



Audit-Protokolle prüfen

StorageGRID software

NetApp
July 23, 2026

Inhalt

Audit-Protokolle prüfen	1
\${post_edited_translations.segment}	1
Wie Audit-Meldungen durch das StorageGRID System in die Datei audit.log zur Aufbewahrung gelangen . .	1
\${post_edited_translations.segment}	1
Greifen Sie auf Revisionsprotokolldateien von der StorageGRID Admin Node Befehlszeile zu	4
Erfahren Sie mehr über die Rotation von Revisionsprotokolldateien in StorageGRID	5
Format der Revisionsprotokolldatei	6
Erfahren Sie mehr über das Format von Revisionsprotokolldateien in StorageGRID	6
Verwenden Sie das Tool „audit-explain“, um StorageGRID Revisionsprotokollmeldungen zu übersetzen.	7
Verwenden Sie das Tool audit-sum, um StorageGRID-Revisionsprotokollmeldungen zusammenzufassen.	9
Format der Revisionsmeldung	18
Erfahren Sie mehr über die Struktur der StorageGRID Revisionsprotokollmeldungen	18
Datentypen in StorageGRID-Revisionsprotokollmeldungen	19
Ereignisspezifische Daten in StorageGRID Revisionsprotokollmeldungen	20
Gemeinsame Elemente in StorageGRID Revisionsprotokollmeldungen	20
StorageGRID Revisionsprotokoll-Nachrichtenformat und Beispiele	22
Audit-Meldungen und der Objektlebenszyklus	23
Wenn Revisionsprotokollmeldungen in StorageGRID generiert werden	23
Audit-Meldungen für Objektaufnahmetransaktionen in StorageGRID	23
Auditmeldungen für Objektlöschvorgänge in StorageGRID	25
Audit-Meldungen für Objektabruftransaktionen in StorageGRID	26
Revisionsprotokoll-Meldungen für Aktualisierungen der S3-Objektmetadaten in StorageGRID	28
Audit-Meldungen	29
Erfahren Sie mehr über die Arten und Codes von Revisionsprotokollmeldungen in StorageGRID	30
Kategorien von Audit-Nachrichten	30
Referenz der Prüfmeldung	35

Audit-Protokolle prüfen

`${post_edited_translations.segment}`

Diese Anleitung enthält Informationen über die Struktur und den Inhalt von StorageGRID Audit-Meldungen und Audit-Protokollen. Sie können diese Informationen verwenden, um den Audit-Trail der Systemaktivitäten zu lesen und zu analysieren.

`${post_edited_translations.segment}`

Um die Textprotokolldatei verwenden zu können, müssen Sie Zugriff auf die konfigurierte Audit-Freigabe auf dem Admin-Node haben.

Informationen zur Konfiguration von Audit-Meldungsebenen und zur Verwendung eines externen Syslog-Servers sind unter "[Logverwaltung und externen Syslog-Server konfigurieren](#)" zu finden.

Wie Audit-Meldungen durch das StorageGRID System in die Datei `audit.log` zur Aufbewahrung gelangen

Alle StorageGRID Dienste generieren während des normalen Systembetriebs Revisionsprotokollmeldungen. Es ist wichtig nachzuvollziehen, wie diese Revisionsprotokollmeldungen durch das StorageGRID System zur `audit.log` Datei gelangen.

Die folgenden Workflows für Revisionsmeldungen und die Aufbewahrung von Revisionsmeldungen sind nur anwendbar, wenn StorageGRID für **Admin-Nodes/lokale Nodes** oder **Admin-Node und externer Syslog-Server** konfiguriert ist. Wenn StorageGRID für „Nur lokale Nodes“ (Standard) oder „Externer Syslog-Server“ konfiguriert ist, werden die Revisionsmeldungen lokal auf jedem Node in der Datei `/var/local/log/localaudit.log` gespeichert und können nicht von Admin-Nodes oder Storage-Nodes verarbeitet werden.

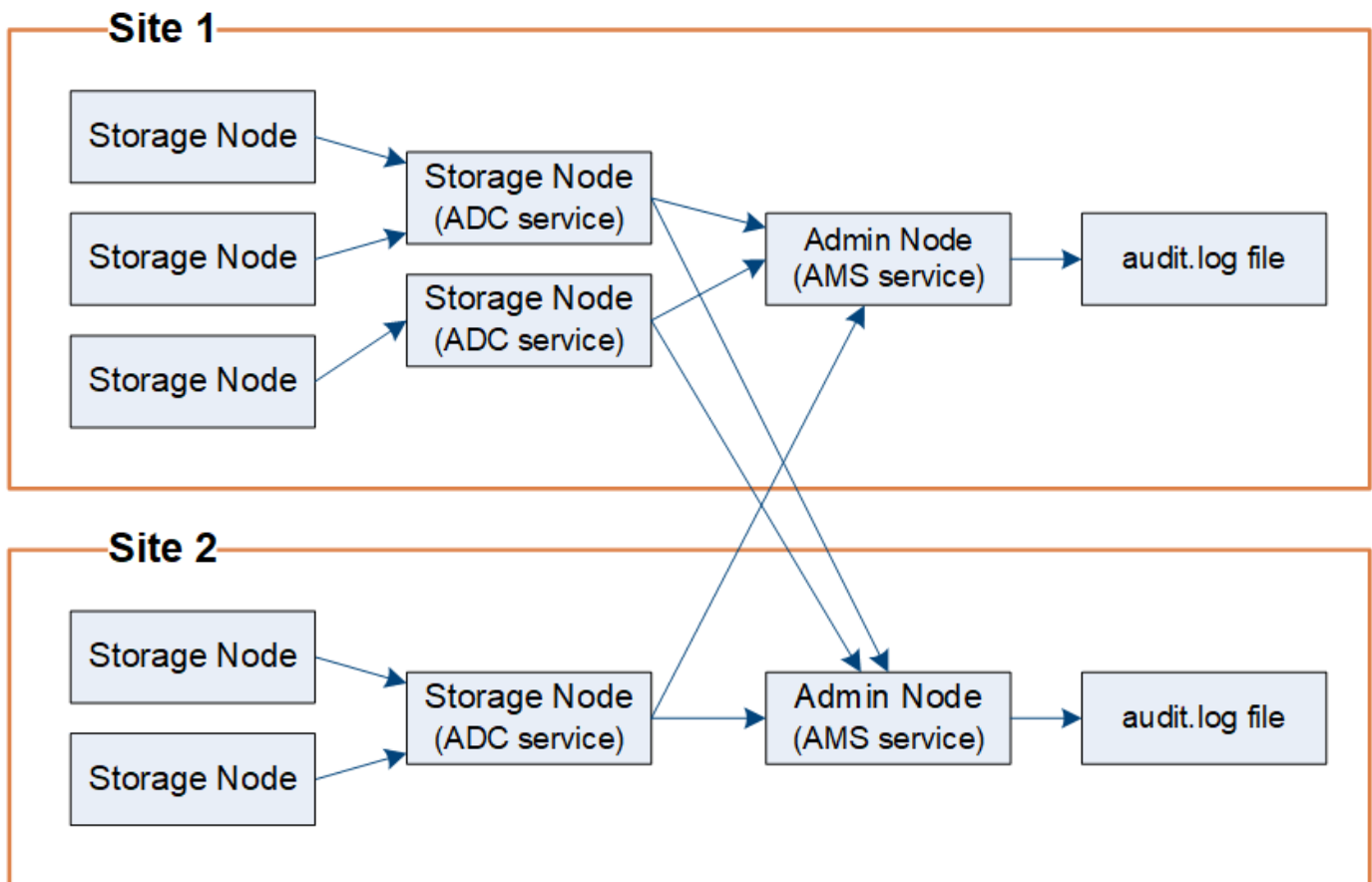
`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Wie im Ablaufdiagramm für Audit-Meldungen dargestellt, sendet jeder StorageGRID Knoten seine Audit-Meldungen an einen der ADC-Dienste am Rechenzentrum-Standort. Der ADC-Dienst wird automatisch für die ersten drei an jedem Standort installierten Storage-Knoten aktiviert.

Im Gegenzug fungiert jeder ADC-Dienst als Relais und sendet seine Sammlung von Revisionsprotokollmeldungen an jeden Admin-Node im StorageGRID System, wodurch jeder Admin-Node eine vollständige Aufzeichnung der Systemaktivität erhält.

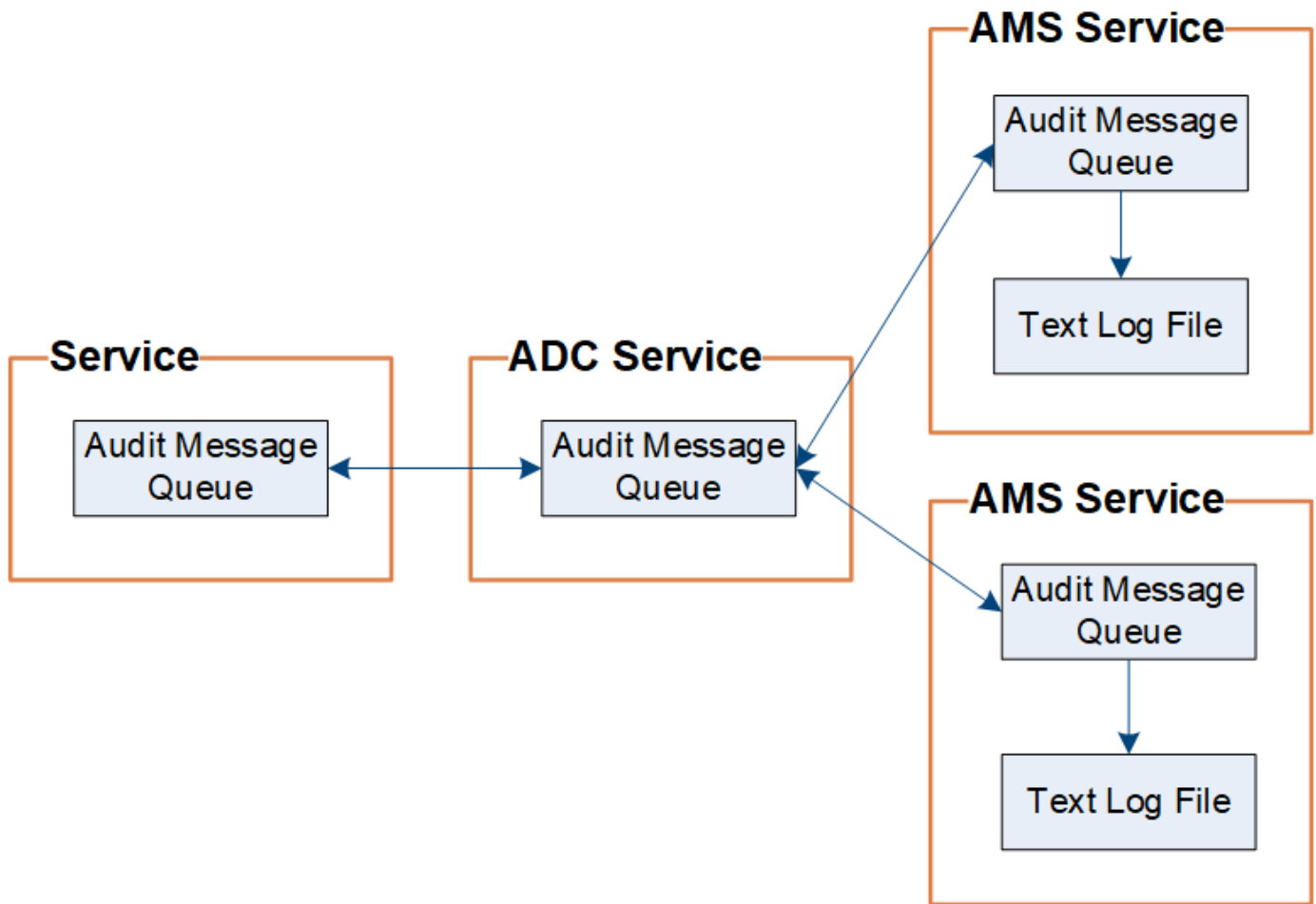
Jeder Admin-Knoten speichert Audit-Meldungen in Textprotokolldateien; die aktive Protokolldatei heißt `audit.log`.



Aufbewahrung von Audit-Meldungen

StorageGRID verwendet einen Kopier- und Löschvorgang, um sicherzustellen, dass keine Audit-Meldungen verloren gehen, bevor sie in das Revisionsprotokoll geschrieben werden können.

Wenn ein Knoten eine Revisionsprotokollmeldung generiert oder weiterleitet, wird die Meldung in einer Revisionsprotokollmeldungwarteschlange auf der Systemfestplatte des Grid-Knotens gespeichert. Eine Kopie der Meldung verbleibt stets in einer Revisionsprotokollmeldungwarteschlange, bis die Meldung in die Revisionsprotokolldatei im `/var/local/audit/export` Verzeichnis des Admin Node geschrieben wird. Dies hilft, den Verlust einer Revisionsprotokollmeldung während des Transports zu verhindern.



Die Warteschlange für Revisionsmeldungen kann sich aufgrund von Netzwerkverbindungsproblemen oder unzureichender Revisionskapazität vorübergehend vergrößern. Mit dem Anwachsen der Warteschlangen verbrauchen sie mehr des verfügbaren Speicherplatzes im `/var/local/`-Verzeichnis jedes Nodes. Wenn das Problem weiterhin besteht und das Verzeichnis für Revisionsmeldungen eines Nodes zu voll wird, priorisieren die einzelnen Nodes die Verarbeitung ihres Rückstands und stehen vorübergehend nicht für neue Meldungen zur Verfügung.

Konkret könnten folgende Verhaltensweisen auftreten:

- Wenn das `/var/local/audit/export` Verzeichnis, das von einem Admin-Knoten verwendet wird, voll ist, wird der Admin-Knoten für neue Revisionsprotokoll-Meldungen als nicht verfügbar markiert, bis das Verzeichnis nicht mehr voll ist. S3 Client-Anfragen sind nicht betroffen. Der XAMS (Unreachable Audit Repositories) Alarm wird ausgelöst, wenn ein Revisionsprotokoll-Repository nicht erreichbar ist.
- Wenn das `/var/local/` Verzeichnis, das von einem Storage Node mit dem ADC-Dienst verwendet wird, zu 92 % gefüllt ist, wird der Node als für Revisionsmeldungen nicht verfügbar gekennzeichnet, bis das Verzeichnis nur noch zu 87 % gefüllt ist. S3-Client-Anfragen an andere Nodes sind nicht betroffen. Der Alarm NRLY (Available Audit Relays) wird ausgelöst, wenn Audit-Relays nicht erreichbar sind.



Falls keine Storage Nodes mit dem ADC-Service verfügbar sind, speichern die Storage Nodes die Audit-Meldungen lokal in der `/var/local/log/localaudit.log` Datei.

- Wenn das von einem Storage Node verwendete `/var/local/` Verzeichnis zu 85 % gefüllt ist, beginnt der Node, S3-Client-Anfragen mit `503 Service Unavailable` abzulehnen.

