUID	UUID dell'oggetto rimosso	L'identificatore dell'oggetto che è stato rimosso.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Identificatore univoco universale	L'identificatore dell'oggetto che esiste ancora. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

LKDM: Pulizia degli oggetti trapelati

Questo messaggio viene generato quando un blocco trapelato viene pulito o eliminato. Un blocco può essere parte di un oggetto replicato o di un oggetto codificato tramite cancellazione.

Codice	Campo	Descrizione
OROLOGIO	Posizione del blocco	Il percorso del file del frammento trapelato che è stato eliminato.

CTYP	Tipo di blocco	Tipo di pezzo:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

LTYP	Tipo di perdita	I cinque tipi di perdite che possono essere rilevate:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Tempo di creazione del blocco	Ora in cui è stato creato il frammento trapelato.
UUID	Identificatore univoco universale	L’identificatore dell’oggetto a cui appartiene il blocco.
CBID	Identificatore del blocco di contenuto	CBID dell’oggetto a cui appartiene il frammento trapelato.
CSIZ	Dimensione del contenuto	La dimensione del blocco in byte.

LLST: Posizione persa

Questo messaggio viene generato ogni volta che non è possibile trovare la posizione per una copia di un oggetto (replicata o con codice di cancellazione).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.
ECPR	Profilo di codifica di cancellazione	Per dati di oggetti codificati tramite cancellazione. ID del profilo di codifica di cancellazione utilizzato.
LTYP	Tipo di posizione	CLDI (online): per dati di oggetti replicati CLEC (online): per dati di oggetti codificati con cancellazione CLNL (Nearline): per dati di oggetti replicati archiviati
NOID	ID nodo sorgente	L'ID del nodo su cui sono andate perse le posizioni.
PCLD	Percorso verso l'oggetto replicato	Il percorso completo alla posizione del disco in cui si trovano i dati dell'oggetto perso. Restituito solo quando LTYP ha un valore di CLDI (ovvero, per oggetti replicati). Prende la forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Risultato	Sempre NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.
TSRC	Sorgente di attivazione	UTENTE: attivato dall'utente SYST: Sistema attivato
UUID	ID univoco universale	Identificatore dell'oggetto interessato nel sistema StorageGRID .

MGAU: Messaggio di audit di gestione

La categoria Gestione registra le richieste degli utenti nell'API di gestione. Ogni richiesta HTTP che non sia una richiesta GET o HEAD a un URI API valido registra una risposta contenente il nome utente, l'IP e il tipo di richiesta all'API. Gli URI API non validi (ad esempio /api/v3-authorize) e le richieste non valide agli URI API validi non vengono registrati.

Codice	Campo	Descrizione
MDIP	Indirizzo IP di destinazione	L'indirizzo IP del server (destinazione).
MDNA	Nome di dominio	Il nome di dominio dell'host.

Codice	Campo	Descrizione
MPAT	Richiedi PATH	Il percorso della richiesta.
MPQP	Richiedi parametri di query	I parametri di query per la richiesta.
MRBD	Corpo della richiesta	Il contenuto del corpo della richiesta. Mentre il corpo della risposta viene registrato per impostazione predefinita, il corpo della richiesta viene registrato in alcuni casi quando il corpo della risposta è vuoto. Poiché le seguenti informazioni non sono disponibili nel corpo della risposta, vengono ricavate dal corpo della richiesta per i seguenti metodi POST: • Nome utente e ID account in **POST authorize** • Nuova configurazione delle subnet in **POST /grid/grid-networks/update** • Nuovi server NTP in **POST /grid/ntp-servers/update** • ID server dismessi in **POST /grid/servers/decommission** **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	Metodo di richiesta HTTP: • INVIARE • METTERE • ELIMINARE • TOPPA
MRSC	Codice di risposta	Il codice di risposta.
Prezzo consigliato al pubblico	Corpo della risposta	Per impostazione predefinita, il contenuto della risposta (il corpo della risposta) viene registrato. **Nota:** le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).
MSIP	Indirizzo IP di origine	L'indirizzo IP del client (sorgente).
MUUN	URN utente	L'URN (nome uniforme della risorsa) dell'utente che ha inviato la richiesta.

