



Operazioni per caricamenti multipart

StorageGRID software

NetApp
July 23, 2026

Sommario

Operazioni per caricamenti multipart	1
Operazioni di caricamento multiparte supportate in StorageGRID	1
Come StorageGRID S3 REST API completa i caricamenti multiparte	2
Risolvere i conflitti	2
Intestazioni di richiesta supportate	2
Intestazioni di richiesta non supportate	3
Versioning	3
Replica, notifica o notifica dei metadati non riuscita	4
Intestazioni e opzioni delle richieste S3 CreateMultipartUpload in StorageGRID	4
Intestazioni di richiesta supportate	5
Intestazioni di richiesta per la crittografia lato server	6
Intestazioni di richiesta non supportate	7
Versioning	7
Operazione S3 ListMultipartUploads e parametri supportati in StorageGRID	7
Versioning	7
Intestazioni di richiesta supportate e non supportate per le operazioni S3 UploadPart in StorageGRID	8
Intestazioni di richiesta supportate	8
Intestazioni di richiesta per la crittografia lato server	8
Intestazioni di richiesta non supportate	8
Versioning	8
Carica una parte di un oggetto in StorageGRID con l'operazione S3 UploadPartCopy	9
Intestazioni di richiesta per la crittografia lato server	9
Versioning	9

Operazioni per caricamenti multipart

Operazioni di caricamento multiparte supportate in StorageGRID

Questa sezione descrive come StorageGRID supporta le operazioni per i caricamenti multipart.

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multipart:

- Non dovresti superare 1.000 caricamenti multipart simultanei in un singolo bucket perché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID applica i limiti di dimensione AWS per le parti multipart. I client S3 devono seguire queste linee guida:
 - Ciascuna parte di un caricamento multipart deve essere compresa tra 5 MiB (5,242,880 byte) e 5 GiB (5,368,709,120 byte).
 - L'ultima parte può essere inferiore a 5 MiB (5.242.880 byte).
 - In generale, le dimensioni delle parti dovrebbero essere le più grandi possibili. Ad esempio, usa parti da 5 GiB per un oggetto da 100 GiB. Poiché ogni parte è considerata un oggetto unico, usare parti di grandi dimensioni riduce il sovraccarico dei metadati di StorageGRID.
 - Per oggetti più piccoli di 5 GiB, considera di usare il caricamento non multipart.
- L'ILM viene valutato per ogni parte di un oggetto multipart durante l'ingestione e per l'oggetto nel suo complesso al termine del caricamento multipart, se la regola ILM utilizza la modalità Balanced o Strict "opzione di ingest". Dovresti sapere come questo influisce sul posizionamento di oggetti e parti:
 - Se ILM cambia durante un caricamento multipart su S3, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento. Qualsiasi parte non posizionata correttamente viene messa in coda per una nuova valutazione da parte di ILM e spostata nella posizione corretta in un secondo momento.
 - Quando valuti ILM per una parte, StorageGRID filtra in base alla dimensione della parte, non alla dimensione dell'oggetto. Questo significa che le parti di un oggetto possono essere archiviate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo insieme. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, ogni parte da 1 GB di un caricamento multipart da 10 parti viene archiviata in DC2 all'ingest. Tuttavia, quando ILM viene valutato per l'oggetto nel suo insieme, tutte le parti dell'oggetto vengono spostate in DC1.
- Tutte le operazioni di caricamento multipart supportano StorageGRID "valori di coerenza".
- Quando un oggetto viene inserito tramite caricamento multipart, "Soglia di segmentazione dell'oggetto (1 GiB)" non viene applicato.
- Come richiesto, puoi usare "crittografia lato server" con i caricamenti multipart. Per usare SSE (crittografia lato server con chiavi gestite da StorageGRID), includi l'`x-amz-server-side-encryption` header della richiesta solo nella richiesta CreateMultipartUpload. Per usare SSE-C (crittografia lato server con chiavi fornite dal cliente), specifichi le stesse tre intestazioni di richiesta della chiave di crittografia sia nella richiesta CreateMultipartUpload che in ogni successiva richiesta UploadPart.
- Un oggetto caricato in più parti viene incluso in un "bucket branch" se l'ingestione è stata avviata prima del timestamp Before del bucket di base, indipendentemente da quando il caricamento viene completato.