Die folgenden Arten von Problemen können dazu führen, dass die Warteschlangen für Prüfmeldungen sehr groß werden:

- Der Ausfall eines Admin-Knotens oder eines Speicherknotens mit dem ADC-Dienst. Wenn einer der Systemknoten ausfällt, können die verbleibenden Knoten einen Rückstau aufweisen.
- Eine kontinuierliche Aktivitätsrate, die die Revisionsprotokoll-Kapazität des Systems übersteigt.
- Der `/var/local/` Speicherplatz auf einem ADC Storage Node füllt sich aus Gründen, die nicht mit Revisionsmeldungen zusammenhängen. Wenn dies geschieht, nimmt der Knoten keine neuen Revisionsmeldungen mehr an und priorisiert seinen aktuellen Rückstau, was zu Rückstaus auf anderen Knoten führen kann.

Warnung bei großer Revisionsprotokoll-Warteschlange und Audit Messages Queued (AMQS) Alarm

`${post_edited_translations.segment}`

Wenn die Warnung **Large audit queue** oder der Legacy-AMQS-Alarm ausgelöst wird, sollte zunächst die Systemlast überprüft werden. Falls in letzter Zeit eine signifikante Anzahl von Transaktionen stattgefunden hat, lösen sich die Warnung und der Alarm im Laufe der Zeit auf und können ignoriert werden.

Wenn die Warnung oder der Alarm weiterhin besteht und der Schweregrad zunimmt, kann ein Diagramm der Warteschlangengröße angezeigt werden. Wenn die Anzahl über Stunden oder Tage hinweg stetig ansteigt, hat die Revisionslast wahrscheinlich die Revisionskapazität des Systems überschritten. Die Client-Operationsrate kann reduziert oder die Anzahl der protokollierten Revisionsmeldungen verringert werden, indem die Revisionsstufe für Client Writes und Client Reads auf Error oder Off geändert wird. Siehe ["Logverwaltung und externen Syslog-Server konfigurieren"](#).

Doppelte Nachrichten

Das StorageGRID System verfolgt bei einem Netzwerk- oder Knotenausfall einen konservativen Ansatz. Aus diesem Grund können doppelte Meldungen im Revisionsprotokoll vorhanden sein.

Greifen Sie auf Revisionsprotokolldateien von der StorageGRID Admin Node Befehlszeile zu

Die Revisionsfreigabe enthält die aktive `audit.log` Datei und alle komprimierten Revisionsprotokolldateien. Sie können direkt über die Befehlszeile des Admin Node auf Revisionsprotokolldateien zugreifen.

Die `audit.log` Datei bleibt leer, sofern StorageGRID für **Admin Nodes/lokale Nodes** oder **Admin Node und externen Syslog-Server** konfiguriert ist. Weitere Informationen sind unter ["Protokollspeicherort auswählen"](#) zu finden.

Bevor Sie beginnen

- Du hast ["spezifische Zugriffsberechtigungen"](#).
- Sie müssen über die Datei `Passwords.txt` verfügen.
- `${post_edited_translations.segment}`

Schritte

1. `${post_edited_translations.segment}`

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
- c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
- d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Wechseln Sie in das Verzeichnis, das die Revisionsprotokolldateien enthält:

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

3. Die aktuelle oder eine gespeicherte Revisionsprotokoll-Datei kann angezeigt werden, je nach Bedarf.

Erfahren Sie mehr über die Rotation von Revisionsprotokolldateien in StorageGRID

Wenn StorageGRID für **Admin Nodes/lokale Nodes** oder **Admin Node und externen Syslog-Server** konfiguriert ist, werden die Revisionsprotokoll-Dateien im `/var/local/audit/export/` Verzeichnis des Admin Node gespeichert. Die aktiven Revisionsprotokoll-Dateien heißen `audit.log`.



Optional kann das Ziel der Revisionsprotokolle geändert und Audit-Informationen an einen externen Syslog-Server gesendet werden. Lokale Protokolle der Revisionsaufzeichnungen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe ["Audit-Meldungen und externer Syslog-Server konfigurieren"](#).

Einmal täglich wird die aktive `audit.log` Datei gespeichert und eine neue `audit.log` Datei begonnen. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format `yyyy-mm-dd.txt`. Wenn an einem Tag mehr als ein Revisionsprotokoll erstellt wird, verwenden die Dateinamen das Datum, an dem die Datei gespeichert wurde, ergänzt um eine Zahl, im Format `yyyy-mm-dd.txt.n`. Beispielsweise sind `2018-04-15.txt` und `2018-04-15.txt.1` die erste und zweite Protokolldatei, die am 15. April 2018 erstellt und gespeichert wurden.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format `yyyy-mm-dd.txt.gz` umbenannt, wobei das ursprüngliche Datum erhalten bleibt. Mit der Zeit wird der für Revisionsprotokolle reservierte Speicherplatz des Admin Node belegt. Ein Skript überwacht den Speicherplatzverbrauch der Revisionsprotokolle und löscht bei Bedarf Protokolldateien, um Speicherplatz im `/var/local/audit/export/` Verzeichnis freizugeben. Revisionsprotokolle werden entsprechend dem Erstellungsdatum gelöscht. Die ältesten Protokolle werden zuerst gelöscht. Die Aktionen des Skripts lassen sich in der folgenden Datei überwachen: `/var/local/log/manage-audit.log`.

Dieses Beispiel zeigt die aktive `audit.log` Datei, die Datei des Vortags (`2018-04-15.txt`) und die komprimierte Datei für den Vortag (`2018-04-14.txt.gz`).

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

Format der Revisionsprotokolldatei

Erfahren Sie mehr über das Format von Revisionsprotokolldateien in StorageGRID

Die Revisionsprotokoll Logdateien befinden sich auf jedem Admin Node und enthalten eine Sammlung einzelner Audit-Meldungen.

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

YYYY-MM-DDTHH:MM:SS.UUUUUU, wobei *UUUUUU* Mikrosekunden sind.

- Die Prüfmeldung selbst, in eckigen Klammern eingeschlossen und beginnend mit `AUDT`.

Das folgende Beispiel zeigt drei Audit-Meldungen in einer Revisionsprotokolldatei (Zeilenumbrüche wurden zur besseren Lesbarkeit hinzugefügt). Diese Meldungen wurden generiert, als ein Mandant einen S3-Bucket erstellte und diesem zwei Objekte hinzufügte.

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]]
```

Im Standardformat sind die Audit-Meldungen in den Revisionsprotokolldateien nicht leicht lesbar oder interpretierbar. Mit ["audit-explain Tool"](#) lassen sich vereinfachte Zusammenfassungen der Audit-Meldungen im Revisionsprotokoll erhalten. Mit ["\\${post_edited_translations.segment}"](#) kann zusammengefasst werden, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge dauerten.

Verwenden Sie das Tool „audit-explain“, um StorageGRID Revisionsprotokollmeldungen zu übersetzen.

Das `audit-explain` Tool kann verwendet werden, um die Audit-Meldungen im

Revisionsprotokoll in ein leicht lesbares Format zu übersetzen.

Bevor Sie beginnen

- Du hast "[spezifische Zugriffsberechtigungen](#)".
- Sie müssen über die Datei `Passwords.txt` verfügen.
- Sie müssen die IP-Adresse des primären Admin-Node kennen.

Über diese Aufgabe

Das `audit-explain` Tool, das auf dem primären Admin-Node verfügbar ist, bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Revisionsprotokoll.



Das `audit-explain` Tool ist primär für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Die Verarbeitung von `audit-explain` Abfragen kann viel CPU-Leistung beanspruchen, was StorageGRID Vorgänge beeinträchtigen kann.

Dieses Beispiel zeigt die typische Ausgabe des `audit-explain` Tools. Diese vier "[\\${post_edited_translations.segment}](#)" Revisionsprotokollmeldungen wurden generiert, als der S3-Tenant mit der Konto-ID 92484777680322627870 S3 PUT-Anfragen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und diesem Bucket drei Objekte hinzuzufügen.

```
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
```

Das `audit-explain` Tool kann Folgendes ausführen:

- Einfache oder komprimierte Revisionsprotokolle werden verarbeitet. Beispielsweise:

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

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

- Mehrere Dateien gleichzeitig verarbeiten. Zum Beispiel:

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

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

- Eingaben aus einer Pipe akzeptieren, was das Filtern und Vorverarbeiten der Eingabe mithilfe des `grep` Befehls oder anderer Methoden ermöglicht. Beispielsweise:

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

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

Da Revisionsprotokolle sehr groß sein und langsam analysiert werden können, lässt sich Zeit sparen, indem Sie die Teile herausfiltern, die Sie sich ansehen möchten, und `audit-explain` auf diese Teile anwenden, anstatt auf die gesamte Datei.



Das `audit-explain` Tool akzeptiert keine komprimierten Dateien als Eingabe über eine Pipe. Um komprimierte Dateien zu verarbeiten, können deren Dateinamen als Befehlszeilenargumente angegeben oder das `zcat` Tool verwendet werden, um die Dateien zuerst zu dekomprimieren. Beispielsweise:

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

Die `help` (`-h`) Option zeigt die verfügbaren Optionen an. Zum Beispiel:

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

Schritte

1. `${post_edited_translations.segment}`

- Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
- Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
- Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` den Namen und den Speicherort der Datei oder Dateien bezeichnet, die Sie analysieren möchten:

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

Das `audit-explain` Tool gibt für Menschen lesbare Interpretationen aller Meldungen in der/den angegebenen Datei(en) aus.



Um die Zeilenlänge zu reduzieren und die Lesbarkeit zu verbessern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn die Zeitstempel angezeigt werden sollen, kann die Option `(-t timestamp)` verwendet werden.

Verwenden Sie das Tool `audit-sum`, um StorageGRID-Revisionsprotokollmeldungen zusammenzufassen.

Das `audit-sum` Tool kann verwendet werden, um die Anzahl der Revisionsprotokoll-Meldungen für Schreiben, Lesen, Head und Löschen zu zählen sowie die minimale, maximale und durchschnittliche Zeit (oder Größe) für jeden Operationstyp anzuzeigen.

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die `Passwords.txt` Datei.
- Sie kennen die IP-Adresse des primären Admin-Knotens.

Über diese Aufgabe

Das `audit-sum` Tool, das auf dem primären Admin-Knoten verfügbar ist, fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.



Das `audit-sum` Tool ist primär für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Die Verarbeitung `audit-sum` von Abfragen kann viel CPU-Leistung beanspruchen, was StorageGRID Vorgänge beeinträchtigen kann.

Dieses Beispiel zeigt die typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokolloperationen dauerten.

```
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
```

Das ``audit-sum`` Tool liefert Anzahl und Zeiten für die folgenden S3- und ILM-Audit-Meldungen in einem Revisionsprotokoll.



Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, sobald Funktionen veraltet sind. Falls ein Prüfcode auftritt, der hier nicht aufgeführt ist, bieten die vorherigen Versionen dieses Themas Informationen zu älteren StorageGRID Releases. Zum Beispiel ["StorageGRID 11.8 Verwendung des audit sum Tools"](#).

Code	Beschreibung	Siehe
IDEL	ILM Initiated Delete: Protokolliert, wenn ILM den Prozess zum Löschen eines Objekts startet.	"\${post_edited_translations.segment}"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	"SDEL: S3-DELETE"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Buckets zu überprüfen.	"SHEA: S3 HEAD"

Code	Beschreibung	Siehe
<code>\${post_edited_translations.segment}</code>	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets.	"SPUT: S3 PUT"

Das `audit-sum` Tool kann Folgendes ausführen:

- Einfache oder komprimierte Revisionsprotokolle werden verarbeitet. Beispielsweise:

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

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

- Mehrere Dateien gleichzeitig verarbeiten. Zum Beispiel:

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

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

- Eingaben aus einer Pipe akzeptieren, was das Filtern und Vorverarbeiten der Eingabe mithilfe des `grep` Befehls oder anderer Methoden ermöglicht. Beispielsweise:

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

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

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



Dieses Tool akzeptiert keine komprimierten Dateien als Eingabe über eine Pipe. Um komprimierte Dateien zu verarbeiten, können deren Dateinamen als Befehlszeilenargumente angegeben oder das `zcat` Tool verwendet werden, um die Dateien zuerst zu dekomprimieren. Beispiel:

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

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

Mithilfe von Befehlszeilenoptionen können Sie Operationen an Buckets getrennt von Operationen an Objekten zusammenfassen oder Nachrichtenübersichten nach Bucket-Name, Zeitraum oder Zieltyp gruppieren. Standardmäßig werden die minimale, maximale und durchschnittliche Operationszeit angezeigt, aber mit der `size (-s)` Option kann stattdessen die Objektgröße betrachtet werden.

Die `help (-h)` Option zeigt die verfügbaren Optionen an. Zum Beispiel:

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

Schritte

1. `${post_edited_translations.segment}`

a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`

b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

- c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
- d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Wenn Sie alle Nachrichten im Zusammenhang mit Schreib-, Lese-, Head- und Löschvorgängen analysieren möchten, gehen Sie wie folgt vor:

- a. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` den Namen und den Speicherort der Datei oder Dateien bezeichnet, die Sie analysieren möchten:

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

Dieses Beispiel zeigt die typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokolloperationen dauerten.

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 diesem Beispiel sind SGET (S3 GET)-Operationen mit durchschnittlich 1,13 Sekunden am langsamsten, aber sowohl SGET- als auch SPUT (S3 PUT)-Operationen zeigen lange Worst-Case-Zeiten von etwa 1.770 Sekunden.

- b. Um die 10 langsamsten Abrufvorgänge anzuzeigen, kann der Befehl `grep` verwendet werden, um nur SGET-Nachrichten auszuwählen, und die Option `long output (-l)` kann hinzugefügt werden, um Objektpfade einzuschließen:

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

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, was es ermöglicht, das Revisionsprotokoll nach anderen Meldungen zu durchsuchen, die sich auf diese bestimmten Objekte beziehen.

```

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

```

+ Anhand dieser Beispielausgabe lässt sich erkennen, dass die drei langsamsten S3 GET-Anfragen Objekte mit einer Größe von jeweils etwa 5 GB betrafen, die deutlich größer sind als die übrigen Objekte. Die große Größe erklärt die langen Abrufzeiten im ungünstigsten Fall.

3. Wenn Sie ermitteln möchten, welche Größen von Objekten in Ihr Grid eingelesen und daraus abgerufen werden, verwenden Sie die Option Größe (-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 diesem Beispiel liegt die durchschnittliche Objektgröße für SPUT unter 2,5 MB, aber die durchschnittliche Größe für SGET ist deutlich größer. Die Anzahl der SPUT-Nachrichten ist wesentlich höher als die Anzahl der SGET-Nachrichten, was darauf hindeutet, dass die meisten Objekte nie abgerufen werden.

4. Wenn festgestellt werden soll, ob die Abrufe gestern langsam waren:

- a. Den Befehl im entsprechenden Revisionsprotokoll mit der Option group-by-time (-gt) ausführen, gefolgt vom Zeitraum (z. B. 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

Diese Ergebnisse zeigen, dass der S3 GET-Traffic zwischen 06:00 und 07:00 sprunghaft anstieg. Sowohl die maximale als auch die durchschnittliche Zeit waren in diesem Zeitraum deutlich höher und stiegen nicht allmählich mit zunehmender Anzahl an. Diese Kennzahlen deuten darauf hin, dass die Kapazität überschritten wurde, möglicherweise im Netzwerk oder in der Fähigkeit des Grids, Anfragen zu verarbeiten.

- b. Um zu ermitteln, welche Größe die gestern stündlich abgerufenen Objekte hatten, die Option (-s) zum Befehl hinzufügen:

```
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

Diese Ergebnisse deuten darauf hin, dass einige sehr große Abrufe stattfanden, als das gesamte Abrufaufkommen seinen Höhepunkt erreichte.

