



Operações para uploads multipartes

StorageGRID software

NetApp
December 03, 2025

Índice

Operações para uploads multipartes	1
Operações para uploads multipartes	1
Upload completo de várias partes	2
Resolver conflitos	2
Cabeçalhos de solicitação suportados	2
Cabeçalhos de solicitação não suportados	3
Controle de versão	3
Falha na replicação, notificação ou notificação de metadados	3
CriarMultipartUpload	4
Cabeçalhos de solicitação suportados	5
Cabeçalhos de solicitação para criptografia do lado do servidor	6
Cabeçalhos de solicitação não suportados	6
Controle de versão	7
ListarMultipartUploads	7
Controle de versão	7
UploadPart	7
Cabeçalhos de solicitação suportados	7
Cabeçalhos de solicitação para criptografia do lado do servidor	8
Cabeçalhos de solicitação não suportados	8
Controle de versão	8
UploadPartCopy	8
Cabeçalhos de solicitação para criptografia do lado do servidor	9
Controle de versão	9

Operações para uploads multipartes

Operações para uploads multipartes

Esta seção descreve como o StorageGRID oferece suporte a operações para uploads multipartes.

As seguintes condições e notas se aplicam a todas as operações de upload multipartes:

- Você não deve exceder 1.000 uploads multipartes simultâneos para um único bucket porque os resultados das consultas ListMultipartUploads para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para partes multipartes. Os clientes do S3 devem seguir estas diretrizes:
 - Cada parte em um upload multiparte deve ter entre 5 MiB (5.242.880 bytes) e 5 GiB (5.368.709.120 bytes).
 - A última parte pode ser menor que 5 MiB (5.242.880 bytes).
 - Em geral, os tamanhos das peças devem ser os maiores possíveis. Por exemplo, use tamanhos de peça de 5 GiB para um objeto de 100 GiB. Como cada parte é considerada um objeto único, o uso de tamanhos de parte grandes reduz a sobrecarga de metadados do StorageGRID .
 - Para objetos menores que 5 GiB, considere usar o upload não multiparte.
- O ILM é avaliado para cada parte de um objeto multiparte à medida que é ingerido e para o objeto como um todo quando o upload multiparte é concluído, se a regra ILM usar o Balanceado ou o Estrito "[opção de ingestão](#)" . Você deve estar ciente de como isso afeta o posicionamento de objetos e peças:
 - Se o ILM for alterado enquanto um upload multiparte do S3 estiver em andamento, algumas partes do objeto poderão não atender aos requisitos atuais do ILM quando o upload multiparte for concluído. Qualquer peça que não seja colocada corretamente é colocada na fila para reavaliação do ILM e movida para o local correto posteriormente.
 - Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos do ILM para o objeto como um todo. Por exemplo, se uma regra especificar que todos os objetos de 10 GB ou maiores sejam armazenados no DC1, enquanto todos os objetos menores sejam armazenados no DC2, cada parte de 1 GB de um upload multiparte de 10 partes será armazenada no DC2 na ingestão. Entretanto, quando o ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.
- Todas as operações de upload multipartes oferecem suporte ao StorageGRID "[valores de consistência](#)" .
- Quando um objeto é ingerido usando upload multipartes, o "[limite de segmentação de objetos \(1 GiB\)](#)" não é aplicado.
- Conforme necessário, você pode usar "[criptografia do lado do servidor](#)" com uploads multipartes. Para usar SSE (criptografia do lado do servidor com chaves gerenciadas StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho de solicitação somente na solicitação CreateMultipartUpload. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), especifique os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação CreateMultipartUpload e em cada solicitação UploadPart subsequente.

Operação	Implementação
AbortarMultipartUpload	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
Upload completo de várias partes	Ver " Upload completo de várias partes "
CriarMultipartUpload (anteriormente chamado de Iniciar Upload Multipartes)	Ver " CriarMultipartUpload "
ListarMultipartUploads	Ver " ListarMultipartUploads "
ListarPartes	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
UploadPart	Ver " UploadPart "
UploadPartCopy	Ver " UploadPartCopy "

Upload completo de várias partes

A operação CompleteMultipartUpload conclui um upload multiparte de um objeto reunindo as partes carregadas anteriormente.



