

Content Delivery Network

Guía del usuario

Edición 01
Fecha 2023-07-18



Copyright © Huawei Technologies Co., Ltd. 2023. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos



HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.

Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Índice

1 Gestión de nombres de dominio.....	1
1.1 Funciones.....	1
1.2 Activación/desactivación de CDN para un nombre de dominio.....	2
1.3 Eliminación de un nombre de dominio.....	5
1.4 Copia de configuraciones de dominio.....	6
1.5 Revisión de un nombre de dominio.....	8
1.6 Política de terminación del servicio.....	9
1.7 Gestión de cuotas de nombres de dominio.....	11
2 Configuración del nombre de dominio.....	14
2.1 Descripción general.....	14
2.2 Configuración básica.....	17
2.2.1 Modificación de los detalles del servidor de origen.....	17
2.2.2 Cambio del área de servicio.....	20
2.2.3 Configuración de IPv6.....	21
2.3 Configuración de recuperación.....	21
2.3.1 Descripción general.....	21
2.3.2 Host de recuperación.....	22
2.3.3 Protocolo de origen.....	24
2.3.4 Reescritura de URL de solicitud de recuperación.....	25
2.3.5 Recuperación basada en rango.....	27
2.3.6 Recuperación de redireccionamiento.....	29
2.3.7 Recuperación de bucket privado de OBS.....	30
2.3.8 Encabezados de solicitud de recuperación.....	33
2.3.9 Intervalo de tiempo de espera de recuperación.....	38
2.3.10 Preguntas Frecuentes.....	39
2.4 Configuración de HTTPS.....	40
2.4.1 Descripción general.....	40
2.4.2 Certificados HTTPS.....	41
2.4.3 Requisitos del certificado HTTPS.....	46
2.4.4 Conversión de formato de certificado HTTPS.....	50
2.4.5 OCSP Stapling.....	50
2.4.6 Forzar redireccionamiento.....	51
2.4.7 HTTP/2.....	51

2.4.8 Versiones de TLS.....	52
2.4.9 Preguntas Frecuentes.....	53
2.5 Configuración de caché.....	54
2.5.1 Descripción general.....	54
2.5.2 Reglas de caché.....	55
2.5.3 Filtrado de parámetros de URL.....	60
2.5.4 Control de caché de origen.....	62
2.5.5 Tiempo de la caché del código de estado.....	64
2.6 Control de acceso.....	65
2.6.1 Descripción general.....	66
2.6.2 Configuración de la validación de referencia.....	66
2.6.3 Configuración de una ACL.....	70
2.6.4 Configuración de una lista negra o una lista blanca de User-Agent.....	72
2.6.5 Configuración de la firma de URL.....	73
2.6.5.1 Método de firma A.....	74
2.6.5.2 Método de firma B.....	78
2.6.5.3 Método de firma C1.....	82
2.6.5.4 Método de firma C2.....	86
2.6.6 Configuración de la autenticación remota.....	90
2.7 Configuración avanzada.....	95
2.7.1 Configuración de encabezado HTTP (solicitudes de origen cruzado).....	95
2.7.2 Páginas de error personalizadas.....	101
2.7.3 Compresión inteligente.....	102
2.8 Configuración de vídeo.....	103
2.8.1 Búsqueda de vídeo.....	103
3 Actualización y precalentamiento de caché.....	106
3.1 Descripción general.....	106
3.2 Actualización de caché.....	106
3.3 Precalentamiento de caché.....	108
3.4 Consulta de Progresos de Tareas.....	109
3.5 Preguntas Frecuentes.....	110
4 Análisis estadístico.....	114
4.1 Descripción de estadísticas.....	114
4.2 Estadísticas de utilización.....	115
4.3 Estadísticas de acceso.....	117
4.4 Estadísticas de servidor original.....	118
4.5 Hotspots.....	120
4.6 Estadísticas de región & operador.....	121
4.7 Códigos de estado.....	123
4.8 Estadísticas de utilización para la aceleración de todo el sitio.....	124
4.9 Preguntas Frecuentes.....	125


5 Gestión de paquetes.....	127
6 Gestión de registros.....	128
7 Gestión de certificados.....	132
8 Comprobación de direcciones IP de nodo.....	138
9 Gestión de permisos.....	140
9.1 Creación de un usuario y concesión de permisos de CDN.....	140
9.2 Creación de una política personalizada.....	141
10 Proyectos empresariales.....	144
11 Auditoría.....	145

1 Gestión de nombres de dominio

1.1 Funciones

Después de agregar un nombre de dominio, puede habilitar, deshabilitar, quitar y revisar el nombre de dominio en la consola de CDN. También puede configurar la política de terminación del nombre de dominio.