- c. Um weitere Details anzuzeigen, kann die Funktion ["audit-explain Tool"](#) verwendet werden, um alle SGET Operationen während dieser Stunde zu überprüfen:

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

Falls die Ausgabe des grep-Befehls voraussichtlich aus vielen Zeilen besteht, kann der less Befehl hinzugefügt werden, um den Inhalt der Revisionsprotokoll-Datei seitenweise (bildschirmweise) anzuzeigen.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen auf Buckets langsamer sind als SPUT-Operationen auf Objekten:

- a. Beginnen Sie mit der Option `-go`, die Meldungen für Objekt- und Bucket-Operationen separat gruppiert:

```
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

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets andere Leistungsmerkmale aufweisen als SPUT-Operationen für Objekte.

- b. Um festzustellen, welche Buckets die langsamsten SPUT-Operationen aufweisen, kann die `-gb` Option verwendet werden, die Nachrichten nach Bucket gruppiert:

```
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. Um zu ermitteln, welche Buckets die größte SPUT-Objektgröße aufweisen, sollten sowohl die `-gb` als auch die `-s` Optionen verwendet werden:

```
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

Format der Revisionsmeldung

Erfahren Sie mehr über die Struktur der StorageGRID Revisionsprotokollmeldungen

`${post_edited_translations.segment}`

Wenn die von den "[Revisionsprotokoll-Erklärung](#)" und "[audit-sum](#)" Tools bereitgestellten zusammenfassenden Informationen nicht ausreichen, enthält dieser Abschnitt Informationen zum allgemeinen Format aller Audit-Meldungen.

`${post_edited_translations.segment}`

```
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]]
```

Jede Prüfmeldung enthält eine Zeichenkette von Attributelementen. Die gesamte Zeichenkette ist in eckigen Klammern eingeschlossen ([]), und jedes Attributelement in der Zeichenkette weist die folgenden Eigenschaften auf:

- In Klammern []
- Eingeleitet durch die Zeichenkette AUDT, die auf eine Revisionsprotokollmeldung hinweist
- Ohne Trennzeichen (keine Kommas oder Leerzeichen) davor oder danach
- Abgeschlossen durch ein Zeilenumbruchzeichen \n

Jedes Element enthält einen Attributcode, einen Datentyp und einen Wert, die in diesem Format angegeben werden:

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

Die Anzahl der Attributelemente in der Nachricht hängt vom Ereignistyp der Nachricht ab. Die Attributelemente sind nicht in einer bestimmten Reihenfolge aufgelistet.

`${post_edited_translations.segment}`

- `ATTR` ist ein vierstelliger Code für das gemeldete Attribut. Einige Attribute sind allen Revisionsprotokollmeldungen gemeinsam, andere sind ereignisspezifisch.
- `type` ist ein vierstelliger Bezeichner des Programmierdatentyps des Wertes, z. B. UI64, FC32 und so weiter. Der Typ ist in Klammern eingeschlossen ().
- `value` ist der Inhalt des Attributs, typischerweise ein numerischer oder Textwert. Werte folgen immer auf einen Doppelpunkt (:). Werte vom Datentyp CSTR sind von doppelten Anführungszeichen " " umgeben.

Datentypen in StorageGRID-Revisionsprotokollmeldungen

In Prüfmeldungen werden unterschiedliche Datentypen verwendet, um Informationen zu speichern.

Typ	Beschreibung
UI32	Vorzeichenlose lange Ganzzahl (32 Bit); sie kann die Zahlen 0 bis 4,294,967,295 speichern.
UI64	Unsigned double long integer (64 Bit); es können die Zahlen 0 bis 18.446.744.073.709.551.615 gespeichert werden.
FC32	Vierstellige Konstante; ein 32-Bit-Ganzzahlwert ohne Vorzeichen, dargestellt als vier ASCII-Zeichen wie „ABCD“.
IPAD	Wird für IP-Adressen verwendet.
CSTR	Ein Array von UTF-8-Zeichen variabler Länge. Zeichen können gemäß den folgenden Konventionen maskiert werden: • Backslash ist \. • Der Wagenrücklauf ist \r. • Doppelte Anführungszeichen sind \". • Zeilenvorschub (neue Zeile) ist \n. • Zeichen können durch ihre hexadezimalen Entsprechungen ersetzt werden (im Format \xHH, wobei HH der hexadezimale Wert ist, der das Zeichen darstellt).

Ereignisspezifische Daten in StorageGRID Revisionsprotokollmeldungen

Jede Prüfmeldung im Revisionsprotokoll erfasst Daten, die spezifisch für ein Systemereignis sind.

Nach dem einleitenden `[AUDT:]` Container, der die Nachricht selbst identifiziert, liefern die nächsten Attribute Informationen über das Ereignis oder die Aktion, die in der Revisionsprotokollmeldung beschrieben wird. Diese Attribute sind im folgenden Beispiel hervorgehoben:

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\ (FC32\):SUCS\]
\[TIME\ (UI64\):11454\]\[SAIP\ (IPAD\):"10.224.0.100"\]\[S3AI\ (CSTR\):"60025
621595611246499"\]
\[SACC\ (CSTR\):"account"\]\[S3AK\ (CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zK1umRsKJA=="\]
\[SUSR\ (CSTR\):"urn:sgws:identity:60025621595611246499:root"\]
\[SBAI\ (CSTR\):"60025621595611246499"\]\[SBAC\ (CSTR\):"account"\]\[S3BK\ (C
STR\):"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] [A
MID (FC32):S3RQ]
\[ATID (UI64):15552417629170647261\]
```

Das ATYP Element (im Beispiel unterstrichen) identifiziert das Ereignis, das die Nachricht ausgelöst hat. Diese Beispielnachricht enthält den "SHEA" Nachrichtencode ([ATYP(FC32):SHEA]), was darauf hinweist, dass sie durch eine erfolgreiche S3 HEAD-Anfrage generiert wurde.

Gemeinsame Elemente in StorageGRID Revisionsprotokollmeldungen

Alle Prüfmeldungen enthalten die gemeinsamen Elemente.

Code	Typ	Beschreibung
AMID	FC32	Modul-ID: Eine vierstellige Kennung des Moduls, das die Meldung generiert hat. Dies gibt den Codeabschnitt an, in dem die Prüfmeldung erzeugt wurde.
ANID	UI32	Knoten-ID: Die Grid-Knoten-ID, die dem Dienst zugewiesen ist, der die Nachricht generiert hat. Jedem Dienst wird bei der Konfiguration und Installation des StorageGRID Systems eine eindeutige Kennung zugewiesen. Diese ID kann nicht geändert werden.

Code	Typ	Beschreibung
ASES	UI64	Audit Session Identifier: In früheren Versionen gab dieses Element den Zeitpunkt an, zu dem das Audit-System nach dem Start des Dienstes initialisiert wurde. Dieser Zeitwert wurde in Mikrosekunden seit dem Betriebssystem-Epoch (00:00:00 UTC am 1. Januar 1970) gemessen. Hinweis: Dieses Element ist veraltet und wird in Prüfmeldungen nicht mehr angezeigt.
ASQN	UI64	Sequenzzähler: In früheren Versionen wurde dieser Zähler für jede generierte Audit-Nachricht auf dem Grid-Knoten (ANID) inkrementiert und beim Neustart des Dienstes auf Null zurückgesetzt. Hinweis: Dieses Element ist veraltet und wird in Prüfmeldungen nicht mehr angezeigt.
ATID	UI64	Trace ID: Eine Kennung, die von allen Nachrichten gemeinsam genutzt wird, die durch ein einzelnes Ereignis ausgelöst wurden.
ATIM	UI64	Zeitstempel: Der Zeitpunkt, zu dem das Ereignis generiert wurde, das die Revisionsprotokollmeldung ausgelöst hat, gemessen in Mikrosekunden seit dem Betriebssystem-Epoch (00:00:00 UTC am 1. Januar 1970). Zu beachten ist, dass die meisten verfügbaren Tools zur Umrechnung des Zeitstempels in lokale Datums- und Zeitangaben auf Millisekunden basieren. Das Runden oder Abschneiden des protokollierten Zeitstempels kann erforderlich sein. Die lesbare Zeitangabe am Anfang der Revisionsprotokollnachricht in der <code>audit.log</code> Datei ist das ATIM-Attribut im ISO 8601-Format. Datum und Uhrzeit werden als <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> dargestellt, wobei T ein Zeichen ist, das den Beginn des Zeitsegments des Datums angibt. <code>UUUUUU</code> sind Mikrosekunden.
ATYP	FC32	Ereignistyp: Eine vierstellige Kennung des protokollierten Ereignisses. Dies bestimmt den „Nutzlast“-Inhalt der Nachricht: die enthaltenen Attribute.
DURCHSCHNITT	UI32	Version: Die Version der Revisionsmeldung. Da die StorageGRID Software weiterentwickelt wird, können neue Versionen von Diensten neue Funktionen in der Revisionsberichterstattung enthalten. Dieses Feld ermöglicht die Abwärtskompatibilität im AMS-Dienst zur Verarbeitung von Meldungen älterer Dienstversionen.
RSLT	FC32	Ergebnis: Das Resultat eines Ereignisses, Prozesses oder einer Transaktion. Ist es für eine Nachricht nicht relevant, wird NONE anstelle von SUCS verwendet, damit die Nachricht nicht versehentlich gefiltert wird.

StorageGRID Revisionsprotokoll-Nachrichtenformat und Beispiele

Detaillierte Informationen finden Sie in jeder Revisionsmeldung. Alle Revisionsmeldungen verwenden dasselbe Format.

Das Folgende ist ein Beispiel für eine Revisionsmeldung, wie sie in der `audit.log`-Datei erscheinen kann:

```
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]]
```

Die Prüfmeldung enthält Informationen über das aufgezeichnete Ereignis sowie Informationen über die Prüfmeldung selbst.

`${post_edited_translations.segment}`

```
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]]
```

Der Wert des Attributs ATYP ist SPUT. "`${post_edited_translations.segment}`" steht für eine S3 PUT-Transaktion, die das Hochladen eines Objekts in einen Bucket protokolliert.

Die folgende Revisionsprotokollmeldung zeigt auch den Bucket an, dem das Objekt zugeordnet ist:

```
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]]
```

Um den Zeitpunkt des PUT-Ereignisses zu ermitteln, ist der UTC-Zeitstempel (Koordinierte Weltzeit) am

Anfang der Revisionsprotokollnachricht zu beachten. Dieser Wert ist eine für Menschen lesbare Version des ATIM-Attributs der Revisionsprotokollnachricht selbst:

```
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):15792241
44102530435]]
```

ATIM erfasst die Zeit in Mikrosekunden seit dem Beginn der UNIX-Epoche. In dem Beispiel entspricht der Wert 1405631878959669 Donnerstag, 17. Juli 2014 21:17:59 UTC.

Audit-Meldungen und der Objektlebenszyklus

Wenn Revisionsprotokollmeldungen in StorageGRID generiert werden

Bei jedem Import, Abruf oder Löschen eines Objekts werden Audit-Meldungen generiert. Diese Transaktionen lassen sich im Revisionsprotokoll anhand der S3-API-spezifischen Audit-Meldungen identifizieren.

`${post_edited_translations.segment}`

Protokoll	Code
<code>\${post_edited_translations.segment}</code>	S3BK (Bucket), S3KY (Key) oder beides
Verknüpfung interner Abläufe	<code>\${post_edited_translations.segment}</code>

Zeitpunkt der Revisionsprotokollmeldungen

`${post_edited_translations.segment}`

Audit-Meldungen für Objektaufnahmetransaktionen in StorageGRID

Client-Ingest-Transaktionen lassen sich im Revisionsprotokoll anhand S3-API-spezifischer Audit-Meldungen identifizieren.

In der folgenden Tabelle sind nicht alle Revisionsmeldungen aufgeführt, die während einer Ingest-Transaktion generiert werden. Es sind nur die Meldungen enthalten, die zur Nachverfolgung der Ingest-Transaktion erforderlich sind.

S3 Ingest Revisionsprotokollnachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
<code>\${post_edited_translations.segment}</code>	S3 PUT Transaktion	<code>\${post_edited_translations.segment}</code>	CBID, S3BK, S3KY	"SPUT: S3 PUT"
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Die ILM Richtlinie ist für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

`${post_edited_translations.segment}`

Die folgende Reihe von Prüfmeldungen ist ein Beispiel für die Prüfmeldungen, die generiert und im Revisionsprotokoll gespeichert werden, wenn ein S3-Client ein Objekt in einen Storage Node (LDR-Service) einliest.

`${post_edited_translations.segment}`



Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Revisionsprotokollmeldungen aufgeführt. Es sind nur diejenigen aufgeführt, die sich auf die S3 Ingest-Transaktion (SPUT) beziehen.

Dieses Beispiel setzt voraus, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Nachricht wird generiert, um anzuzeigen, dass eine S3 PUT-Transaktion ausgelöst wurde, um ein Objekt in einem bestimmten Bucket zu erstellen.

```
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: Objektregeln erfüllt

Die ORLM-Meldung signalisiert, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Meldung enthält die CBID des Objekts und den Namen der angewendeten ILM-Regel.

Bei replizierten Objekten enthält das Feld LOCS die LDR-Knoten-ID und die Volumen-ID der Objektstandorte.

```
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]]
```

Bei Objekten, die mit einem Löschcodierverfahren versehen sind, enthält das Feld LOCS die Löschcodierungsprofil-ID und die Löschcodierungsgruppen-ID

```
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]]
```

Das Feld PATH enthält Informationen zu S3-Bucket und Schlüssel.

```
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]]
```

Auditmeldungen für Objektlöschvorgänge in StorageGRID

Objektlöschvorgänge im Revisionsprotokoll lassen sich durch das Auffinden von S3-API-spezifischen Audit-Meldungen identifizieren.

Nicht alle während einer Löschtransaktion generierten Revisionsprotokollmeldungen sind in den folgenden Tabellen aufgeführt. Nur Meldungen, die zur Nachverfolgung der Löschtransaktion erforderlich sind, sind enthalten.

`${post_edited_translations.segment}`

Code	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	<code>\${post_edited_translations.segment}</code>	CBID, S3KY	"SDEL: S3-DELETE"

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt von einem Storage Node (LDR-Service) löscht, wird eine Audit-Meldung generiert und im Revisionsprotokoll gespeichert.



Im folgenden Beispiel sind nicht alle während einer Löschtransaktion generierten Revisionsmeldungen aufgeführt. Es sind nur diejenigen aufgeführt, die sich auf die S3-Löschtransaktion (SDEL) beziehen.

SDEL: S3 Löschen

Die Objektlöschung beginnt, wenn der Client eine DeleteObject-Anfrage an einen LDR-Service sendet. Die Nachricht enthält den Bucket, aus dem das Objekt gelöscht werden soll, sowie den S3 Key des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
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]]
```

Audit-Meldungen für Objektabruftransaktionen in StorageGRID

Objektabruftransaktionen lassen sich im Revisionsprotokoll anhand S3-API-spezifischer Audit-Meldungen identifizieren.

Nicht alle während einer Abruftransaktion generierten Revisionsprotokollmeldungen sind in der folgenden Tabelle aufgeführt. Nur Meldungen, die zur Nachverfolgung der Abruftransaktion erforderlich sind, sind enthalten.

