



Formato del file di log di audit

StorageGRID software

NetApp
July 23, 2026

Sommario

- Formato del file di log di audit 1
 - Scopri il formato dei file di log di audit in StorageGRID 1
 - Utilizzare lo strumento audit-explain per tradurre i messaggi di audit di StorageGRID 3
 - Utilizzare lo strumento audit-sum per riepilogare i messaggi di audit di StorageGRID 4

Formato del file di log di audit

Scopri il formato dei file di log di audit in StorageGRID

I file di log di audit si trovano su ogni Admin Node e contengono una raccolta di singoli messaggi di audit.

Ogni messaggio di audit contiene quanto segue:

- `${post_edited_translations.segment}`

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

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

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

2019-08-07T18:43:30.247711

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

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):13489590586043706682]]
```

Nel loro formato predefinito, i messaggi di audit nei file di log di audit non sono facili da leggere o interpretare. Puoi usare ["strumento audit-explain"](#) per ottenere riepiloghi semplificati dei messaggi di audit nel file di log di audit. Puoi usare ["strumento audit-sum"](#) per riepilogare quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno impiegato queste operazioni.

Utilizzare lo strumento audit-explain per tradurre i messaggi di audit di StorageGRID

Puoi usare lo `audit-explain` strumento per tradurre i messaggi di audit presenti nel registro di audit in un formato facile da leggere.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Devi avere il file `Passwords.txt`.
- `${post_edited_translations.segment}`

Informazioni su questa attività

Lo strumento `audit-explain`, disponibile sull'Admin Node primario, fornisce riepiloghi semplificati dei messaggi di audit in un log di audit.



Lo strumento `audit-explain` è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. L'elaborazione `audit-explain` delle query può consumare una grande quantità di potenza della CPU, il che potrebbe influire sulle operazioni di StorageGRID.

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

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

Lo `audit-explain` strumento può fare quanto segue:

- Elabora i log di controllo, sia semplici che compressi. Ad esempio:

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

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

- Elabora più file contemporaneamente. Ad esempio:

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

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

- Accetta input da una pipe, che ti consente di filtrare e pre-elaborare l'input utilizzando il `grep` comando o

altri mezzi. Ad esempio:

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

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

Poiché i file di log di controllo possono essere molto grandi e lenti da analizzare, puoi risparmiare tempo filtrando le parti che vuoi esaminare ed eseguendo `audit-explain` su quelle parti, invece che sull'intero file.



Lo `audit-explain` strumento non accetta file compressi come input tramite pipe. Per elaborare i file compressi, specifica i loro nomi come argomenti della riga di comando oppure usa lo `zcat` strumento per decomprimere prima i file. Ad esempio:

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

Usa l' `'help (-h)'` opzione per vedere le opzioni disponibili. Per esempio:

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

Passaggi

1. Accedi al nodo amministratore principale:
 - a. Inserisci il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Inserisci la password indicata nel file `Passwords.txt`.
 - c. Inserisci il seguente comando per passare all'utente root: `su -`
 - d. Inserisci la password indicata nel file `Passwords.txt`.

Quando sei connesso come root, il prompt cambia da `$` a `#`.

2. Inserisci il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e il percorso del file o dei file che desideri analizzare:

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

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



Per ridurre la lunghezza delle righe e migliorare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se vuoi vedere i timestamp, usa l'opzione `timestamp (-t)`.

Utilizzare lo strumento `audit-sum` per riepilogare i messaggi di audit di StorageGRID

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

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Hai il file Passwords.txt.
- \${post_edited_translations.segment}

Informazioni su questa attività

Lo audit-sum strumento, disponibile sul nodo di amministrazione principale, riassume quante operazioni di scrittura, lettura ed eliminazione sono state registrate e quanto tempo hanno impiegato queste operazioni.



Lo `audit-sum` strumento è pensato principalmente per l'uso da parte del supporto tecnico durante le operazioni di troubleshooting. L'elaborazione delle `audit-sum` query può consumare una grande quantità di potenza della CPU, il che potrebbe influire sulle operazioni di StorageGRID.

Questo esempio mostra l'output tipico dello audit-sum strumento. Questo esempio mostra quanto tempo hanno impiegato le operazioni del protocollo.

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

Lo `audit-sum` strumento fornisce conteggi e tempi per i seguenti messaggi di audit S3 e ILM in un file di log di audit.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione man mano che le funzionalità vengono deprecate. Se incontri un codice di controllo che non è presente in questo elenco, controlla le versioni precedenti di questo argomento per le release precedenti di StorageGRID. Ad esempio, "[StorageGRID 11.8 Utilizzo dello strumento audit sum](#)".

Codice	Descrizione	\${post_edited_translations.segment}
IDEL	Eliminazione avviata da ILM: registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"
\${post_edited_translations.segment}	S3 DELETE: Registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: S3 DELETE"

Codice	Descrizione	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	"SGET: S3 GET"
SHEA	<code>\${post_edited_translations.segment}</code>	"SHEA: S3 HEAD"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"

Lo `audit-sum` strumento può fare quanto segue:

- Elabora i log di controllo, sia semplici che compressi. Ad esempio:

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

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

- Elabora più file contemporaneamente. Ad esempio:

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

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

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

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

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

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



Questo strumento non accetta file compressi come input tramite pipe. Per elaborare i file compressi, specifica i loro nomi come argomenti della riga di comando oppure utilizza lo `zcat` strumento per decomprimere prima i file. Ad esempio:

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

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

Puoi usare le opzioni della riga di comando per riepilogare le operazioni sui bucket separatamente da quelle sugli oggetti oppure per raggruppare i riepiloghi dei messaggi per nome del bucket, periodo di tempo o tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di operazione minimo, massimo e medio, ma puoi usare l' `size (-s)` opzione per visualizzare invece la dimensione dell'oggetto.

Usa l' `help (-h)` opzione per vedere le opzioni disponibili. Per esempio:

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

Passaggi

1. Accedi al nodo amministratore principale:

- a. Inserisci il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password indicata nel file `Passwords.txt`.
- c. Inserisci il seguente comando per passare all'utente root: `su -`
- d. Inserisci la password indicata nel file `Passwords.txt`.

Quando sei connesso come root, il prompt cambia da `$` a `#`.

2. Se vuoi analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, head ed eliminazione, segui questi passaggi:

- a. Inserisci il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e il percorso del file o dei file che desideri analizzare:

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

Questo esempio mostra l'output tipico dello `audit-sum` strumento. Questo esempio mostra quanto tempo hanno impiegato le operazioni del protocollo.

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

In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media, con un tempo di 1,13 secondi, ma sia le operazioni SGET che SPUT (S3 PUT) mostrano tempi massimi elevati, pari a circa 1.770 secondi.

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

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

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

