



멀티파트 업로드 작업 StorageGRID software

NetApp
July 23, 2026

목차

멀티파트 업로드 작업	1
StorageGRID에서 지원되는 멀티파트 업로드 작업	1
StorageGRID S3 REST API가 멀티파트 업로드를 완료하는 방법	2
충돌 해결	2
지원되는 요청 헤더	2
지원되지 않는 요청 헤더	3
버전 관리	3
복제, 알림 또는 메타데이터 알림 실패	4
StorageGRID의 S3 CreateMultipartUpload 요청 헤더 및 옵션	4
지원되는 요청 헤더	5
서버 측 암호화에 대한 요청 헤더	6
지원되지 않는 요청 헤더	6
버전 관리	7
S3 ListMultipartUploads 작업 및 StorageGRID에서 지원되는 매개 변수	7
버전 관리	7
StorageGRID의 S3 UploadPart 작업에 대해 지원되는 요청 헤더 및 지원되지 않는 요청 헤더	7
지원되는 요청 헤더	7
서버 측 암호화에 대한 요청 헤더	8
지원되지 않는 요청 헤더	8
버전 관리	8
S3 UploadPartCopy 작업을 사용하여 StorageGRID에 객체의 일부를 업로드합니다	8
서버 측 암호화에 대한 요청 헤더	9
버전 관리	9

멀티파트 업로드 작업

StorageGRID에서 지원되는 멀티파트 업로드 작업

이 섹션에서는 StorageGRID가 멀티파트 업로드 작업을 지원하는 방법을 설명합니다.

모든 멀티파트 업로드 작업에는 다음과 같은 조건과 유의사항이 적용됩니다.

- 단일 버킷에 대한 동시 멀티파트 업로드는 1,000개를 초과해서는 안 됩니다. 초과할 경우 해당 버킷에 대한 ListMultipartUploads 쿼리 결과가 불완전하게 반환될 수 있습니다.
- StorageGRID는 멀티파트 파트에 대한 AWS 크기 제한을 적용합니다. S3 클라이언트는 다음 지침을 준수해야 합니다.
 - 멀티파트 업로드의 각 파트는 5MiB(5,242,880바이트)에서 5GiB(5,368,709,120바이트) 사이여야 합니다.
 - 마지막 부분의 크기는 5MiB(5,242,880바이트)보다 작을 수 있습니다.
 - 일반적으로 파트 크기는 가능한 한 크게 설정하는 것이 좋습니다. 예를 들어 100GiB 객체의 경우 5GiB의 파트 크기를 사용하십시오. 각 파트는 고유한 객체로 간주되므로 큰 파트 크기를 사용하면 StorageGRID 메타데이터 오버헤드를 줄일 수 있습니다.
 - 5GiB보다 작은 객체의 경우 멀티파트가 아닌 업로드 방식을 사용하는 것을 고려하십시오.
- ILM 규칙이 균형(Balanced) 또는 엄격(Strict) "[수집 옵션](#)"을 사용하는 경우, 멀티파트 객체가 수집될 때 각 파트에 대해 ILM이 평가되고, 멀티파트 업로드가 완료될 때 객체 전체에 대해 평가됩니다. 이러한 점이 객체 및 파트 배치에 미치는 영향을 숙지해야 합니다.
 - S3 멀티파트 업로드가 진행되는 동안 ILM이 변경되면, 멀티파트 업로드가 완료될 때 객체의 일부 파트가 현재 ILM 요구 사항을 충족하지 못할 수 있습니다. 올바르게 배치되지 않은 파트는 ILM 재평가를 위해 대기열에 추가된 후 나중에 올바른 위치로 이동됩니다.
 - StorageGRID는 파트에 대한 ILM을 평가할 때 객체 전체의 크기가 아닌 파트의 크기를 기준으로 필터링합니다. 즉, 객체의 일부는 객체 전체에 대한 ILM 요구 사항을 충족하지 않는 위치에 저장될 수 있습니다. 예를 들어, 10GB 이상의 모든 객체는 DC1에 저장하고 10GB 미만의 모든 객체는 DC2에 저장하도록 규칙이 지정된 경우, 10개 파트로 구성된 멀티파트 업로드의 각 1GB 파트는 수집 시 DC2에 저장됩니다. 그러나 객체 전체에 대한 ILM이 평가되면 객체의 모든 파트가 DC1으로 이동됩니다.
- 모든 멀티파트 업로드 작업은 StorageGRID "[일관성 값](#)"을 지원합니다.
- 멀티파트 업로드를 사용하여 객체를 수집할 경우, "[객체 분할 임계값\(1 GiB\)](#)"이 적용되지 않습니다.
- 필요에 따라 "[서버 측 암호화](#)" 멀티파트 업로드를 사용할 수 있습니다. SSE(StorageGRID에서 관리하는 키를 사용하는 서버 측 암호화)를 사용하려면 x-amz-server-side-encryption 요청 헤더를 CreateMultipartUpload 요청에만 포함하면 됩니다. SSE-C(고객이 제공하는 키를 사용하는 서버 측 암호화)를 사용하려면 CreateMultipartUpload 요청과 이후의 각 UploadPart 요청에 동일한 세 가지 암호화 키 요청 헤더를 지정해야 합니다.
- 멀티파트 업로드 객체는 업로드 완료 시점과 관계없이 기본 버킷의 'Before' 타임스탬프 이전에 수집이 시작된 경우 "[브랜치 버킷](#)"에 포함됩니다.