Puede hacer clic en  en la esquina superior derecha de la página **Domains** para exportar las configuraciones básicas de nombres de dominio a un archivo de Excel.

Escenarios

En la siguiente tabla se describen las funciones.

Tabla 1-1 Escenarios

Artículo	Descripción
Activación/ desactivación de CDN para un nombre de dominio	Enable: Puede habilitar un nombre de dominio en el estado Disabled . Disable: Puede deshabilitar un nombre de dominio en el estado Enabled o Error .
Eliminación de un nombre de dominio	Puede quitar un nombre de dominio en el estado Disabled o Rejected . NOTA Después de eliminar un nombre de dominio, el sistema elimina automáticamente la configuración correspondiente del nombre de dominio. Si desea utilizar CDN para el nombre de dominio eliminado de nuevo, vuelva a agregar y configurar el nombre de dominio.
Copia de configuraciones de dominio	Puede copiar la configuración de un nombre de dominio a otros nombres de dominio.

Artículo	Descripción
Revisión de un nombre de dominio	Si un nombre de dominio está prohibido debido a la expiración de la licencia ICP, puede solicitar que se revise después de que se vuelva a licenciar el nombre de dominio. Una vez que la revisión pasa, CDN desbanca el nombre de dominio.
Política de terminación del servicio	El servicio de CDN en la nube de Huawei finaliza según una política preestablecida. Puede seleccionar Redirect to origin server o Disable domain name para la política de terminación.
Gestión de cuotas de nombres de dominio	Se aplican cuotas para los recursos de servicio en la plataforma para evitar picos imprevistos en el uso de recursos. Las cuotas pueden limitar el número o la cantidad de recursos disponibles para los usuarios. Si la cuota de nombre de dominio existente no puede cumplir con sus requisitos de servicio, envíe un ticket de servicio para solicitar una cuota más alta.

1.2 Activación/desactivación de CDN para un nombre de dominio

Escenarios

Puede habilitar o deshabilitar la CDN para sus nombres de dominio en la página **Domains** de la consola de CDN.

Consulta de información básica del dominio

En la página **Domains** de la [consola de CDN](#), haga clic en **Configure** en la fila que contiene el nombre de dominio de destino. En la página de la pestaña **Basic Settings**, vea la información básica sobre el nombre de dominio.

Los estados de dominio incluyen **Enabled**, **Disabled**, **Configuring**, **Error**, **Reviewing**, **Rejected**, y **Removing**.

Desactivación de CDN para nombres de dominio

Puede deshabilitar CDN para un nombre de dominio cuyo estado es **Enabled** o **Error**. Después de deshabilitar CDN, CDN ya no proporcionará servicios de aceleración para su nombre de dominio, pero las configuraciones de dominio permanecerán. Para restaurar el servicio de aceleración, habilite CDN de nuevo.

Para mantener su sitio accesible, apunte su nombre de dominio a un registro CNAME que no esté asignado por Huawei Cloud CDN a su proveedor de DNS antes de deshabilitar CDN.

NOTA

Los servicios de CDN para nombres de dominio a los que no se ha accedido durante más de 180 días se desactivarán automáticamente.


Disabling CDN for a single domain name

En la página **Domains** de la **consola de CDN**, elija **More > Disable** en la fila que contiene el nombre de dominio para el que se va a deshabilitar CDN.

<input type="checkbox"/>	Domain Name	Status	CNAME	Service T...	Modified	Operation
<input type="checkbox"/>	ex: [redacted] awe...	Enabled	ex: [redacted] aw...	File downlo...	Sep 16, 20...	Monitor Settings Copy Configuration More
<input type="checkbox"/>	ex: [redacted] ua...	Enabled	ex: [redacted] hu...	File downlo...	Sep 16, 20...	Monitor Settings Copy Configuration Review
<input type="checkbox"/>	ex: [redacted] aw...	Enabled	ex: [redacted] ja...	File downlo...	Aug 10, 2...	Monitor Settings Copy Configuration Disable
<input type="checkbox"/>	ww: [redacted] 1.h...	Enabled	ww: [redacted] 31...	Whole site	Apr 06, 20...	Monitor Settings Copy Configuration Remove

Confirme la información sobre el nombre de dominio y haga clic en **Yes**.

Disable CDN

 Are you sure you want to disable CDN for the following domain name?

Domain Name	Status	Service Type
ex: [redacted] ei.com	Enabled	File download

Disabling CDN for multiple domain names

En la página **Domains** de la **consola de CDN**, seleccione los nombres de dominio para los que CDN se va a deshabilitar y haga clic en **Disable** encima de la lista de nombres de dominio.

