



# **Esaminare i registri di audit**

StorageGRID software

NetApp

February 12, 2026

# Sommario

Esaminare i registri di audit .....	1
Messaggi e registri di controllo .....	1
Controllare il flusso e la conservazione dei messaggi .....	1
Controllare il flusso dei messaggi .....	1
Accedere al file di log di audit .....	4
Controllo della rotazione del file di log .....	5
Formato del file di log di audit .....	5
Formato del file di log di audit .....	6
Utilizzare lo strumento di verifica e spiegazione .....	7
Utilizzare lo strumento audit-sum .....	9
Formato del messaggio di audit .....	18
Formato del messaggio di audit .....	18
Tipi di dati .....	19
Dati specifici dell'evento .....	19
Elementi comuni nei messaggi di audit .....	20
Esempi di messaggi di audit .....	21
Messaggi di audit e ciclo di vita degli oggetti .....	23
Quando vengono generati i messaggi di audit? .....	23
Transazioni di acquisizione degli oggetti .....	23
Transazioni di eliminazione degli oggetti .....	25
Transazioni di recupero degli oggetti .....	26
Messaggi di aggiornamento dei metadati .....	28
Messaggi di audit .....	29
Descrizioni dei messaggi di controllo .....	29
Controllare le categorie dei messaggi .....	30
Riferimento del messaggio di audit .....	34

# Esaminare i registri di audit

## Messaggi e registri di controllo

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

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

Per utilizzare il file di log di testo, è necessario disporre dell'accesso alla condivisione di audit configurata nel nodo di amministrazione.

Per informazioni sulla configurazione dei livelli dei messaggi di controllo e sull'utilizzo di un server syslog esterno, vedere ["Configurare la gestione dei log e il server syslog esterno"](#).

## Controllare il flusso e la conservazione dei messaggi

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. È necessario comprendere in che modo questi messaggi di controllo passano dal sistema StorageGRID al `audit.log` file.

I seguenti flussi di lavoro per i messaggi di controllo e la conservazione dei messaggi di controllo sono applicabili solo se StorageGRID è configurato per **Nodi amministrativi/nodi locali** o **Nodo amministrativo e server syslog esterno**. Se StorageGRID è configurato per "Solo nodi locali" (predefinito) o "Server syslog esterno", i messaggi di controllo vengono salvati localmente su ciascun nodo nel `/var/local/log/localaudit.log` file e non può essere elaborato dai nodi di amministrazione o dai nodi di archiviazione.

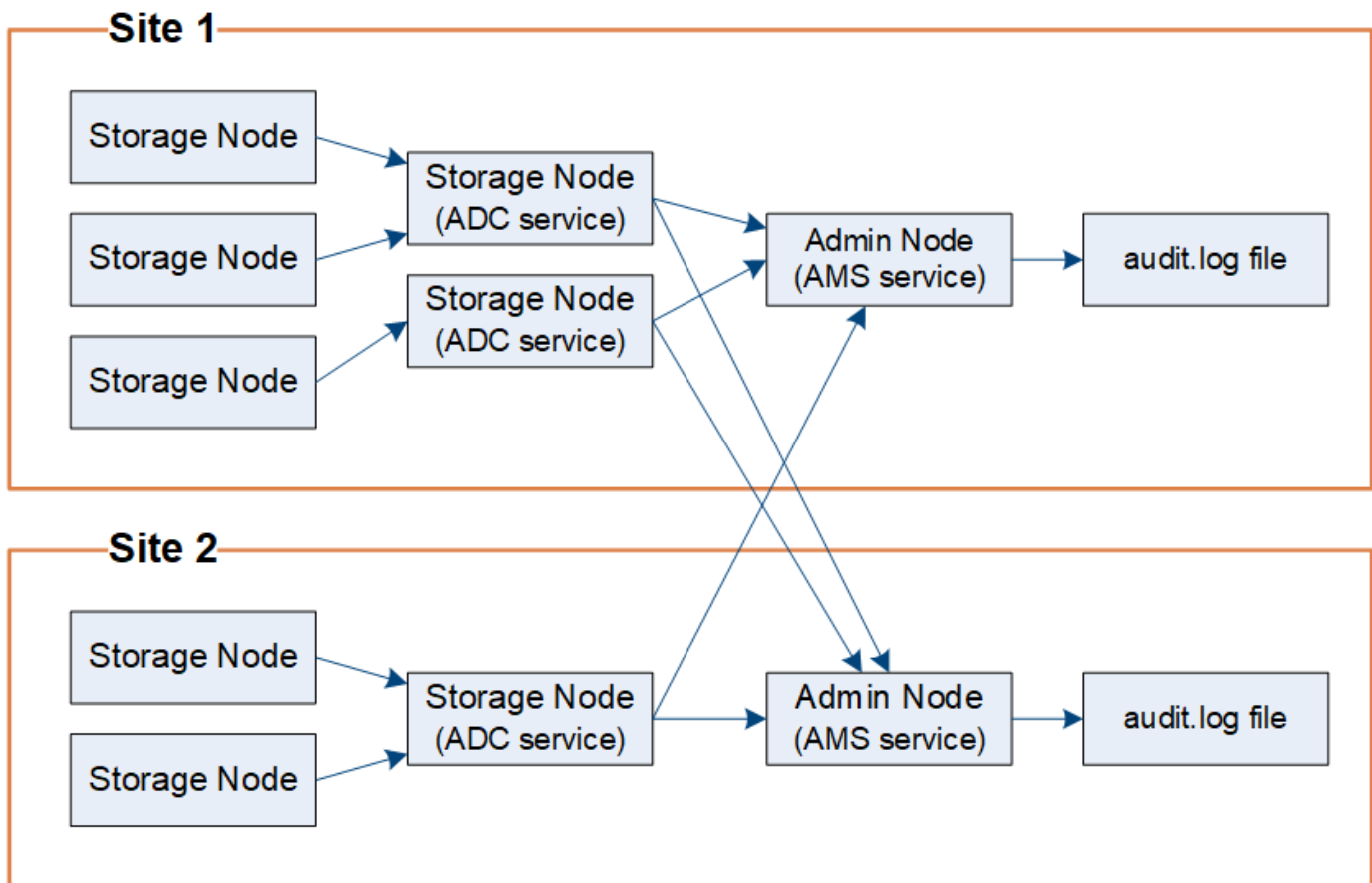
### Controllare il flusso dei messaggi

I messaggi di controllo vengono elaborati dai nodi amministrativi quando StorageGRID è configurato per **nodi amministrativi/nodi locali** o **nodo amministrativo e server syslog esterno** e dai nodi di archiviazione che dispongono di un servizio di controller di dominio amministrativo (ADC).