작업	구현
AbortMultipartUpload	모든 Amazon S3 REST API 동작에 맞춰 구현되었습니다. 예고 없이 변경될 수 있습니다.

작업	구현
CompleteMultipartUpload	"CompleteMultipartUpload"을 참조하십시오
CreateMultipartUpload (이전 명칭: Initiate Multipart Upload)	"CreateMultipartUpload"을 참조하십시오
ListMultipartUploads	"ListMultipartUploads"을 참조하십시오
ListParts	모든 Amazon S3 REST API 동작에 맞춰 구현되었습니다. 예고 없이 변경될 수 있습니다.
UploadPart	"UploadPart"을 참조하십시오
UploadPartCopy	"UploadPartCopy"을 참조하십시오

StorageGRID S3 REST API가 멀티파트 업로드를 완료하는 방법

CompleteMultipartUpload 작업은 이전에 업로드된 부분들을 조합하여 객체의 멀티파트 업로드를 완료합니다.



StorageGRID는 CompleteMultipartUpload와 함께 사용되는 `partNumber` 요청 매개변수에 대해 오름차순의 비연속적인 값을 지원합니다. 매개변수는 어떤 값으로든 시작할 수 있습니다.

충돌 해결

두 클라이언트가 동일한 키에 쓰기를 시도하는 등 클라이언트 요청이 충돌하는 경우 "최신 요청 우선" 원칙에 따라 처리됩니다. "최신 요청 우선" 평가 시점은 S3 클라이언트가 작업을 시작한 시점이 아니라 StorageGRID 시스템이 해당 요청을 완료한 시점을 기준으로 합니다.

지원되는 요청 헤더

다음과 같은 요청 헤더가 지원됩니다.

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

``x-amz-storage-class`` 헤더는 일치하는 ILM 규칙이

`xref:{relative_path}../ilm/data-protection-options-for-ingest.html["이중 커밋 또는 균형 잡힌 수집 옵션"]`을(를) 지정하는 경우 StorageGRID가 생성하는 객체 복사본 수에 영향을 미칩니다.

- STANDARD

(기본값) ILM 규칙에서 이중 커밋 옵션을 사용하거나 균형 옵션이 임시 복사본 생성으로 대체될 때 이중 커밋 수집 작업을 지정합니다.

- REDUCED_REDUNDANCY

ILM 규칙에서 이중 커밋 옵션을 사용하거나 균형 옵션이 임시 복사본 생성으로 대체될 때 단일 커밋 수집 작업을 지정합니다.