Codice	Campo	Descrizione
RSLT	Risultato	Restituisce l'esito positivo (SUCS) oppure l'errore segnalato dal backend.

OLST: il sistema ha rilevato un oggetto smarrito

Questo messaggio viene generato quando il servizio DDS non riesce a individuare alcuna copia di un oggetto all'interno del sistema StorageGRID .

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto smarrito.
NOID	Nodo ID	Se disponibile, l'ultima posizione nota, diretta o prossima alla linea, dell'oggetto smarrito. È possibile avere solo l'ID nodo senza un ID volume se le informazioni sul volume non sono disponibili.
SENTIERO	Secchio/chiave S3	Se disponibili, il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.
UUID	ID univoco universale	Identificatore dell'oggetto smarrito all'interno del sistema StorageGRID .
VOLI	ID volume	Se disponibile, l'ID volume del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

ORLM: Regole dell'oggetto soddisfatte

Questo messaggio viene generato quando l'oggetto viene archiviato e copiato correttamente come specificato dalle regole ILM.

> Il messaggio ORLM non viene generato quando un oggetto viene archiviato correttamente dalla regola predefinita Crea 2 copie se un'altra regola nel criterio utilizza il filtro avanzato Dimensione oggetto.

Codice	Campo	Descrizione
COSTRUIRE	Testata della benna	Campo ID bucket. Utilizzato per operazioni interne. Appare solo se STAT è PRGD.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCATION	Posizioni	Posizione di archiviazione dei dati degli oggetti all'interno del sistema StorageGRID . Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato eliminato). CLEC: per gli oggetti con codifica di cancellazione, l'ID del profilo di codifica di cancellazione e l'ID del gruppo di codifica di cancellazione applicati ai dati dell'oggetto. CLDI: per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID del nodo ARC della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
SENTIERO	Secchio/chiave S3	Nome del bucket S3 e nome della chiave S3.
RSLT	Risultato	Il risultato dell'operazione ILM. SUCS: L'operazione ILM ha avuto successo.
REGOLA	Etichetta delle regole	Etichetta leggibile dall'uomo assegnata alla regola ILM applicata a questo oggetto.
SEGC	UUID del contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	Contenitore CBID	CBID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo per oggetti segmentati e multiparte.
STATISTICHE	Stato	Lo stato di funzionamento dell'ILM. FATTO: le operazioni ILM sull'oggetto sono state completate. DFER: L'oggetto è stato contrassegnato per una futura rivalutazione ILM. PRGD: L'oggetto è stato eliminato dal sistema StorageGRID . NLOC: i dati dell'oggetto non sono più disponibili nel sistema StorageGRID . Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.

Codice	Campo	Descrizione
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

Il messaggio di controllo ORLM può essere emesso più di una volta per un singolo oggetto. Ad esempio, viene emesso ogni volta che si verifica uno dei seguenti eventi:

- Le regole ILM per l'oggetto sono soddisfatte per sempre.
- Per questa epoca sono soddisfatte le regole ILM per l'oggetto.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati dell'oggetto replicato è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto danneggiato.

Informazioni correlate

- "Transazioni di acquisizione di oggetti"
- "Transazioni di eliminazione degli oggetti"

OVWR: sovrascrittura oggetto

Questo messaggio viene generato quando un'operazione esterna (richiesta dal client) causa la sovrascrittura di un oggetto da parte di un altro oggetto.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto (nuovo)	Il CBID del nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto sovrascritto.
Disturbo ossessivo-compulsivo (OCBD)	Identificatore del blocco di contenuto (precedente)	Il CBID dell'oggetto precedente.
UUID	ID univoco universale (nuovo)	Identificatore del nuovo oggetto all'interno del sistema StorageGRID .

Codice	Campo	Descrizione
OUID	ID univoco universale (precedente)	Identificatore dell'oggetto precedente all'interno del sistema StorageGRID .
SENTIERO	Percorso oggetto S3	Il percorso dell'oggetto S3 utilizzato sia per l'oggetto precedente che per quello nuovo
RSLT	Codice risultato	Risultato della transazione di sovrascrittura dell'oggetto. Il risultato è sempre: SUCS: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.

