



# Formato de arquivo de log de auditoria

## StorageGRID

NetApp  
March 10, 2025

# Índice

- Formato de arquivo de log de auditoria ..... 1
- Utilizando a ferramenta de auditoria-explicação ..... 3
- Usando a ferramenta audit-sum. .... 5

# Formato de arquivo de log de auditoria

Os arquivos de log de auditoria são encontrados em cada nó Admin e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O tempo Universal coordenado (UTC) do evento que acionou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido de um espaço:

*YYYY-MM-DDTHH:MM:SS.UUUUUU*, onde *UUUUUU* estão microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com AUDT.

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha adicionadas para legibilidade). Essas mensagens foram geradas quando um locatário criou um bucket do S3 e adicionou dois objetos a esse bucket.

2019-08-07T18:43:30.247711

```
[AUDT: [RSLT (FC32) :SUCS] [CNID (UI64) :1565149504991681] [TIME (UI64) :73520] [SAI
P (IPAD) : "10.224.2.255"] [S3AI (CSTR) : "17530064241597054718"]
[SACC (CSTR) : "s3tenant"] [S3AK (CSTR) : "SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="] [SUSR (CSTR) : "urn:sgws:identity::175300642415970547
18:root"]
[SBAI (CSTR) : "17530064241597054718"] [SBAC (CSTR) : "s3tenant"] [S3BK (CSTR) : "buc
ket1"] [AVER (UI32) :10] [ATIM (UI64) :1565203410247711]
[ATYP (FC32) :SPUT] [ANID (UI32) :12454421] [AMID (FC32) :S3RQ] [ATID (UI64) :7074142
142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT: [RSLT (FC32) :SUCS] [CNID (UI64) :1565149504991696] [TIME (UI64) :120713] [SA
IP (IPAD) : "10.224.2.255"] [S3AI (CSTR) : "17530064241597054718"]
[SACC (CSTR) : "s3tenant"] [S3AK (CSTR) : "SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="] [SUSR (CSTR) : "urn:sgws:identity::175300642415970547
18:root"]
[SBAI (CSTR) : "17530064241597054718"] [SBAC (CSTR) : "s3tenant"] [S3BK (CSTR) : "buc
ket1"] [S3KY (CSTR) : "fh-small-0"]
[CBID (UI64) :0x779557A069B2C037] [UUID (CSTR) : "94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"] [CSIZ (UI64) :1024] [AVER (UI32) :10]
[ATIM (UI64) :1565203410783597] [ATYP (FC32) :SPUT] [ANID (UI32) :12454421] [AMID (F
C32) :S3RQ] [ATID (UI64) :8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT: [RSLT (FC32) :SUCS] [CNID (UI64) :1565149504991693] [TIME (UI64) :121666] [SA
IP (IPAD) : "10.224.2.255"] [S3AI (CSTR) : "17530064241597054718"]
[SACC (CSTR) : "s3tenant"] [S3AK (CSTR) : "SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="] [SUSR (CSTR) : "urn:sgws:identity::175300642415970547
18:root"]
[SBAI (CSTR) : "17530064241597054718"] [SBAC (CSTR) : "s3tenant"] [S3BK (CSTR) : "buc
ket1"] [S3KY (CSTR) : "fh-small-2000"]
[CBID (UI64) :0x180CBD8E678EED17] [UUID (CSTR) : "19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"] [CSIZ (UI64) :1024] [AVER (UI32) :10]
[ATIM (UI64) :1565203410784558] [ATYP (FC32) :SPUT] [ANID (UI32) :12454421] [AMID (F
C32) :S3RQ] [ATID (UI64) :13489590586043706682]]
```

Em seu formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou interpretar. Você pode usar a `audit-explain` ferramenta para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar a `audit-sum` ferramenta para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.

### Informações relacionadas

["Utilizando a ferramenta de auditoria-explicação"](#)

["Usando a ferramenta audit-sum"](#)

# Utilizando a ferramenta de auditoria-explicação

Você pode usar a `audit-explain` ferramenta para traduzir as mensagens de auditoria no log de auditoria em um formato fácil de ler.