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

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

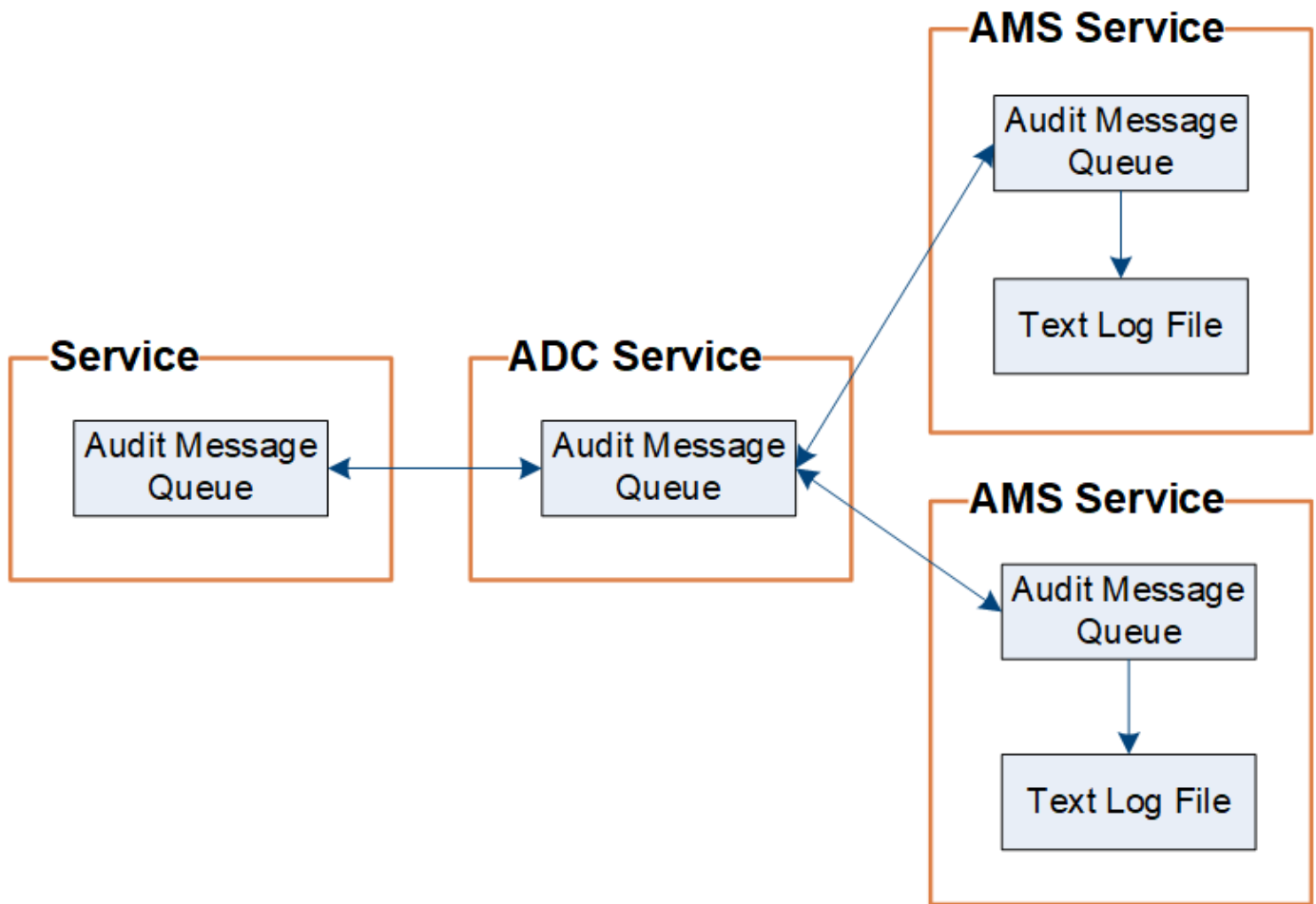
Ogni nodo amministrativo memorizza i messaggi di controllo in file di registro di testo; il file di registro attivo è denominato `audit.log`.



### Controllare la conservazione dei messaggi

StorageGRID utilizza un processo di copia e cancellazione per garantire che non vengano persi messaggi di controllo prima di poter essere scritti nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di 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/audit/export` 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 danno priorità all'elaborazione del loro arretrato e diventano temporaneamente non disponibili per nuovi messaggi.

In particolare, potrebbero verificarsi i seguenti comportamenti:

- Se il `/var/local/audit/export` Quando la directory utilizzata da un nodo di amministrazione diventa piena, il nodo di amministrazione viene contrassegnato come non disponibile per nuovi messaggi di controllo finché la directory non è 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 viene contrassegnato come non disponibile per i messaggi di controllo finché la directory non è 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 vi sono nodi di archiviazione disponibili con il servizio ADC, i nodi di archiviazione memorizzano i messaggi di controllo localmente nel `/var/local/log/localaudit.log` file.

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

I seguenti tipi di problemi possono causare un aumento delle code dei messaggi di audit:

- Interruzione di un nodo amministrativo o di un nodo di storage con il servizio ADC. Se uno dei nodi del sistema non è attivo, i nodi rimanenti potrebbero diventare backlogged.
- Tasso di attività sostenuta che supera la capacità di audit del sistema.
- Lo `/var/local/` spazio su un nodo di archiviazione ADC si riempie per motivi non correlati ai messaggi di controllo. In questo caso, il nodo smette di accettare nuovi messaggi di audit e assegna la priorità al backlog corrente, che può causare backlog su altri nodi.

### Avviso di coda di audit estesa e allarme di messaggi di audit in coda (AMQS)

Per facilitare il monitoraggio delle dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Large audit queue** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda Storage Node o Admin Node raggiunge determinate soglie.

Se viene attivato l'avviso **Large audit queue** o l'allarme AMQS legacy, iniziare controllando il carico sul sistema. Se si è verificato un numero significativo di transazioni recenti, l'avviso e l'allarme devono essere risolti nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di 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 la gestione dei log e il server syslog esterno"](#).

### Messaggi duplicati

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

## Accedere al file di log di audit

La condivisione di controllo contiene il file attivo `audit.log` ed eventuali file di registro di controllo compressi. È possibile accedere ai file di log di controllo direttamente dalla riga di comando del nodo amministrativo.

IL `audit.log` il file rimane vuoto a meno che non si configuri StorageGRID per **Nodi amministrativi/nodi locali** o **Nodo amministrativo e server syslog esterno**. Per ulteriori informazioni, fare riferimento a ["Seleziona la posizione del registro"](#).

### Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- È necessario disporre del `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

### Fasi

1. Accedere a un nodo amministratore:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla directory principale: `su -`

d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Accedere alla directory contenente i file di log di controllo:

```
cd /var/local/audit/export/
```

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

## Controllo della rotazione del file di log

Se StorageGRID è configurato per **Nodi amministrativi/nodi locali** o **Nodo amministrativo e server syslog esterno**, i file dei registri di controllo vengono salvati nel nodo amministrativo `/var/local/audit/export/` 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. Fare riferimento a ["Configurare i messaggi di controllo e il server syslog esterno"](#).

Una volta al giorno, il file attivo `audit.log` viene salvato e viene avviato un nuovo `audit.log` file. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`. Se in un solo giorno vengono creati più log di controllo, i nomi dei file utilizzano la data in cui il file è stato salvato, seguita da un numero, nel formato `yyyy-mm-dd.txt.n`. Ad esempio, `2018-04-15.txt` e `2018-04-15.txt.1` sono il primo e il secondo file di 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, lo spazio di archiviazione del nodo di amministrazione assegnato ai registri di controllo viene consumato. 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/audit/export/` elenco. I registri di controllo vengono eliminati in base alla data in cui sono stati creati. I registri più vecchi vengono eliminati per primi. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

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

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

## Formato del file di log di audit

## Formato del file di log di audit

I file di log di audit si trovano in ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di audit.

Ogni messaggio di audit contiene quanto segue:

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

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

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

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



2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):S3RQ][ATID(UI64):13489590586043706682]]
```

Nel loro formato predefinito, i messaggi di audit nei file di log di audit non sono facili da leggere o interpretare. È possibile utilizzare ["tool di verifica-spiegazione"](#) per ottenere riepiloghi semplificati dei messaggi di controllo nel registro di controllo. È possibile utilizzare ["tool audit-sum"](#) per riepilogare il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.

## Utilizzare lo strumento di verifica e spiegazione

È possibile utilizzare `audit-explain` lo strumento per convertire i messaggi di controllo nel registro di controllo in un formato di facile lettura.

## Prima di iniziare

- Si dispone di "autorizzazioni di accesso specifiche".
- È necessario disporre del `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

## A proposito di questa attività

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



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

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

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Lo `audit-explain` strumento può effettuare le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

```
audit-explain audit.log
```

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

- Elaborazione simultanea di più file. Ad esempio:

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

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

- Accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando il `grep` comando o altri mezzi. Ad 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 eseguire `audit-explain` sulle parti, anziché sull'intero file.



``audit-explain`` Lo strumento non accetta file compressi come input di pipeline. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando o utilizzare ``zcat`` lo strumento per decomprimere prima i file. Ad esempio:

```
zcat audit.log.gz | audit-explain
```

Utilizzare l' ``help (-h)`` opzione per visualizzare le opzioni disponibili. Ad esempio:

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

## Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

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

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



Per ridurre le lunghezze delle linee e agevolare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se si desidera visualizzare i timestamp, utilizzare l' ``-t`` opzione timestamp ).

## Utilizzare lo strumento audit-sum

È possibile utilizzare `audit-sum` lo strumento per contare i messaggi di controllo di scrittura, lettura, testa ed eliminazione e per visualizzare il tempo (o le dimensioni) minimo, massimo e medio per ogni tipo di operazione.

### Prima di iniziare

- Si dispone di "autorizzazioni di accesso specifiche".
- Si dispone del `Passwords.txt` file.
- Si conosce l'indirizzo IP del nodo di amministrazione primario.

#### A proposito di questa attività

``audit-sum`` Lo strumento, disponibile nel nodo amministrativo principale, riepiloga il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo necessario per tali operazioni.



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

Questo esempio mostra l'output tipico `audit-sum` dello strumento. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

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

IL `audit-sum` Lo strumento fornisce conteggi e orari per i seguenti messaggi di controllo S3 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 precedenti StorageGRID . Ad esempio, ["StorageGRID 11.8 Utilizzo dello strumento di somma di controllo"](#) .

Codice	Descrizione	Fare riferimento a.
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Registra quando ILM avvia il processo di eliminazione di un oggetto.	<a href="#">"IDEL: Eliminazione avviata da ILM"</a>

Codice	Descrizione	Fare riferimento a.
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: ELIMINAZIONE S3"
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	"SHEA: TESTA S3"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"

Lo `audit-sum` strumento può effettuare le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

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

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

- Elaborazione simultanea di più file. Ad esempio:

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

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

- Accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando il `grep` comando o altri mezzi. Ad esempio:

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

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

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



Questo strumento non accetta 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 o per raggruppare i riepiloghi dei messaggi in base al nome del bucket, al periodo di tempo o al tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di funzionamento minimo, massimo e medio, ma è possibile utilizzare l' `'size (-s)'` opzione per esaminare le dimensioni dell'oggetto.

Utilizzare l' `'help (-h)'` opzione per visualizzare le opzioni disponibili. Ad esempio:

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

## Fasi

### 1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

### 2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, testa ed eliminazione, attenersi alla seguente procedura:

- Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

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

Questo esempio mostra l'output tipico `audit-sum` dello strumento. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

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

In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media a 1.13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano tempi lunghi nel caso peggiore di circa 1,770 secondi.

- Per visualizzare le operazioni di recupero 10 più lente, utilizzare il comando `grep` per selezionare solo i messaggi SGET e aggiungere l'opzione di output lungo (`-l`) per includere i percorsi oggetto:

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

I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di eseguire il `grep` del log di audit per altri messaggi relativi a questi oggetti specifici.

```

Total:          201906 operations
Slowest:        1740.290 sec
Average:        1.132 sec
Fastest:        0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====
      1740289662      10.96.101.125      object      5663711385
backup/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
backup/r90l0aQ8JB-1566861764-4518.iso
      70839      10.96.101.125      object      28338
bucket3/dat.1566861764-6619
      68487      10.96.101.125      object      27890
bucket3/dat.1566861764-6615
      67798      10.96.101.125      object      27671
bucket5/dat.1566861764-6617
      67027      10.96.101.125      object      27230
bucket5/dat.1566861764-4517
      60922      10.96.101.125      object      26118
bucket3/dat.1566861764-4520
      35588      10.96.101.125      object      11311
bucket3/dat.1566861764-6616
      23897      10.96.101.125      object      10692
bucket3/dat.1566861764-4516

```

+ Da questo esempio di output, è possibile notare che le tre richieste S3 GET più lente erano per oggetti di dimensioni pari a circa 5 GB, che sono molto più grandi degli altri oggetti. Le grandi dimensioni rappresentano i tempi di recupero lenti dei casi peggiori.

3. Per determinare le dimensioni degli oggetti inseriti e recuperati dalla griglia, utilizzare l'opzione dimensioni (-s):

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

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

In questo esempio, la dimensione media degli oggetti per SPUT è inferiore a 2.5 MB, ma la dimensione media per SGET è molto maggiore. Il numero di messaggi SPUT è molto superiore al numero di messaggi SGET, a indicare che la maggior parte degli oggetti non viene mai recuperata.

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

- a. Immettere il comando nel registro di controllo appropriato e utilizzare l'opzione Group-by-Time (-gt), seguita dal periodo di tempo (ad esempio, 15M, 1H, 10S):

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



message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Questi risultati mostrano che il traffico S3 GET ha registrato un picco tra le 06:00 e le 07:00. Sia i tempi massimi che quelli medi sono considerevolmente più alti durante questo intervallo di tempo e non aumentano gradualmente con l'aumentare del conteggio. Questi parametri suggeriscono che la capacità è stata superata, probabilmente nella rete o nella capacità della griglia di elaborare le richieste.

- b. Per determinare le dimensioni degli oggetti recuperati ogni ora ieri, aggiungere l'opzione size (-s) al comando:

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

message group average(B)	count	min(B)	max(B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Questi risultati indicano che si sono verificati alcuni recuperi molto grandi quando il traffico di recupero complessivo era al massimo.

- c. Per ulteriori dettagli, utilizzare il ["tool di verifica-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 costituito da molte righe, aggiungere il `less` comando per visualizzare 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 per gli oggetti:

- a. Iniziare utilizzando l' ``-go`` opzione, che raggruppa i messaggi per le operazioni di oggetti e bucket separatamente:

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

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

I risultati mostrano che le operazioni SPUT per i bucket hanno caratteristiche di performance diverse rispetto alle operazioni SPUT per gli oggetti.

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

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

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ltd002 0.361	1564563	0.011	51.569

- c. Per determinare quali bucket hanno la dimensione massima dell'oggetto SPUT, utilizzare sia le `-gb` opzioni e `-s`:

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

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ltd002 0.352	1564563	0.000	999.972

## Formato del messaggio di audit

### Formato del messaggio di audit

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

Se le informazioni di riepilogo fornite dagli ["audit-spiegare"](#) strumenti e ["audit-sum"](#) non sono sufficienti, fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di controllo.

Di seguito viene riportato un esempio di messaggio di audit che potrebbe essere visualizzato nel file di log dell'audit:

```
2014-07-17T03:50:47.484627
[AUDT: [RSLT (FC32) :VRGN] [AVER (UI32) :10] [ATIM (UI64) :1405569047484627] [ATYP (FC32) :SYSU] [ANID (UI32) :11627225] [AMID (FC32) :ARNI] [ATID (UI64) :9445736326500603516]]
```

Ogni messaggio di audit 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 [ ]
- Introdotta 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 di attributo, un tipo di dati e un valore che vengono riportati in questo formato:

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

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

L'elenco seguente descrive gli elementi degli attributi:

- **ATTR** è un codice di quattro caratteri per l'attributo riportato. Esistono alcuni attributi comuni a tutti i messaggi di audit e ad altri specifici degli eventi.
- **type** È un identificatore di quattro caratteri del tipo di dati di programmazione del valore, come 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 audit vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero senza segno (32 bit); può memorizzare i numeri da 0 a 4,294,967,295.
UI64	Numero intero doppio senza segno (64 bit); può memorizzare i numeri da 0 a 18,446,744,073,709,551,615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32 bit rappresentato da quattro caratteri ASCII, ad esempio "ABCD".
IPAD	Utilizzato per gli indirizzi IP.
CSTR	Matrice a lunghezza variabile di caratteri UTF-8. È possibile eseguire l'escape dei caratteri con le seguenti convenzioni: <ul style="list-style-type: none"><li>• La barra rovesciata è</li><li>• Il ritorno a capo è</li><li>• Le virgolette doppie sono ".</li><li>• L'avanzamento riga (nuova riga) è il n.</li><li>• I caratteri possono essere sostituiti dai rispettivi equivalenti esadecimali (nel formato HH, dove HH è il valore esadecimale che rappresenta il carattere).</li></ul>

## Dati specifici dell'evento

Ogni messaggio di audit nel registro di audit registra i dati specifici di un evento di

sistema.

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

[illegible]

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

## Elementi comuni nei messaggi di audit

Tutti i messaggi di audit contengono gli elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	Module ID (ID modulo): Identificatore di quattro caratteri dell'ID modulo che ha generato il messaggio. Indica il segmento di codice all'interno del quale è stato generato il messaggio di audit.
ANID	UI32	Node ID (ID nodo): L'ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID. Impossibile modificare questo ID.
ASE	UI64	<p>Audit Session Identifier (identificatore sessione di audit): Nelle release precedenti, questo elemento indica l'ora in cui il sistema di audit è stato inizializzato dopo l'avvio del servizio. Questo valore di tempo è stato misurato in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970).</p> <p><b>Nota:</b> questo elemento è obsoleto e non compare più nei messaggi di audit.</p>
ASQN	UI64	<p>Sequence Count (Conteggio sequenze): Nelle release precedenti, questo contatore è stato incrementato per ogni messaggio di audit generato sul nodo della griglia (ANID) e azzerato al riavvio del servizio.</p> <p><b>Nota:</b> questo elemento è obsoleto e non compare più nei messaggi di audit.</p>

Codice	Tipo	Descrizione
ATID	UI64	Trace ID (ID traccia): Identificatore condiviso dalla serie di messaggi attivati da un singolo evento.
ATIM	UI64	<p>Timestamp: L'ora in cui è stato generato l'evento che ha attivato il messaggio di audit, misurata in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per la conversione dell'indicatore data e ora in data e ora locali si basano su millisecondi.</p> <p>Potrebbe essere richiesto l'arrotondamento o il troncamento dell'indicatore data e ora registrato. L'ora leggibile dall'uomo che appare all'inizio del messaggio di controllo nel <code>audit.log</code> file è l'attributo ATIM in formato ISO 8601. La data e l'ora sono rappresentate come <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, dove T è un carattere stringa letterale che indica l'inizio del segmento temporale della data. <code>UUUUUU</code> sono microsecondi.</p>
ATYP	FC32	Event Type (tipo di evento): Identificatore di quattro caratteri dell'evento registrato. Questo regola il contenuto "payload" del messaggio: Gli attributi che sono inclusi.
MEDIA	UI32	Version (versione): La versione del messaggio di audit. Man mano che il software StorageGRID si evolve, le nuove versioni dei servizi potrebbero incorporare nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti del servizio AMS per l'elaborazione dei messaggi provenienti da versioni precedenti dei servizi.
RSLT	FC32	Risultato: Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

## Esempi di messaggi di audit

È possibile trovare informazioni dettagliate in ciascun messaggio di audit. Tutti i messaggi di audit utilizzano lo stesso formato.

Di seguito è riportato un esempio di messaggio di controllo che potrebbe essere visualizzato 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):"s3small11"] [S3K
Y(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):0
] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SPUT
] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):1579224144
102530435]]
```

