



감사 로그 파일 형식

StorageGRID 11.8

NetApp
March 19, 2024

목차

감사 로그 파일 형식	1
감사 로그 파일 형식: 개요	1
감사 설명 도구를 사용합니다	2
감사 집계 도구를 사용합니다	4

감사 로그 파일 형식

감사 로그 파일 형식: 개요

감사 로그 파일은 모든 관리 노드에서 찾을 수 있으며 개별 감사 메시지 모음을 포함합니다.

각 감사 메시지는 다음이 포함됩니다.

- ISO 8601 형식의 감사 메시지(ATIM)를 트리거한 이벤트의 UTC(협정 세계시) 다음에 공백이 옵니다.

YYYY-MM-DDTHH:MM:SS.UUUUUU, 위치 *UUUUUU* 마이크로초

- 감사 메시지 자체는 대괄호로 묶이고 로 시작합니다 AUDT.

다음 예제에서는 감사 로그 파일에 포함된 세 가지 감사 메시지를 보여 줍니다(가독성을 위해 줄 바꿈이 추가됨). 이러한 메시지는 테넌트가 S3 버킷을 생성하고 이 버킷에 두 개의 오브젝트를 추가할 때 생성되었습니다.

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]]
```

감사 로그 파일의 감사 메시지는 기본적으로 읽기 또는 해석하기가 쉽지 않습니다. 를 사용할 수 있습니다 ["감사 - 설명 도구"](#) 감사 로그의 감사 메시지에 대한 간단한 요약 을 얻으려면 다음을 수행합니다. 를 사용할 수 있습니다 ["감사 합계 도구"](#) 얼마나 많은 쓰기, 읽기 및 삭제 작업이 기록되었는지 그리고 얼마나 오래 걸렸는지 요약합니다.

감사 설명 도구를 사용합니다

를 사용할 수 있습니다 `audit-explain` 감사 로그의 감사 메시지를 읽기 쉬운 형식으로 변환하는 도구입니다.

시작하기 전에

- 있습니다 "특정 액세스 권한".
- 에 가 있어야 합니다 Passwords.txt 파일.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

를 클릭합니다 audit-explain 기본 관리 노드에서 사용할 수 있는 도구는 감사 로그의 감사 메시지에 대한 간단한 요약を提供합니다.



를 클릭합니다 audit-explain 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하도록 설계되었습니다. 처리 중입니다 audit-explain 쿼리는 많은 양의 CPU 성능을 소모하여 StorageGRID 작업에 영향을 줄 수 있습니다.

이 예는 의 일반적인 출력을 보여줍니다 audit-explain 도구. 요거 네네 "SPUT" 계정 ID 92484777680322627870이 있는 S3 테넌트가 S3 PUT 요청을 사용하여 "bucket1"이라는 이름의 버킷을 생성하고 해당 버킷에 세 개의 오브젝트를 추가할 때 감사 메시지가 생성되었습니다.

```
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
```

를 클릭합니다 audit-explain 도구는 다음을 수행할 수 있습니다.

- 일반 또는 압축 감사 로그를 처리합니다. 예를 들면 다음과 같습니다.

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

- 여러 파일을 동시에 처리합니다. 예를 들면 다음과 같습니다.

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
audit-explain /var/local/log/*
```

- 파이프에서 입력을 받아 을 사용하여 입력을 필터링하고 사전 처리할 수 있습니다 grep 명령 또는 기타 방법. 예를 들면 다음과 같습니다.

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

감사 로그는 매우 크고 구문 분석 속도가 느릴 수 있으므로 보고 실행할 부분을 필터링하여 시간을 절약할 수 있습니다

audit-explain 전체 파일 대신 파트에서.



를 클릭합니다 audit-explain 도구는 압축된 파일을 파이프된 입력으로 허용하지 않습니다. 압축된 파일을 처리하려면 파일 이름을 명령줄 인수로 제공하거나 를 사용합니다 zcat 먼저 파일의 압축을 푸는 도구입니다. 예를 들면 다음과 같습니다.

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

를 사용합니다 help (-h) 옵션을 클릭하여 사용 가능한 옵션을 표시합니다. 예를 들면 다음과 같습니다.

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

단계

1. 기본 관리자 노드에 로그인합니다.

- 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

2. 다음 명령을 입력합니다. 여기서 /var/local/log/audit.log 분석할 파일의 이름과 위치를 나타냅니다.

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

를 클릭합니다 audit-explain 도구는 지정된 파일 또는 파일의 모든 메시지에 대해 사람이 읽을 수 있는 해석을 인쇄합니다.