## O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

## Sobre esta tarefa

A `audit-explain` ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.



A `audit-explain` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-explain` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-explain` ferramenta. Essas quatro mensagens de auditoria do SPUT foram geradas quando o locatário S3 com ID de conta 92484777680322627870 usou S3 SOLICITAÇÕES PUT para criar um bucket chamado "bucket1" e adicionar três objetos a esse 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
```

A `audit-explain` ferramenta pode processar logs de auditoria simples ou compactados. Por exemplo:

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

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

A `audit-explain` ferramenta também pode processar vários arquivos de uma só vez. Por exemplo:

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

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

Finalmente, a `audit-explain` ferramenta pode aceitar entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

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

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

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo filtrando partes que você deseja olhar e executar `audit-explain` nas partes, em vez de todo o arquivo.



A `audit-explain` ferramenta não aceita arquivos compactados como entrada pipeada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descompactar os arquivos primeiro. Por exemplo:

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

Utilize a `help` (`-h`) opção para ver as opções disponíveis. Por exemplo:

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

## Passos

1. Faça login no nó de administração principal:

- a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

2. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

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

A `audit-explain` ferramenta imprime interpretações humanamente legíveis de todas as mensagens no arquivo ou arquivos especificados.



Para reduzir o comprimento das linhas e facilitar a legibilidade, os carimbos de data/hora não são apresentados por predefinição. Se você quiser ver os carimbos de data/hora, use a opção carimbo de data/hora (`-t`).

## Informações relacionadas

["SPUT: S3 PUT"](#)

# Usando a ferramenta audit-sum

Você pode usar a `audit-sum` ferramenta para contar as mensagens de auditoria de gravação, leitura, cabeçalho e exclusão e ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

## O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP do nó de administração principal.

## Sobre esta tarefa

A `audit-sum` ferramenta, disponível no nó de administração principal, resume quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações demoraram.



A `audit-sum` ferramenta destina-se principalmente ao uso por suporte técnico durante operações de solução de problemas. As consultas de processamento `audit-sum` podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID.

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
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
```

A `audit-sum` ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria S3, Swift e ILM em um log de auditoria:

Código	Descrição	Consulte
ARCT	Recuperação de arquivamento do Cloud-Tier	"ARCT: Recuperação de arquivos do Cloud-Tier"
ASCT	Archive Store Cloud-Tier	"ASCT: Archive Store Cloud-Tier"

<b>Código</b>	<b>Descrição</b>	<b>Consulte</b>
IDEL	ILM iniciado Excluir: Registra quando ILM inicia o processo de exclusão de um objeto.	"IDEL: ILM iniciou Excluir"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou um bucket.	"SDEL: S3 DELETE"
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	"SHEA: S3 CABEÇA"
SPUT	S3 put: Registra uma transação bem-sucedida para criar um novo objeto ou bucket.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contentor.	"WDEL: Swift DELETE"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contentor.	"WGET: Rápido"
BEM-VINDO	Swift head: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contentor.	"WHEA: CABEÇA rápida"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contentor.	"WPUT: Swift PUT"

A `audit-sum` ferramenta pode processar logs de auditoria simples ou compactados. Por exemplo:

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

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

A `audit-sum` ferramenta também pode processar vários arquivos de uma só vez. Por exemplo:

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



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

Finalmente, a `audit-sum` ferramenta também pode aceitar entrada de um pipe, que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

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

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

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



Esta ferramenta não aceita arquivos compactados como entrada pipeada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use a `zcat` ferramenta para descomprimir os arquivos primeiro. Por exemplo:

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

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

Você pode usar as opções de linha de comando para resumir as operações em intervalos separadamente das operações em objetos ou agrupar resumos de mensagens por nome de intervalo, por período de tempo ou por tipo de destino. Por padrão, os resumos mostram o tempo de operação mínimo, máximo e médio, mas você pode usar a `size (-s)` opção para olhar o tamanho do objeto.

