



# **Operaciones para cargas multiparte**

## StorageGRID software

NetApp  
December 03, 2025

# Tabla de contenidos

Operaciones para cargas multiparte .....	1
Operaciones para cargas multiparte .....	1
Carga completa de varias partes .....	2
Resolver conflictos .....	2
Encabezados de solicitud admitidos .....	2
Encabezados de solicitud no admitidos .....	3
Control de versiones .....	3
Error de replicación, notificación o notificación de metadatos .....	3
Crear carga de varias partes .....	4
Encabezados de solicitud admitidos .....	5
Encabezados de solicitud para el cifrado del lado del servidor .....	6
Encabezados de solicitud no admitidos .....	6
Control de versiones .....	6
Lista de cargas de varias partes .....	7
Control de versiones .....	7
Subir parte .....	7
Encabezados de solicitud admitidos .....	7
Encabezados de solicitud para el cifrado del lado del servidor .....	7
Encabezados de solicitud no admitidos .....	8
Control de versiones .....	8
Subir copia parcial .....	8
Encabezados de solicitud para el cifrado del lado del servidor .....	8
Control de versiones .....	9

# Operaciones para cargas multipart

## Operaciones para cargas multipart

Esta sección describe cómo StorageGRID admite operaciones para cargas multipart.

Las siguientes condiciones y notas se aplican a todas las operaciones de carga multipart:

- No debe exceder las 1000 cargas multipart simultáneas en un solo depósito porque los resultados de las consultas ListMultipartUploads para ese depósito podrían devolver resultados incompletos.
- StorageGRID aplica límites de tamaño de AWS para partes multipart. Los clientes de S3 deben seguir estas pautas:
  - Cada parte de una carga multipart debe tener entre 5 MiB (5.242.880 bytes) y 5 GiB (5.368.709.120 bytes).
  - La última parte puede ser menor a 5 MiB (5.242.880 bytes).
  - En general, los tamaños de las piezas deben ser lo más grandes posible. Por ejemplo, utilice tamaños de piezas de 5 GiB para un objeto de 100 GiB. Dado que cada parte se considera un objeto único, el uso de partes de gran tamaño reduce la sobrecarga de metadatos de StorageGRID .
  - Para objetos más pequeños que 5 GiB, considere usar una carga que no sea multipart.
- ILM se evalúa para cada parte de un objeto multipart a medida que se ingiere y para el objeto como un todo cuando se completa la carga multipart, si la regla ILM usa Equilibrado o Estricto.["opción de ingestión"](#) . Debes tener en cuenta cómo esto afecta la colocación de objetos y piezas:
  - Si ILM cambia mientras una carga multipart de S3 está en progreso, es posible que algunas partes del objeto no cumplan con los requisitos de ILM actuales cuando se complete la carga multipart. Cualquier pieza que no esté colocada correctamente se pone en cola para la reevaluación de ILM y se mueve a la ubicación correcta más tarde.
  - Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su totalidad. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1, mientras que todos los objetos más pequeños se almacenan en DC2, cada parte de 1 GB de una carga multipart de 10 partes se almacena en DC2 en la ingestión. Sin embargo, cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.
- Todas las operaciones de carga multipart son compatibles con StorageGRID["valores de consistencia"](#) .
- Cuando se ingiere un objeto mediante una carga multipart, el["umbral de segmentación de objetos \(1 GiB\)"](#) no se aplica
- Según sea necesario, puede utilizar["cifrado del lado del servidor"](#) con cargas multipart. Para utilizar SSE (cifrado del lado del servidor con claves administradas por StorageGRID), incluya el x-amz-server-side-encryption encabezado de solicitud únicamente en la solicitud CreateMultipartUpload. Para utilizar SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud CreateMultipartUpload y en cada solicitud UploadPart posterior.

Operación	Implementación
AbortarMultipartUpload	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.

Operación	Implementación
Carga completa de varias partes	Ver " <a href="#">Carga completa de varias partes</a> "
Crear carga de varias partes  (anteriormente llamado Iniciar carga multiparte)	Ver " <a href="#">Crear carga de varias partes</a> "
Lista de cargas de varias partes	Ver " <a href="#">Lista de cargas de varias partes</a> "
Lista de partes	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Subir parte	Ver " <a href="#">Subir parte</a> "
Subir copia parcial	Ver " <a href="#">Subir copia parcial</a> "

## Carga completa de varias partes

La operación CompleteMultipartUpload completa una carga multiparte de un objeto ensamblando las partes cargadas previamente.



StorageGRID admite valores no consecutivos en orden ascendente para el `partNumber` parámetro de solicitud con CompleteMultipartUpload. El parámetro puede comenzar con cualquier valor.

## Resolver conflictos

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

## Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

El `x-amz-storage-class` El encabezado afecta la cantidad de copias de objetos que crea StorageGRID si la regla ILM correspondiente especifica "[Opción de doble confirmación o ingestión equilibrada](#)".