선 길이를 줄이고 가독성을 높이기 위해 타임스탬프가 기본적으로 표시되지 않습니다. 타임스탬프를 보려면 타임스탬프를 사용합니다 (-t) 옵션을 선택합니다.

감사 합계 도구를 사용합니다

를 사용할 수 있습니다 audit-sum 감사 메시지 쓰기, 읽기, 헤드 및 삭제 횟수를 세고 각 작업 유형에 대한 최소, 최대 및 평균 시간(또는 크기)을 확인하는 도구입니다.

시작하기 전에

- 있습니다 "특정 액세스 권한".
- 에 가 있어야 합니다 Passwords.txt 파일.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

를 클릭합니다 audit-sum 기본 관리 노드에서 사용할 수 있는 도구는 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업이 소요된 시간을 요약합니다.



를 클릭합니다 audit-sum 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하도록 설계되었습니다. 처리 중입니다 audit-sum 쿼리는 많은 양의 CPU 성능을 소모하여 StorageGRID 작업에 영향을 줄 수 있습니다.

이 예는 의 일반적인 출력을 보여줍니다 audit-sum 도구. 이 예에서는 프로토콜 작업이 얼마나 오래 걸렸는지 보여줍니다.

```

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

```

를 클릭합니다 audit-sum 툴에서 감사 로그에 다음 S3, Swift 및 ILM 감사 메시지의 수와 시간을 제공합니다.

코드	설명	을 참조하십시오
ARCT	클라우드 계층에서 아카이브 검색 - 계층	"ARCT: 클라우드 계층에서 아카이브 검색"
ASCT	Archive Store Cloud - Tier 를 선택합니다	"ASCT: Archive Store Cloud - Tier(아카이브 저장소 클라우드 - 계층)"
IDEL	ILM에서 삭제 시작: ILM이 개체 삭제 프로세스를 시작할 때 기록합니다.	"IDEL: ILM 삭제 시작"
SDEL	S3 삭제: 오브젝트 또는 버킷을 삭제하기 위해 트랜잭션을 성공적으로 기록합니다.	"SDEL: S3 삭제"
SGET	S3 GET: 성공적인 트랜잭션을 로그하여 객체를 검색하거나 버킷의 오브젝트를 나열합니다.	"SGET: S3 GET"
셰어	S3 HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 버킷의 존재 여부를 확인합니다.	"Shea: S3 헤드"
SPUT	S3 PUT: 새 오브젝트 또는 버킷을 생성하기 위한 성공적인 트랜잭션을 기록합니다.	"SPUT: S3 PUT"

코드	설명	을 참조하십시오
WDEL	SWiFT DELETE(빠른 삭제): 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너를 삭제합니다.	"WDEL: Swift 삭제"
WINGIP	SWiFT GET: 성공한 트랜잭션을 로그하여 객체를 검색하거나 컨테이너의 객체를 나열합니다.	"wget: Swift get"
WHEA	SWiFT HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너의 존재를 확인합니다.	"WHEA: 스윙프트 헤드"
WPUT	SWiFT PUT: 새 개체 또는 컨테이너를 생성하기 위해 트랜잭션을 성공적으로 기록합니다.	"WPUT: Swift Put"

를 클릭합니다 `audit-sum` 도구는 다음을 수행할 수 있습니다.

- 일반 또는 압축 감사 로그를 처리합니다. 예를 들면 다음과 같습니다.

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

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

- 여러 파일을 동시에 처리합니다. 예를 들면 다음과 같습니다.

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

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

- 파이프에서 입력을 받아 을 사용하여 입력을 필터링하고 사전 처리할 수 있습니다 `grep` 명령 또는 기타 방법. 예를 들면 다음과 같습니다.

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

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

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



이 도구는 압축된 파일을 파이프된 입력으로 허용하지 않습니다. 압축된 파일을 처리하려면 파일 이름을 명령줄 인수로 제공하거나 `l` 를 사용합니다 `zcat` 먼저 파일의 압축을 푸는 도구입니다. 예를 들면 다음과 같습니다.

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

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

명령줄 옵션을 사용하여 객체에 대한 작업과 별도로 버킷 작업을 요약하거나 버킷 이름, 기간 또는 목표 유형별로 메시지 요약을 그룹화할 수 있습니다. 기본적으로 요약에는 최소, 최대 및 평균 작동 시간이 표시되지만 을 사용할 수 있습니다 `size (-s)` 대신 개체 크기를 보는 옵션입니다.