S3 객체 잠금이 활성화된 버킷에 객체를 수집하는 경우 REDUCED_REDUNDANCY 옵션은 무시됩니다. 레거시 규정 준수 버킷에 객체를 수집하는 경우 REDUCED_REDUNDANCY 옵션은 오류를 반환합니다. StorageGRID는 규정 준수 요구 사항을 충족하기 위해 항상 이중 커밋 수집을 수행합니다.



멀티파트 업로드가 15일 이내에 완료되지 않으면 해당 작업은 비활성으로 표시되고 관련 데이터는 시스템에서 모두 삭제됩니다.



반환되는 ETag 값은 데이터의 MD5 합계가 아니라, 멀티파트 객체에 대한 ETag 값의 Amazon S3 API 구현 방식을 따릅니다.

지원되지 않는 요청 헤더

다음 요청 헤더는 지원되지 않습니다.

- If-Match

`If-Match header`은 (는) 승인되었지만 작동하지 않습니다.

- If-None-Match

`If-None-Match header`은 (는) 승인되었지만 작동하지 않습니다.

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

버전 관리

이 작업은 멀티파트 업로드를 완료합니다. 버킷에 버전 관리가 활성화된 경우, 멀티파트 업로드가 완료된 후 객체 버전이 생성됩니다.

버킷에 버전 관리가 활성화된 경우, 저장된 객체의 버전에 대한 고유 `versionId`가 자동으로 생성됩니다. 이 `versionId`는 `x-amz-version-id` 응답 헤더를 사용하여 응답에도 반환됩니다.

버전 관리가 일시 중단되면 객체 버전은 null `versionId`로 저장되며, 이미 null 버전이 존재하는 경우 덮어쓰여집니다.



버킷에 버전 관리가 활성화된 경우, 동일한 객체 키에 대해 동시에 여러 개의 멀티파트 업로드가 완료되더라도 멀티파트 업로드가 완료되면 항상 새 버전이 생성됩니다. 버킷에 버전 관리가 활성화되지 않은 경우, 멀티파트 업로드를 시작한 후 동일한 객체 키에 대해 다른 멀티파트 업로드가 먼저 시작되어 완료될 수 있습니다. 버전 관리가 되지 않는 버킷에서는 마지막으로 완료된 멀티파트 업로드가 우선 순위를 갖습니다.

복제, 알림 또는 메타데이터 알림 실패

멀티파트 업로드가 발생하는 버킷이 플랫폼 서비스용으로 구성된 경우, 관련 복제 또는 알림 작업이 실패하더라도 멀티파트 업로드는 성공합니다.

테넌트는 객체의 메타데이터 또는 태그를 업데이트하여 복제 실패 또는 알림을 발생시킬 수 있습니다. 테넌트는 원치 않는 변경을 방지하려면 기존 값을 다시 제출할 수 있습니다.

"플랫폼 서비스 문제 해결"을 참조하십시오.

StorageGRID의 S3 CreateMultipartUpload 요청 헤더 및 옵션

CreateMultipartUpload(이전 명칭: Initiate Multipart Upload) 작업은 객체에 대한 멀티파트 업로드를 시작하고 업로드 ID를 반환합니다.

``x-amz-storage-class`` 요청 헤더가 지원됩니다. ``x-amz-storage-class``에 제출된 값은 StorageGRID 수집 중에 객체 데이터를 보호하는 방식에 영향을 미치며, StorageGRID 시스템에 객체의 영구 복사본이 몇 개 저장되는지(ILM에 의해 결정됨)에는 영향을 미치지 않습니다.

수집된 객체와 일치하는 ILM 규칙이 Strict "**수집 옵션**"를 사용하는 경우, `x-amz-storage-class` 헤더는 아무런 효과가 없습니다.