S3SL: Richiesta di selezione S3

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere dettagli sul messaggio di errore e sul codice di errore. La richiesta potrebbe non essere andata a buon fine.

Codice	Campo	Descrizione
BYSC	Byte scansionati	Numero di byte scansionati (ricevuti) dai nodi di archiviazione. È probabile che BYSC e BYPR siano diversi se l'oggetto è compresso. Se l'oggetto è compresso, BYSC avrà il conteggio dei byte compressi e BYPR i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "Byte scansionati" sono stati effettivamente elaborati o utilizzati da un processo S3 Select.
BYRT	Byte restituiti	Numero di byte restituiti al client da un processo S3 Select.
RIPRISTINO	Record elaborati	Numero di record o righe che un processo S3 Select ha ricevuto dai nodi di archiviazione.
RERT	Record restituiti	Numero di record o righe che un processo S3 Select ha restituito al client.
JOFI	Lavoro terminato	Indica se l'elaborazione del lavoro S3 Select è terminata o meno. Se questo è falso, il lavoro non è stato completato e i campi di errore probabilmente conterranno dei dati. Il cliente potrebbe aver ricevuto risultati parziali o nessun risultato.
REID	ID richiesta	Identificatore per la richiesta S3 Select.

Codice	Campo	Descrizione
EXTM	Tempo di esecuzione	Tempo, in secondi, impiegato per completare il processo S3 Select.
ERMG	Messaggio di errore	Messaggio di errore generato dal processo S3 Select.
ERTY	Tipo di errore	Tipo di errore generato dal processo S3 Select.
PRIMO	Stacktrace degli errori	Stacktrace di errore generato dal processo S3 Select.
S3BK	Secchio S3	Nome del bucket S3.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 dell'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket.

SADD: Disabilitazione controllo sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di controllo; i messaggi di controllo non vengono più raccolti o recapitati.

Codice	Campo	Descrizione
AETM	Abilita metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Nome utente che ha eseguito il comando per disabilitare la registrazione degli audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.

Il messaggio implica che la registrazione era precedentemente abilitata, ma ora è stata disabilitata. In genere, questa opzione viene utilizzata solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. Dopo l'attività di massa, l'audit viene ripristinato (SADE) e la possibilità di disabilitarlo viene bloccata in modo permanente.

SADE: Abilitazione controllo sicurezza

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione dei messaggi di controllo; i messaggi di controllo vengono nuovamente raccolti e recapitati.

Codice	Campo	Descrizione
AETM	Abilita metodo	Il metodo utilizzato per abilitare l'audit.
AEUN	Nome utente	Nome utente che ha eseguito il comando per abilitare la registrazione di controllo.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato NONE anziché SUCS in modo che questo messaggio non venga filtrato.

Il messaggio implica che la registrazione era stata precedentemente disabilitata (SADD), ma ora è stata ripristinata. In genere, questa opzione viene utilizzata solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. Dopo l'attività di massa, l'audit viene ripristinato e la possibilità di disabilitarlo viene bloccata in modo permanente.

SCMT: Commit dell'archivio oggetti

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato finché non viene eseguito il commit (ovvero finché non viene memorizzato in modo persistente). Il contenuto memorizzato in modo persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene visualizzato quando un blocco di contenuto viene salvato nell'archivio.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto impegnato nell'archiviazione permanente.
RSLT	Codice risultato	Stato al momento in cui l'oggetto è stato memorizzato sul disco: SUCS: Oggetto memorizzato correttamente.

Questo messaggio significa che un determinato blocco di contenuto è stato completamente archiviato e verificato e ora può essere richiesto. Può essere utilizzato per tracciare il flusso di dati all'interno del sistema.