<input type="button" value="Add Domain Name"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Remove"/>
<input type="checkbox"/>	Domain Name	Status	CNAME
<input checked="" type="checkbox"/>	ex: [redacted] awe...	Enabled	ex: [redacted] aw...
<input checked="" type="checkbox"/>	ex: [redacted] ua...	Enabled	ex: [redacted] hu...

1. En la página **Domains** de la consola de CDN, seleccione **More > Disable** en la fila que contiene el nombre de dominio para el que se va a deshabilitar CDN. (Para deshabilitar CDN para varios nombres de dominio, seleccione los nombres de dominio y haga clic en **Disable** encima de la lista de nombres de dominio.)
2. Confirme la información del nombre de dominio y haga clic en **Yes**.

Habilitación de CDN para nombres de dominio

Puede habilitar la CDN para un nombre de dominio cuyo estado es **Disabled**.

1. En la página **Domains** de la consola de CDN, seleccione **More > Enable** en la fila que contiene el nombre de dominio para el que se va a habilitar la CDN. (Para habilitar la CDN para varios nombres de dominio, seleccione los nombres de dominio y haga clic en **Enable** encima de la lista de nombres de dominio.)
2. Confirme la información del nombre de dominio y haga clic en **Yes**.

Enabling CDN for a single domain name

En la página **Domains** de la [consola de CDN](#), seleccione **More > Enable** en la fila que contiene el nombre de dominio para el que se va a habilitar la CDN.

<input type="checkbox"/>	Domain Name	Status	CNAME	Service T...	Modified	Operation
<input type="checkbox"/>	exa...en...	Disabled	exa...en...	File downlo...	Sep 16, 2021 ...	Monitor Settings Copy Configuratio More
<input type="checkbox"/>	exa...h...	Disabled	exa...hu...	File downlo...	Sep 16, 2021 ...	Monitor Settings Copy Configura Review Enable Disable
<input type="checkbox"/>	exa...h...	Enabled	exa...h...	File downlo...	Aug 10, 2021...	Monitor Settings Copy Configura
<input type="checkbox"/>	ww...le...	Enabled	ww...ple...	Whole site	Apr 06, 2021 ...	Monitor Settings Copy Configura

Confirme la información sobre el nombre de dominio y haga clic en **Yes**.

Enable CDN

i Are you sure you want to enable CDN for the following domain name?

Domain Name	Status	Service Type
exa...ei.co...	Disabled	File download

Enabling CDN for multiple domain names

En la página **Domains** de la [consola de CDN](#), seleccione los nombres de dominio para los que se va a habilitar CDN y haga clic en **Enable** encima de la lista de nombres de dominio.

Add Domain Name	Enable	Disable	Remove	
<input checked="" type="checkbox"/>	Domain Name	Status	CNAME	Service T...
<input checked="" type="checkbox"/>	exa...en...	Disabled	exa...en...	File downlo...
<input checked="" type="checkbox"/>	exa...h...	Disabled	exa...hu...	File downlo...

1.3 Eliminación de un nombre de dominio

Escenarios

Si ya no desea acelerar un nombre de dominio, puede eliminarlo de la página **Domains** de la consola de CDN. El sistema eliminará automáticamente la configuración correspondiente del nombre de dominio. Si desea acelerar de nuevo el nombre de dominio eliminado, vuelva a agregar y reconfigurar el nombre de dominio.

Solo se pueden quitar los nombres de dominio que se encuentren en el estado **Disabled** o **Rejected**.

NOTA

Si un nombre de dominio ha estado en el estado **Disabled** o **Rejected** durante más de 120 días, el sistema elimina automáticamente este nombre de dominio. Si se requiere la aceleración de CDN para el nombre de dominio, agregue el nombre de dominio de nuevo.


Eliminación de un solo nombre de dominio

En la página **Domains** de la [consola de CDN](#), elija **More > Remove** en la fila que contiene el nombre de dominio que se va a eliminar.

<input type="checkbox"/>	Domain Name	Status	CNAME	Service T...	Modified	Operation
<input type="checkbox"/>	exa...en...	Disabled	exa...en...	File downlo...	Sep 16, 2021 ...	Monitor Settings Copy Configuratio... More
<input type="checkbox"/>	exa...0.h...	Disabled	exa...hu...	File downlo...	Sep 16, 2021 ...	Monitor Settings Copy Configuratio... Review
<input type="checkbox"/>	exa...0.h...	Enabled	exa...0.h...	File downlo...	Aug 10, 2021...	Monitor Settings Copy Configuratio... Enable
<input type="checkbox"/>	ww...pl...	Enabled	ww...le...	Whole site	Apr 06, 2021 ...	Monitor Settings Copy Configuratio... Disable
<input type="checkbox"/>						Remove

Confirme la información sobre el nombre de dominio y haga clic en **Yes**.