다음 값을 사용할 수 있습니다 `x-amz-storage-class`:

- STANDARD (기본값)
 - 듀얼 커밋: ILM 규칙에 듀얼 커밋 수집 옵션이 지정된 경우, 객체가 수집되는 즉시 해당 객체의 두 번째 복사본이 생성되어 다른 스토리지 노드에 배포됩니다(듀얼 커밋). ILM을 평가할 때 StorageGRID는 이러한 초기 임시 복사본이 규칙의 배치 지침을 충족하는지 확인합니다. 충족하지 않는 경우, 다른 위치에 새 객체 복사본을 생성하고 초기 임시 복사본을 삭제해야 할 수 있습니다.
 - 균형: ILM 규칙에 균형 옵션이 지정되어 있고 StorageGRID가 규칙에 지정된 모든 복사본을 즉시 생성할 수 없는 경우 StorageGRID는 서로 다른 스토리지 노드에 두 개의 임시 복사본을 생성합니다.

StorageGRID가 ILM 규칙에 지정된 모든 객체 복사본을 즉시 생성할 수 있는 경우(동기 배치), `x-amz-storage-class` 헤더는 아무런 효과가 없습니다.

- REDUCED_REDUNDANCY
 - 듀얼 커밋: ILM 규칙에서 듀얼 커밋 옵션을 지정하면 StorageGRID는 객체가 수집될 때 단일 임시 복사본을 생성합니다(싱글 커밋).
 - 균형: ILM 규칙에 균형 옵션이 지정된 경우, StorageGRID 시스템이 규칙에 지정된 모든 복사본을 즉시 생성할 수 없는 경우에만 임시 복사본을 하나만 생성합니다. StorageGRID 동기 배치를 수행할 수 있는 경우에는 이

헤더가 아무런 효과가 없습니다. 이 `REDUCED_REDUNDANCY` 옵션은 객체와 일치하는 ILM 규칙이 단일 복제본을 생성하는 경우에 가장 적합합니다. 이 경우 `'REDUCED_REDUNDANCY'`를 사용하면 모든 수집 작업마다 불필요한 객체 복사본 생성 및 삭제를 방지할 수 있습니다.

다른 상황에서는 `REDUCED_REDUNDANCY` 옵션을 사용하는 것을 권장하지 않습니다.

`'REDUCED_REDUNDANCY'`은(는) 수집 중 오브젝트 데이터 손실 위험을 증가시킵니다. 예를 들어, ILM 평가가 수행되기 전에 장애가 발생한 Storage Node에 단일 복사본이 처음에 저장되는 경우 데이터를 손실할 수 있습니다.



특정 기간 동안 복제본이 하나만 존재하는 경우 데이터가 영구적으로 손실될 위험이 있습니다. 객체의 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 중대한 오류가 발생하면 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지 관리 절차 중에도 해당 객체에 대한 액세스가 일시적으로 제한됩니다.

이 설정을 지정하면 `REDUCED_REDUNDANCY` 객체가 처음 수집될 때 생성되는 복사본 수에만 영향을 미칩니다. 활성 ILM 정책에 따라 객체를 평가할 때 생성되는 객체 복사본 수에는 영향을 미치지 않으며, StorageGRID 시스템에서 데이터가 더 낮은 수준의 중복성으로 저장되는 결과를 초래하지도 않습니다.



S3 객체 잠금이 활성화된 버킷에 객체를 수집하는 경우 `REDUCED_REDUNDANCY` 옵션은 무시됩니다. 레거시 규정 준수 버킷에 객체를 수집하는 경우 `REDUCED_REDUNDANCY` 옵션은 오류를 반환합니다. StorageGRID는 규정 준수 요구 사항을 충족하기 위해 항상 이중 커밋 수집을 수행합니다.

지원되는 요청 헤더

다음과 같은 요청 헤더가 지원됩니다.

- `Content-Type`
- `x-amz-checksum-algorithm`

현재는 `'x-amz-checksum-algorithm'`의 SHA256 값만 지원됩니다.