S3-Abruf-Revisionsprotokollmeldungen

Code	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 GET	Anfrage zum Abrufen eines Objekts aus einem Bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Speicherknoten (LDR-Dienst) abrufen, wird eine Audit-Meldung generiert und im Revisionsprotokoll gespeichert.

Beachten Sie, dass im folgenden Beispiel nicht alle während einer Transaktion generierten Revisionsprotokollmeldungen aufgeführt sind. Es sind nur diejenigen aufgeführt, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET: S3 GET

Die Objektabfrage beginnt, wenn der Client eine GetObject-Anfrage an einen LDR Service sendet. Die Nachricht enthält den Bucket, aus dem das Objekt abgerufen werden soll, sowie den S3 Key des Objekts, der zur Identifizierung des Objekts dient.

```
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]
]
```

Wenn die Bucket-Richtlinie dies zulässt, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört. Die Revisionsmeldung enthält Informationen über das Mandantenkonto des Bucket-Besitzers, sodass Sie diese anonymen und kontoübergreifenden Anforderungen nachverfolgen können.

In der folgenden Beispielnachricht sendet der Client eine GetObject-Anfrage für ein Objekt, das in einem Bucket gespeichert ist, der ihm nicht gehört. Die Werte für SBAI und SBAC geben die Mandantenkonto-ID und den Namen des Bucket-Inhabers an, die sich von der Mandantenkonto-ID und dem Namen des Clients unterscheiden, die in S3AI und SACC aufgezeichnet sind.

```
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]]
```

Beispiel: S3 Select für ein Objekt

Wenn ein S3-Client eine S3 Select-Abfrage für ein Objekt ausführt, werden Audit-Meldungen generiert und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Revisionsmeldungen im folgenden Beispiel aufgeführt sind. Es sind nur die Meldungen aufgeführt, die sich auf die S3 Select Transaktion (SelectObjectContent) beziehen.

Jede Abfrage führt zu zwei Prüfmeldungen: einer, die die Autorisierung der S3 Select-Anfrage durchführt (das Feld S3SR ist auf "select" gesetzt) und einer nachfolgenden Standard-GET-Operation, die die Daten während der Verarbeitung aus dem Speicher abruft.

```
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][SAI
P(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]]
```

Revisionsprotokoll-Meldungen für Aktualisierungen der S3-Objektmetadaten in StorageGRID

Audit-Meldungen werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

S3 Metadatenaktualisierungs-Auditmeldungen

Code	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3 Metadaten aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein ingestiertes Objekt aktualisiert.	CBID, S3KY, HTRH	"SUPD: S3 Metadaten aktualisiert"

Beispiel: S3-Metadatenaktualisierung

Das Beispiel zeigt eine erfolgreiche Transaktion zur Aktualisierung der Metadaten eines bestehenden S3-Objekts.

SUPD: S3 Metadatenaktualisierung

Der S3-Client sendet eine Anfrage (SUPD) zur Aktualisierung der angegebenen Metadaten (`x-amz-meta-*` für das S3-Objekt (S3KY). In diesem Beispiel sind die Anfrageheader im Feld HTRH enthalten, da es als Audit-Protokollheader konfiguriert wurde (*Configuration* > **Monitoring** > **Audit and syslog server**). Siehe ["Logverwaltung und externen Syslog-Server konfigurieren"](#).

```
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]]
```

Audit-Meldungen

Erfahren Sie mehr über die Arten und Codes von Revisionsprotokollmeldungen in StorageGRID

Detaillierte Beschreibungen der vom System zurückgegebenen Revisionsprotokollmeldungen sind in den folgenden Abschnitten aufgeführt. Jede Revisionsprotokollmeldung wird zunächst in einer Tabelle aufgeführt, die zusammengehörige Meldungen nach der Aktivitätsklasse gruppiert, die die Meldung repräsentiert. Diese Gruppierungen sind sowohl für das Verständnis der Arten von Aktivitäten, die protokolliert werden, als auch für die Auswahl der gewünschten Art der Filterung von Revisionsprotokollmeldungen nützlich.

Die Revisionsprotokoll-Meldungen sind ebenfalls alphabetisch nach ihren vierstelligen Codes aufgelistet. Diese alphabetische Liste ermöglicht es Ihnen, Informationen zu bestimmten Meldungen zu finden.

Die in diesem Kapitel verwendeten vierstelligen Codes sind die ATYP-Werte, die in den Revisionsprotokollmeldungen zu finden sind, wie im folgenden Beispiel gezeigt:

```
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]]
```

Informationen zum Festlegen von Ebenen für Revisionsmeldungen, zum Ändern von Protokollzielen und zur Verwendung eines externen Syslog-Servers für Ihre Revisionsinformationen siehe ["Logverwaltung und externen Syslog-Server konfigurieren"](#)

Kategorien von Audit-Nachrichten

Auditmeldungen für Systemereignisse in StorageGRID

Die zur Kategorie „Systemprüfung“ gehörenden Prüfmeldungen werden für Ereignisse verwendet, die mit dem Prüfsystem selbst, Grid-Knotenzuständen, systemweiten Aufgabenaktivitäten (Grid-Aufgaben) und Service-Backup-Operationen zusammenhängen.

Code	\${post_edited_translations.segment}	Siehe
ECMC	Fehlendes löschcodiertes Datenfragment: Gibt an, dass ein fehlendes löschcodiertes Datenfragment erkannt wurde.	"ECMC: Fehlendes löschcodiertes Datenfragment"
ECOC	Beschädigtes Erasure-Coded-Datenfragment: Gibt an, dass ein beschädigtes Erasure-Coded-Datenfragment erkannt wurde.	"ECOC: Beschädigtes löschcodiertes Datenfragment"

Code	<code>\${post_edited_translations.segment}</code>	Siehe
ETAF	Sicherheitsauthentifizierung fehlgeschlagen: Ein Verbindungsversuch mit Transport Layer Security (TLS) schlug fehl.	"ETAF: Sicherheitsauthentifizierung fehlgeschlagen"
GNRG	GNDS-Registrierung: Ein Dienst hat Informationen über sich selbst im StorageGRID System aktualisiert oder registriert.	"GNRG: GNDS-Registrierung"
GNUR	GNDS-Abmeldung: Ein Dienst hat sich vom StorageGRID System abgemeldet.	"GNUR: GNDS Abmeldung"
GTED	Grid Task beendet: Der CMN-Dienst hat die Verarbeitung der Grid Task abgeschlossen.	"GTED: Grid-Task beendet"
GTST	Grid Task gestartet: Der CMN-Dienst hat mit der Verarbeitung der Grid Task begonnen.	"GTST: Grid Task gestartet"
GTSU	Grid-Aufgabe eingereicht: Eine Grid-Aufgabe wurde an den CMN-Service übermittelt.	"GTSU: Grid Task eingereicht"
LLST	Standort verloren: Diese Revisionsprotokollmeldung wird generiert, wenn ein Standort verloren geht.	"LLST: Standort verloren"
OLST	Objekt verloren: Ein angefordertes Objekt konnte im StorageGRID System nicht gefunden werden.	"OLST: System hat verlorenes Objekt erkannt"
SADD	Security Audit Disable: Die Protokollierung von Revisionsprotokollnachrichten wurde deaktiviert.	"SADD: Deaktivierung des Security Audit"
SADE	Sicherheitsüberwachung aktiviert: Die Protokollierung von Audit-Meldungen wurde wiederhergestellt.	"SADE: Sicherheitsaudit-Aktivierung"
SVRF	Objektspeicher Überprüfung fehlgeschlagen: Ein Inhaltsblock hat die Überprüfungsprüfungen nicht bestanden.	"SVRF: Objektspeicherüberprüfung fehlgeschlagen"
SVRU	Objektspeicherprüfung Unbekannt: Unerwartete Objektdaten im Objektspeicher erkannt.	"SVRU: Objektspeicher Überprüfung unbekannt"
SYSD	Knoten-Stopp: Ein Herunterfahren wurde angefordert.	"SYSD: Knotenstopp"
SYST	Knotenstopp: Ein Dienst hat einen ordnungsgemäßen Stopp eingeleitet.	"SYST: Knoten wird gestoppt"

Code	<code>\${post_edited_translations.segment}</code>	Siehe
SYSU	Knotenstart: Ein Dienst wurde gestartet; die Art des vorherigen Herunterfahrens ist in der Meldung angegeben.	"SYSU: Knotenstart"

Audit-Meldungen für Objektspeicher-Ereignisse in StorageGRID

Die zur Kategorie „Objektspeicher-Audit“ gehörenden Audit-Meldungen werden für Ereignisse im Zusammenhang mit der Speicherung und Verwaltung von Objekten innerhalb des StorageGRID Systems verwendet. Dazu gehören das Speichern und Abrufen von Objekten, Grid-Node zu Grid-Node Transfers sowie Verifizierungen.



Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, sobald Funktionen veraltet sind. Falls ein Prüfcode nicht aufgeführt ist, bieten frühere Versionen dieses Themas Informationen zu älteren SG Releases. Zum Beispiel, "[StorageGRID 11.8 Objektspeicher Revisionsprotokollmeldungen](#)".

Code	Beschreibung	Siehe
<code>\${post_edited_translation s.segment}</code>	Bucket Read Only-Anfrage: Ein Bucket ist in den schreibgeschützten Modus gewechselt oder hat diesen verlassen.	" <code>\${post_edited_translation s.segment}</code> "
CBSE	Object Send End: Die Quellentität hat einen Datentransfer von Grid-Node zu Grid-Node abgeschlossen.	"CBSE: Objekt Send End"
<code>\${post_edited_translation s.segment}</code>	Objektempfangsende: Die Zielentität hat einen Datentransfer von Grid-Node zu Grid-Node abgeschlossen.	"CBRE: Objekt-Empfangsende"
CGRR	Gridübergreifende Replikationsanforderung: StorageGRID hat versucht, eine gridübergreifende Replikationsoperation durchzuführen, um Objekte zwischen Buckets in einer Grid Federation-Verbindung zu replizieren.	" <code>\${post_edited_translation s.segment}</code> "
EBDL	Löschen eines leeren Buckets: Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, der alle Objekte löscht (führt eine Bucket-Leerungsoperation durch).	"EBDL: Leerer Bucket löschen"
EBKR	Anfrage zum Leeren eines Buckets: Ein Benutzer hat eine Anfrage gesendet, um das Leeren eines Buckets zu aktivieren oder zu deaktivieren (d. h. Bucket-Objekte zu löschen oder das Löschen von Objekten zu stoppen).	" <code>\${post_edited_translation s.segment}</code> "

Code	Beschreibung	Siehe
<code>\${post_edited_translation s.segment}</code>	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	"\${post_edited_translation s.segment}"
<code>\${post_edited_translation s.segment}</code>	Object Store Remove: Ein Inhaltsblock wurde von einem Grid-Node gelöscht und kann nicht mehr direkt angefordert werden.	"\${post_edited_translation s.segment}"

Audit-Meldungen für Client-Lesevorgänge in StorageGRID

Client-Lese-Auditmeldungen werden protokolliert, wenn eine S3-Clientanwendung eine Anfrage zum Abrufen eines Objekts stellt.

Code	Beschreibung	Wird verwendet von	Siehe
S3SL	S3 Select-Anfrage: Protokolliert den Abschluss einer S3 Select-Anfrage, die an den Client zurückgesendet wurde. Die S3SL-Nachricht kann Details zu Fehlermeldung und Fehlercode enthalten. Die Anfrage war möglicherweise nicht erfolgreich.	S3 Client	"S3SL: S3 Select Anfrage"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfmeldung das Feld S3SR.	S3 Client	"SGET: S3 GET"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Buckets zu überprüfen.	S3 Client	"SHEA: S3 HEAD"

Audit-Meldungen für Client-Schreibvorgänge in StorageGRID

Client-Schreib-Auditmeldungen werden protokolliert, wenn eine S3-Clientanwendung eine Anfrage zum Erstellen oder Ändern eines Objekts stellt.

Code	Beschreibung	Wird verwendet von	Siehe
OVWR	Objektüberschreibung: Protokolliert eine Transaktion zum Überschreiben eines Objekts mit einem anderen Objekt.	S3 Client	"OVWR: Objektüberschreibung"

Code	Beschreibung	Wird verwendet von	Siehe
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfmeldung das Feld S3SR.	S3 Client	"SDEL: S3-DELETE"
SPOS	S3 POST: Protokolliert eine erfolgreiche Transaktion zur Wiederherstellung eines Objekts aus dem AWS Glacier Speicher in einen Cloud Storage Pool.	S3 Client	"SPOS: S3 POST"
`\${post_edited_translations.segment}`	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfmeldung das Feld S3SR.	S3 Client	"SPUT: S3 PUT"
SUPD	S3 Metadata aktualisiert: Protokolliert eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein bestehendes Objekt oder einen Bucket.	S3 Client	"SUPD: S3 Metadaten aktualisiert"

StorageGRID-Verwaltungs-Revisionsprotokollmeldungen

Die Kategorie „Management“ protokolliert Benutzeranfragen an die Management API.

Code	`\${post_edited_translations.segment}`	Siehe
MGAU	Management API Auditmeldung: Ein Protokoll der Benutzeranfragen.	"MGAU: Management-Audit-Mitteilung"

StorageGRID ILM-Revisionsprotokollmeldungen

Die zur ILM-Auditkategorie gehörenden Audit-Meldungen werden für Ereignisse im Zusammenhang mit Information Lifecycle Management (ILM)-Operationen verwendet.

Code	`\${post_edited_translations.segment}`	Siehe
IDEL	`\${post_edited_translations.segment}`	"`\${post_edited_translations.segment}`"

Code	<code>\${post_edited_translations.segment}</code>	Siehe
<code>\${post_edited_translations.segment}</code>	Bereinigung überschriebener Objekte. Diese Audit-Meldung wird generiert, wenn ein überschriebenes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	"LKCU: Bereinigung überschriebener Objekte"
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	"ORLM: Objektregeln erfüllt"

Referenz der Prüfmeldung

BROR Revisionsprotokollmeldung für schreibgeschützte Bucket-Anfragen in StorageGRID

Der LDR Service generiert diese Revisionsprotokollmeldung, wenn ein Bucket in den schreibgeschützten Modus wechselt oder diesen verlässt. Zum Beispiel wechselt ein Bucket in den schreibgeschützten Modus, während alle Objekte gelöscht werden.

Code	Feld	Beschreibung
BKHD	Bucket-UUID	Die Bucket-ID.
BROV	<code>\${post_edited_translations.segment}</code>	Ob der Bucket in den schreibgeschützten Zustand versetzt wird oder den schreibgeschützten Zustand verlässt (1 = schreibgeschützt, 0 = nicht schreibgeschützt).
BROS	Bucket-Schreibschutzgrund	Der Grund, warum der Bucket schreibgeschützt wird oder den schreibgeschützten Zustand verlässt. Zum Beispiel emptyBucket.
S3AI	S3 Mandantenkonto-ID	Die ID des Mandantenkontos, das die Anfrage gesendet hat. Ein leerer Wert zeigt anonymer Zugriff an.
S3BK	S3 Bucket	Der Name des S3 Buckets.