SDEL: S3 ELIMINA

Quando un client S3 emette una transazione DELETE, viene effettuata una richiesta per rimuovere l'oggetto o il bucket specificato oppure per rimuovere una sotto-risorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto eliminato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marcatore	ID versione del marcatore di eliminazione creato durante l'eliminazione di un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
GFID	ID di connessione della federazione di griglia	ID di connessione della federazione di griglia associata a una richiesta di eliminazione della replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
GFSA	ID account sorgente della federazione di griglia	ID account del tenant sulla griglia di origine per una richiesta di eliminazione della replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `` `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). `` `x-amz-bypass-governance-retention`viene incluso automaticamente se presente nella richiesta.
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione DELETE. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.

Codice	Campo	Descrizione
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUDM	Identificatore univoco universale per un marcatore di eliminazione	L'identificatore di un marcatore di eliminazione. I messaggi del registro di controllo specificano UUDM o UUID, dove UUDM indica un marcatore di eliminazione creato in seguito a una richiesta di eliminazione di un oggetto e UUID indica un oggetto.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto che è stato eliminato. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SGET: S3 GET

Quando un client S3 emette una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket, oppure per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
LITÀ	ListObjectsV2	È stata richiesta una risposta in formato *v2*. Per i dettagli, vedere "AWS ListObjectsV2" . Solo per operazioni bucket GET.
NCHD	Numero di bambini	Include chiavi e prefissi comuni. Solo per operazioni bucket GET.
RANG	Lettura dell'intervallo	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) indica la dimensione dell'intero oggetto.
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
Repubblica Ceca del Nord	Troncato o non troncato	Impostare su false se sono stati restituiti tutti i risultati. Impostare su true se sono disponibili più risultati da restituire. Solo per operazioni bucket GET.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SHEA: TESTA S3

Quando un client S3 emette una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un oggetto o di un bucket e recuperare i metadati relativi a un oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto controllato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `` `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). ``
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SPOS: S3 POST

Quando un client S3 invia una richiesta POST Object, questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). (Non previsto per SPOS).
RSLT	Codice risultato	Risultato della richiesta RestoreObject. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando. Impostare su "seleziona" per un'operazione di selezione S3.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	L'ID della versione specifica di un oggetto richiesto. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SPUT: S3 PUT

Quando un client S3 emette una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket oppure per rimuovere una sotto-risorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di conformità	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	ID di connessione della federazione di griglia	ID di connessione della federazione di griglia associata a una richiesta PUT di replicazione tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
GFSA	ID account sorgente della federazione di griglia	ID account del tenant sulla griglia di origine per una richiesta PUT di replica tra griglie. Incluso solo nei registri di controllo sulla griglia di destinazione.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). `x-amz-bypass-governance-retention`viene incluso automaticamente se presente nella richiesta.

Codice	Campo	Descrizione
LKEN	Blocco oggetto abilitato	Valore dell'intestazione della richiesta `x-amz-bucket-object-lock-enabled` , se presente nella richiesta.
LKLH	Blocco oggetto in attesa legale	Valore dell'intestazione della richiesta `x-amz-object-lock-legal-hold` , se presente nella richiesta PutObject.
LKMD	Modalità di mantenimento del blocco degli oggetti	Valore dell'intestazione della richiesta `x-amz-object-lock-mode` , se presente nella richiesta PutObject.
LKRU	Blocco oggetto Conserva fino alla data	Valore dell'intestazione della richiesta `x-amz-object-lock-retain-until-date` , se presente nella richiesta PutObject. I valori sono limitati a 100 anni dalla data in cui l'oggetto è stato ingerito.
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUCS: Riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	Sottorisorsa S3	Se applicabile, il bucket o la sottorisorsa oggetto su cui si sta operando.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.

Codice	Campo	Descrizione
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
ULID	Carica ID	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.
VSST	Stato di controllo delle versioni	Il nuovo stato di controllo delle versioni di un bucket. Vengono utilizzati due stati: "abilitato" o "sospeso". Le operazioni sugli oggetti non includono questo campo.

SREM: Rimozione dell'archivio oggetti

Questo messaggio viene visualizzato quando il contenuto viene rimosso dall'archiviazione persistente e non è più accessibile tramite le API standard.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto eliminato dalla memoria permanente.
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è: SUCS: Contenuto rimosso dall'archiviazione persistente

Questo messaggio di controllo indica che un determinato blocco di contenuto è stato eliminato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tracciare il flusso di contenuti eliminati all'interno del sistema.