- `x-amz-meta-`, 그 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 옵니다

사용자 정의 메타데이터의 이름-값 쌍을 지정할 때 다음 일반 형식을 사용하십시오.

```
x-amz-meta-__name__: `value`
```

ILM 규칙의 참조 시간으로 사용자 정의 생성 시간 옵션을 사용하려면 `'creation-time'`을(를) 객체가 생성된 시점을 기록하는 메타데이터의 이름으로 사용해야 합니다. 예를 들면 다음과 같습니다.

```
x-amz-meta-creation-time: 1443399726
```

`'creation-time'`의 값은 1970년 1월 1일 이후 경과된 초 단위로 평가됩니다.



`'creation-time'`을(를) 사용자 정의 메타데이터로 추가하는 것은 레거시 규정 준수가 활성화된 버킷에 객체를 추가하는 경우 허용되지 않습니다. 오류가 반환됩니다.

- S3 객체 잠금 요청 헤더:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

이러한 헤더 없이 요청이 이루어지면 버킷의 기본 보존 설정이 사용되어 객체 버전의 보존 기간이 계산됩니다.

"S3 REST API를 사용하여 S3 Object Lock 구성"

- SSE 요청 헤더:

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

서버 측 암호화에 대한 요청 헤더



StorageGRID가 UTF-8 문자를 처리하는 방법에 대한 자세한 내용은 ["PutObject"](#)을 참조하십시오.

서버 측 암호화에 대한 요청 헤더

다음 요청 헤더를 사용하여 서버 측 암호화로 멀티파트 객체를 암호화할 수 있습니다. SSE와 SSE-C 옵션은 상호 배타적입니다.

- **SSE:** StorageGRID에서 관리하는 고유 키로 객체를 암호화하려면 CreateMultipartUpload 요청에 다음 헤더를 사용하십시오. UploadPart 요청에는 이 헤더를 지정하지 마십시오.
 - x-amz-server-side-encryption
- **SSE-C:** 제공하고 관리하는 고유 키로 객체를 암호화하려면 CreateMultipartUpload 요청(및 이후의 각 UploadPart 요청)에 이 세 가지 헤더를 모두 사용하십시오.
 - x-amz-server-side-encryption-customer-algorithm: `AES256`을(를) 지정합니다.
 - x-amz-server-side-encryption-customer-key: 새 객체에 사용할 암호화 키를 지정하십시오.
 - x-amz-server-side-encryption-customer-key-MD5: 새 객체의 암호화 키의 MD5 다이제스트를 지정합니다.



고객이 제공하는 암호화 키는 절대 저장되지 않습니다. 암호화 키를 분실하면 해당 객체도 손실됩니다. 고객이 제공한 키를 사용하여 객체 데이터를 보호하기 전에 ["서버 측 암호화 사용"](#)에 대한 고려 사항을 검토하십시오.

지원되지 않는 요청 헤더

다음 요청 헤더는 지원되지 않습니다.

- x-amz-website-redirect-location

The `x-amz-website-redirect-location` 헤더는 'XNotImplemented'을 반환합니다.

버전 관리

멀티파트 업로드는 업로드 시작, 업로드 목록 보기, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 개별 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행되면 객체가 생성됩니다(해당하는 경우 버전 관리도 수행됨).

S3 ListMultipartUploads 작업 및 StorageGRID에서 지원되는 매개 변수

ListMultipartUploads 작업은 버킷에 대해 진행 중인 멀티파트 업로드 목록을 표시합니다.

다음 요청 매개변수가 지원됩니다.

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

버전 관리

멀티파트 업로드는 업로드 시작, 업로드 목록 보기, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 개별 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행되면 객체가 생성됩니다(해당하는 경우 버전 관리도 수행됨).

StorageGRID의 S3 UploadPart 작업에 대해 지원되는 요청 헤더 및 지원되지 않는 요청 헤더

UploadPart 작업은 객체의 멀티파트 업로드에서 파트를 업로드합니다.

지원되는 요청 헤더

다음과 같은 요청 헤더가 지원됩니다.