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

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [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 PUT S3 KB, che registra l'acquisizione di un oggetto in un bucket.

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR\): "s3small11"] [S3
KY(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):
0] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SPU
T] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):157922414
4102530435]]
```

Per scoprire quando si è verificato l'evento PUT, prendere nota dell'indicatore orario UTC (Universal Coordinated Time) all'inizio del messaggio di audit. Questo valore è una versione leggibile dell'attributo ATIM del messaggio di audit stesso:



**2014-07-17T21:17:58.959669**

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3KY(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):1579224144102530435]]
```

ATIM registra il tempo, in microsecondi, dall'inizio dell'epoca UNIX. Nell'esempio, il valore 1405631878959669 viene convertito in giovedì, 17-lug-2014 21:17:59:00 UTC.

## Messaggi di audit e ciclo di vita degli oggetti

### Quando vengono generati i messaggi di audit?

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

I messaggi di audit sono collegati tramite identificatori specifici di ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (bucket), S3KY (chiave) o entrambi
Collegamento delle operazioni interne	CBID (identificatore interno dell'oggetto)

### Tempistiche dei messaggi di audit

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

### Transazioni di acquisizione degli oggetti

Nell'audit log, puoi identificare le transazioni di acquisizione dei client individuando S3 messaggi di audit specifici di API.

Non tutti i messaggi di controllo generati durante una transazione di acquisizione sono elencati nella tabella seguente. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

### S3: Acquisizione di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione S3 PUT ingest è stata completata correttamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	"ORLM: Regole oggetto soddisfatte"

### Esempio: Acquisizione di oggetti S3

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

In questo esempio, il criterio ILM attivo include la regola ILM Make 2 Copies.



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

Questo esempio presuppone che sia stato precedentemente creato un bucket S3.

#### SPUT: S3 PUT

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

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID(UI64):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP(FC32):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

#### ORLM: Regole oggetto soddisfatte

Il messaggio ORLM indica che il criterio ILM è stato soddisfatto per questo oggetto. Il messaggio include il CBID dell'oggetto e il nome della regola ILM applicata.

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

2019-07-

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

Per gli oggetti sottoposti a erasure coding, il campo LOCS include l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding

2019-02-23T01:52:54.647537

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

Il campo PATH include informazioni sul bucket S3 e sulla chiave.

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 audit S3 specifici per API.

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

### S3 eliminare i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta di eliminazione dell'oggetto da un bucket.	CBID, S3KY	<a href="#">"SDEL: ELIMINAZIONE S3"</a>

### Esempio: Eliminazione di oggetti S3

Quando un client S3 elimina un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.



Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

#### SDEL: S3 Elimina

L'eliminazione degli oggetti ha inizio 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 identificare l'oggetto.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_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 audit S3 specifici per API.

Non tutti i messaggi di controllo generati durante una transazione di recupero sono elencati nella tabella seguente. Sono inclusi solo i messaggi necessari per tracciare la transazione di recupero.

#### Messaggi di controllo per il recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta di recupero di un oggetto da un bucket.	CBID, S3BK, S3KY	<a href="#">"SGET: S3 GET"</a>

### Esempio: Recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio

di audit e salvato nel registro di audit.

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

#### **SGET: S3 GET**

Il recupero degli oggetti ha inizio 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 identificare l'oggetto.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEW=="][SUSR(CSTR):"urn:sgws:identity:43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK(CSTR):"bucket-
anonymous"]\[S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP(FC32):SGE
T]\[ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se la policy bucket lo consente, un client può recuperare in modo anonimo oggetti o recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di audit contiene informazioni sull'account tenant del proprietario del bucket, in modo da poter tenere traccia di queste richieste anonime e multiaccount.

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

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
(CSTR):"17915054115450519830"]\[SACC(CSTR):"s3-account-
b"]\[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity:17915054115450519830:root"]\[SBAI(CSTR):"4397929817
8977966408"]\[SBAC(CSTR):"s3-account-a"]\[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

#### **Esempio: S3 selezionare su un oggetto**

Quando un client S3 esegue una query S3 Select su un oggetto, i messaggi di audit vengono generati e salvati nel registro di audit.

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

Ogni query genera due messaggi di audit: Uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "Select") e un'operazione GET standard successiva che recupera i dati dallo storage durante l'elaborazione.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::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 audit vengono generati quando un client S3 aggiorna i metadati di un oggetto.