Operazione	Implementazione
AbortMultipartUpload	Implementato con tutte le funzionalità dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
CompleteMultipartUpload	Vedi " CompleteMultipartUpload "
CreateMultipartUpload (precedentemente denominato Initiate Multipart Upload)	Vedi " CreateMultipartUpload "
ListMultipartUploads	Vedi " ListMultipartUploads "
ListParts	Implementato con tutte le funzionalità dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
UploadPart	Vedi " UploadPart "
UploadPartCopy	Vedi " UploadPartCopy "

Come StorageGRID S3 REST API completa i caricamenti multiparte

L'operazione CompleteMultipartUpload completa il caricamento di un oggetto suddiviso in più parti assemblando le parti precedentemente caricate.



StorageGRID supporta valori non consecutivi in ordine crescente per il parametro di richiesta `partNumber` con CompleteMultipartUpload. Il parametro può iniziare con qualsiasi valore.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". Il momento in cui viene effettuata la valutazione "latest-wins" si basa su quando il sistema StorageGRID completa una determinata richiesta, e non su quando i client S3 iniziano un'operazione.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

L'`x-amz-storage-class`intestazione influisce su quante copie di oggetti StorageGRID crea se la regola ILM corrispondente specifica il "[Opzione di doppio commit o di acquisizione bilanciata](#)".

- STANDARD

(Predefinito) Specifica un'operazione di ingestione a doppio commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ripiega sulla creazione di copie intermedie.

- REDUCED_REDUNDANCY

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ripiega sulla creazione di copie intermedie.



Se stai inserendo un oggetto in un bucket con S3 Object Lock abilitato, l'`REDUCED\_REDUNDANCY` opzione viene ignorata. Se stai inserendo un oggetto in un bucket Compliant legacy, l'`REDUCED\_REDUNDANCY` opzione restituisce un errore. StorageGRID esegue sempre un ingest con doppio commit per garantire che i requisiti di conformità siano soddisfatti.



Se un caricamento in più parti non viene completato entro 15 giorni, l'operazione viene contrassegnata come inattiva e tutti i dati associati vengono eliminati dal sistema.



Il ETag valore restituito non è una somma MD5 dei dati, ma segue l'implementazione dell'API di Amazon S3 del ETag valore per gli oggetti multipart.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- If-Match

The If-Match header è accettato ma non funzionale.

- If-None-Match

The If-None-Match header è accettato ma non funzionale.

- x-amz-sdk-checksum-algorithm

- x-amz-trailer

Versioning

Questa operazione completa un caricamento in più parti. Se la gestione delle versioni è abilitata per un bucket, la versione dell'oggetto viene creata al termine del caricamento in più parti.

Se il versioning è abilitato per un bucket, un identificativo univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene inoltre restituito nella risposta tramite l'intestazione di risposta `x-amz-version-id`.

Se la gestione delle versioni viene sospesa, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione con valore nullo, verrà sovrascritta.



Quando la gestione delle versioni è abilitata per un bucket, il completamento di un caricamento multipart crea sempre una nuova versione, anche se sono presenti caricamenti multipart simultanei completati sulla stessa chiave oggetto. Quando la gestione delle versioni non è abilitata per un bucket, è possibile avviare un caricamento multipart e poi far sì che un altro caricamento multipart venga avviato e completato prima sulla stessa chiave oggetto. Nei bucket senza gestione delle versioni, ha la precedenza il caricamento multipart che viene completato per ultimo.

Replica, notifica o notifica dei metadati non riuscita

Se il bucket in cui avviene il caricamento multipart è configurato per un servizio di piattaforma, il caricamento multipart ha esito positivo anche se l'azione di replica o notifica associata non riesce.

Un tenant può attivare la replica non riuscita o la notifica aggiornando i metadati o i tag dell'oggetto. Un tenant può inviare nuovamente i valori esistenti per evitare di apportare modifiche indesiderate.

Consulta ["Risolvi i problemi dei servizi della piattaforma"](#).

Intestazioni e opzioni delle richieste S3 CreateMultipartUpload in StorageGRID

L'operazione CreateMultipartUpload (precedentemente denominata Initiate Multipart Upload) avvia un caricamento multipart per un oggetto e restituisce un ID di caricamento.