CBRB-Revisionsprotokollmeldung für Objektempfangsbeginn in StorageGRID

Im normalen Systembetrieb werden Inhaltsblöcke kontinuierlich zwischen verschiedenen Knoten übertragen, während Daten abgerufen, repliziert und gespeichert werden. Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen initiiert wird, wird diese Nachricht von der Zielentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungsken-nung	Die eindeutige Kennung der Node-to-Node-Sitzung/Verbindung.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Transferrichtung	Gibt an, ob die CBID-Übertragung per Push- oder Pull-Anfrage initiiert wurde: \${post_edited_translations.segment} PULL: Die Übertragungsoperation wurde von der empfangenden Entität angefordert.
CTSR	Quellentität	Die Knoten-ID der Quelle (des Absenders) des CBID-Transfers.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) des CBID-Transfers.
CTSS	Startsequenzanzahl	Zeigt die erste angeforderte Sequenznummer an. Bei Erfolg beginnt der Datentransfer ab dieser Sequenznummer.
CTES	Anzahl der erwarteten Endsequenzen	Zeigt die zuletzt angeforderte Sequenzanzahl an. Bei Erfolg gilt der Datentransfer als abgeschlossen, sobald diese Sequenzanzahl empfangen wurde.
RSLT	Transfer-Startstatus	Status zum Zeitpunkt des Transferbeginns: SUCS: Übertragung erfolgreich gestartet.

Diese Prüfmeldung bedeutet, dass eine Node-to-Node-Datentransferoperation für ein einzelnes Inhaltselement initiiert wurde, das anhand seiner Content Block Identifier identifiziert wird. Die Operation fordert Daten von „Start Sequence Count“ bis „Expected End Sequence Count“ an. Sendende und empfangende Knoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss im System nachzuvollziehen und, in Kombination mit Storage-Auditmeldungen, die Anzahl der Replikate zu verifizieren.

CBRE-Revisionsprotokollmeldung für das Ende des Objektempfangs in StorageGRID

Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen abgeschlossen ist, wird diese Nachricht von der Zielentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.

Code	Feld	Beschreibung
CTDR	Transferrichtung	Gibt an, ob die CBID-Übertragung per Push- oder Pull-Anfrage initiiert wurde: \${post_edited_translations.segment} PULL: Die Übertragungsoperation wurde von der empfangenden Entität angefordert.
CTSR	Quellentität	Die Knoten-ID der Quelle (des Absenders) des CBID-Transfers.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) des CBID-Transfers.
CTSS	Startsequenzanzahl	Gibt die Sequenznummer an, bei der der Datentransfer begonnen hat.
CTAS	Tatsächliche Endsequenzanzahl	Gibt die zuletzt erfolgreich übertragene Sequenzanzahl an. Wenn die tatsächliche Endsequenzanzahl mit der Startsequenzanzahl übereinstimmt und das Übertragungsergebnis nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Transferergebnis	Das Ergebnis des Datentransfers (aus Sicht der sendenden Instanz): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während des Transfers verloren CTMO: Zeitüberschreitung bei Verbindungsaufbau oder Übertragung UNRE: Zielknoten-ID nicht erreichbar CRPT: Die Übertragung endete aufgrund des Empfangs beschädigter oder ungültiger Daten.

Diese Prüfmeldung bedeutet, dass eine Node-to-Node-Datentransfer-Operation abgeschlossen wurde. War das Übertragungsergebnis erfolgreich, wurden Daten vom „Start Sequence Count“ bis zum „Actual End Sequence Count“ übertragen. Sendende und empfangende Knoten werden anhand ihrer Knoten-IDs identifiziert. Diese Informationen können dazu verwendet werden, den Systemdatenfluss nachzuverfolgen sowie Fehler zu lokalisieren, zu erfassen und zu analysieren. In Verbindung mit Storage Audit-Meldungen kann damit auch die Anzahl der Replikate überprüft werden.

CBSB-Revisionsprotokollmeldung für Objektsendebeginn in StorageGRID

Im normalen Systembetrieb werden Inhaltsblöcke kontinuierlich zwischen verschiedenen Knoten übertragen, während Daten abgerufen, repliziert und gespeichert werden. Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen initiiert wird, gibt die Quellentität diese Nachricht aus.

Code	Feld	Beschreibung
CNID	Verbindungs- kennung	Die eindeutige Kennung der Node-to-Node-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Transferrichtung	Gibt an, ob die CBID-Übertragung per Push- oder Pull-Anfrage initiiert wurde: <code>#{post_edited_translations.segment}</code> PULL: Die Übertragungsoperation wurde von der empfangenden Entität angefordert.
CTSR	Quellentität	Die Knoten-ID der Quelle (des Absenders) des CBID-Transfers.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) des CBID-Transfers.
CTSS	Startsequenzanzahl	Zeigt die erste angeforderte Sequenznummer an. Bei Erfolg beginnt der Datentransfer ab dieser Sequenznummer.
CTES	Anzahl der erwarteten Endsequenzen	Zeigt die zuletzt angeforderte Sequenzanzahl an. Bei Erfolg gilt der Datentransfer als abgeschlossen, sobald diese Sequenzanzahl empfangen wurde.
RSLT	Transfer-Startstatus	Status zum Zeitpunkt des Transferbeginns: SUCS: Übertragung erfolgreich gestartet.

Diese Prüfmeldung bedeutet, dass eine Node-to-Node-Datentransferoperation für ein einzelnes Inhaltselement initiiert wurde, das anhand seiner Content Block Identifier identifiziert wird. Die Operation fordert Daten von „Start Sequence Count“ bis „Expected End Sequence Count“ an. Sendende und empfangende Knoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss im System nachzuvollziehen und, in Kombination mit Storage-Auditmeldungen, die Anzahl der Replikate zu verifizieren.

CBSE-Revisionsprotokollmeldung für das Ende des Objektsendens in StorageGRID

Wenn der Datentransfer eines Inhaltsblocks von einem Knoten zu einem anderen abgeschlossen ist, wird diese Meldung von der Quellentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungs- kennung	Die eindeutige Kennung der Node-to-Node-Sitzung/Verbindung.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Transferrichtung	Gibt an, ob die CBID-Übertragung per Push- oder Pull-Anfrage initiiert wurde: \${post_edited_translations.segment} PULL: Die Übertragungsoperation wurde von der empfangenden Entität angefordert.
CTSR	Quellentität	Die Knoten-ID der Quelle (des Absenders) des CBID-Transfers.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) des CBID-Transfers.
CTSS	Startsequenzanzahl	Gibt die Sequenznummer an, bei der der Datentransfer begonnen hat.
CTAS	Tatsächliche Endsequenzanzahl	Gibt die zuletzt erfolgreich übertragene Sequenzanzahl an. Wenn die tatsächliche Endsequenzanzahl mit der Startsequenzanzahl übereinstimmt und das Übertragungsergebnis nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Transferergebnis	Das Ergebnis des Datentransfers (aus Sicht der sendenden Instanz): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während des Transfers verloren CTMO: Zeitüberschreitung bei Verbindungsaufbau oder Übertragung UNRE: Zielknoten-ID nicht erreichbar CRPT: Die Übertragung endete aufgrund des Empfangs beschädigter oder ungültiger Daten.

Diese Prüfmeldung bedeutet, dass eine Node-to-Node-Datentransfer-Operation abgeschlossen wurde. War das Übertragungsergebnis erfolgreich, wurden Daten vom „Start Sequence Count“ bis zum „Actual End Sequence Count“ übertragen. Sendende und empfangende Knoten werden anhand ihrer Knoten-IDs identifiziert. Diese Informationen können dazu verwendet werden, den Systemdatenfluss nachzuverfolgen sowie Fehler zu lokalisieren, zu erfassen und zu analysieren. In Verbindung mit Storage Audit-Meldungen kann damit auch die Anzahl der Replikate überprüft werden.

CGRR-Revisionsprotokollmeldung für netzübergreifende Replikationsanforderungen in StorageGRID

Diese Meldung wird generiert, wenn StorageGRID versucht, eine netzübergreifende Replikationsoperation durchzuführen, um Objekte zwischen Buckets in einer Grid-Federation-Verbindung zu replizieren.

Code	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Bytes. Das CSIZ-Attribut wurde in StorageGRID 11.8 eingeführt. Infolgedessen kann es bei Cross-Grid-Replikationsanforderungen, die ein Upgrade von StorageGRID 11.7 auf 11.8 umfassen, zu einer ungenauen Gesamtobjektgröße kommen.
S3AI	S3 Mandantenkonto-ID	Die ID des Mandantenkontos, dem der Bucket gehört, aus dem das Objekt repliziert wird.
GFID	Grid Federation Verbindungs-ID	Die ID der Grid Federation-Verbindung, die für die netzübergreifende Replikation verwendet wird.
BEDIENUNG	CGR Betrieb	Die Art der versuchten netzübergreifenden Replikationsoperation: • 0 = Objekt replizieren • 1 = Mehrteiliges Objekt replizieren • 2 = Replikat-Löschmarkierung
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket Namen.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, das repliziert wurde.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder allgemeinen Fehler (GERR) zurück.

EBDL-Revisionsprotokollmeldung für das Löschen leerer Bucket-Objekte in StorageGRID

Der ILM Scanner hat ein Objekt in einem Bucket gelöscht, der alle Objekte löscht (eine Bucket-Leerungsoperation wird durchgeführt).

Code	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Bytes.
WEG	S3 Bucket/Schlüssel	Der S3 Bucket Name und der S3 Key Name.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.

Code	Feld	Beschreibung
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
RSLT	Ergebnis des Löschvorgangs	Das Ergebnis eines Ereignisses, Prozesses oder einer Transaktion. Falls dies für eine Nachricht nicht relevant ist, wird NONE anstelle von SUCS verwendet, damit die Nachricht nicht versehentlich gefiltert wird.

EBKR-Revisionsprotokollmeldung für leere Bucket-Anfragen in StorageGRID

Diese Meldung bedeutet, dass ein Benutzer eine Anfrage gesendet hat, um den leeren Bucket zu aktivieren oder zu deaktivieren (d. h. Bucket Objekte zu löschen oder das Löschen von Objekten zu stoppen).

Code	Feld	Beschreibung
BUID	Bucket-UUID	Die Bucket-ID.
EBJS	Leere Bucket JSON-Konfiguration	Enthält das JSON, das die aktuelle Empty Bucket-Konfiguration darstellt.
S3AI	S3 Mandantenkonto-ID	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymer Zugriff vorliegt.
S3BK	S3 Bucket	Der Name des S3 Buckets.

ECMC-Revisionsprotokollmeldung für fehlende erasure-coded Daten in StorageGRID

Diese Revisionsprotokollmeldung weist darauf hin, dass das System ein fehlendes, mit Löschcodierung versehenes Datenfragment erkannt hat.

Code	Feld	Beschreibung
VCMC	VCS ID	Der Name des Versionskontrollsystems, das das fehlende Chunk enthält.
MCID	Chunk-ID	Die Kennung des fehlenden, mit Löschcode versehenen Fragments.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NONE'. RSLT ist ein Pflichtfeld in Nachrichten, aber für diese Nachricht nicht relevant. 'NONE' wird anstelle von 'SUCS' verwendet, damit diese Nachricht nicht gefiltert wird.

ECOC audit message für beschädigte, löschcodierte Daten in StorageGRID

Diese Revisionsprotokollmeldung weist darauf hin, dass das System ein beschädigtes, mit Löschcodierung versehenes Datenfragment erkannt hat.

Code	Feld	Beschreibung
VCCO	VCS ID	Der Name des VCS, das den beschädigten Chunk enthält.
VLID	Volume-ID	Das RangeDB Volume, das das beschädigte, mit einem Löschcode versehene Fragment enthält.
CCID	Chunk-ID	Die Kennung des beschädigten, mit einem Löschcode versehenen Fragments.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NONE'. RSLT ist ein Pflichtfeld in Nachrichten, aber für diese Nachricht nicht relevant. 'NONE' wird anstelle von 'SUCS' verwendet, damit diese Nachricht nicht gefiltert wird.

ETAF-Revisionsprotokollmeldung für Sicherheits-Authentifizierungsfehler in StorageGRID

Diese Meldung wird generiert, wenn ein Verbindungsversuch mit Transport Layer Security (TLS) fehlgeschlagen ist.

Code	Feld	Beschreibung
CNID	Verbindungsken nung	Die eindeutige Systemkennung für die TCP/IP-Verbindung, über die die Authentifizierung fehlgeschlagen ist.
RUID	Benutzeridentität	Ein dienstabhängiger Bezeichner, der die Identität des Remote-Benutzers repräsentiert.

Code	Feld	Beschreibung
RSLT	Grundcode	Der Grund für den Fehler: SCNI: Sichere Verbindungsherstellung fehlgeschlagen. CERM: Das Zertifikat fehlte. CERT: Das Zertifikat war ungültig. CERE: Das Zertifikat ist abgelaufen. CERR: Das Zertifikat wurde widerrufen. CSGN: Die Zertifikatssignatur war ungültig. CSGU: Der Zertifikatsunterzeichner war unbekannt. UCRM: Die Benutzeranmeldeinformationen fehlten. UCRI: Die Benutzeranmeldeinformationen waren ungültig. UCRU: Benutzeranmeldeinformationen wurden nicht akzeptiert. TOUT: Zeitüberschreitung bei der Authentifizierung.

Wird eine Verbindung zu einem sicheren Dienst hergestellt, der TLS verwendet, werden die Anmeldeinformationen der Gegenstelle mithilfe des TLS-Profiles und zusätzlicher, im Dienst integrierter Logik überprüft. Schlägt diese Authentifizierung aufgrund ungültiger, unerwarteter oder nicht erlaubter Zertifikate oder Anmeldeinformationen fehl, wird eine Revisionsprotokollmeldung protokolliert. Dies ermöglicht Abfragen nach unautorisierten Zugriffsversuchen und anderen sicherheitsbezogenen Verbindungsproblemen.

Diese Meldung kann durch eine fehlerhafte Konfiguration eines entfernten Systems oder durch Versuche, ungültige oder unzulässige Anmeldeinformationen an das System zu übermitteln, verursacht werden. Diese Revisionsprotokollmeldung sollte überwacht werden, um Versuche zu erkennen, unbefugten Zugriff auf das System zu erlangen.

GNRG audit message für GNDS registration in StorageGRID

Der CMN-Dienst generiert diese Revisionsprotokollmeldung, wenn ein Dienst Informationen über sich selbst im StorageGRID System aktualisiert oder registriert hat.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • SUCS: Erfolgreich • SUNV: Dienst nicht verfügbar • GERR: Sonstiger Fehler
GNID	Knoten-ID	Die Knoten-ID des Dienstes, der die Aktualisierungsanforderung initiiert hat.

Code	Feld	Beschreibung
GNTP	Gerätetyp	Gerätetyp des Grid-Knotens (z. B. BLDR für einen LDR-Dienst).
GNDV	Gerätemodellversion	Die Zeichenkette, die die Gerätemodellversion des Grid-Knotens im DMDL-Bundle identifiziert.
GNGP	Gruppe	Die Gruppe, zu der der Grid-Knoten gehört (im Kontext von Verbindungskosten und Dienstanfrage-Ranking).
GNIA	IP-Adresse	Die IP-Adresse des Grid-Node.

Diese Meldung wird immer dann generiert, wenn ein Grid-Knoten seinen Eintrag im Grid Nodes Bundle aktualisiert.