### I metadati S3 aggiornano i messaggi di audit

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

## Esempio: Aggiornamento dei metadati S3

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

### SUPD: Aggiornamento dei metadati S3

Il client S3 effettua una richiesta (SUPD) per aggiornare i metadati specificati(`x-amz-meta-*`) per l'oggetto S3 (S3KY). In questo esempio, le intestazioni delle richieste sono incluse nel campo HTRH perché è stato configurato come intestazione del protocollo di controllo (`*Configurazione* > Monitoraggio > Server di controllo e syslog`). Vedere ["Configurare la gestione dei log e il server syslog esterno"](#).

```
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 audit

### Descrizioni dei messaggi di controllo

Le descrizioni dettagliate dei messaggi di controllo restituiti dal sistema sono elencate nelle sezioni seguenti. Ciascun messaggio di audit viene elencato per primo in una tabella che raggruppa i messaggi correlati in base alla classe di attività rappresentata dal messaggio. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit che per selezionare il tipo di filtro dei messaggi di audit desiderato.

I messaggi di audit sono anche elencati in ordine alfabetico in base ai codici a quattro caratteri. Questo elenco alfabetico consente di trovare informazioni su messaggi specifici.

I codici a quattro caratteri utilizzati in questo capitolo sono i valori ATYP presenti nei messaggi di 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 la gestione dei log e il server syslog esterno"](#)

## Controllare le categorie dei messaggi

### Messaggi di audit del sistema

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

Codice	Titolo e descrizione del messaggio	Vedere
ECMC	Manca un frammento di dati con erasure coding: Indica che è stato rilevato un frammento di dati con erasure coding mancante.	<a href="#">"ECMC: Frammento di dati con codice di cancellazione mancante"</a>
ECOC	Fragment di dati con erasure coding corrotto: Indica che è stato rilevato un frammento di dati sottoposto a erasure coding corrotto.	<a href="#">"ECOC: Frammento di dati con codice di cancellazione corrotto"</a>
ETAF	Autenticazione di sicurezza non riuscita: Tentativo di connessione con Transport Layer Security (TLS) non riuscito.	<a href="#">"ETAF: Autenticazione di sicurezza non riuscita"</a>
GNRG	Registrazione GNDS: Un servizio aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.	<a href="#">"GNRG: Registrazione GNDS"</a>
NUR	Annullamento registrazione GNDS: Un servizio non si è registrato dal sistema StorageGRID.	<a href="#">"GNUR: Annullamento registrazione GNDS"</a>
GTED	Grid Task Ended (attività griglia terminata): Il servizio CMN ha terminato l'elaborazione dell'attività Grid.	<a href="#">"GTED: Task Grid terminato"</a>
GTST	Grid Task Started (attività griglia avviata): Il servizio CMN ha avviato l'elaborazione dell'attività Grid.	<a href="#">"GTST: Task Grid avviato"</a>
GTSU	Grid Task Submitted (attività griglia inviata): È stata inviata un'attività Grid al servizio CMN.	<a href="#">"GTSU: Task Grid inviato"</a>



Codice	Titolo e descrizione del messaggio	Vedere
LLST	Location Lost (posizione persa): Questo messaggio di audit viene generato quando una posizione viene persa.	"LLST: Località persa"
OLST	Object Lost (oggetti persi): Non è possibile individuare un oggetto richiesto all'interno del sistema StorageGRID.	"OLST: Il sistema ha rilevato un oggetto perso"
SADD	Security Audit Disable (Disattiva controllo protezione): La registrazione del messaggio di controllo è stata disattivata.	"SADD: Disattivazione dell'audit di sicurezza"
SADE	Security Audit Enable (attiva controllo di sicurezza): La registrazione del messaggio di controllo è stata ripristinata.	"SADE: Abilitazione controllo di sicurezza"
SVRF	Verifica archivio oggetti non riuscita: Un blocco di contenuto non ha superato i controlli di verifica.	"SVRF: Verifica archivio oggetti non riuscita"
SVRU	Object Store Verify Unknown (verifica archivio oggetti sconosciuto): Dati di oggetti imprevisti rilevati nell'archivio oggetti.	"SVRU: Verifica archivio oggetti sconosciuta"
SYSD	Node Stop (arresto nodo): È stato richiesto lo spegnimento.	"SYSD: Interruzione nodo"
SIST	Node stopping (interruzione nodo): Un servizio ha avviato un'interruzione senza interruzioni.	"SYST: Interruzione del nodo"
SISU	Node Start (Avvio nodo): Un servizio avviato; la natura dello shutdown precedente viene indicata nel messaggio.	"SYSU: Avvio nodo"

### Messaggi di audit dello storage a oggetti

I messaggi di audit appartenenti alla categoria di audit dello storage a oggetti vengono utilizzati per gli eventi correlati allo storage e alla gestione degli oggetti all'interno del sistema StorageGRID. Tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione poiché le funzioni sono obsolete. Se si riscontra un codice di controllo non elencato qui, controllare le versioni precedenti di questo argomento per le versioni SG precedenti. Ad esempio, "[Messaggi di audit dello storage a oggetti StorageGRID 11,8](#)".

Codice	Descrizione	Vedere
BROR	Bucket Read Only Request (richiesta di sola lettura bucket): Un bucket è entrato o è uscito dalla modalità di sola lettura.	"BROR: Richiesta di sola lettura bucket"
CBSE	Object Send End (fine invio oggetto): L'entità di origine ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBSE: Fine invio oggetto"
CBRE	Object Receive End (fine ricezione oggetto): L'entità di destinazione ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBRE: Fine ricezione oggetto"
CGRR	Richiesta di replica cross-grid: StorageGRID ha tentato un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di grid.	"CGRR: Richiesta di replica cross-grid"
EBDL	Empty bucket Delete (Elimina bucket vuoto): Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione bucket vuoto).	"EBDL: Eliminazione bucket vuoto"
EBKR	Empty bucket Request (richiesta 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 memorizzato e verificato e può essere richiesto.	"SCMT: Richiesta di commit dell'archivio di oggetti"
SREM	Rimozione archivio oggetti: Un blocco di contenuto è stato cancellato da un nodo griglia e non può più essere richiesto direttamente.	"SREM: Rimozione dell'archivio di oggetti"

### Messaggi di audit in lettura del client

I messaggi di controllo in lettura dei client vengono registrati quando un'applicazione client S3 richiede di recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
S3SL	S3 Select request (richiesta S3 Select): Registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.	Client S3	"S3SL: Richiesta S3 Select"
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.  <b>Nota:</b> se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Client S3	"SHEA: TESTA S3"

### Messaggi di audit di scrittura del client

I messaggi di controllo in scrittura del client vengono registrati quando un'applicazione client S3 richiede di creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Object Overwrite: Registra una transazione per sovrascrivere un oggetto con un altro oggetto.	Client S3	"OVWR: Sovrascrittura degli oggetti"
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket.  <b>Nota:</b> se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SDEL: ELIMINAZIONE S3"
SPOS	S3 POST: Registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Client S3	"SPOS: POST S3"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.  <b>Nota:</b> se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SPUT: S3 PUT"
SUPD	S3 Metadata Updated: Registra una transazione riuscita per aggiornare i metadati di un oggetto o bucket esistente.	Client S3	"SUPD: Metadati S3 aggiornati"

## Messaggio di audit della gestione

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

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di audit API di gestione: Un registro delle richieste degli utenti.	<a href="#">"MGAU: Messaggio di audit della gestione"</a>

## Messaggi di controllo ILM

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per gli eventi relativi alle operazioni ILM (Information Lifecycle Management).

Codice	Titolo e descrizione del messaggio	Vedere
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	<a href="#">"IDEL: Eliminazione avviata da ILM"</a>
LKCU	Pulitura oggetto sovrascritto. Questo messaggio di audit viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di storage.	<a href="#">"LKCU: Pulitura oggetto sovrascritta"</a>
ORLM	Regole oggetto soddisfatte: Questo messaggio di audit viene generato quando i dati oggetto vengono memorizzati come specificato dalle regole ILM.	<a href="#">"ORLM: Regole oggetto soddisfatte"</a>

## Riferimento del messaggio di audit

### BROR: Richiesta di sola lettura bucket

Il servizio LDR genera questo messaggio di audit 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 cancellati.

Codice	Campo	Descrizione
BKHD	UUID bucket	L'ID bucket.
BROV	Valore della richiesta di sola lettura del bucket	Se il bucket viene reso di sola lettura o se esce dallo stato di sola lettura (1 = sola lettura, 0 = non di sola lettura).
BROS	Motivo di sola lettura del bucket	Il motivo per cui il bucket viene reso di sola lettura o viene lasciato lo stato di sola lettura. Ad esempio, emptyBucket.

Codice	Campo	Descrizione
S3AI	ID account tenant S3	L'ID dell'account tenant che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

#### CBRB: Inizio ricezione oggetto

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull:  PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente.  PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento:  SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da

"Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

#### **CBRE: Fine ricezione oggetto**

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

<b>Codice</b>	<b>Campo</b>	<b>Descrizione</b>
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull:  PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente.  PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.

Codice	Campo	Descrizione
RSLT	Risultato del trasferimento	<p>Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente):</p> <p>SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati.</p> <p>CONL: Connessione persa durante il trasferimento</p> <p>CTMO: Timeout della connessione durante la creazione o il trasferimento</p> <p>UNRE: ID nodo di destinazione non raggiungibile</p> <p>CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi</p>

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

#### **CBSB: Inizio invio oggetto**

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

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

Codice	Campo	Descrizione
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento:  SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

#### **CBSE: Fine invio oggetto**

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