Remove Domain Name

 Are you sure you want to remove the following domain name from CDN?

Domain Name	Status	Service Type
exa...ei.co...	Disabled	File download

Eliminación de varios nombres de dominio

En la página **Domains** de la [consola de CDN](#), seleccione los nombres de dominio que desea quitar y haga clic en **Remove** encima de la lista de nombres de dominio.

Add Domain Name		Enable	Disable	Remove
<input type="checkbox"/>	Domain Name	Status	CNAME	Service T...
<input checked="" type="checkbox"/>	exa...4.en...	Disabled	exa...n...	File downlo...
<input checked="" type="checkbox"/>	exa...h...	Disabled	exar...u...	File downlo...

1.4 Copia de configuraciones de dominio

Puede copiar la configuración de un nombre de dominio a otros nombres de dominio.

Precauciones

- Solo se puede copiar la configuración de un nombre de dominio en el estado **Enabled**.
- No se puede deshacer la copia de configuración. Antes de copiar la configuración de un nombre de dominio, asegúrese de que la configuración es correcta.
- Las configuraciones de dominio especiales no se pueden copiar.
- Para un nombre de dominio con alto tráfico o ancho de banda, tenga cuidado al copiar su configuración para evitar pérdidas económicas.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la página **Domains**, haga clic en **Copy Configuration** en la columna **Operation** de la fila que contiene el nombre de dominio de destino. Se muestra la página **Confirm Domain Configuration**.

4 Confirm Domain Configuration 2 Select Domain Names 3 Finish

Domain Configuration to Copy

This operation will overwrite existing configurations of target domain names.
 • You cannot copy configurations to domain names with special configurations.
 • Private bucket retrieval settings can only be copied to domain names whose origin server is an OBS bucket. HTTPS certificate, retrieval host, and basic information of the source domain name cannot be copied.

Domain Name:

Configuration Item

Origin Server Settings

Range-based Retrieval

Follow Redirect

Private Bucket Retrieval

Retrieval Request Headers

Cache Rules, URL Parameter Filtering, Origin Cache Control

GZIP Compression

Referer Validation

ACL

User-Agent Access Control

URL Signing

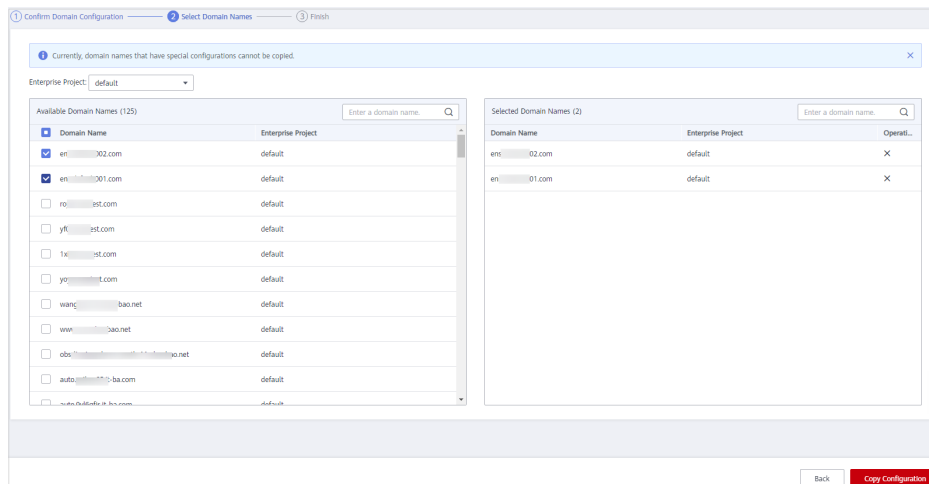
HTTP Header

Next

 **NOTA**

Si copia la configuración a otros nombres de dominio, se sobrescribirán las configuraciones originales de estos nombres de dominio.

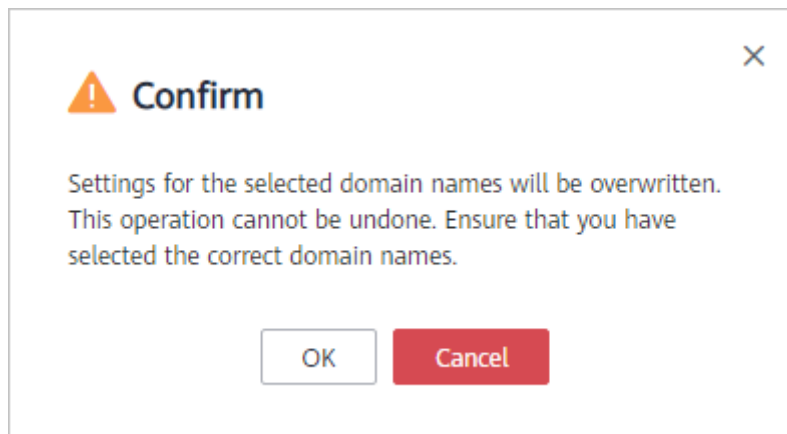
4. Seleccione los elementos de configuración que desea copiar y haga clic en **Next**.