L'`x-amz-storage-class` intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` influisce su come StorageGRID protegge i dati degli oggetti durante l'ingest e non su quante copie persistenti dell'oggetto vengono memorizzate nel sistema StorageGRID (che è determinato da ILM).

Se la regola ILM corrispondente a un oggetto ingerito utilizza la modalità Strict ["opzione di ingest"](#), l'`x-amz-storage-class` intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class`:

- STANDARD (Predefinito)
 - **Doppio commit:** Se la regola ILM specifica l'opzione di acquisizione a doppio commit, non appena un oggetto viene acquisito, viene creata una seconda copia di quell'oggetto e distribuita a un nodo di archiviazione diverso (doppio commit). Quando viene valutato l'ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento nella regola. Se non lo fanno, potrebbe essere necessario creare nuove copie dell'oggetto in posizioni diverse e potrebbe essere necessario eliminare le copie intermedie iniziali.
 - **Bilanciato:** Se la regola ILM specifica l'opzione Bilanciato e StorageGRID non può creare immediatamente tutte le copie specificate nella regola, StorageGRID crea due copie intermedie su nodi di storage diversi.

Se StorageGRID può creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), l'`x-amz-storage-class` intestazione non ha alcun effetto.

- REDUCED_REDUNDANCY
 - **Doppio commit:** Se la regola ILM specifica l'opzione Doppio commit, StorageGRID crea una singola

copia intermedia durante l'acquisizione dell'oggetto (commit singolo).

- **Bilanciato:** Se la regola ILM specifica l'opzione Bilanciato, StorageGRID crea una singola copia intermedia solo se il sistema non può creare immediatamente tutte le copie specificate nella regola. Se StorageGRID può eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L'opzione `REDUCED_REDUNDANCY` è più indicata quando la regola ILM che corrisponde all'oggetto crea una singola copia replicata. In questo caso, usare `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia aggiuntiva dell'oggetto per ogni operazione di ingest.

Usare l' `REDUCED_REDUNDANCY` opzione non è consigliato in altre circostanze. `REDUCED_REDUNDANCY` Aumenta il rischio di perdita di dati degli oggetti durante l'ingestione. Ad esempio, potresti perdere dati se la singola copia viene inizialmente memorizzata su un Storage Node che si guasta prima che possa avvenire la valutazione ILM.



Avere una sola copia replicata per un determinato periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quell'oggetto viene perso se un Storage Node si guasta o presenta un errore significativo. Perdi anche temporaneamente l'accesso all'oggetto durante procedure di manutenzione come gli aggiornamenti.

La specifica `REDUCED_REDUNDANCY` influisce solo su quante copie vengono create quando un oggetto viene acquisito per la prima volta. Non influisce su quante copie dell'oggetto vengono create quando l'oggetto viene valutato dalle policy ILM attive e non comporta che i dati vengano archiviati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se stai inserendo un oggetto in un bucket con S3 Object Lock abilitato, l' `REDUCED_REDUNDANCY` opzione viene ignorata. Se stai inserendo un oggetto in un bucket Compliant legacy, l' `REDUCED_REDUNDANCY` opzione restituisce un errore. StorageGRID esegue sempre un ingest con doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

Attualmente è supportato solo il valore `SHA256` per `x-amz-checksum-algorithm`.

- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente

Quando specifichi la coppia nome-valore per i metadati definiti dall'utente, usa questo formato generale:

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

Se vuoi usare l'opzione **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, devi usare `creation-time` come nome del metadato che registra quando è stato creato l'oggetto. Ad esempio:

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

Il valore per `creation-time` viene valutato come secondi dal 1° gennaio 1970.



Aggiungere `creation-time` come metadati definiti dall'utente non è consentito se aggiungi un oggetto a un bucket con la Compliance legacy abilitata. Viene restituito un errore.

- Intestazioni della richiesta S3 Object Lock:

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

Se una richiesta viene effettuata senza queste intestazioni, vengono utilizzate le impostazioni di periodo di conservazione predefinite del bucket per calcolare la `retain-until-date` della versione dell'oggetto.

["Utilizza l'API REST S3 per configurare S3 Object Lock"](#)

- Intestazioni della richiesta SSE:

- `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`

[Intestazioni di richiesta per la crittografia lato server](#)



Per informazioni su come StorageGRID gestisce i caratteri UTF-8, vedi ["PutObject"](#).