SUPD: Metadati S3 aggiornati

Questo messaggio viene generato dall'API S3 quando un client S3 aggiorna i metadati per un oggetto acquisito. Il messaggio viene emesso dal server se l'aggiornamento dei metadati ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione di controllo della coerenza	Valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, durante l'aggiornamento delle impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore di sistema univoco per la connessione TCP/IP.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUCS: riuscito
S3AI	ID account tenant S3 (mittente della richiesta)	ID dell'account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3AK	ID chiave di accesso S3 (mittente della richiesta)	ID della chiave di accesso S3 con hash per l'utente che ha inviato la richiesta. Un valore vuoto indica un accesso anonimo.
S3BK	Secchio S3	Nome del bucket S3.
S3KY	Chiave S3	Nome della chiave S3, escluso il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome dell'account tenant S3 (mittente della richiesta)	Nome dell'account tenant dell'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (mittente della richiesta)	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SBAC	Nome dell'account tenant S3 (proprietario del bucket)	Nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso multiaccount o anonimo.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario del bucket)	ID dell'account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso multiaccount o anonimo.
SUSR	URN utente S3 (mittente della richiesta)	L'ID dell'account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o un utente LDAP. Ad esempio: `urn:sgws:identity::03393893651506583485:root` Vuoto per richieste anonime.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
VSID	ID versione	ID della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni sui bucket e sugli oggetti nei bucket senza versione non includono questo campo.

SVRF: Errore di verifica dell'archivio oggetti

Questo messaggio viene visualizzato ogni volta che un blocco di contenuto non supera il processo di verifica. Ogni volta che i dati degli oggetti replicati vengono letti o scritti sul disco, vengono eseguiti diversi controlli di verifica e integrità per garantire che i dati inviati all'utente richiedente siano identici ai dati originariamente inseriti nel sistema. Se uno di questi controlli fallisce, il sistema mette automaticamente in quarantena i dati dell'oggetto replicato corrotti per impedirne il recupero.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto che non ha superato la verifica.

Codice	Campo	Descrizione
RSLT	Codice risultato	Tipo di errore di verifica: CRCF: Controllo di ridondanza ciclico (CRC) non riuscito. HMAC: controllo del codice di autenticazione dei messaggi basato su hash (HMAC) non riuscito. EHSH: Hash del contenuto crittografato inaspettato. PHSH: Hash del contenuto originale inaspettato. SEQC: sequenza di dati errata sul disco. PERR: Struttura non valida del file su disco. DERR: Errore del disco. FNAM: Nome file errato.

Questo messaggio deve essere monitorato attentamente. Gli errori nella verifica del contenuto possono indicare imminenti guasti hardware.

Per determinare quale operazione ha attivato il messaggio, vedere il valore del campo AMID (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, ovvero una verifica in background, mentre STOR indica che il messaggio è stato attivato dal recupero del contenuto.

SVRU: Verifica archivio oggetti sconosciuto

Il componente di archiviazione del servizio LDR esegue continuamente la scansione di tutte le copie dei dati degli oggetti replicati nell'archivio oggetti. Questo messaggio viene visualizzato quando una copia sconosciuta o imprevista di dati di oggetti replicati viene rilevata nell'archivio oggetti e spostata nella directory di quarantena.

Codice	Campo	Descrizione
FPTH	Percorso del file	Percorso del file della copia dell'oggetto inaspettato.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo del messaggio obbligatorio, ma non è rilevante per questo messaggio. Viene utilizzato 'NONE' anziché 'SUCS' in modo che il messaggio non venga filtrato.

Il messaggio di controllo SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie inaspettate di dati oggetto nell'archivio oggetti. Questa situazione dovrebbe essere indagata immediatamente per stabilire come sono state create queste copie, perché potrebbe indicare imminenti guasti hardware.