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



Codice	Campo	Descrizione
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	<p>Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente):</p> <p>SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati.</p> <p>CONL: Connessione persa durante il trasferimento</p> <p>CTMO: Timeout della connessione durante la creazione o il trasferimento</p> <p>UNRE: ID nodo di destinazione non raggiungibile</p> <p>CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi</p>

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

### **CGRR: Richiesta di replica cross-grid**

Questo messaggio viene generato quando StorageGRID tenta di eseguire un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di griglie.

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	<p>La dimensione dell'oggetto in byte.</p> <p>L'attributo CSIZ è stato introdotto in StorageGRID 11,8. Di conseguenza, le richieste di replica cross-grid su un aggiornamento da StorageGRID 11,7 a 11,8 potrebbero presentare dimensioni totali degli oggetti imprecise.</p>
S3AI	ID account tenant S3	L'ID dell'account tenant proprietario del bucket da cui l'oggetto viene replicato.

Codice	Campo	Descrizione
GFID	ID connessione federazione griglia	L'ID della connessione a federazione di griglie utilizzata per la replica cross-grid.
OPER	Funzionamento CGR	Il tipo di operazione di replica cross-grid che è stata tentata: <ul style="list-style-type: none"> <li>• 0 = oggetto replicato</li> <li>• 1 = Replica oggetto multiparte</li> <li>• 2 = marcatore di eliminazione replicato</li> </ul>
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.
VSID	ID versione	L'ID versione della versione specifica di un oggetto replicato.
RSLT	Codice risultato	Restituisce Successful (SUCS) o General error (GERR).

#### EBDL: Eliminazione bucket vuoto

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

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	La dimensione dell'oggetto in byte.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'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, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

#### EBKR: Richiesta bucket vuoto

Questo messaggio indica che 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).

Codice	Campo	Descrizione
BUID (BUID)	UUID bucket	L'ID bucket.
EBJS	Configurazione JSON bucket vuoto	Contiene il JSON che rappresenta la configurazione vuota corrente del bucket.
S3AI	ID account tenant S3	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

#### **ECMC: Frammento di dati con codice di cancellazione mancante**

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

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

#### **ECOC: Frammento di dati con codice di cancellazione corrotto**

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

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco corrotto.
VLID	ID volume	Volume RangeDB contenente il frammento corrotto con codifica di cancellazione.
CCID	ID chunk	L'identificatore del frammento corrotto con codifica in cancellazione.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

#### ETAF: Autenticazione di sicurezza non riuscita

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

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP su cui l'autenticazione non è riuscita.
MALEDUCATO	Identità dell'utente	Identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.
RSLT	Codice di motivazione	<p>Il motivo del guasto:</p> <p>SCNI: Connessione sicura non riuscita.</p> <p>CERM: Certificato mancante.</p> <p>CERT: Certificato non valido.</p> <p>CERE: Certificato scaduto.</p> <p>CER: Certificato revocato.</p> <p>CSGN: Firma del certificato non valida.</p> <p>CSGU: Il firmatario del certificato non era noto.</p> <p>UCRM: Credenziali utente mancanti.</p> <p>UCRI: Credenziali utente non valide.</p> <p>UCRU: Le credenziali dell'utente non sono consentite.</p> <p>TOUT: Timeout dell'autenticazione.</p>

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

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

rilevare i tentativi di accesso non autorizzato al sistema.

### **GNRG: Registrazione GNDS**

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

<b>Codice</b>	<b>Campo</b>	<b>Descrizione</b>
RSLT	Risultato	Risultato della richiesta di aggiornamento: <ul style="list-style-type: none"><li>• SUC: Riuscito</li><li>• SUNV: Servizio non disponibile</li><li>• GERR: Altro guasto</li></ul>
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.
GNTTP	Tipo di dispositivo	Il tipo di dispositivo del nodo Grid (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello di dispositivo del nodo Grid nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo grid (nel contesto dei costi di collegamento e della classificazione delle query di servizio).
GNIA	Indirizzo IP	L'indirizzo IP del nodo della griglia.

Questo messaggio viene generato ogni volta che un nodo della griglia aggiorna la propria voce nel bundle dei nodi della griglia.

### **GNUR: Annullamento registrazione GNDS**

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

<b>Codice</b>	<b>Campo</b>	<b>Descrizione</b>
RSLT	Risultato	Risultato della richiesta di aggiornamento: <ul style="list-style-type: none"><li>• SUC: Riuscito</li><li>• SUNV: Servizio non disponibile</li><li>• GERR: Altro guasto</li></ul>
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.

#### GTED: Task Grid terminato

Questo messaggio di audit indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e che l'attività è stata spostata nella tabella Cronologia. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato un messaggio di audit Grid Task Started (attività griglia avviata) corrispondente. Gli altri risultati indicano che l'elaborazione di questa attività della griglia non è mai stata avviata.

Codice	Campo	Descrizione
TSID	ID attività	<p>Questo campo identifica in modo univoco un'attività Grid generata e consente di gestire l'attività Grid nel suo ciclo di vita.</p> <p><b>Nota:</b> l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.</p>
RSLT	Risultato	<p>Risultato finale dello stato dell'attività Grid:</p> <ul style="list-style-type: none"><li>• SUCS: L'attività Grid è stata completata correttamente.</li><li>• ABRT: L'attività Grid è stata terminata senza un errore di rollback.</li><li>• ROLF: L'attività Grid è stata terminata e non è stato possibile completare il processo di rollback.</li><li>• CANC: L'attività della griglia è stata annullata dall'utente prima dell'avvio.</li><li>• EXPR: L'attività Grid è scaduta prima dell'avvio.</li><li>• IVLD: L'attività della griglia non era valida.</li><li>• AUTH: L'attività della rete non è stata autorizzata.</li><li>• DUPL: L'attività Grid è stata rifiutata come duplicata.</li></ul>

#### GTST: Task Grid avviato

Questo messaggio di audit indica che il servizio CMN ha avviato l'elaborazione dell'attività Grid specificata. Il messaggio di audit segue immediatamente il messaggio Grid Task Submitted per le attività Grid avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inoltrate nella tabella Pending (in sospeso), questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	<p>Questo campo identifica in maniera univoca un'attività grid generata e consente di gestirne l'intero ciclo di vita.</p> <p><b>Nota:</b> l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.</p>
RSLT	Risultato	<p>Il risultato. Questo campo ha un solo valore:</p> <ul style="list-style-type: none"> <li>• SUCS: L'attività Grid è stata avviata correttamente.</li> </ul>

### GTSU: Task Grid inviato

Questo messaggio di audit indica che un'attività Grid è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	<p>Identifica in modo univoco un'attività grid generata e consente di gestarla per l'intero ciclo di vita.</p> <p><b>Nota:</b> l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.</p>
TTIP	Tipo di attività	Il tipo di attività della griglia.
VER	Versione attività	Un numero che indica la versione dell'attività Grid.
TDSC	Descrizione dell'attività	Una descrizione leggibile dell'attività Grid.
VAT	Valido dopo l'indicatore di data e ora	Il primo tempo (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui l'attività grid è valida.
VBTS	Valido prima dell'indicatore di data e ora	L'ultima ora (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui è valida l'attività grid.

Codice	Campo	Descrizione
TSRC	Origine	<p>L'origine dell'attività:</p> <ul style="list-style-type: none"> <li>• TXTB: L'attività Grid è stata inviata tramite il sistema StorageGRID come blocco di testo firmato.</li> <li>• GRID: L'attività Grid è stata inviata tramite il Grid Task Submission Service interno.</li> </ul>
ACTV	Tipo di attivazione	<p>Il tipo di attivazione:</p> <ul style="list-style-type: none"> <li>• AUTO: L'attività della griglia è stata inviata per l'attivazione automatica.</li> <li>• PEND: L'attività Grid è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per l'origine TXTB.</li> </ul>
RSLT	Risultato	<p>Risultato dell'invio:</p> <ul style="list-style-type: none"> <li>• SUCS: L'attività Grid è stata inviata correttamente.</li> <li>• ERRORE: L'attività è stata spostata direttamente nella tabella storica.</li> </ul>

#### IDEL: Eliminazione avviata da ILM

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

Il messaggio IDEL viene generato in una delle seguenti situazioni:

- **Per gli oggetti nei bucket S3 conformi:** Questo messaggio viene generato quando ILM avvia il processo di eliminazione automatica di un oggetto perché il relativo periodo di conservazione è scaduto (supponendo che l'impostazione di eliminazione automatica sia attivata e che la sospensione legale sia disattivata).
- **Per oggetti in bucket S3 non conformi.** Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto poiché all'oggetto non sono attualmente applicate istruzioni di posizionamento nei criteri ILM attivi.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Compliance: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (false) o 1 (true), che indica se un oggetto conforme deve essere cancellato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a una conservazione legale.



Codice	Campo	Descrizione
CMPL	Compliance: Conservazione a fini legali	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), che indica se il bucket è attualmente in stato di conservazione legale.
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. La durata del periodo di conservazione dell'oggetto in minuti.
CTME	Compliance: Tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Il tempo di acquisizione dell'oggetto. È possibile aggiungere il periodo di conservazione in minuti a questo valore per determinare quando l'oggetto può essere cancellato dal bucket.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	<p>La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato).</p> <p>CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto.</p> <p>CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto.</p> <p>CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.</p>