- STANDARD

(Predeterminado) Especifica una operación de ingestión de confirmación dual cuando la regla ILM usa la opción Confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

- REDUCED\_REDUNDANCY

Especifica una operación de ingestión de confirmación única cuando la regla ILM usa la opción de confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

 Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, REDUCED\_REDUNDANCY La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el REDUCED\_REDUNDANCY La opción devuelve un error. StorageGRID siempre realizará una ingestión de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

 Si una carga de varias partes no se completa dentro de los 15 días, la operación se marca como inactiva y todos los datos asociados se eliminan del sistema.

 El ETag El valor devuelto no es una suma MD5 de los datos, sino que sigue la implementación de la API de Amazon S3 de la ETag valor para objetos multiparte.

## Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

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

## Control de versiones

Esta operación completa una carga de varias partes. Si el control de versiones está habilitado para un bucket, la versión del objeto se crea después de completar la carga de varias partes.

Si el control de versiones está habilitado para un bucket, se creará un único `versionId` Se genera automáticamente para la versión del objeto que se está almacenando. Este `versionId` También se devuelve en la respuesta utilizando el `x-amz-version-id` encabezado de respuesta.

Si se suspende el control de versiones, la versión del objeto se almacena con un valor nulo. `versionId` y si ya existe una versión nula, se sobrescribirá.

 Cuando el control de versiones está habilitado para un bucket, completar una carga multiparte siempre crea una nueva versión, incluso si hay cargas multiparte simultáneas completadas en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bucket, es posible iniciar una carga multiparte y luego iniciar y completar primero otra carga multiparte en la misma clave de objeto. En los depósitos sin versiones, la carga multiparte que se completa en último lugar tiene prioridad.

## Error de replicación, notificación o notificación de metadatos

Si el depósito donde se produce la carga multiparte está configurado para un servicio de plataforma, la carga multiparte se realiza correctamente incluso si falla la acción de replicación o notificación asociada.

Un inquilino puede activar la replicación o notificación fallida actualizando los metadatos o las etiquetas del objeto. Un inquilino puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

Consulte "Solucionar problemas de servicios de la plataforma".

## Crear carga de varias partes

La operación CreateMultipartUpload (anteriormente denominada Iniciar carga multiparte) inicia una carga multiparte para un objeto y devuelve un ID de carga.

El `x-amz-storage-class` Se admite el encabezado de solicitud. El valor presentado para `x-amz-storage-class` afecta la forma en que StorageGRID protege los datos de los objetos durante la ingestión y no la cantidad de copias persistentes del objeto que se almacenan en el sistema StorageGRID (lo cual está determinado por ILM).

Si la regla ILM que coincide con un objeto ingerido utiliza el método Estricto "[opción de ingestión](#)" , el `x-amz-storage-class` El encabezado no tiene ningún efecto.

Los siguientes valores se pueden utilizar para `x-amz-storage-class` :

- STANDARD(Por defecto)
  - **Confirmación dual:** si la regla ILM especifica la opción de ingestión de confirmación dual, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación dual). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de ubicación de la regla. De lo contrario, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y eliminar las copias provisionales iniciales.
  - **Equilibrado:** si la regla ILM especifica la opción Equilibrado y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en diferentes nodos de almacenamiento.

Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla ILM (ubicación sincrónica), `x-amz-storage-class` El encabezado no tiene ningún efecto.

- REDUCED\_REDUNDANCY
  - **Confirmación dual:** si la regla ILM especifica la opción de confirmación dual, StorageGRID crea una única copia provisional a medida que se ingiere el objeto (confirmación única).
  - **Equilibrado:** si la regla ILM especifica la opción Equilibrado, StorageGRID realiza una única copia provisional solo si el sistema no puede realizar inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar la colocación sincrónica, este encabezado no tiene ningún efecto. **REDUCED\_REDUNDANCY** Esta opción se utiliza mejor cuando la regla ILM que coincide con el objeto crea una única copia replicada. En este caso se utiliza `REDUCED_REDUNDANCY` Elimina la creación y eliminación innecesarias de una copia de objeto adicional para cada operación de ingestión.

Usando el `REDUCED_REDUNDANCY` Esta opción no se recomienda en otras circunstancias.

`REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante la ingestión. Por ejemplo, podría perder datos si la copia única se almacena inicialmente en un nodo de almacenamiento que falla antes de que pueda ocurrir la evaluación de ILM.

 Tener solo una copia replicada por un período de tiempo determinado pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

Especificando REDUCED\_REDUNDANCY Sólo afecta la cantidad de copias que se crean cuando se ingiere un objeto por primera vez. No afecta la cantidad de copias del objeto que se realizan cuando las políticas ILM activas evalúan el objeto y no hace que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID .

 Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, REDUCED\_REDUNDANCY La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el REDUCED\_REDUNDANCY La opción devuelve un error. StorageGRID siempre realizará una ingestión de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

## Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

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

Actualmente, solo el valor SHA256 para x-amz-checksum-algorithm es compatible.