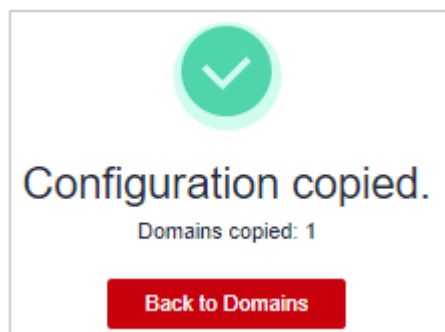
 **NOTA**

- Si ha habilitado la función de proyecto de empresa, los nombres de dominio disponibles se mostrarán por proyecto de empresa.
- Puede seleccionar hasta 10 nombres de dominio de destino.
- Las configuraciones no se pueden copiar en nombres de dominio con configuraciones especiales.

5. Seleccione los nombres de dominio cuyas configuraciones deben sobrescribirse y haga clic en **Copy Configuration**.



6. Haga clic en **OK**.



1.5 Revisión de un nombre de dominio

Escenarios

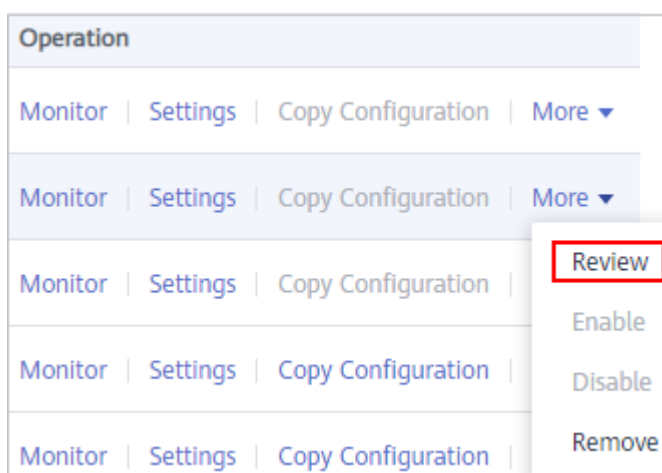
Si un nombre de dominio está prohibido debido a la expiración de la licencia ICP, puede solicitar que se revise después de que se vuelva a licenciar el nombre de dominio. Una vez que la revisión pasa, CDN desbanca el nombre de dominio.

NOTA

- Si un nombre de dominio está prohibido por otras razones, no se puede desbancar a través de las revisiones.
- Si un nombre de dominio es prohibido debido a violaciones de las regulaciones de contenido (sexualmente explícito, drogas ilegales, juegos de azar o contenido extremista) o siendo atacado, será prohibido permanentemente.

Procedimiento

En la página **Domains** de la [consola de CDN](#), elija **More > Review** en la fila que contiene el nombre de dominio que se va a revisar.



Los resultados de la revisión dependen de si el nombre de dominio fue prohibido porque la licencia ICP expiró o por alguna otra razón.

- Prohibido porque la licencia de ICP ha caducado:
 - Si el nombre de dominio se ha vuelto a licenciar, el sistema muestra un mensaje que indica que el nombre de dominio se ha desbancado.

- Si el nombre de dominio no se ha vuelto a licenciar todavía, el sistema muestra un mensaje que indica que el nombre de dominio no se ha licenciado. En este caso, obtenga la licencia del Ministerio de Industria y Tecnología de la Información (MIIT) e inténtelo de nuevo.
 - Prohibido por otras razones
- Si el nombre de dominio fue bloqueado por razones distintas o adicionales a una licencia ICP caducada, se mostrará un mensaje después de hacer clic en **Review**, informándole de las razones. Resuelve los problemas en función de las razones y envía un ticket de servicio para volver a intentarlo.

1.6 Política de terminación del servicio

Si un nombre de dominio cumple con las condiciones para la terminación del servicio, Huawei Cloud CDN dejará de proporcionar servicios de aceleración para él y no podrá configurar los ajustes para el nombre de dominio.