SYSD: arresto del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto l'arresto. In genere questo messaggio viene inviato solo dopo un successivo riavvio, perché la coda dei messaggi di controllo non viene cancellata prima dell'arresto. Se il servizio non è stato riavviato, cercare il messaggio SYST, inviato all'inizio della sequenza di arresto.

Codice	Campo	Descrizione
RSLT	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente.

Il messaggio non indica se il server host è stato arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno spegnimento "sporco", perché il messaggio viene generato solo da spegnimenti "puliti".

SYST: Arresto del nodo

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto l'arresto e che il servizio ha avviato la sequenza di arresto. SYST può essere utilizzato per determinare se l'arresto è stato richiesto prima del riavvio del servizio (a differenza di SYSD, che in genere viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente.

Il messaggio non indica se il server host è stato arrestato, ma solo il servizio di reporting. Il codice RSLT di un messaggio SYST non può indicare uno spegnimento "sporco", perché il messaggio viene generato solo da spegnimenti "puliti".

SYSU: Avvio del nodo

Quando un servizio viene riavviato, questo messaggio viene generato per indicare se l'arresto precedente è stato pulito (comandato) o disordinato (inaspettato).

Codice	Campo	Descrizione
RSLT	Arresto pulito	La natura della chiusura: SUCS: Il sistema è stato spento correttamente. DSDN: Il sistema non è stato arrestato correttamente. VRGN: il sistema è stato avviato per la prima volta dopo l'installazione (o la reinstallazione) del server.

Il messaggio non indica se il server host è stato avviato, ma solo il servizio di reporting. Questo messaggio può essere utilizzato per:

- Rilevare discontinuità nella traccia di controllo.
- Determinare se un servizio non funziona correttamente durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio non riuscito.

WDEL: CANCELLA rapida

Quando un client Swift emette una transazione DELETE, viene effettuata una richiesta per rimuovere l'oggetto o il contenitore specificato. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto eliminato in byte. Le operazioni sui contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DELETE. Il risultato è sempre: SUCS: Riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.

Codice	Campo	Descrizione
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni sui contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WGET: GET rapido

Quando un client Swift emette una transazione GET, viene effettuata una richiesta per recuperare un oggetto, elencare gli oggetti in un contenitore o elencare i contenitori in un account. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni su account e contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni su account e contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WHEA: TESTA Veloce

Quando un client Swift emette una transazione HEAD, viene effettuata una richiesta per verificare l'esistenza di un account, di un contenitore o di un oggetto e recuperare eventuali metadati rilevanti. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni su account e contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni su account e contenitori non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
RSLT	Codice risultato	Risultato della transazione HEAD. Il risultato è sempre: SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift. Le operazioni sui conti non includono questo campo.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni su account e contenitori non includono questo campo.
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

WPUT: PUT rapido

Quando un client Swift emette una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o contenitore. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto richiesto. Se il CBID è sconosciuto, questo campo è impostato su 0. Le operazioni sui contenitori non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui contenitori non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrate, selezionati durante la configurazione. `X-Forwarded-For`viene automaticamente incluso se è presente nella richiesta e se il `X-Forwarded-For` il valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
MTME	Ultima modifica	Timestamp Unix, in microsecondi, che indica quando l'oggetto è stato modificato l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUCS: riuscito
SAIP	Indirizzo IP del client richiedente	L'indirizzo IP dell'applicazione client che ha effettuato la richiesta.
TEMPO	Tempo	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciatore di carico attendibile	Se la richiesta è stata instradata da un bilanciatore del carico di Livello 7 attendibile, l'indirizzo IP del bilanciatore del carico.
UUID	Identificatore univoco universale	Identificatore dell'oggetto all'interno del sistema StorageGRID .
WACC	ID account Swift	ID account univoco specificato dal sistema StorageGRID .
WCON	Contenitore rapido	Nome del contenitore Swift.
WOBJ	Oggetto rapido	Identificatore dell'oggetto Swift. Le operazioni sui contenitori non includono questo campo.

Codice	Campo	Descrizione
WUSR	Utente dell'account Swift	Il nome utente dell'account Swift che identifica in modo univoco il cliente che esegue la transazione.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI 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.