GNUR-Revisionsprotokollmeldung für die GNDS-Abmeldung in StorageGRID

Der CMN-Dienst generiert diese Revisionsprotokollmeldung, wenn ein Dienst Informationen über sich selbst aus dem StorageGRID-System abgemeldet hat.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • SUCS: Erfolgreich • SUNV: Dienst nicht verfügbar • GERR: Sonstiger Fehler
GNID	Knoten-ID	Die Knoten-ID des Dienstes, der die Aktualisierungsanforderung initiiert hat.

GTED-Revisionsprotokollmeldung für beendete Grid-Aufgaben in StorageGRID

Diese Revisionsprotokollmeldung signalisiert, dass der CMN Service die Verarbeitung der angegebenen Grid Task abgeschlossen und die Task in die Tabelle Historical verschoben hat. Ist das Ergebnis SUCS, ABRT oder ROLF, gibt es eine entsprechende Revisionsprotokollmeldung Grid Task Started. Die anderen Ergebnisse zeigen an, dass die Verarbeitung dieser Grid Task nie begonnen hat.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Grid-Aufgabe über ihren gesamten Lebenszyklus. Hinweis: Die Aufgaben-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe vergeben, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach übermittelt wird. In diesem Fall reicht das Aufgaben-ID-Feld nicht aus, um die Audit-Meldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.
RSLT	Ergebnis	Das Endergebnis der Grid-Task: • <code>\${post_edited_translations.segment}</code> • <code>\${post_edited_translations.segment}</code> • ROLF: Der Grid-Task wurde beendet und konnte den Rollback-Prozess nicht abschließen. • ABRUCH: Die Grid-Aufgabe wurde vom Benutzer abgebrochen, bevor sie gestartet wurde. • EXPR: Die Grid-Task ist abgelaufen, bevor sie gestartet wurde. • <code>\${post_edited_translations.segment}</code> • <code>\${post_edited_translations.segment}</code> • DUPL: Die Grid-Aufgabe wurde als Duplikat abgelehnt.

GTST-Revisionsprotokollmeldung für gestartete Grid-Tasks in StorageGRID

Diese Audit-Meldung weist darauf hin, dass der CMN-Service mit der Verarbeitung des angegebenen Grid-Tasks begonnen hat. Die Audit-Meldung folgt unmittelbar auf die Meldung „Grid Task Submitted“ für Grid-Tasks, die vom internen Grid Task Submission-Service initiiert und für die automatische Aktivierung ausgewählt wurden. Für Grid-Tasks, die an die Tabelle „Pending“ übermittelt wurden, wird diese Meldung generiert, wenn der Benutzer den Grid-Task startet.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	<code>\${post_edited_translations.segment}</code> Hinweis: Die Aufgaben-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe vergeben, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach übermittelt wird. In diesem Fall reicht das Aufgaben-ID-Feld nicht aus, um die Audit-Meldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.
RSLT	Ergebnis	Das Ergebnis. Dieses Feld hat nur einen Wert: • <code>\${post_edited_translations.segment}</code>

GTSU-Revisionsprotokollmeldung für übermittelte Grid-Aufgaben in StorageGRID

`${post_edited_translations.segment}`

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über ihren Lebenszyklus. Hinweis: Die Aufgaben-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe vergeben, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach übermittelt wird. In diesem Fall reicht das Aufgaben-ID-Feld nicht aus, um die Audit-Meldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
TVER	Aufgabenversion	<code>\${post_edited_translations.segment}</code>
TDSC	Aufgabenbeschreibung	Eine für Menschen lesbare Beschreibung der Grid-Aufgabe.
<code>\${post_edited_translations.segment}</code>	Gültig ab Zeitstempel	Der früheste Zeitpunkt (UINT64 Mikrosekunden ab dem 1. Januar 1970 - UNIX-Zeit), zu dem die Grid-Aufgabe gültig ist.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Der späteste Zeitpunkt (UINT64 Mikrosekunden seit dem 1. Januar 1970 - UNIX-Zeit), zu dem die Grid-Aufgabe gültig ist.
TSRC	Quelle	<code>\${post_edited_translations.segment}</code> • TXTB: Die Grid-Aufgabe wurde über das StorageGRID System als signierter Textblock übermittelt. • GRID: Die Grid-Aufgabe wurde über den internen Grid Task Submission Service übermittelt.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Die Art der Aktivierung: • <code>\${post_edited_translations.segment}</code> • PEND: Die Grid-Task wurde in die Pending-Tabelle aufgenommen. Dies ist die einzige Möglichkeit für die TXTB-Quelle.
RSLT	Ergebnis	Das Ergebnis der Einreichung: • SUCS: Die Grid-Aufgabe wurde erfolgreich übermittelt. • <code>\${post_edited_translations.segment}</code>

IDEAL-Revisionsprotokollmeldung für von ILM initiierte Löschungen in StorageGRID

Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.

`${post_edited_translations.segment}`

- **Für Objekte in konformen S3-Buckets:** Diese Meldung wird generiert, wenn ILM den Prozess des automatischen Löschens eines Objekts startet, weil dessen Aufbewahrungsfrist abgelaufen ist (vorausgesetzt, die Einstellung für das automatische Löschen ist aktiviert und Legal Hold ist deaktiviert).
- **Für Objekte in nicht kompatiblen S3-Buckets.** Diese Meldung wird generiert, wenn ILM den Löschvorgang eines Objekts startet, da derzeit keine Platzierungsanweisungen in den aktiven ILM-Richtlinien auf das Objekt zutreffen.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Nur für Objekte in konformen S3 Buckets. 0 (falsch) oder 1 (wahr), gibt an, ob ein konformes Objekt nach Ablauf seines Aufbewahrungszeitraums automatisch gelöscht werden soll, es sei denn, der Bucket unterliegt einem Legal Hold.
CMPL	Compliance: Legal Hold	Nur für Objekte in konformen S3-Buckets. 0 (falsch) oder 1 (wahr), was angibt, ob der Bucket derzeit unter einer rechtlichen Sperre steht.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Nur für Objekte in konformen S3-Buckets. Die Dauer des Aufbewahrungszeitraums des Objekts in Minuten.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Nur für Objekte in konformen S3 Buckets. Die Ingest-Zeit des Objekts. Sie können die Aufbewahrungsfrist in Minuten zu diesem Wert addieren, um zu bestimmen, wann das Objekt aus dem Bucket gelöscht werden kann.
DMRK	<code>\${post_edited_translations.segment}</code>	Die Versions-ID des Löschmarkers, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wird. Operationen an Buckets schließen dieses Feld nicht ein.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.

Code	Feld	Beschreibung
<code>\${post_edited_translations.segment}</code>	Standorte	Der Speicherort der Objektdaten innerhalb des StorageGRID Systems. Der Wert für LOCS ist "", wenn das Objekt keine Speicherorte hat (zum Beispiel, wenn es gelöscht wurde). <code>\${post_edited_translations.segment}</code> CLDI: Bei replizierten Objekten die LDR-Knoten-ID und die Volume-ID des Objektstandorts. CLNL: ARC-Knoten-ID des Objektstandorts, falls die Objektdaten archiviert sind.
WEG	S3 Bucket/Schlüssel	Der S3 Bucket Name und der S3 Key Name.
RSLT	Ergebnis	Das Ergebnis der ILM-Operation. <code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	• Wenn ein Objekt in einem konformen S3-Bucket automatisch gelöscht wird, weil seine Aufbewahrungsfrist abgelaufen ist, ist dieses Feld leer. • Wird das Objekt gelöscht, weil keine Platzierungsanweisungen mehr auf das Objekt zutreffen, zeigt dieses Feld die für Menschen lesbare Bezeichnung der letzten ILM-Regel an, die auf das Objekt angewendet wurde.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines gelöschten Objekts. Operationen an Buckets und Objekten in nicht versionierten Buckets enthalten dieses Feld nicht.

LKCU-Revisionsprotokollmeldung zur Bereinigung überschriebener Objekte in StorageGRID

Diese Meldung wird generiert, wenn StorageGRID ein überschriebenes Objekt entfernt, das zuvor bereinigt werden musste, um Speicherplatz freizugeben. Ein Objekt wird überschrieben, wenn ein S3-Client ein Objekt in einen Pfad schreibt, der bereits ein Objekt enthält. Die Entfernung erfolgt automatisch und im Hintergrund.

Code	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.
LTyp	Art der Bereinigung	<i>Nur für den internen Gebrauch.</i>
LUID	Entfernte Objekt-UUID	Die Kennung des entfernten Objekts.
WEG	S3 Bucket/Schlüssel	Der S3 Bucket Name und der S3 Key Name.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
UUID	Universell eindeutiger Bezeichner	Die Kennung des noch existierenden Objekts. Dieser Wert ist nur verfügbar, wenn das Objekt nicht gelöscht wurde.

LKDM-Revisionsprotokollmeldung zur Bereinigung von geleakten Objekten in StorageGRID

Diese Meldung wird generiert, wenn ein geleakter Chunk bereinigt oder gelöscht wurde. Ein Chunk kann Teil eines replizierten Objekts oder eines erasure-codierten Objekts sein.

Code	Feld	Beschreibung
CLOC	Chunk-Position	Der Dateipfad des gelöschten, durchgesickerten Datenblocks.
CTYP	Chunk Typ	Chunk-Typ: ec: Erasure-coded object chunk repl: Replicated object chunk

Code	Feld	Beschreibung
LTyp	Lecktyp	Die fünf Arten von Lecks, die erkannt werden können: <code>object_leaked</code>: Object doesn't exist in the grid <code>location_leaked</code>: Object exists in the grid, but found location doesn't belong to object <code>mup_seg_leaked</code>: Multipart upload was stopped or not completed, and the segment/part was left out <code>segment_leaked</code>: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment <code>no_parent</code>: Container object is deleted, but object segment was left out and not deleted
CTIM	Chunk-Erstellungszeit	Zeitpunkt der Erstellung des durchgesickerten Datenblocks.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts, zu dem der Chunk gehört.
CBID	Inhaltsblockkennung	CBID des Objekts, zu dem der geleakte Chunk gehört.
CSIZ	Inhaltsgröße	Die Größe des Chunks in Bytes.

LLST-Revisionsprotokollmeldung für verlorene Objektkopiespeicherorte in StorageGRID

Diese Meldung wird immer dann generiert, wenn kein Speicherort für eine Objektkopie (repliziert oder erasure-codiert) gefunden werden kann.

Code	Feld	Beschreibung
CBIL	CBID	Die betroffene CBID.
ECPR	Erasure-Coding Profil	Für mit Erasure-Codierung versehene Objektdaten. Die ID des verwendeten Erasure-Codierungsprofils.
LTyp	Standorttyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für löschcodierte Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten

Code	Feld	Beschreibung
NOID	Quellknoten-ID	Die Knoten-ID, auf der die Standorte verloren gingen.
PCLD	Pfad zum replizierten Objekt	Der vollständige Pfad zum Speicherort der verlorenen Objektdaten auf der Festplatte. Wird nur zurückgegeben, wenn LTYP den Wert CLDI hat (das heißt für replizierte Objekte). Nimmt die Form an <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Ergebnis	Immer NONE. RSLT ist ein Pflichtfeld, aber für diese Nachricht irrelevant. Anstelle von SUCS wird NONE verwendet, damit diese Nachricht nicht gefiltert wird.
TSRC	Auslösende Quelle	BENUTZER: Vom Benutzer ausgelöst SYST: System ausgelöst
UUID	Universell eindeutige ID	Die Kennung des betroffenen Objekts im StorageGRID System.

MGAU-Revisionsprotokollmeldung für Management-API-Anfragen in StorageGRID

Die Kategorie „Management“ protokolliert Benutzeranfragen an die Management-API. Jede HTTP-Anfrage, die keine GET- oder HEAD-Anfrage an eine gültige API-URI ist, protokolliert eine Antwort mit Benutzername, IP und Anfragetyp an die API. Ungültige API-URIs (wie /api/v3-authorize) und ungültige Anfragen an gültige API-URIs werden nicht protokolliert.

Code	Feld	Beschreibung
MDIP	Ziel-IP-Adresse	Die IP-Adresse des Servers (Ziel).
MDNA	Domainname	Der Host-Domänenname.
MPAT	Anfragepfad	Der Anfragepfad.
MPQP	Abfrageparameter für Anfragen	Die Abfrageparameter für die Anfrage.

Code	Feld	Beschreibung
MRBD	Anfragekörper	Der Inhalt des Anfragetextes. Während der Antworttext standardmäßig protokolliert wird, wird der Anfragetext in bestimmten Fällen protokolliert, wenn der Antworttext leer ist. Da die folgenden Informationen im Antworttext nicht verfügbar sind, werden sie für die folgenden POST-Methoden aus dem Anfragetext entnommen: • Benutzername und Konto-ID in POST authorize • Neue Subnetzkonfiguration in POST /grid/grid-networks/update • Neue NTP Server in POST /grid/ntp-servers/update • Außer Betrieb genommene Server-IDs in POST /grid/servers/decommission Hinweis: Sensible Informationen werden entweder gelöscht (zum Beispiel ein S3 access key) oder mit Sternchen maskiert (zum Beispiel ein Passwort).
MRMD	Anfragemethode	Die HTTP-Anfragemethode: • POST • PUT • LÖSCHEN • PATCH
MRSC	Antwortcode	Der Antwortcode.
MRSP	Antworttext	Der Inhalt der Antwort (der Antworttext) wird standardmäßig protokolliert. Hinweis: Sensible Informationen werden entweder gelöscht (zum Beispiel ein S3 access key) oder mit Sternchen maskiert (zum Beispiel ein Passwort).
MSIP	Quell-IP-Adresse	Die Client-IP-Adresse (Quell-IP-Adresse).
<code>\${post_edited_translations.segment}</code>	Benutzer-URN	Der URN (Uniform Resource Name) des Benutzers, der die Anfrage gesendet hat.
RSLT	Ergebnis	Gibt erfolgreich (SUCS) oder den vom Backend gemeldeten Fehler zurück.

OLST-Revisionsprotokollmeldung für vom System erkannte verlorene Objekte in StorageGRID

`${post_edited_translations.segment}`

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	\${post_edited_translations.segment}
NOID	Knoten-ID	Falls verfügbar, der letzte bekannte direkte oder Nearline-Speicherort des verlorenen Objekts. Es ist möglich, dass nur die Node-ID ohne eine Volume-ID vorliegt, wenn die Volume-Informationen nicht verfügbar sind.
WEG	S3 Bucket/Schlüssel	Falls verfügbar, der S3-Bucket-Name und der S3-Key-Name.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld in der Nachricht, aber für diese Nachricht nicht relevant. Anstelle von SUCS wird NONE verwendet, damit diese Nachricht nicht gefiltert wird.
UUID	Universell eindeutige ID	Die Kennung des verloren gegangenen Objekts innerhalb des StorageGRID Systems.
VOLI	Volume-ID	\${post_edited_translations.segment}

ORLM-Revisionsprotokollmeldung für ILM-Regeln, die in StorageGRID erfüllt wurden

Diese Meldung wird generiert, wenn das Objekt gemäß den ILM-Regeln erfolgreich gespeichert und kopiert wurde.



Die ORLM-Meldung wird nicht generiert, wenn ein Objekt durch die Standardregel "2 Kopien erstellen" erfolgreich gespeichert wird, wenn eine andere Regel in der Richtlinie den erweiterten Filter "Objektgröße" verwendet.

Code	Feld	Beschreibung
BUID	Bucket-Header	Bucket ID-Feld. Wird für interne Vorgänge verwendet. Erscheint nur, wenn STAT PRGD ist.
CBID	Inhaltsblockkennung	\${post_edited_translations.segment}
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.