Escenarios

Huawei Cloud CDN finalizará los servicios para un nombre de dominio en el siguiente escenario:

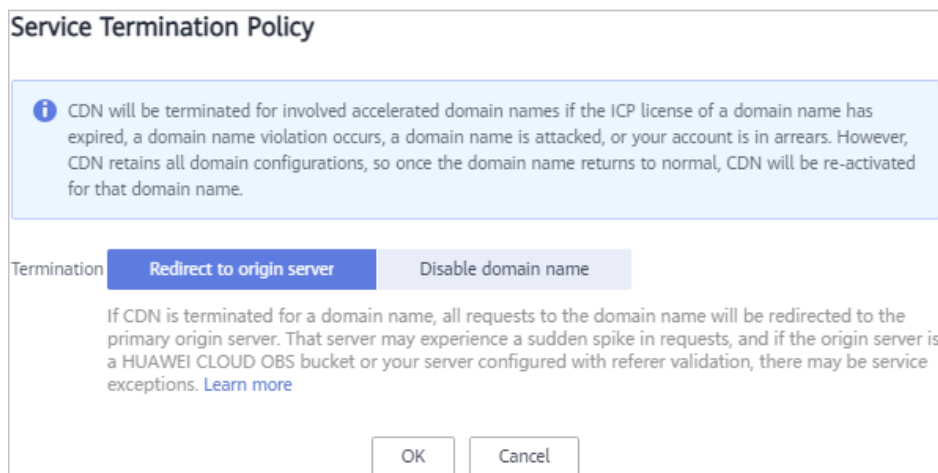
Escenario	Descripción
Cuenta en mora	Si su cuenta está en mora y no se recarga dentro del tiempo especificado, Huawei Cloud cancelará los servicios de CDN para todos los nombres de dominio de su cuenta.

NOTA

- Cuando se termina el servicio de CDN para un nombre de dominio, CDN enviará una notificación por SMS o correo electrónico a su número de teléfono o dirección de correo electrónico reservado. Puede recargar su cuenta para restaurar el servicio CDN.
- Su nombre de dominio será bloqueado si es atacado, su licencia de ICP ha expirado o si tiene contenido inapropiado. Su servicio de CDN no se cancelará.

Configuración de la política de terminación del servicio

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. Haga clic en **Service Termination Policy** en la esquina superior derecha de la página **Domains**. Se muestra la página de configuración de política de terminación de servicio.



3. Seleccione una política de terminación de servicio.

El servicio de CDN de Huawei Cloud finaliza según una política preestablecida. Puede seleccionar **Redirect to origin server** o **Disable domain name** para la política de terminación. En la siguiente tabla se describen las políticas.

Política	Descripción
Redirect to origin server	<p>Todas las solicitudes a su nombre de dominio de aceleración se redirigen al servidor de origen principal. El estado del nombre de dominio se convierte en Disabled. El servicio de aceleración de CDN se detiene para el nombre de dominio. CDN conserva los detalles de configuración de este nombre de dominio. Después de resolver el problema del nombre de dominio, las solicitudes para el nombre de dominio se reenviarán a los nodos CDN para su aceleración.</p> <p>NOTA</p> <ul style="list-style-type: none"> ● Después de finalizar un nombre de dominio de aceleración durante 30 días, Huawei Cloud CDN ya no proporciona el servicio de recuperación y no se puede acceder al nombre de dominio de aceleración. ● Si selecciona Redirect to origin server, el nombre de dominio o la dirección IP de su servidor de origen estarán expuestos a los usuarios. Si no desea exponer el dominio de origen o la dirección IP de origen, seleccione Disable domain name. ● Si su sitio funciona correctamente después de que las solicitudes se redirigen a su servidor de origen depende del servidor de origen.
Disable domain name	<p>CDN pone su nombre de dominio de aceleración fuera de línea cuyo estado se convierte en Disabled. No se puede acceder al nombre de dominio, pero se conserva su configuración. Después de que el nombre de dominio vuelva a la normalidad, CDN lo habilitará.</p>

NOTA

- La política de terminación predeterminada es **Redirect to origin server**.
- La política de terminación de servicio de CDN es una política global. Esto tiene efecto para todos los nombres de dominio bajo su cuenta.

4. Haga clic en **OK**.

Proceso de terminación del servicio

En la siguiente tabla se describe el proceso de deshabilitar el servicio CDN para un nombre de dominio.

Escenario	Proceso de terminación del servicio
Cuenta en mora	<ul style="list-style-type: none"> ● Sus recursos de Huawei Cloud (como los recursos de dominio CDN) entran en un período de retención. Para obtener más información sobre el período de retención, consulte Período de retención. ● CDN finalizará los servicios para el nombre de dominio de aceleración según la política de terminación que establezca.