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

서버 측 암호화에 대한 요청 헤더

암호화 CreateMultipartUpload 요청에 SSE-C 암호화를 지정한 경우, 각 UploadPart 요청에 다음 요청 헤더도 포함해야 합니다.

- x-amz-server-side-encryption-customer-algorithm: `AES256`을(를) 지정합니다.
- x-amz-server-side-encryption-customer-key: CreateMultipartUpload 요청 시 제공했던 것과 동일한 암호화 키를 지정하십시오.
- x-amz-server-side-encryption-customer-key-MD5: CreateMultipartUpload 요청에서 제공한 것과 동일한 MD5 다이제스트를 지정하십시오.



고객이 제공하는 암호화 키는 절대 저장되지 않습니다. 암호화 키를 분실하면 해당 객체도 손실됩니다. 고객이 제공한 키를 사용하여 객체 데이터를 보호하기 전에 "[서버 측 암호화 사용](#)"의 고려 사항을 검토하십시오.

체크섬 CreateMultipartUpload 요청 시 SHA-256 체크섬을 지정한 경우, 각 UploadPart 요청에 다음 요청 헤더를 포함해야 합니다.

- x-amz-checksum-sha256: 이 부분에 대한 SHA-256 체크섬을 지정하십시오.

지원되지 않는 요청 헤더

다음 요청 헤더는 지원되지 않습니다.

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

버전 관리

멀티파트 업로드는 업로드 시작, 업로드 목록 보기, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 개별 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행되면 객체가 생성됩니다(해당하는 경우 버전 관리도 수행됨).

S3 UploadPartCopy 작업을 사용하여 StorageGRID에 객체의 일부를 업로드합니다

UploadPartCopy 작업은 기존 객체의 데이터를 데이터 소스로 복사하여 객체의 일부를 업로드합니다.

UploadPartCopy 작업은 모든 Amazon S3 REST API 동작 방식을 따릅니다. 예고 없이 변경될 수 있습니다.

이 요청은 StorageGRID 시스템 내의 `x-amz-copy-source-range`에 지정된 객체 데이터를 읽고 씁니다.

다음과 같은 요청 헤더가 지원됩니다.

- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match

- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since

서버 측 암호화에 대한 요청 헤더

암호화 CreateMultipartUpload 요청에 SSE-C 암호화를 지정한 경우, 각 UploadPartCopy 요청에도 다음 요청 헤더를 포함해야 합니다.

- x-amz-server-side-encryption-customer-algorithm: `AES256`을(를) 지정합니다.
- x-amz-server-side-encryption-customer-key: CreateMultipartUpload 요청 시 제공했던 것과 동일한 암호화 키를 지정하십시오.
- x-amz-server-side-encryption-customer-key-MD5: CreateMultipartUpload 요청에서 제공한 것과 동일한 MD5 다이제스트를 지정하십시오.

원본 객체가 고객 제공 키(SSE-C)를 사용하여 암호화된 경우, 객체를 복호화한 후 복사할 수 있도록 UploadPartCopy 요청에 다음 세 가지 헤더를 포함해야 합니다.

- x-amz-copy-source-server-side-encryption-customer-algorithm: `AES256`을(를) 지정합니다.
- x-amz-copy-source-server-side-encryption-customer-key: 소스 객체를 생성할 때 제공한 암호화 키를 지정하십시오.
- x-amz-copy-source-server-side-encryption-customer-key-MD5: 소스 객체를 생성할 때 제공한 MD5 다이제스트를 지정하십시오.



고객이 제공하는 암호화 키는 절대 저장되지 않습니다. 암호화 키를 분실하면 해당 객체도 손실됩니다. 고객이 제공한 키를 사용하여 객체 데이터를 보호하기 전에 "[서버 측 암호화 사용](#)"의 고려 사항을 검토하십시오.

버전 관리

멀티파트 업로드는 업로드 시작, 업로드 목록 보기, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 개별 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행되면 객체가 생성됩니다(해당하는 경우 버전 관리도 수행됨).

저작권 정보

Copyright © 2026 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.