Code	Feld	Beschreibung
<code>\${post_edited_translations.segment}</code>	Standorte	Der Speicherort der Objektdaten innerhalb des StorageGRID Systems. Der Wert für LOCS ist "", wenn das Objekt keine Speicherorte hat (zum Beispiel, wenn es gelöscht wurde). <code>\${post_edited_translations.segment}</code> CLDI: Bei replizierten Objekten die LDR-Knoten-ID und die Volume-ID des Objektstandorts. CLNL: ARC-Knoten-ID des Objektstandorts, falls die Objektdaten archiviert sind.
WEG	S3 Bucket/Schlüssel	Der S3 Bucket Name und der S3 Key Name.
RSLT	Ergebnis	Das Ergebnis der ILM-Operation. <code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Die für Menschen lesbare Bezeichnung der ILM-Regel, die auf dieses Objekt angewendet wurde.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
SGCB	Container-CBID	CBID des Containers für das segmentierte Objekt. Dieser Wert ist nur für segmentierte und mehrteilige Objekte verfügbar.
STAT	Status	Der Status des ILM Betriebs. ERLEDIGT: Die ILM-Operationen für das Objekt sind abgeschlossen. DFER: Das Objekt wurde für eine zukünftige ILM Neubewertung markiert. PRGD: Das Objekt wurde aus dem StorageGRID System gelöscht. NLOC: Die Objektdaten konnten im StorageGRID System nicht mehr gefunden werden. Dieser Status kann darauf hindeuten, dass alle Kopien der Objektdaten fehlen oder beschädigt sind.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID eines neuen Objekts, das in einem versionierten Bucket erstellt wurde. Operationen an Buckets und Objekten in nicht versionierten Buckets enthalten dieses Feld nicht.

Die ORLM-Prüfmeldung kann für ein einzelnes Objekt mehr als einmal ausgegeben werden. Sie wird beispielsweise ausgegeben, wenn eines der folgenden Ereignisse eintritt:

- Die ILM Regeln für das Objekt sind dauerhaft erfüllt.
- Die ILM-Regeln für das Objekt sind für diese Epoche erfüllt.
- Die ILM Regeln haben das Objekt gelöscht.
- Der Hintergrundprüfungsprozess erkennt, dass eine Kopie replizierter Objektdaten beschädigt ist. Das StorageGRID System führt eine ILM-Auswertung durch, um das beschädigte Objekt zu ersetzen.

Verwandte Informationen

- ["Objektaufnahmetransaktionen"](#)
- ["Objekt-Löschtransaktionen"](#)

OVWR-Revisionsprotokollmeldung für Objektüberschreibungen in StorageGRID

Diese Meldung wird generiert, wenn eine externe (vom Client angeforderte) Operation dazu führt, dass ein Objekt durch ein anderes Objekt überschrieben wird.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung (neu)	Die CBID für das neue Objekt.
CSIZ	Vorherige Objektgröße	Die Größe des zu überschreibenden Objekts in Bytes.
OCBD	Inhaltsblockkennung (vorherige)	Die CBID des vorherigen Objekts.
UUID	Universally Unique ID (neu)	Die Kennung des neuen Objekts innerhalb des StorageGRID Systems.
OID	Universally Unique ID (vorherige)	Die Kennung des vorherigen Objekts innerhalb des StorageGRID Systems.
WEG	S3 Objektpfad	Der S3-Objektpfad, der sowohl für das vorherige als auch für das neue Objekt verwendet wird
RSLT	Ergebniscode	Ergebnis der Objektüberschreibungstransaktion. Das Ergebnis ist immer: SUCS: Erfolgreich
\${post_edited_translations.segment}	\${post_edited_translations.segment}	Falls vorhanden, wurde das überschriebene Objekt an dem angegebenen Standort gelöscht, der nicht der Standort ist, an dem das überschriebene Objekt aufgenommen wurde.

S3SL-Revisionsprotokollnachricht für S3 Select-Anfragen in StorageGRID

Diese Meldung protokolliert den Abschluss einer S3 Select-Anfrage, nachdem sie an den Client zurückgegeben wurde. Die S3SL-Meldung kann Details zu Fehlermeldung und Fehlercode enthalten. Die Anfrage war möglicherweise nicht erfolgreich.

Code	Feld	Beschreibung
BYSC	Gescannte Bytes	Anzahl der von den Storage Nodes gescannten (empfangenen) Bytes. BYSC und BYPR unterscheiden sich wahrscheinlich, wenn das Objekt komprimiert ist. Wenn das Objekt komprimiert ist, enthält BYSC die Anzahl der komprimierten Bytes und BYPR die Anzahl der Bytes nach Dekomprimierung.
BYPR	Verarbeitete Bytes	Anzahl der verarbeiteten Bytes. Gibt an, wie viele Bytes von „Gescannte Bytes“ tatsächlich von einem S3 Select Job verarbeitet oder bearbeitet wurden.
BYRT	Zurückgegebene Bytes	Anzahl der Bytes, die ein S3 Select Job an den Client zurückgegeben hat.
REPR	Verarbeitete Datensätze	<code>\${post_edited_translations.segment}</code>
RERT	<code>\${post_edited_translations.segment}</code>	Anzahl der Datensätze oder Zeilen, die ein S3 Select Job an den Client zurückgegeben hat.
JOFI	Auftrag abgeschlossen	Gibt an, ob die Verarbeitung des S3 Select Jobs abgeschlossen wurde oder nicht. Wenn dieser Wert „false“ ist, konnte der Job nicht abgeschlossen werden, und die Fehlerfelder enthalten wahrscheinlich Daten. Der Client hat möglicherweise unvollständige oder gar keine Ergebnisse erhalten.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Kennung für die S3 Select Anfrage.
EXTM	Ausführungszeit	Die Zeit in Sekunden, die der S3 Select Job zum Abschließen benötigte.
ERMG	Fehlermeldung	<code>\${post_edited_translations.segment}</code>
ERTY	Fehlertyp	<code>\${post_edited_translations.segment}</code>
ERST	Fehler-Stacktrace	Fehler-Stacktrace, der vom S3 Select Job generiert wurde.
S3BK	S3 Bucket	Der Name des S3 Buckets.

Code	Feld	Beschreibung
S3AK	S3 Access Key ID (Absender der Anfrage)	Die S3-Zugriffsschlüssel-ID des Benutzers, der die Anfrage gesendet hat.
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket Namen.

SADD-Revisionsprotokollmeldung zur Deaktivierung der Sicherheitsprüfung in StorageGRID

Diese Meldung weist darauf hin, dass der Ursprungsdienst (Knoten-ID) die Protokollierung von Audit-Meldungen deaktiviert hat. StorageGRID erfasst und übermittelt keine Audit-Meldungen mehr.

Code	Feld	Beschreibung
AETM	Methode aktivieren	Die Methode, die zum Deaktivieren der Auditierung verwendet wurde.
AEUN	Benutzername	Der Benutzername, mit dem der Befehl zum Deaktivieren der Protokollierung ausgeführt wurde.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld in der Nachricht, aber für diese Nachricht nicht relevant. Anstelle von SUCS wird NONE verwendet, damit diese Nachricht nicht gefiltert wird.

Die Meldung deutet darauf hin, dass Protokollierung zuvor aktiviert, nun aber deaktiviert wurde. Dies wird üblicherweise nur während der Massenaufnahme verwendet, um die Systemleistung zu verbessern. Nach Abschluss der Massenaufnahme wird die Auditierung wiederhergestellt (SADE), und die Möglichkeit, die Auditierung zu deaktivieren, ist dann dauerhaft gesperrt.

SADE-Revisionsprotokollmeldung zur Aktivierung der Sicherheitsüberwachung in StorageGRID

Diese Meldung signalisiert, dass der Ursprungsdienst (Knoten-ID) die Protokollierung von Audit-Meldungen wiederhergestellt hat. StorageGRID erfasst und übermittelt wieder Audit-Meldungen.

Code	Feld	Beschreibung
AETM	Methode aktivieren	Die Methode, mit der die Protokollierung aktiviert wurde.

Code	Feld	Beschreibung
AEUN	Benutzername	Der Benutzername, mit dem der Befehl zum Aktivieren der Protokollierung ausgeführt wurde.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld in der Nachricht, aber für diese Nachricht nicht relevant. Anstelle von SUCS wird NONE verwendet, damit diese Nachricht nicht gefiltert wird.

Die Meldung deutet darauf hin, dass die Protokollierung zuvor deaktiviert (SADD) war, nun jedoch wiederhergestellt wurde. Dies wird üblicherweise nur während der Massenerfassung verwendet, um die Systemleistung zu verbessern. Nach Abschluss der Massenerfassung wird die Protokollierung wiederhergestellt und die Möglichkeit, die Protokollierung zu deaktivieren, anschließend dauerhaft gesperrt.

SCMT-Revisionsprotokollmeldung für Objektspeicher-Commits in StorageGRID

Grid-Inhalte sind erst verfügbar oder werden als gespeichert erkannt, wenn sie endgültig gespeichert wurden (das heißt, sie wurden dauerhaft abgelegt). Dauerhaft gespeicherte Inhalte wurden vollständig auf die Festplatte geschrieben und haben die zugehörigen Integritätsprüfungen bestanden. Diese Meldung wird ausgegeben, wenn ein Inhaltsblock endgültig gespeichert wurde.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des Inhaltsblocks, der im permanenten Speicher abgelegt wurde.
RSLT	Ergebniscode	Status zum Zeitpunkt der Speicherung des Objekts auf der Festplatte: SUCS: Objekt erfolgreich gespeichert.

Diese Meldung bedeutet, dass ein bestimmter Inhaltsblock vollständig gespeichert und verifiziert wurde und nun angefordert werden kann. Sie kann verwendet werden, um den Datenfluss innerhalb des Systems zu verfolgen.

SDEL-Revisionsprotokollmeldung für S3 DELETE-Transaktionen in StorageGRID

Wenn ein S3-Client eine DELETE-Transaktion ausführt, wird eine Anfrage zum Entfernen des angegebenen Objekts oder Buckets oder zum Entfernen einer Bucket-/Objekt-Subressource gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Ist die CBID unbekannt, wird dieses Feld auf 0 gesetzt. Operationen an Buckets berücksichtigen dieses Feld nicht.

Code	Feld	Beschreibung
CNCH	Konsistenzkontroll-Header	Der Wert des HTTP-Anforderungs-Headers „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungsken- nung	Die eindeutige Systemkennung für die TCP/IP Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Bytes. Operationen auf Buckets berücksichtigen dieses Feld nicht.
DMRK	<code>\${post_edited_translations.segment}</code>	Die Versions-ID des Löschmarkers, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wird. Operationen an Buckets schließen dieses Feld nicht ein.
GFID	Grid Federation Verbindungs-ID	Die Verbindungs-ID der Grid Federation-Verbindung, die einer gridübergreifenden Replikationslöschanforderung zugeordnet ist. Nur in den Audit-Protokollen des Ziel-Grids enthalten.
GFSA	Grid Federation Quellkonto-ID	Die Konto-ID des Mandanten im Quell-Grid für eine gitterübergreifende Replikations-Löschanforderung. Nur in den Audit-Protokollen des Ziel-Grids enthalten.
HTRH	HTTP-Request-Header	Liste der protokollierten HTTP-Anforderungsheader-Namen und -Werte, wie während der Konfiguration ausgewählt. <code>`X-Forwarded-For`</code> wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist und der <code>`X-Forwarded-For`</code> Wert von der IP-Adresse des Anfrageabsenders abweicht (SAIP Audit-Feld). <code>x-amz-bypass-governance-retention</code> wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist.
MTME	Letzte Änderungszeit	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der DELETE Transaktion. Das Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3- Mandantenkonto- ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymer Zugriff vorliegt.

Code	Feld	Beschreibung
S3AK	S3 Access Key ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymer Zugriff erfolgt.
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.
S3SR	S3 Subressource	Die Bucket- oder Objekt-Subressource, auf die sich der Vorgang gegebenenfalls bezieht.
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Client-Anwendung, die die Anfrage gestellt hat.
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Inhaber)	Die Mandantenkonto-ID des Besitzers des Ziel-Buckets. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
`\${post_edited_translations.segment}`	`\${post_edited_translations.segment}`	`\${post_edited_translations.segment}`
SUSR	S3 User URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des anfragenden Benutzers. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anfrage von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.

Code	Feld	Beschreibung
UUDM	Universell eindeutiger Bezeichner für eine Löschemarkierung	Die Kennung eines Löschemarkers. Audit-Log-Meldungen geben entweder UUDM oder UUID an, wobei UUDM einen Löschemarker angibt, der als Ergebnis einer Objektlöschanforderung erstellt wurde, und UUID ein Objekt angibt.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines gelöschten Objekts. Operationen an Buckets und Objekten in nicht versionierten Buckets enthalten dieses Feld nicht.

SGET-Revisionsprotokollmeldung für S3 GET-Transaktionen in StorageGRID

Wenn ein S3-Client eine GET-Transaktion ausführt, wird eine Anfrage gestellt, um ein Objekt abzurufen, die Objekte in einem Bucket aufzulisten oder eine Bucket-/Objekt-Subressource zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Ist die CBID unbekannt, wird dieses Feld auf 0 gesetzt. Operationen an Buckets berücksichtigen dieses Feld nicht.
CNCH	Konsistenzkontroll-Header	Der Wert des HTTP-Anforderungs-Headers „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen auf Buckets berücksichtigen dieses Feld nicht.
HTRH	HTTP-Request-Header	Liste der protokollierten HTTP-Anforderungsheader-Namen und -Werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For` wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist und der `X-Forwarded-For` Wert von der IP-Adresse des Anfrageabsenders abweicht (SAIP Audit-Feld).

Code	Feld	Beschreibung
LITY	ListObjectsV2	Es wurde eine Antwort im <i>v2 Format</i> angefordert. Weitere Informationen finden Sie unter " AWS ListObjectsV2 ". Nur für GET-Bucket-Operationen.
NCHD	Anzahl der Kinder	Beinhaltet Schlüssel und gängige Präfixe. Nur für GET-Bucket-Operationen.
Rang	Bereichslesen	Nur für Bereichsleseoperationen. Gibt den Bereich der Bytes an, die durch diese Anforderung gelesen wurden. Der Wert nach dem Schrägstrich (/) zeigt die Größe des gesamten Objekts an.
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymen Zugriff vorliegt.
S3AK	S3 Access Key ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymen Zugriff erfolgt.
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.
S3SR	S3 Subressource	Die Bucket- oder Objekt-Subressource, auf die sich der Vorgang gegebenenfalls bezieht.
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Client-Anwendung, die die Anfrage gestellt hat.
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.

Code	Feld	Beschreibung
SBAI	S3-Mandantenkonto-ID (Bucket-Inhaber)	Die Mandantenkonto-ID des Besitzers des Ziel-Buckets. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SUSR	S3 User URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des anfragenden Benutzers. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anfrage von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
TRNC	Abgeschnitten oder nicht abgeschnitten	Auf „false“ setzen, wenn alle Ergebnisse zurückgegeben wurden. Auf „true“ setzen, wenn weitere Ergebnisse verfügbar sind. Nur für GET-Bucket-Operationen.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, die angefordert wurde. Operationen an Buckets und Objekten in nicht versionierten Buckets beinhalten dieses Feld nicht.