CDN finalizará los servicios para el nombre de dominio de aceleración según la política de terminación que establezca, ya sea **Redirect to origin server** o **Disable domain name**.

- **Redirect to origin server**
 - Las solicitudes al nombre de dominio se redirigen al servidor de origen principal.
 - CDN deshabilita el nombre de dominio de aceleración.
 - CDN cambia el estado del nombre de dominio a **Disabled** y detiene el servicio de aceleración.
- **Disable domain name**
 - CDN deshabilita el nombre de dominio de aceleración.
 - CDN cambia el estado del nombre de dominio a **Disabled** y detiene el servicio de aceleración.

1.7 Gestión de cuotas de nombres de dominio

Cuota total de nombres de dominio

Se aplican cuotas para los recursos de servicio en la plataforma para evitar picos imprevistos en el uso de recursos. Las cuotas limitan la cantidad y la capacidad de los recursos disponibles para los usuarios. Si una cuota de recursos existente no puede cumplir sus requisitos de servicio, envíe un ticket de servicio para aumentar la cuota. En la siguiente tabla se enumeran las cuotas predeterminadas para los nombres de dominio CDN.

Recurso	Cuota por defecto
Nombres de dominio de aceleración	100
Archivos a actualizar	2000 per day
Directorios a actualizar	100 per day
URLs a precalentar	1000 per day

 **NOTA**

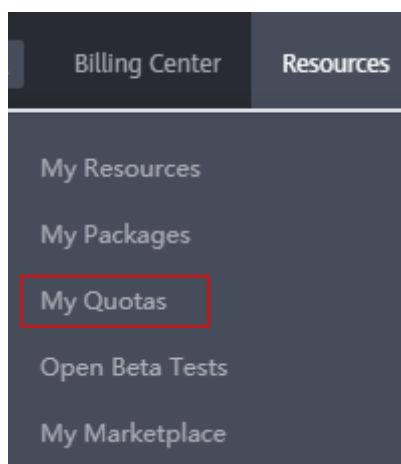
Si cualquier nombre de dominio bajo su cuenta está prohibido debido a una violación, no puede agregar nuevos nombres de dominio de aceleración y realizar la actualización de caché o el precalentamiento.

¿Cómo puedo ver mi cuota?

1. Inicie sesión en la [consola de HUAWEI CLOUD](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En la esquina superior derecha de la página, seleccione **Resources > My Quotas**. Se muestra la página **Service Quota**.



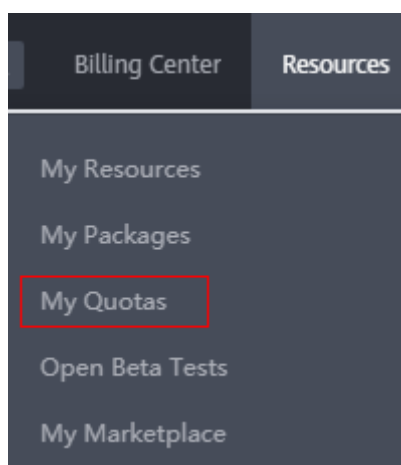
3. Vea la cuota usada y total de cada tipo de recursos de CDN en la página mostrada.

¿Cómo solicito una cuota más alta?

1. Inicie sesión en la [consola de HUAWEI CLOUD](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En la esquina superior derecha de la página, seleccione **Resources > My Quotas**. Se muestra la página **Service Quota**.



3. Haga clic en **Increase Quota**.

4. En la página **Create Service Ticket**, configure los parámetros según sea necesario.
En el área **Problem Description**, complete el contenido y describa por qué necesita el ajuste.
5. Después de configurar todos los parámetros obligatorios, seleccione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** y haga clic en **Submit**.
Puede hacer clic en **My Service Ticket** para ver los tickets de servicio que ha enviado.

2 Configuración del nombre de dominio

2.1 Descripción general

Después de agregar un nombre de dominio para la aceleración, puede configurar el nombre de dominio en función de los requisitos del servicio. Las configuraciones personalizables incluyen aquellas para servidores de origen, recuperación (host de recuperación, recuperación basada en rango, recuperación de bucket privada de OBS, y recuperación de redirección), HTTPS, caché y control de acceso (protección de enlace activo y lista negra/lista blanca de direcciones IP) y configuraciones avanzadas (encabezados HTTP).

Configuración básica

Asegúrese de que el nombre de dominio está en el estado **Enabled** o **Configuring** y no está bloqueado o prohibido por CDN antes de configurar la configuración.

