Formato del file di registro di controllo

StorageGRID software

NetApp
December 03, 2025

Sommario

Formato del file di registro di controllo

Formato del file di registro di controllo

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

Ogni messaggio di controllo contiene quanto segue:

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

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

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

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

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Nel loro formato predefinito, i messaggi di controllo nei file di registro di controllo non sono facili da leggere o interpretare. Puoi usare il"strumento di verifica e spiegazione" per ottenere riepiloghi semplificati dei messaggi di controllo nel registro di controllo. Puoi usare il"strumento di somma di controllo" per riepilogare quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto queste operazioni.

Utilizzare lo strumento di verifica e spiegazione

Puoi usare il `audit-explain` strumento per tradurre i messaggi di controllo nel registro di controllo in un formato di facile lettura.

Prima di iniziare

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

Informazioni su questo compito

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

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

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

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

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

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

  ```
  audit-explain audit.log

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

- Elaborare più file contemporaneamente. Per esempio:

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

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

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

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

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

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

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

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

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

Passi

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

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

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

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

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

Utilizzare lo strumento audit-sum

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

Prima di iniziare

- Hai"autorizzazioni di accesso specifiche" .

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

Informazioni su questo compito

IL `audit-sum` strumento, disponibile sul nodo di amministrazione primario, riepiloga quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno richiesto tali operazioni.

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

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

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

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

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

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

Codice	Descrizione	Fare riferimento a
KARITÉ	S3 HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	"SHEA: TESTA S3"
SPUT	S3 PUT: registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"
WDEL	Swift DELETE: registra una transazione riuscita per eliminare un oggetto o un contenitore.	"WDEL: CANCELLA rapida"
WGET	Swift GET: registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un contenitore.	"WGET: GET rapido"
WHEA	Swift HEAD: registra una transazione riuscita per verificare l'esistenza di un oggetto o di un contenitore.	"WHEA: TESTA Veloce"
WPUT	Swift PUT: registra una transazione riuscita per creare un nuovo oggetto o contenitore.	"WPUT: PUT rapido"

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

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

```
audit-sum audit.log

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

- Elaborare più file contemporaneamente. Per esempio:

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

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

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

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

grep bucket1 audit.log | audit-sum

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

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

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

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

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

Passi

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

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

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

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

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

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

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

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

I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di cercare nel registro di controllo altri messaggi relativi a questi oggetti specifici.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+ Da questo output di esempio, è possibile vedere che le tre richieste S3 GET più lente riguardavano oggetti di circa 5 GB di dimensione, ovvero molto più grandi degli altri oggetti. Le grandi dimensioni spiegano i lenti tempi di recupero nel caso peggiore.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Informazioni sul copyright

Informazioni sul marchio commerciale