- x-amz-meta-, seguido de un par nombre-valor que contiene metadatos definidos por el usuario

Al especificar el par nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

```
x-amz-meta-_name_: `value`
```

Si desea utilizar la opción **Hora de creación definida por el usuario** como Hora de referencia para una regla ILM, debe utilizar creation-time como el nombre de los metadatos que registran cuándo se creó el objeto. Por ejemplo:

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

El valor de creation-time se evalúa en segundos desde el 1 de enero de 1970.



Añadiendo creation-time ya que no se permiten metadatos definidos por el usuario si está agregando un objeto a un depósito que tiene habilitado el Cumplimiento heredado. Se devolverá un error.

- Encabezados de solicitud de bloqueo de objetos S3:

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

Si se realiza una solicitud sin estos encabezados, se utilizan las configuraciones de retención predeterminadas del depósito para calcular la fecha de retención de la versión del objeto.

## "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

- Encabezados de solicitud 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

### Encabezados de solicitud para el cifrado del lado del servidor



Para obtener información sobre cómo StorageGRID maneja los caracteres UTF-8, consulte "["PonerObjeto"](#)".

## Encabezados de solicitud para el cifrado del lado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto multipart con cifrado del lado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE**: utilice el siguiente encabezado en la solicitud CreateMultipartUpload si desea cifrar el objeto con una clave única administrada por StorageGRID. No especifique este encabezado en ninguna de las solicitudes UploadPart.

- x-amz-server-side-encryption

- **SSE-C**: utilice estos tres encabezados en la solicitud CreateMultipartUpload (y en cada solicitud UploadPart posterior) si desea cifrar el objeto con una clave única que usted proporcione y administre.

- x-amz-server-side-encryption-customer-algorithm: Especificar AES256 .

- x-amz-server-side-encryption-customer-key: Especifique su clave de cifrado para el nuevo objeto.

- x-amz-server-side-encryption-customer-key-MD5: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.



Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones para "["utilizando cifrado del lado del servidor"](#)".

## Encabezados de solicitud no admitidos

El siguiente encabezado de solicitud no es compatible:

- x-amz-website-redirect-location

El x-amz-website-redirect-location el encabezado regresa XNotImplemented .

## Control de versiones

La carga multipart consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar

partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

## **Lista de cargas de varias partes**

La operación ListMultipartUploads enumera las cargas multipart en curso para un depósito.

Se admiten los siguientes parámetros de solicitud:

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

## **Control de versiones**

La carga multipart consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

## **Subir parte**

La operación UploadPart carga una parte en una carga multipart para un objeto.

### **Encabezados de solicitud admitidos**

Se admiten los siguientes encabezados de solicitud:

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

### **Encabezados de solicitud para el cifrado del lado del servidor**

Si especificó el cifrado SSE-C para la solicitud CreateMultipartUpload, también debe incluir los siguientes encabezados de solicitud en cada solicitud UploadPart:

- x-amz-server-side-encryption-customer-algorithm: Especificar AES256 .
- x-amz-server-side-encryption-customer-key:Especifique la misma clave de cifrado que proporcionó en la solicitud CreateMultipartUpload.

- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen MD5 que proporcionó en la solicitud `CreateMultipartUpload`.

 Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones en "["Utilice cifrado del lado del servidor"](#)" .

Si especificó una suma de comprobación SHA-256 durante la solicitud `CreateMultipartUpload`, también debe incluir el siguiente encabezado de solicitud en cada solicitud `UploadPart`:

- `x-amz-checksum-sha256`: Especifique la suma de comprobación SHA-256 para esta parte.

## Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

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

## Control de versiones

La carga multipart consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación `CompleteMultipartUpload`.

## Subir copia parcial

La operación `UploadPartCopy` carga una parte de un objeto copiando datos de un objeto existente como fuente de datos.

La operación `UploadPartCopy` se implementa con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.

Esta solicitud lee y escribe los datos del objeto especificados en `x-amz-copy-source-range` dentro del sistema StorageGRID .

Se admiten los siguientes encabezados de solicitud:

- `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`

## Encabezados de solicitud para el cifrado del lado del servidor

Si especificó el cifrado SSE-C para la solicitud `CreateMultipartUpload`, también debe incluir los siguientes encabezados de solicitud en cada solicitud `UploadPartCopy`:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256 .
- `x-amz-server-side-encryption-customer-key`:Especifique la misma clave de cifrado que proporcionó en la solicitud `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el mismo resumen MD5 que proporcionó en la solicitud `CreateMultipartUpload`.

Si el objeto de origen está cifrado mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud `UploadPartCopy`, para que el objeto pueda descifrarse y luego copiarse:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar AES256 .
- `x-amz-copy-source-server-side-encryption-customer-key`:Especifique la clave de cifrado que proporcionó cuando creó el objeto de origen.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.

 Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de los objetos, revise las consideraciones en "["Utilice cifrado del lado del servidor"](#) .

## Control de versiones

La carga multipart consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación `CompleteMultipartUpload`.

## **Información de copyright**

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

**ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.**

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

**LEYENDA DE DERECHOS LIMITADOS:** el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## **Información de la marca comercial**

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.