



File di log di audit e formati dei messaggi

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

- File di log di audit e formati dei messaggi 1
 - Formato del file di log di audit 1
 - Formato del messaggio di audit 14

File di log di audit e formati dei messaggi

È possibile utilizzare i registri di controllo per raccogliere informazioni sul sistema e risolvere i problemi. È necessario conoscere il formato del file di log di audit e il formato generale utilizzato per i messaggi di audit.

Formato del file di log di audit

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

Ogni messaggio di audit contiene quanto segue:

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

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

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

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

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][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 `audit-explain` tool per ottenere riepiloghi semplificati dei messaggi di audit nel log di audit. È possibile utilizzare `audit-sum` tool per riepilogare il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.

Informazioni correlate

["Utilizzando lo strumento audit-spiegate"](#)

["Utilizzando lo strumento audit-sum"](#)

Utilizzando lo strumento audit-spiegate

È possibile utilizzare `audit-explain` strumento per tradurre i messaggi di audit nel log di audit in un formato di facile lettura.

Di cosa hai bisogno

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

A proposito di questa attività

Il `audit-explain` Tool, disponibile nel nodo di amministrazione principale, fornisce riepiloghi semplificati dei messaggi di audit in un registro di audit.



Il `audit-explain` lo strumento è destinato principalmente all'utilizzo da parte del supporto tecnico durante le operazioni di troubleshooting. Elaborazione in corso `audit-explain` Le query possono consumare una grande quantità di potenza della CPU, con un conseguente impatto sulle operazioni StorageGRID.

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

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

Il `audit-explain` può elaborare registri di audit semplici o compressi. Ad esempio:

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

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

Il `audit-explain` può anche elaborare più file contemporaneamente. Ad esempio:

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

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

Infine, il `audit-explain` lo strumento può accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando `grep` comando o altro mezzo. Ad esempio:

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

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

Poiché i log di audit possono essere molto grandi e lenti da analizzare, è possibile risparmiare tempo filtrando le parti che si desidera esaminare ed eseguire `audit-explain` sulle parti, invece dell'intero file.



Il `audit-explain` lo strumento non accetta i file compressi come input di tipo pipped. Per elaborare i file compressi, specificare i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` per decomprimere prima i file. Ad esempio:

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

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

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

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
2. Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

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

Il `audit-explain` consente di stampare interpretazioni leggibili di tutti i messaggi contenuti nel file o nei file specificati.



Per ridurre le lunghezze delle linee e agevolare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se si desidera visualizzare gli indicatori di data e ora, utilizzare l'indicatore di data e ora (-t).

Informazioni correlate

["SPUT: S3 PUT"](#)

Utilizzando lo strumento audit-sum

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

Di cosa hai bisogno

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

A proposito di questa attività

Il `audit-sum` Tool, disponibile sul nodo di amministrazione primario, riepiloga il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.



Il `audit-sum` lo strumento è destinato principalmente all'utilizzo da parte del supporto tecnico durante le operazioni di troubleshooting. Elaborazione in corso `audit-sum` Le query possono consumare una grande quantità di potenza della CPU, con un conseguente impatto sulle operazioni StorageGRID.

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

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

Il `audit-sum` Lo strumento fornisce conteggi e tempi per i seguenti messaggi di audit S3, Swift e ILM in un registro di audit:

Codice	Descrizione	Fare riferimento a.
ARCT	Recupero archivio da Cloud-Tier	"ARCT: Recupero archivio da Cloud-Tier"
ASTT	Archivio Store Cloud-Tier	"ASCT: Archivio Store Cloud-Tier"

Codice	Descrizione	Fare riferimento a.
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: ELIMINAZIONE S3"
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	"SHEA: TESTA S3"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"
WDEL	Eliminazione rapida: Registra una transazione riuscita per eliminare un oggetto o un container.	"WDEL: ELIMINAZIONE rapida"
WGET	Swift GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un container.	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un container.	"WHEA: TESTA veloce"
WPUT	Swift PUT: Registra una transazione riuscita per creare un nuovo oggetto o container.	"WPUT: MESSA rapida"

Il `audit-sum` può elaborare registri di audit semplici o compressi. Ad esempio:

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

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

Il `audit-sum` può anche elaborare più file contemporaneamente. Ad esempio:

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



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

Infine, il `audit-sum` lo strumento può anche accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando `grep` comando o altro mezzo. Ad esempio:

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

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

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



Questo strumento non accetta i file compressi come input di tipo piped. Per elaborare i file compressi, specificare i nomi dei file come argomenti della riga di comando oppure utilizzare `zcat` per decomprimere prima i file. Ad esempio:

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

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

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

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

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

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, testa ed eliminazione, attenersi alla seguente procedura:
 - a. Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

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

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

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

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

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

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

```

Total:          201906 operations
Slowest:       1740.290 sec
Average:       1.132 sec
Fastest:       0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====      =====      =====      =====
      1740289662    10.96.101.125    object    5663711385
backup/r9010aQ8JB-1566861764-4519.iso
      1624414429    10.96.101.125    object    5375001556
backup/r9010aQ8JB-1566861764-6618.iso
      1533143793    10.96.101.125    object    5183661466
backup/r9010aQ8JB-1566861764-4518.iso
      70839         10.96.101.125    object     28338
bucket3/dat.1566861764-6619
      68487         10.96.101.125    object     27890
bucket3/dat.1566861764-6615
      67798         10.96.101.125    object     27671
bucket5/dat.1566861764-6617
      67027         10.96.101.125    object     27230
bucket5/dat.1566861764-4517
      60922         10.96.101.125    object     26118
bucket3/dat.1566861764-4520
      35588         10.96.101.125    object     11311
bucket3/dat.1566861764-6616
      23897         10.96.101.125    object     10692
bucket3/dat.1566861764-4516

```

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

3. Se si desidera determinare le dimensioni degli oggetti da acquisire e recuperare dalla griglia, utilizzare l'opzione size (dimensione) (-s):

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

message group 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. Eseguire il comando sul registro di controllo appropriato e utilizzare l'opzione group-by-time (-gt), seguito dal periodo di tempo (ad esempio, 15M, 1H, 10S):

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

message group 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 S3 OTTIENE un incremento del traffico tra le 06:00 e le 07:00. Anche in questi casi, i tempi massimi e medi sono notevolmente più elevati e non sono aumentati gradualmente con l'aumentare del numero. Ciò suggerisce che la capacità è stata superata da qualche parte, ad esempio nella rete o nella capacità della rete di elaborare le richieste.

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

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

message group 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 `audit-explain` Tool per esaminare tutte le operazioni SGET durante quell'ora:

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

Se si prevede che l'output del comando `grep` sia costituito da molte righe, aggiungere `less` comando per visualizzare il contenuto del file di log di audit una pagina (una schermata) alla volta.

- 5. Se si desidera determinare se le operazioni SPUT sui bucket sono più lente delle operazioni SPUT per gli oggetti:
 - a. Iniziare utilizzando `-go` opzione, che raggruppa i messaggi per le operazioni a oggetti e a bucket separatamente:

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

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

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

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

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

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

c. Per determinare quali bucket hanno la dimensione maggiore dell'oggetto SPUT, utilizzare entrambi i campi `-gb` e `a. -s` opzioni:

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

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

Informazioni correlate

["Utilizzando lo strumento audit-spiegate"](#)

Formato del messaggio di audit

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

Se le informazioni di riepilogo fornite da `audit-explain` e `audit-sum` gli strumenti non sono sufficienti, fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di audit.

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

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(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 di attributo nella stringa ha le seguenti caratteristiche:

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

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


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

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

L'elenco seguente descrive gli elementi degli attributi:

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

Informazioni correlate

["Utilizzando lo strumento audit-spiegate"](#)

["Utilizzando lo strumento audit-sum"](#)

["Messaggi di audit"](#)

["Elementi comuni nei messaggi di audit"](#)

["Tipi di dati"](#)

["Esempi di messaggi di audit"](#)

Tipi di dati

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

Tipo	Descrizione
UI32	Intero senza segno (32 bit); può memorizzare i numeri da 0 a 4,294,967,295.
UI64	Numero intero doppio senza segno (64 bit); può memorizzare i numeri da 0 a 18,446,744,073,709,551,615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32-bit rappresentato da quattro caratteri ASCII, ad esempio "ABCD".
IPAD	Utilizzato per gli indirizzi IP.