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	<p>Risultato dell'operazione ILM.</p> <p>SUCS: Operazione ILM riuscita.</p>
REGOLA	Etichetta regole	<ul style="list-style-type: none"> <li>Se un oggetto in un bucket S3 conforme viene cancellato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto.</li> <li>Se l'oggetto viene eliminato perché non sono presenti ulteriori istruzioni di posizionamento attualmente applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM applicata all'oggetto.</li> </ul>

Codice	Campo	Descrizione
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

#### LKCU: Pulitura oggetto sovrascritta

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza richiedeva la pulizia per liberare spazio di storage. Un oggetto viene sovrascritto quando un client S3 scrive un oggetto in un percorso già contenente 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	<i>Solo per uso interno.</i>
LUID	UUID oggetto rimosso	L'identificativo dell'oggetto rimosso.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificativo dell'oggetto ancora esistente. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

#### LKDM: Pulizia degli oggetti con perdite

Questo messaggio viene generato quando un frammento fuoriuscito è stato pulito o eliminato. Un blocco può far parte di un oggetto replicato o di un oggetto codificato per la cancellazione.

Codice	Campo	Descrizione
CLOC	Posizione del frammento	Il percorso del file del blocco fuoriuscito che è stato eliminato.
CTYP	Tipo di frammento	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	Crea il tempo	Ora in cui è stato creato il frammento fuoriuscito.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto a cui appartiene il blocco.
CBID	Identificatore del blocco di contenuto	CBID dell'oggetto a cui appartiene il blocco fuoriuscito.
CSIZ	Dimensione del contenuto	La dimensione del blocco in byte.

### LLST: Località persa

Questo messaggio viene generato ogni volta che non è possibile trovare una posizione per una copia dell'oggetto (replicata o con erasure coding).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.

Codice	Campo	Descrizione
ECPR	Profilo di erasure coding	Per i dati degli oggetti con codifica erasure coding utilizzato.
LTYP	Tipo di ubicazione	CLDI (online): Per i dati degli oggetti replicati CLEC (Online): Per i dati degli oggetti con codifica erasure CLNL (Nearline): Per i dati degli oggetti replicati archiviati
NOID. (NOIDE	ID nodo di origine	L'ID del nodo in cui sono state perse le posizioni.
PCLD	Percorso dell'oggetto replicato	Il percorso completo alla posizione del disco dei dati dell'oggetto perso. Viene restituito solo quando LTYP ha un valore di CLDI (vale a dire, per gli oggetti replicati).  Assume la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
RSLT	Risultato	SEMPRE NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
TSRC	Fonte di attivazione	UTENTE: Attivato dall'utente  SYST: Attivato dal sistema
UUID	ID universalmente univoco	L'identificativo dell'oggetto interessato nel sistema StorageGRID.

#### MGAU: Messaggio di audit della gestione

La categoria Gestione registra le richieste degli utenti all'API di gestione. Ogni richiesta HTTP che non è 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 (come `/api/v3-autorizza`) e le richieste non valide agli URI API validi non vengono registrate.

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

Codice	Campo	Descrizione
MPAT	PERCORSO di richiesta	Il percorso della richiesta.
MPQP	Parametri di query della richiesta	I parametri di query per la richiesta.
MRBD	Corpo della richiesta	<p>Il contenuto dell'organismo di richiesta. Mentre il corpo della risposta viene registrato per impostazione predefinita, il corpo della richiesta viene registrato in alcuni casi quando il corpo della risposta è vuoto. Poiché le seguenti informazioni non sono disponibili nel corpo della risposta, vengono prese dal corpo della richiesta per i seguenti metodi POST:</p> <ul style="list-style-type: none"> <li>• Nome utente e ID account in <b>POST authorize</b></li> <li>• Nuova configurazione delle subnet in <b>POST /grid/grid-networks/update</b></li> <li>• Nuovi server NTP in <b>POST /grid/ntp-servers/update</b></li> <li>• ID server decommissionati in <b>POST /grid/servers/decommissionation</b></li> </ul> <p><b>Nota:</b> le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).</p>
MRMD	Metodo di richiesta	<p>Il metodo di richiesta HTTP:</p> <ul style="list-style-type: none"> <li>• POST</li> <li>• IN PRIMO PIANO</li> <li>• ELIMINARE</li> <li>• PATCH</li> </ul>
MRSC	Codice di risposta	Il codice di risposta.
MRSP	Corpo di risposta	<p>Il contenuto della risposta (il corpo della risposta) viene registrato per impostazione predefinita.</p> <p><b>Nota:</b> le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).</p>
MSIP	Indirizzo IP di origine	L'indirizzo IP (di origine) del client.
MUN	URN utente	L'URN (Uniform resource name) dell'utente che ha inviato la richiesta.

Codice	Campo	Descrizione
RSLT	Risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.

#### OLST: Il sistema ha rilevato un oggetto perso

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

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto perso.
NOID. (NOIDE	ID nodo	Se disponibile, l'ultima posizione nota diretta o near-line dell'oggetto perso. Se le informazioni sul volume non sono disponibili, è possibile avere solo l>ID nodo senza un ID volume.
PERCORSO	Bucket/chiave S3	Se disponibile, il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
UUID	ID universalmente univoco	L'identificativo dell'oggetto perso nel sistema StorageGRID.
VOLO	ID volume	Se disponibile, l>ID del volume del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

#### ORLM: Regole oggetto soddisfatte

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



Il messaggio ORLM non viene generato quando un oggetto viene memorizzato correttamente dalla regola predefinita Make 2 Copies se un'altra regola del criterio utilizza il filtro avanzato dimensione oggetto.

Codice	Campo	Descrizione
BUID (BUID)	Testata benna	Campo ID bucket. Utilizzato per operazioni interne. Viene visualizzato solo se STAT è PRGD.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	<p>La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato).</p> <p>CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto.</p> <p>CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto.</p> <p>CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.</p>
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	<p>Risultato dell'operazione ILM.</p> <p>SUCS: Operazione ILM riuscita.</p>
REGOLA	Etichetta regole	Etichetta leggibile assegnata alla regola ILM applicata a questo oggetto.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	CBID contenitore	CBID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo per gli oggetti segmentati e multiparte.
URGENZA	Stato	<p>Lo stato del funzionamento di ILM.</p> <p>FATTO: Operazioni ILM rispetto all'oggetto completate.</p> <p>DFER: L'oggetto è stato contrassegnato per la futura rivalutazione ILM.</p> <p>PRGD: L'oggetto è stato cancellato dal sistema StorageGRID.</p> <p>NLOC: I dati dell'oggetto non possono più essere trovati nel sistema StorageGRID. Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.</p>

Codice	Campo	Descrizione
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Il messaggio di audit 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.
- Le regole ILM per l'oggetto sono soddisfatte per questa epoca.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati degli oggetti replicati è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto corrotto.

#### Informazioni correlate

- ["Transazioni di acquisizione degli oggetti"](#)
- ["Transazioni di eliminazione degli oggetti"](#)

#### OVWR: Sovrascrittura degli oggetti

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

Codice	Campo	Descrizione
CBID	Content Block Identifier (nuovo)	Il CBID per il nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto da sovrascrivere.
OCBD	Content Block Identifier (precedente)	Il CBID dell'oggetto precedente.
UUID	ID universally Unique (nuovo)	L'identificativo del nuovo oggetto all'interno del sistema StorageGRID.
ID OUID	ID universally Unique (precedente)	L'identificativo dell'oggetto precedente all'interno del sistema StorageGRID.



Codice	Campo	Descrizione
PERCORSO	Percorso oggetto S3	Il percorso dell'oggetto S3 utilizzato sia per l'oggetto precedente che per quello nuovo
RSLT	Codice risultato	Risultato della transazione Object Overwrite. Il risultato è sempre:  SUC: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato cancellato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto sovrascritto.

### S3SL: Richiesta S3 Select

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.

Codice	Campo	Descrizione
BYSC	Byte sottoposti a scansione	Numero di byte sottoposti a scansione (ricevuti) dai nodi di storage.  BYSC e BYPR potrebbero essere diversi se l'oggetto viene compresso. Se l'oggetto è compresso, BYSC avrebbe il conteggio dei byte compressi e BYPR i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "byte sottoposti a scansione" sono stati effettivamente elaborati o utilizzati da un lavoro S3 Select.
BYRT	Byte restituiti	Numero di byte restituiti al client da un lavoro S3 Select.
RPR	Record elaborati	Numero di record o righe ricevuti da un processo S3 Select dai nodi di storage.
RERT	Record restituiti	Numero di record o righe di un lavoro S3 Select restituito al client.
JOFI	Lavoro terminato	Indica se il lavoro S3 Select ha terminato o meno l'elaborazione. Se questo è falso, il lavoro non è stato completato e i campi di errore probabilmente contengono dei dati. Il client potrebbe aver ricevuto risultati parziali o non avere alcun risultato.
RID	ID richiesta	Identificatore della richiesta S3 Select.
ETM	Tempo di esecuzione	Il tempo, in secondi, impiegato per il completamento del processo S3 Select.

Codice	Campo	Descrizione
ERMG	Messaggio di errore	Messaggio di errore generato dal lavoro S3 Select.
EROSO	Tipo di errore	Tipo di errore generato dal lavoro S3 Select.
ERST	Errore StackTrace	Errore StackTrace generato dal lavoro S3 Select.
S3BK	Bucket S3	Il nome del bucket S3.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 per l'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.

#### **SADD: Disattivazione dell'audit di sicurezza**

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

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per disattivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione era stata precedentemente attivata, ma ora è stata disattivata. Questo viene generalmente utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato (SADE) e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