O StorageGRID suporta valores não consecutivos em ordem crescente para `partNumber` parâmetro de solicitação com `CompleteMultipartUpload`. O parâmetro pode começar com qualquer valor.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

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

O `x-amz-storage-class` cabeçalho afeta quantas cópias de objeto o StorageGRID cria se a regra ILM correspondente especificar o "[Opção de confirmação dupla ou ingestão balanceada](#)".

- STANDARD

(Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

- REDUCED_REDUNDANCY

Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o REDUCED_REDUNDANCY a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o REDUCED_REDUNDANCY opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.



Se um upload multipart não for concluído em 15 dias, a operação será marcada como inativa e todos os dados associados serão excluídos do sistema.



O ETag o valor retornado não é uma soma MD5 dos dados, mas segue a implementação da API do Amazon S3 ETag valor para objetos multipartes.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

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

Controle de versão

Esta operação conclui um upload multipart. Se o controle de versão estiver habilitado para um bucket, a versão do objeto será criada após a conclusão do upload multipart.

Se o controle de versão estiver habilitado para um bucket, um único `versionId` é gerado automaticamente para a versão do objeto que está sendo armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão for suspenso, a versão do objeto será armazenada com um valor nulo `versionId` e se uma versão nula já existir, ela será substituída.



Quando o controle de versão está habilitado para um bucket, a conclusão de um upload multipart sempre cria uma nova versão, mesmo que haja uploads multipartes simultâneos concluídos na mesma chave de objeto. Quando o controle de versão não está habilitado para um bucket, é possível iniciar um upload multipart e, em seguida, fazer com que outro upload multipart seja iniciado e concluído primeiro na mesma chave de objeto. Em buckets não versionados, o upload multipart concluído por último tem precedência.

Falha na replicação, notificação ou notificação de metadados

Se o bucket onde o upload multipart ocorre estiver configurado para um serviço de plataforma, o upload multipart será bem-sucedido mesmo se a ação de replicação ou notificação associada falhar.

Um locatário pode acionar a replicação com falha ou a notificação atualizando os metadados ou as tags do objeto. Um locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

Consulte "["Solucionar problemas de serviços de plataforma"](#)" .

Criar Multipart Upload

A operação CreateMultipartUpload (anteriormente chamada de Initiate Multipart Upload) inicia um upload multipart para um objeto e retorna um ID de upload.

O `x-amz-storage-class` O cabeçalho da solicitação é suportado. O valor submetido para `x-amz-storage-class` afeta como o StorageGRID protege os dados do objeto durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (o que é determinado pelo ILM).

Se a regra ILM correspondente a um objeto ingerido usar o Strict "["opção de ingestão"](#)" , o `x-amz-storage-class` cabeçalho não tem efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class` :

- STANDARD(Padrão)
 - **Confirmação dupla:** se a regra do ILM especificar a opção de ingestão de confirmação dupla, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais atendem às instruções de posicionamento na regra. Caso contrário, talvez seja necessário fazer novas cópias de objetos em locais diferentes e as cópias provisórias iniciais talvez precisem ser excluídas.
 - **Balanceado:** Se a regra do ILM especificar a opção Balanceado e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes Nós de Armazenamento.

Se o StorageGRID puder criar imediatamente todas as cópias de objetos especificadas na regra ILM (posicionamento síncrono), o `x-amz-storage-class` cabeçalho não tem efeito.

- REDUCED_REDUNDANCY
 - **Confirmação dupla:** se a regra do ILM especificar a opção Confirmação dupla, o StorageGRID criará uma única cópia provisória à medida que o objeto for ingerido (confirmação única).
 - **Balanceado:** Se a regra ILM especificar a opção Balanceado, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. O REDUCED_REDUNDANCY A opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso usando REDUCED_REDUNDANCY elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

Usando o REDUCED_REDUNDANCY opção não é recomendada em outras circunstâncias.