Utilize a `help (-h)` opção para ver as opções disponíveis. Por exemplo:

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

## Passos

1. Faça login no nó de administração principal:
  - a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
  - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Se você quiser analisar todas as mensagens relacionadas às operações de gravação, leitura, cabeçalho e exclusão, siga estas etapas:
  - a. Digite o seguinte comando, onde `/var/local/audit/export/audit.log` representa o nome e a localização do arquivo ou arquivos que você deseja analisar:

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

Este exemplo mostra a saída típica da `audit-sum` ferramenta. Este exemplo mostra quanto tempo as operações de protocolo demoraram.

```
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
```

Neste exemplo, as operações de SGET (S3 GET) são as mais lentas em média em 1,13 segundos, mas as operações de SGET e SPUT (S3 PUT) mostram tempos piores longos de cerca de 1.770 segundos.

- b. Para mostrar as operações de recuperação 10 mais lentas, use o comando `grep` para selecionar apenas mensagens SGET e adicionar a opção de saída longa (`-l`) para incluir caminhos de objeto:
- ```
grep SGET audit.log | audit-sum -l
```

Os resultados incluem o tipo (objeto ou bucket) e o caminho, que permite que você `grep` o log de auditoria para outras mensagens relacionadas a esses objetos específicos.

```

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

```

+ A partir deste exemplo de saída, você pode ver que os três pedidos mais lentos de S3 GET foram para objetos de tamanho de cerca de 5 GB, que é muito maior do que os outros objetos. O tamanho grande é responsável pelos tempos de recuperação lentos do pior caso.

3. Se você quiser determinar em que tamanhos de objetos estão sendo ingeridos e recuperados da grade, use a opção tamanho (-s):

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

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

Neste exemplo, o tamanho médio do objeto para SPUT é inferior a 2,5 MB, mas o tamanho médio para SGET é muito maior. O número de mensagens SPUT é muito maior do que o número de mensagens SGET, indicando que a maioria dos objetos nunca são recuperados.

4. Se você quiser determinar se as recuperações foram lentas ontem:
  - a. Emita o comando no log de auditoria apropriado e use a opção Group-by-time (-gt), seguida pelo período de tempo (por exemplo, 15M, 1H, 10S):

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

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

Esses resultados mostram que S3 RECEBEM tráfego aumentado entre 06:00 e 07:00. Os tempos máximos e médios são consideravelmente mais elevados nestes tempos também, e eles não aumentaram gradualmente à medida que a contagem aumentou. Isso sugere que a capacidade foi excedida em algum lugar, talvez na rede ou na capacidade da grade de processar solicitações.

- b. Para determinar que objetos de tamanho estavam sendo recuperados a cada hora ontem, adicione a opção tamanho (-s) ao comando:

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

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

Esses resultados indicam que algumas recuperações muito grandes ocorreram quando o tráfego geral de recuperação estava no seu máximo.

- c. Para ver mais detalhes, use a `audit-explain` ferramenta para revisar todas as operações SGET durante essa hora:

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

Se a saída do comando `grep` for esperada para ser muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) de cada vez.

- 5. Se você quiser determinar se as operações do SPUT em buckets são mais lentas do que as operações do SPUT para objetos:
  - a. Comece usando a `-go` opção, que agrupa as mensagens para operações de objeto e bucket separadamente:

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

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

Os resultados mostram que as operações do SPUT para buckets têm características de desempenho diferentes das operações do SPUT para objetos.

- b. Para determinar quais buckets têm as operações de SPUT mais lentas, use a `-gb` opção, que agrupa as mensagens por bucket:

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

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

- c. Para determinar quais buckets têm o maior tamanho de objeto SPUT, use as `-gb` opções e `-s`:

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

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

**Informações relacionadas**

["Utilizando a ferramenta de auditoria-explicação"](#)



## Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.