SHEA audit message für S3 HEAD-Operationen in StorageGRID

Wenn ein S3-Client eine HEAD-Operation ausführt, wird eine Anfrage gesendet, um die Existenz eines Objekts oder Buckets zu prüfen und die Metadaten über ein Objekt abzurufen. Diese Meldung wird vom Server ausgegeben, wenn die Operation erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Ist die CBID unbekannt, wird dieses Feld auf 0 gesetzt. Operationen an Buckets berücksichtigen dieses Feld nicht.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP Verbindung.

Code	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des geprüften Objekts in Bytes. Operationen auf Buckets berücksichtigen dieses Feld nicht.
HTRH	HTTP-Request-Header	Liste der protokollierten HTTP-Anforderungsheader-Namen und -Werte, wie während der Konfiguration ausgewählt. <code>`X-Forwarded-For`</code> wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist und der <code>`X-Forwarded-For`</code> Wert von der IP-Adresse des Anfrageabsenders abweicht (SAIP Audit-Feld).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymer Zugriff vorliegt.
S3AK	S3 Access Key ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymer Zugriff erfolgt.
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Client-Anwendung, die die Anfrage gestellt hat.
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.

Code	Feld	Beschreibung
SBAI	S3-Mandantenkonto-ID (Bucket-Inhaber)	Die Mandantenkonto-ID des Besitzers des Ziel-Buckets. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SUSR	S3 User URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des anfragenden Benutzers. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anfrage von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, die angefordert wurde. Operationen an Buckets und Objekten in nicht versionierten Buckets beinhalten dieses Feld nicht.

SPOS-Revisionsprotokollmeldung für S3 POST-Transaktionen in StorageGRID

Wenn ein S3 Client eine POST Object-Anforderung sendet, wird diese Meldung vom Server ausgegeben, falls die Transaktion erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt.
CNCH	Konsistenzkontroll-Header	Der Wert des HTTP-Anforderungs-Headers „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes.

Code	Feld	Beschreibung
HTRH	HTTP-Request-Header	Liste der protokollierten HTTP-Anforderungsheader-Namen und -Werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For` wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist und der `X-Forwarded-For` Wert von der IP-Adresse des Anfrageabsenders abweicht (SAIP Audit-Feld). (Nicht für SPOS zu erwarten).
RSLT	Ergebniscode	Ergebnis der RestoreObject Anfrage. Das Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymer Zugriff vorliegt.
S3AK	S3 Access Key ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymer Zugriff erfolgt.
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.
S3SR	S3 Subressource	Die Bucket- oder Objekt-Subressource, auf die sich der Vorgang gegebenenfalls bezieht. Auf „select“ für eine S3 Select-Operation setzen.
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Client-Anwendung, die die Anfrage gestellt hat.

Code	Feld	Beschreibung
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Inhaber)	Die Mandantenkonto-ID des Besitzers des Ziel-Buckets. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SRCF	Subressourcen-Konfiguration	Informationen wiederherstellen.
SUSR	S3 User URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des anfragenden Benutzers. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anfrage von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, die angefordert wurde. Operationen an Buckets und Objekten in nicht versionierten Buckets beinhalten dieses Feld nicht.

SPUT-Revisionsprotokollmeldung für S3 PUT-Transaktionen in StorageGRID

Wenn ein S3-Client eine PUT-Transaktion ausführt, wird eine Anfrage zum Erstellen eines neuen Objekts oder Buckets oder zur Entfernung einer Bucket-/Objekt-Subressource gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Ist die CBID unbekannt, wird dieses Feld auf 0 gesetzt. Operationen an Buckets berücksichtigen dieses Feld nicht.

Code	Feld	Beschreibung
CMPS	Compliance Einstellungen	Die beim Erstellen des Buckets verwendeten Compliance-Einstellungen, sofern in der Anfrage vorhanden (auf die ersten 1024 Zeichen gekürzt).
CNCH	Konsistenzkontroll-Header	Der Wert des HTTP-Anforderungs-Headers „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungs-kennung	Die eindeutige Systemkennung für die TCP/IP Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen auf Buckets berücksichtigen dieses Feld nicht.
GFID	Grid Federation Verbindungs-ID	Die Verbindungs-ID der Grid Federation-Verbindung, die einer PUT-Anforderung für die netzübergreifende Replikation zugeordnet ist. Nur in den Audit-Protokollen des Ziel-Grids enthalten.
GFSA	Grid Federation Quellkonto-ID	Die Konto-ID des Mandanten im Quell-Grid für eine PUT-Anfrage zur gridübergreifenden Replikation. Nur in den Audit-Protokollen des Ziel-Grids enthalten.
HTRH	HTTP-Request-Header	Liste der protokollierten HTTP-Anforderungsheader-Namen und -Werte, wie während der Konfiguration ausgewählt. <code>`X-Forwarded-For`</code> wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist und der <code>`X-Forwarded-For`</code> Wert von der IP-Adresse des Anfrageabsenders abweicht (SAIP Audit-Feld). <code>x-amz-bypass-governance-retention</code> wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist.
LKEN	Objektsperre aktiviert	Wert des Anfrageheaders <code>x-amz-bucket-object-lock-enabled</code> , falls dieser in der Anfrage vorhanden ist.
LKLH	Object Lock Legal Hold	Wert des Anfrageheaders <code>x-amz-object-lock-legal-hold</code> , falls dieser in der PutObject-Anfrage vorhanden ist.
LKMD	Objektsperre Beibehaltungsmodus	Wert des Anfrageheaders <code>x-amz-object-lock-mode</code> , falls dieser in der PutObject-Anfrage vorhanden ist.

Code	Feld	Beschreibung
LKRU	Objektsperre Beibehalten-bis-Datum	Wert des Anfrageheaders <code>x-amz-object-lock-retain-until-date</code> , sofern in der PutObject-Anfrage vorhanden. Die Werte sind auf einen Zeitraum von maximal 100 Jahren ab dem Datum der Objekterfassung beschränkt.
MTME	Letzte Änderungszeit	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymen Zugriff vorliegt.
S3AK	S3 Access Key ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymen Zugriff erfolgt.
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.
S3SR	S3 Subressource	Die Bucket- oder Objekt-Subressource, auf die sich der Vorgang gegebenenfalls bezieht.
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Client-Anwendung, die die Anfrage gestellt hat.
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Inhaber)	Die Mandantenkonto-ID des Besitzers des Ziel-Buckets. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.

Code	Feld	Beschreibung
SRCF	Subressourcen-Konfiguration	Die neue Subressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).
SUSR	S3 User URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des anfragenden Benutzers. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anfrage von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
ULID	Upload-ID	Nur in SPUT-Meldungen für CompleteMultipartUpload Operationen enthalten. Gibt an, dass alle Teile hochgeladen und zusammengefügt wurden.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID eines neuen Objekts, das in einem versionierten Bucket erstellt wurde. Operationen an Buckets und Objekten in nicht versionierten Buckets enthalten dieses Feld nicht.
VSST	Versionsstatus	Der neue Versionsstatus eines Buckets. Es werden zwei Zustände verwendet: „aktiviert“ oder „angehalten“. Operationen an Objekten berücksichtigen dieses Feld nicht.

SREM-Revisionsprotokollmeldung für Objektspeicher-Entfernung in StorageGRID

Diese Meldung wird ausgegeben, wenn Inhalte aus dem persistenten Speicher entfernt wurden und nicht mehr über reguläre APIs zugänglich sind.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des aus dem permanenten Speicher entfernten Inhaltsblocks.
RSLT	Ergebniscode	Gibt das Ergebnis der Inhaltsentfernungsoperationen an. Der einzige definierte Wert ist: SUCS: Inhalt aus dem persistenten Speicher entfernt

Diese Prüfmeldung bedeutet, dass ein bestimmter Inhaltsblock von einem Knoten gelöscht wurde und nicht mehr direkt angefordert werden kann. Die Meldung kann verwendet werden, um den Fluss gelöschter Inhalte innerhalb des Systems nachzuverfolgen.

SUPD-Revisionsprotokollmeldung für S3-Metadatenaktualisierungen in StorageGRID

Diese Meldung wird von der S3 API generiert, wenn ein S3 Client die Metadaten für ein ingestiertes Objekt aktualisiert. Die Meldung wird vom Server ausgegeben, wenn die Metadatenaktualisierung erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Ist die CBID unbekannt, wird dieses Feld auf 0 gesetzt. Operationen an Buckets berücksichtigen dieses Feld nicht.
CNCH	Konsistenzkontroll-Header	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern dieser in der Anfrage vorhanden ist, beim Aktualisieren der Compliance-Einstellungen eines Buckets.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen auf Buckets berücksichtigen dieses Feld nicht.
HTRH	HTTP-Request-Header	Liste der protokollierten HTTP-Anforderungsheader-Namen und -Werte, wie während der Konfiguration ausgewählt. <code>`X-Forwarded-For`</code> wird automatisch miteinbezogen, wenn es in der Anfrage vorhanden ist und der <code>`X-Forwarded-For`</code> Wert von der IP-Adresse des Anfrageabsenders abweicht (SAIP Audit-Feld).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: SUCS: erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymen Zugriff vorliegt.
S3AK	S3 Access Key ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert gibt an, dass anonymen Zugriff erfolgt.

Code	Feld	Beschreibung
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Client-Anwendung, die die Anfrage gestellt hat.
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Inhaber)	Die Mandantenkonto-ID des Besitzers des Ziel-Buckets. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
SUSR	S3 User URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des anfragenden Benutzers. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anfrage von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutiger Bezeichner	Die Kennung des Objekts innerhalb des StorageGRID Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Operationen an Buckets und Objekten in nicht versionierten Buckets enthalten dieses Feld nicht.

SVRF-Revisionsprotokollmeldung für Verifizierungsfehler des Objektspeichers in StorageGRID

Diese Meldung wird ausgegeben, wenn ein Inhaltsblock den Verifizierungsprozess nicht besteht. Jedes Mal, wenn replizierte Objektdaten von oder auf die Festplatte gelesen beziehungsweise geschrieben werden, erfolgen mehrere Verifizierungs- und Integritätsprüfungen, um sicherzustellen, dass die an den anfragenden Benutzer gesendeten Daten mit den ursprünglich in das System eingelesenen Daten identisch sind. Wenn eine dieser Prüfungen fehlschlägt, isoliert das System die beschädigten replizierten Objektdaten automatisch, um zu verhindern, dass sie erneut abgerufen werden.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des Inhaltsblocks, bei dem die Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	Typ des Verifizierungsfehlers: CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen. HMAC: Die Überprüfung des Hash-basierten Message Authentication Code (HMAC) ist fehlgeschlagen. EHSB: Unerwarteter Hashwert des verschlüsselten Inhalts. PHSH: Unerwarteter Hash des Originalinhalts. SEQC: Falsche Datenreihenfolge auf der Festplatte. PERR: Ungültige Struktur der Datenträgerdatei. DERR: Festplattenfehler. FNAM: Ungültiger Dateiname.



Diese Meldung sollte aufmerksam verfolgt werden. Fehler bei der Inhaltsprüfung können auf bevorstehende Hardwareausfälle hinweisen.

Um festzustellen, welcher Vorgang die Meldung ausgelöst hat, kann der Wert des Felds AMID (Modul-ID) eingesehen werden. Beispielsweise weist der Wert SVFY darauf hin, dass die Meldung vom Storage Verifier Modul generiert wurde, also im Rahmen einer Hintergrundüberprüfung, und STOR zeigt an, dass die Meldung durch den Abruf von Inhalten ausgelöst wurde.

SVRU-Revisionsprotokollmeldung für unbekannten Objektspeicherinhalt in StorageGRID

Die Speicherkomponente des LDR-Dienstes scannt kontinuierlich alle Kopien replizierter Objektdaten im Objektspeicher. Diese Meldung wird ausgegeben, wenn eine unbekannte oder unerwartete Kopie replizierter Objektdaten im Objektspeicher erkannt und in das Quarantäneverzeichnis verschoben wird.

Code	Feld	Beschreibung
FPTH	Dateipfad	Der Dateipfad der unerwarteten Objektkopie.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NONE'. RSLT ist ein Pflichtfeld in der Nachricht, aber für diese Nachricht nicht relevant. 'NONE' wird anstelle von 'SUCS' verwendet, damit diese Nachricht nicht gefiltert wird.



Die Meldung „SVRU: Object Store Verify Unknown“ sollte genau überwacht werden. Sie bedeutet, dass unerwartete Kopien von Objektdaten im Objektspeicher erkannt wurden. Dieser Sachverhalt sollte umgehend untersucht werden, um die Entstehung dieser Kopien zu ermitteln, da dies auf drohende Hardwareausfälle hindeuten kann.

SYSD Revisionsprotokollmeldung für ordnungsgemäße Knotenstopps in StorageGRID

Wird ein Dienst ordnungsgemäß beendet, wird diese Meldung generiert, um anzuzeigen, dass die Beendigung angefordert wurde. Normalerweise wird diese Meldung erst nach einem anschließenden Neustart gesendet, da die Überwachungsmeldungswarteschlange vor der Beendigung nicht geleert wird. Die SYST-Meldung, die zu Beginn der Beendigungssequenz gesendet wird, ist zu beachten, falls der Dienst nicht neu gestartet wurde.

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren.

Die Meldung gibt nicht an, ob der Hostserver gestoppt wird, sondern nur den meldenden Dienst. Die RSLT eines SYSD kann kein „unsauberes“ Herunterfahren anzeigen, da die Meldung nur bei „sauberen“ Herunterfahren generiert wird.

SYST-Revisionsprotokollmeldung für das Anhalten eines Knotens in StorageGRID

Wird ein Dienst ordnungsgemäß beendet, wird diese Meldung generiert, um anzuzeigen, dass die Beendigung angefordert wurde und der Dienst seine Beendigungssequenz eingeleitet hat. Mit SYST kann festgestellt werden, ob die Beendigung angefordert wurde, bevor der Dienst neu gestartet wird (im Gegensatz zu SYSD, das typischerweise nach dem Neustart des Dienstes gesendet wird).

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren.

Die Meldung gibt nicht an, ob der Hostserver gestoppt wird, sondern nur den meldenden Dienst. Der RSLT-Code einer SYST-Meldung kann kein „unsauberes“ Herunterfahren anzeigen, da die Meldung nur bei

„sauberen“ Herunterfahren generiert wird.

SYSU-Revisionsprotokollnachricht für Knotenstarts in StorageGRID

Wenn ein Dienst neu gestartet wird, wird diese Meldung generiert, um anzuzeigen, ob das vorherige Herunterfahren ordnungsgemäß (befohlen) oder ungeordnet (unerwartet) war.

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren. DSDN: Das System wurde nicht ordnungsgemäß heruntergefahren. VRGN: Das System wurde nach der Serverinstallation (oder Neuinstallation) zum ersten Mal gestartet.

Die Meldung gibt nicht an, ob der Host-Server gestartet wurde, sondern nur, ob der meldende Dienst gestartet wurde. Diese Meldung kann verwendet werden, um:

- Diskontinuität im Revisionsprotokoll erkennen.
- Es kann festgestellt werden, ob ein Dienst während des Betriebs ausfällt (da die verteilte Architektur des StorageGRID Systems solche Ausfälle verschleiern kann). Server-Manager startet einen ausgefallenen Dienst automatisch neu.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.