Intestazioni di richiesta per la crittografia lato server

Puoi usare le seguenti intestazioni di richiesta per crittografare un oggetto multipart con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE:** Usa la seguente intestazione nella richiesta `CreateMultipartUpload` se vuoi crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste `UploadPart`.
 - `x-amz-server-side-encryption`
- **SSE-C:** Utilizza tutte e tre queste intestazioni nella richiesta `CreateMultipartUpload` (e in ogni richiesta `UploadPart` successiva) se vuoi crittografare l'oggetto con una chiave univoca che fornisci e gestisci tu.
 - `x-amz-server-side-encryption-customer-algorithm`: Specifica AES256.
 - `x-amz-server-side-encryption-customer-key`: Specifica la tua chiave di crittografia per il nuovo oggetto.

- `x-amz-server-side-encryption-customer-key-MD5`: Specifica l'MD5 digest della chiave di crittografia del nuovo oggetto.



Le chiavi di crittografia che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi l'oggetto corrispondente. Prima di utilizzare chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedi le considerazioni per ["utilizzando la crittografia lato server"](#).

Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata:

- `x-amz-website-redirect-location`

L'`x-amz-website-redirect-location` intestazione restituisce ``XNotImplemented`.

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e versionati, se applicabile) quando viene eseguita l'operazione `CompleteMultipartUpload`.

Operazione S3 ListMultipartUploads e parametri supportati in StorageGRID

L'operazione `ListMultipartUploads` elenca i caricamenti multipart in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

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

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e versionati, se applicabile) quando viene eseguita l'operazione `CompleteMultipartUpload`.

Intestazioni di richiesta supportate e non supportate per le operazioni S3 UploadPart in StorageGRID

L'operazione UploadPart carica una parte di un caricamento multipart per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

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

Intestazioni di richiesta per la crittografia lato server

Se hai specificato la crittografia SSE-C per la richiesta CreateMultipartUpload, devi includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Specifica AES256.
- `x-amz-server-side-encryption-customer-key`: Specifica la stessa chiave di crittografia che hai fornito nella richiesta CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica lo stesso digest MD5 che hai fornito nella richiesta CreateMultipartUpload.



Le chiavi di crittografia che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi anche l'oggetto corrispondente. Prima di usare chiavi fornite dal cliente per proteggere i dati degli oggetti, consulta le considerazioni in ["\\${post_edited_translations.segment}"](#).

Se hai specificato un checksum SHA-256 durante la richiesta CreateMultipartUpload, devi includere anche la seguente intestazione di richiesta in ogni richiesta UploadPart:

- `x-amz-checksum-sha256`: Specifica il checksum SHA-256 per questa parte.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

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

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e versionati, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

Carica una parte di un oggetto in StorageGRID con l'operazione S3 UploadPartCopy

L'operazione UploadPartCopy carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione UploadPartCopy è implementata con tutto il comportamento dell'API REST di Amazon S3. Soggetta a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificato in `x-amz-copy-source-range` all'interno del sistema StorageGRID.

Sono supportate le seguenti intestazioni di richiesta:

- `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`

Intestazioni di richiesta per la crittografia lato server

Se hai specificato la crittografia SSE-C per la richiesta CreateMultipartUpload, devi includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Specifica AES256.
- `x-amz-server-side-encryption-customer-key`: Specifica la stessa chiave di crittografia che hai fornito nella richiesta CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica lo stesso digest MD5 che hai fornito nella richiesta CreateMultipartUpload.

Se l'oggetto sorgente è crittografato utilizzando una chiave fornita dal cliente (SSE-C), devi includere le seguenti tre intestazioni nella richiesta UploadPartCopy, così l'oggetto può essere decrittografato e poi copiato:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specifica AES256.
- ``x-amz-copy-source-server-side-encryption-customer-key``: Specifica la chiave di crittografia che hai fornito quando hai creato l'oggetto sorgente.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 che hai fornito quando hai creato l'oggetto sorgente.



Le chiavi di crittografia che fornisci non vengono mai memorizzate. Se perdi una chiave di crittografia, perdi anche l'oggetto corrispondente. Prima di usare chiavi fornite dal cliente per proteggere i dati degli oggetti, consulta le considerazioni in ["\\${post_edited_translations.segment}"](#).

Versioning

Il caricamento in più parti consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e

versionati, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

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.