Tipo	Descrizione
CSTR	<p>Matrice a lunghezza variabile di UTF-8 caratteri. È possibile eseguire l'escape dei caratteri con le seguenti convenzioni:</p> <ul style="list-style-type: none"> • La barra rovesciata è • Il ritorno a capo è • Le virgolette doppie sono ". • L'avanzamento riga (nuova riga) è il n. • I caratteri possono essere sostituiti dai rispettivi equivalenti esadecimali (nel formato HH, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento

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

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

```
2018-12-05T08:24:45.921845 [AUDT: [RSLT (FC32) :SUCS]
[TIME (UI64) :11454] [SAIP (IPAD) : "10.224.0.100"]
[S3AI (CSTR) : "60025621595611246499"] [SACC (CSTR) : "account"]
[S3AK (CSTR) : "SGKH4_Nc8S01H6w3w0nCOFCGgk_E6dYzKlumRsKJA=="]
[SUSR (CSTR) : "urn:sgws:identity::60025621595611246499:root"]
[SBAI (CSTR) : "60025621595611246499"] [SBAC (CSTR) : "account"] [S3BK (CSTR) : "bucket"]
[S3KY (CSTR) : "object"] [CBID (UI64) : 0xCC128B9B9E428347]
[UUID (CSTR) : "B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"] [CSIZ (UI64) : 30720]
[AVER (UI32) : 10] [ATIM (UI64) : 1543998285921845] [ATYP (FC32) : SHEA]
[ANID (UI32) : 12281045] [AMID (FC32) : S3RQ] [ATID (UI64) : 15552417629170647261]]
```

Il ATYP element (sottolineato nell'esempio) identifica l'evento che ha generato il messaggio. Questo messaggio di esempio include il codice del messaggio SHEA ([ATYP(FC32):SHEA]), che indica che è stato generato da una richiesta S3 HEAD riuscita.

Informazioni correlate

["Elementi comuni nei messaggi di audit"](#)

["Messaggi di audit"](#)

Elementi comuni nei messaggi di audit

Tutti i messaggi di audit contengono gli elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	Module ID (ID modulo): Identificatore di quattro-caratteri dell'ID modulo che ha generato il messaggio. Indica il segmento di codice all'interno del quale è stato generato il messaggio di audit.
ANID	UI32	Node ID (ID nodo): L'ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID. Questo ID non può essere modificato.
ASE	UI64	Audit Session Identifier (identificatore sessione di audit): Nelle release precedenti, questo elemento indica l'ora in cui il sistema di audit è stato inizializzato dopo l'avvio del servizio. Questo valore di tempo è stato misurato in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Nota: questo elemento è obsoleto e non compare più nei messaggi di audit.
ASQN	UI64	Sequence Count (Conteggio sequenze): Nelle release precedenti, questo contatore è stato incrementato per ogni messaggio di audit generato sul nodo della griglia (ANID) e azzerato al riavvio del servizio. Nota: questo elemento è obsoleto e non compare più nei messaggi di audit.
ATID	UI64	Trace ID (ID traccia): Identificatore condiviso dalla serie di messaggi attivati da un singolo evento.
ATIM	UI64	Timestamp: L'ora in cui è stato generato l'evento che ha attivato il messaggio di audit, misurata in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per la conversione dell'indicatore data e ora in data e ora locali si basano su millisecondi. Potrebbe essere richiesto l'arrotondamento o il troncamento dell'indicatore data e ora registrato. Il tempo di lettura-umano visualizzato all'inizio del messaggio di audit in <code>audit.log</code> File è l'attributo ATIM nel formato ISO 8601. La data e l'ora sono rappresentate come <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> , dove il <code>T</code> è un carattere di stringa letterale che indica l'inizio del segmento temporale della data. <code>UUUUUU</code> sono microsecondi.
ATYP	FC32	Event Type (tipo di evento): Identificatore di quattro-caratteri dell'evento registrato. Questo regola il contenuto "payload" del messaggio: Gli attributi che sono inclusi.
MEDIA	UI32	Version (versione): La versione del messaggio di audit. Man mano che il software StorageGRID si evolve, le nuove versioni dei servizi potrebbero incorporare nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti del servizio AMS per l'elaborazione dei messaggi provenienti da versioni precedenti dei servizi.

Codice	Tipo	Descrizione
RSLT	FC32	Risultato: Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

Esempi di messaggi di audit

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

Di seguito viene riportato un esempio di messaggio di audit come potrebbe essere visualizzato in `audit.log` file:

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

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

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"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]]
```

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

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"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 Tradotto a Giovedì, 17-lug-2014 21:17:59 UTC.

Informazioni correlate

["SPUT: S3 PUT"](#)

["Elementi comuni nei messaggi di audit"](#)

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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