```

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

```

+ Da questo esempio di output, puoi vedere che le tre richieste GET S3 più lente erano per oggetti di circa 5 GB di dimensione, molto più grandi rispetto agli altri oggetti. Le grandi dimensioni spiegano i tempi di recupero più lenti nel caso peggiore.

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

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

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

In questo esempio, la dimensione media degli oggetti per SPUT è inferiore a 2,5 MB, mentre la dimensione media per SGET è molto maggiore. Il numero di messaggi SPUT è molto più alto del numero di messaggi SGET, il che indica che la maggior parte degli oggetti non viene mai recuperata.

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

a. Esegui il comando sul file di log di audit appropriato e usa l'opzione group-by-time (-gt, seguita dal periodo di tempo (ad esempio, 15M, 1H, 10S):

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

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

Questi risultati mostrano che il traffico S3 GET ha raggiunto un picco tra le 06:00 e le 07:00. I tempi massimi e medi sono entrambi considerevolmente più elevati in questo intervallo di tempo e non sono aumentati gradualmente con l'aumentare del numero di richieste. Queste metriche suggeriscono che la capacità è stata superata, probabilmente nella rete o nella capacità della grid di elaborare le richieste.

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

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

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

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

- c. Per vedere più dettagli, usa ["strumento audit-explain"](#) per rivedere tutte le operazioni SGET durante quell'ora:

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

Se ti aspetti che l'output del comando `grep` sia composto da molte righe, aggiungi il comando `less` per mostrare il contenuto del file di log di audit una pagina (una schermata) alla volta.

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

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

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

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

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

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

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

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

- c. Per determinare quali bucket hanno la dimensione dell'oggetto SPUT più grande, usa sia le opzioni `-gb` che `-s`:

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

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

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.