### SADE: Abilitazione controllo di sicurezza

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

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Il metodo utilizzato per attivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per attivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione è stata precedentemente disattivata (SADD), ma ora è stata ripristinata. In genere viene utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

### SCMT: Commit dell'archivio di oggetti

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato fino a quando non viene assegnato (ovvero viene memorizzato in modo persistente). Il contenuto memorizzato in maniera persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene emesso quando un blocco di contenuto viene assegnato allo storage.

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

Questo messaggio indica che un dato blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto. Può essere utilizzato per tenere traccia del flusso di dati all'interno del sistema.

### SDEL: ELIMINAZIONE S3

Quando un client S3 esegue una transazione DI ELIMINAZIONE, viene effettuata una richiesta per rimuovere l'oggetto o il bucket specificato o 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	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta di eliminazione della replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta di eliminazione della replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div><p><code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p></div> <p><code>x-amz-bypass-governance-retention</code> viene incluso automaticamente se è presente nella richiesta.</p>
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.

<b>Codice</b>	<b>Campo</b>	<b>Descrizione</b>
RSLT	Codice risultato	Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre:  SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.

Codice	Campo	Descrizione
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code>  Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UDM	Identificatore univoco universale per un marcatore di cancellazione	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 come risultato di una richiesta di eliminazione dell'oggetto e UUID indica un oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

## SGET: S3 GET

Quando un client S3 esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket o 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	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.

Codice	Campo	Descrizione
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div> <p>`X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div>
LITY	ListObjectsV2	È stata richiesta una risposta <i>formato v2</i> . Per ulteriori informazioni, vedere <a href="#">"AWS ListObjectsV2"</a> . Solo per operazioni CON benna GET.
NCHD	Numero di bambini	Include tasti e prefissi comuni. Solo per operazioni CON benna GET.
RANG	Range Read (lettura intervallo)	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) mostra la dimensione dell'intero oggetto.
RSLT	Codice risultato	<p>Risultato della transazione GET. Il risultato è sempre:</p> <p>SUC: Riuscito</p>
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L>ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L>ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code>  Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
TRNC	Troncato o non troncato	Impostare su false se sono stati restituiti tutti i risultati. Impostare su true se sono disponibili ulteriori risultati da restituire. Solo per operazioni CON benna GET.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L>ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

## SHEA: TESTA S3

Quando un client S3 emette un'operazione 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 l'operazione ha esito positivo.

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

Codice	Campo	Descrizione
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code>  Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

### SPOS: POST S3

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

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0.

Codice	Campo	Descrizione
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div> <p>`X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> </div> <p>(Non previsto per SPOS).</p>
RSLT	Codice risultato	<p>Risultato della richiesta RestoreObject. Il risultato è sempre:</p> <p>SUC: Riuscito</p>
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	<p>Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.</p> <p>Impostare su "SELECT" per un'operazione di selezione S3.</p>

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L>ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	S3 User URN (richiesta mittente)	L>ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code>  Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L>ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

## SPUT: S3 PUT

Quando un client S3 esegue una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket o 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	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di compliance	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta DI PUT di replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta DI PUT di replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.
HTRH	Intestazione richiesta HTTP	<p>Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.</p> <div> <p>`X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</p> <p><code>x-amz-bypass-governance-retention</code> viene incluso automaticamente se è presente nella richiesta.</p> </div>
LKEN	Blocco oggetto attivato	Valore dell'intestazione della richiesta <code>x-amz-bucket-object-lock-enabled</code> , se presente nella richiesta.
LKSX	Blocco oggetto Legal Hold	Valore dell'intestazione della richiesta <code>x-amz-object-lock-legal-hold</code> , se presente nella richiesta PutObject.

Codice	Campo	Descrizione
LKMD	Modalità di conservazione del blocco degli oggetti	Valore dell'intestazione della richiesta <code>x-amz-object-lock-mode</code> , se presente nella richiesta PutObject.
LKRU	Blocco oggetto conserva fino alla data	Valore dell'intestazione della richiesta <code>x-amz-object-lock-retain-until-date</code> , se presente nella richiesta PutObject. I valori sono limitati entro 100 anni dalla data di acquisizione dell'oggetto.
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre:  SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code>  Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
ULID	ID upload	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.
VSST	Stato di versione	Il nuovo stato di versione di un bucket. Vengono utilizzati due stati: "Attivato" o "sospeso". Le operazioni sugli oggetti non includono questo campo.

### SREM: Rimozione dell'archivio di oggetti

Questo messaggio viene inviato quando il contenuto viene rimosso dallo storage persistente e non è più accessibile tramite API regolari.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto cancellato dallo storage permanente.

Codice	Campo	Descrizione
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è:  SUC: Contenuto rimosso dallo storage persistente

Questo messaggio di audit indica che un dato blocco di contenuto è stato cancellato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tenere traccia del flusso di contenuti cancellati all'interno del sistema.

### SUPD: Metadati S3 aggiornati

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

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, quando si aggiornano le impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione.  <div> `X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). </div>
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre:  SUC: Riuscito



Codice	Campo	Descrizione
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code>  Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.

Codice	Campo	Descrizione
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

#### SVRF: Verifica archivio oggetti non riuscita

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

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto che non ha superato la verifica.
RSLT	Codice risultato	<p>Tipo di errore di verifica:</p> <p>CRCF: Controllo di ridondanza ciclico (CRC) non riuscito.</p> <p>HMAC: Controllo HMAC (hash-based message Authentication code) non riuscito.</p> <p>ESH: Hash di contenuto crittografato inatteso.</p> <p>PHSH: Hash di contenuto originale inaspettato.</p> <p>SEQC: Sequenza di dati errata sul disco.</p> <p>PERR: Struttura del file di disco non valida.</p> <p>DERR: Errore del disco.</p> <p>FNAM: Nome file non valido.</p>



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

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

### SVRU: Verifica archivio oggetti sconosciuta

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

Codice	Campo	Descrizione
FPTH	Percorso del file	Il percorso del file della copia imprevista dell'oggetto.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.



Il messaggio di audit SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie impreviste dei dati dell'oggetto nell'archivio di oggetti. Questa situazione deve essere esaminata immediatamente per determinare come sono state create queste copie, perché può indicare guasti hardware imminenti.

### SYSD: Interruzione nodo

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

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown:  SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno shutdown "anomalo", perché il messaggio viene generato solo dagli shutdown "puliti".

### SYST: Interruzione del nodo

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

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown:  SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. Il codice RSLT di un messaggio SYST non può indicare uno shutdown "dirty", perché il messaggio viene generato solo dagli shutdown "clean".

#### **SYSU: Avvio nodo**

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

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown:  SUCS: Il sistema è stato spento in modo pulito.  DSDN: Il sistema non è stato spento correttamente.  VRGN: Il sistema è stato avviato per la prima volta dopo l'installazione (o la reinstallazione) del server.

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

- Rilevare la discontinuità nel registro di controllo.
- Determinare se un servizio si guasta durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio guasto.

## Informazioni sul copyright

Copyright © 2026 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.