REDUCED_REDUNDANCY aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um nó de armazenamento que falhe antes que a avaliação do ILM possa ocorrer.



Ter apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

Especificando `REDUCED_REDUNDANCY` afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Isso não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas de ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID .



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

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

Atualmente, apenas o valor `SHA256` para `x-amz-checksum-algorithm` é suportado.

- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário

Ao especificar o par nome-valor para metadados definidos pelo usuário, use este formato geral:

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

Se você quiser usar a opção **Tempo de criação definido pelo usuário** como o Tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que registram quando o objeto foi criado. Por exemplo:

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

O valor para `creation-time` é avaliado como segundos desde 1º de janeiro de 1970.



Adicionando `creation-time` pois metadados definidos pelo usuário não são permitidos se você estiver adicionando um objeto a um bucket que tenha a Conformidade legada habilitada. Um erro será retornado.

- Cabeçalhos de solicitação de bloqueio de objeto S3:

- `x-amz-object-lock-mode`

- x-amz-object-lock-retain-until-date

- x-amz-object-lock-legal-hold

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular a versão do objeto retain-until-date.

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

- Cabeçalhos de solicitação 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

[Cabeçalhos de solicitação para criptografia do lado do servidor](#)



Para obter informações sobre como o StorageGRID lida com caracteres UTF-8, consulte "[ColocarObjeto](#)".

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os seguintes cabeçalhos de solicitação para criptografar um objeto multipart com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE:** Use o seguinte cabeçalho na solicitação CreateMultipartUpload se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações UploadPart.

- x-amz-server-side-encryption

- **SSE-C:** Use todos esses três cabeçalhos na solicitação CreateMultipartUpload (e em cada solicitação UploadPart subsequente) se quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.

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

- x-amz-server-side-encryption-customer-key: Especifique sua chave de criptografia para o novo objeto.

- x-amz-server-side-encryption-customer-key-MD5: Especifique o resumo MD5 da chave de criptografia do novo objeto.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para "[usando criptografia do lado do servidor](#)".

Cabeçalhos de solicitação não suportados

O seguinte cabeçalho de solicitação não é suportado:

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

O `x-amz-website-redirect-location` retorna o cabeçalho `XNotImplemented`.

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação `CompleteMultipartUpload` é executada.

Listar MultipartUploads

A operação `ListMultipartUploads` lista uploads multipartes em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

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

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação `CompleteMultipartUpload` é executada.

UploadPart

A operação `UploadPart` carrega uma parte em um upload multipart para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

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

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256 .
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia que você forneceu na solicitação CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em "["Use criptografia do lado do servidor"](#)" .

Se você especificou uma soma de verificação SHA-256 durante a solicitação CreateMultipartUpload, também deverá incluir o seguinte cabeçalho de solicitação em cada solicitação UploadPart:

- `x-amz-checksum-sha256`: Especifique a soma de verificação SHA-256 para esta parte.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

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

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

UploadPartCopy

A operação UploadPartCopy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação UploadPartCopy é implementada com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.

Esta solicitação lê e grava os dados do objeto especificados em `x-amz-copy-source-range` dentro do sistema StorageGRID .

Os seguintes cabeçalhos de solicitação são suportados:

- `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`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação `CreateMultipartUpload`, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação `UploadPartCopy`:

- `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256 .
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia que você forneceu na solicitação `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação `CreateMultipartUpload`.

Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deverá incluir os três cabeçalhos a seguir na solicitação `UploadPartCopy` para que o objeto possa ser descriptografado e copiado:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especifique AES256 .
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu quando criou o objeto de origem.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.

 As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em "["Use criptografia do lado do servidor"](#)" .

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação `CompleteMultipartUpload` é executada.

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 DESTE DOCUMENTO. 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 SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO 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 DESTE SOFTWARE, 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.