를 사용합니다 help (-h) 옵션을 클릭하여 사용 가능한 옵션을 표시합니다. 예를 들면 다음과 같습니다.

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

단계

1. 기본 관리자 노드에 로그인합니다.

- a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
- c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

루트로 로그인하면 프롬프트가 `에서` 변경됩니다 `$` 를 선택합니다 `#`.

2. 쓰기, 읽기, 헤드 및 삭제 작업과 관련된 모든 메시지를 분석하려면 다음 단계를 수행하십시오.

- a. 다음 명령을 입력합니다. 여기서 `/var/local/log/audit.log` 분석할 파일의 이름과 위치를 나타냅니다.

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

이 예는 의 일반적인 출력을 보여줍니다 `audit-sum` 도구. 이 예에서는 프로토콜 작업이 얼마나 오래 걸렸는지 보여 줍니다.

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			

이 예에서 SGET(S3 GET) 작업은 평균 1.13초 동안 가장 느리지만, SGET 및 SPUT(S3 PUT) 작업은 모두 1,770초 정도의 긴 최악의 경우를 나타냅니다.

- b. 가장 느린 10개의 검색 작업을 표시하려면 `grep` 명령을 사용하여 SGET 메시지만 선택하고 긴 출력 옵션을 추가합니다 (-l) 개체 경로를 포함하려면 다음을 수행합니다.

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

결과에 유형(오브젝트 또는 버킷) 및 경로가 포함되어 있어 이러한 특정 오브젝트와 관련된 다른 메시지에 대해 감사 로그를 작성할 수 있습니다.

```

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

```

+ 이 예제 출력에서 세 개의 가장 느린 S3 GET 요청은 크기가 약 5GB인 오브젝트에 대해 다른 오브젝트보다 훨씬 크다는 것을 알 수 있습니다. 크기가 크면 검색 시간이 느려질 수 있습니다.

3. 그리드에서 인제스트되고 검색되는 오브젝트 크기를 결정하려면 크기 옵션을 사용합니다 (-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

이 예에서 SPUT의 평균 개체 크기는 2.5MB 미만이지만 SGET의 평균 크기는 훨씬 큼니다. SPUT 메시지 수가 SGET 메시지 수보다 훨씬 많음을 나타내며, 이는 대부분의 개체가 검색되지 않음을 나타냅니다.

4. 어제 검색 속도가 느리는지 확인하려면:

- a. 적절한 감사 로그에 명령을 실행하고 GROUP-By-TIME 옵션을 사용합니다 (-gt), 그 다음에 시간(예: 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

이러한 결과는 S3이 06:00에서 07:00 사이에 트래픽이 증가하는 것을 보여줍니다. 최대 시간과 평균 시간도 이 시기에 상당히 높으면서, 수가 증가할수록 점차 증가하지는 않았습니다. 이는 네트워크 또는 그리드의 요청 처리 능력 중 어느 곳보다 용량이 초과된 것을 의미합니다.

b. 어제 매시간 검색되는 개체의 크기를 확인하려면 크기 옵션을 추가합니다 (-s) 명령으로:

```
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

이러한 결과는 전체 검색 트래픽이 최대값일 때 매우 큰 검색 결과가 발생했음을 나타냅니다.

c. 자세한 내용은 를 참조하십시오 "감사 - 설명 도구" 해당 시간 동안 모든 SGET 작업을 검토하려면:

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

grep 명령의 출력이 여러 줄로 예상되는 경우 를 추가합니다 less 한 번에 한 페이지(한 화면)씩 감사 로그 파일의 내용을 표시하는 명령입니다.

5. 버킷의 SPUT 작업이 개체에 대한 SPUT 작업보다 느리는지 확인하려면 다음을 수행합니다.

a. 을 사용하여 시작합니다 -go 오브젝트 및 버킷 작업에 대한 메시지를 개별적으로 그룹화하는 옵션:

```
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			

결과는 버킷에 대한 SPUT 작업의 성능 특성이 객체에 대한 SPUT 작업과 다르다는 것을 보여줍니다.

- b. 어떤 버킷이 가장 느린 SPUT 작업을 가지는지 확인하려면 `l` 를 사용합니다 `-gb` 버킷별로 메시지를 그룹화하는 옵션:

```
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. 어떤 버킷이 최대 SPUT 객체 크기를 가지는지 확인하려면 두 가지를 모두 사용하십시오 `-gb` 및 `-s` 옵션:

```
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			

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.