Artículo	Descripción
Modificación de los detalles del servidor de origen	Si cambia la dirección IP o el nombre de dominio del servidor de origen, la información del servidor de origen es incorrecta o se necesita un servidor de origen en espera, modifique la configuración del servidor de origen.
Cambio del área de servicio	Si cambia la región donde se encuentran los usuarios, puede cambiar el área de servicio del nombre de dominio de aceleración para que se ajuste mejor a sus servicios.
Configuración de IPv6	Para permitir que los usuarios accedan a los nodos de CDN mediante IPv6, habilite IPv6 en la consola de CDN.

Configuración de recuperación

Asegúrese de que el nombre de dominio está en el estado **Enabled** o **Configuring** y no está bloqueado o prohibido por CDN antes de configurar la configuración.

Artículo	Descripción
Host de recuperación	Si necesita especificar el nombre de dominio del sitio donde se encuentra el recurso, establezca los parámetros relacionados con el host de recuperación de contenido en este elemento de configuración.
Protocolo de origen	Puede configurar el protocolo de solicitud utilizado por CDN para la recuperación de contenido.
Reescritura de URL de solicitud de recuperación	Si las direcciones URL de las solicitudes de recuperación de contenido no coinciden con las direcciones URL del servidor de origen, puede volver a escribir las direcciones URL de solicitud para mejorar la relación de aciertos de recuperación de contenido.
Recuperación basada en rango	Si necesita mejorar la eficiencia de distribución de archivos de gran tamaño, puede habilitar la recuperación basada en intervalos en este elemento de configuración.
Recuperación de redirección	Supongamos que la redirección 302/301 se realiza para la dirección del servidor de origen. Si no desea que CDN envíe directamente una dirección de redirección 302/301 a los usuarios, sino que en su lugar guarde en caché el contenido solicitado y luego reenvíe el contenido a los usuarios, puede habilitar la recuperación de redirección.
Recuperación de bucket privado de OBS	Si configura un bucket privado de Huawei Cloud OBS como servidor de origen, debe habilitar la recuperación de bucket privado para que CDN pueda recuperar contenido de su bucket privado.
Encabezados de solicitud de recuperación	Si desea reescribir el encabezado de una solicitud de recuperación de contenido, debe configurar el encabezado de solicitud de recuperación en la consola de CDN.
Intervalo de tiempo de espera de recuperación	Puede ajustar el intervalo de tiempo de espera de recuperación en función de las características y los escenarios de servicio del servidor de origen.

Configuración de HTTPS

Asegúrese de que el nombre de dominio está en el estado **Enabled** o **Configuring** y no está bloqueado o prohibido por CDN antes de configurar la configuración.

Función	Descripción
Certificados HTTPS	Puede agregar un certificado para la aceleración de HTTPS.
Versión de TLS	Puede habilitar o deshabilitar las versiones de TLS según sea necesario.

Función	Descripción
Requisitos del certificado HTTPS	Describe la combinación y la secuencia de carga de certificados emitidos por diferentes autoridades
Conversión de formato de certificado HTTPS	Puede convertir certificados en otros formatos al formato PEM que admite CDN.
OCSF Stapling	Si habilita esta función, CDN almacenará en caché el estado de los certificados en línea por adelantado y devolverá el estado a los navegadores. Los navegadores no necesitan consultar el estado de las CA, lo que acelera la verificación.
Forzar redirección	Puede forzar la redirección a HTTP o HTTPS.
HTTP/2	Describe los antecedentes y ventajas de HTTP/2.

Configuración de caché

Asegúrese de que el nombre de dominio está en el estado **Enabled** o **Configuring** y no está bloqueado o prohibido por CDN antes de configurar la configuración.

Artículo	Descripción
Reglas de caché	Puede establecer la edad y la prioridad máximas de la caché para diferentes recursos para aumentar la proporción de aciertos y reducir la tasa de retorno al origen.
Filtrado de parámetros de URL	Puede filtrar los parámetros de URL para permitir que los nodos CDN ignoren los parámetros siguiendo un signo de interrogación (?) al almacenar recursos en caché, mejorando la relación de aciertos de caché y acelerando la distribución.
Control de caché de origen	Puede establecer que el tiempo de caducidad de la caché en los nodos CDN sea el mismo que el de su servidor de origen.
Tiempo de la caché del código de estado	Puede configurar la vigencia de la caché de los códigos de estado para permitir que la CDN almacene en caché y devuelva los códigos de estado a los usuarios, reduciendo la relación de recuperación y la presión sobre el servidor de origen.

Control de acceso

Asegúrese de que el nombre de dominio está en el estado **Enabled** o **Configuring** y no está bloqueado o prohibido por CDN antes de configurar la configuración.

Artículo	Descripción
Configuración de la validación de referencia	Configure este elemento cuando necesite identificar y filtrar visitantes para restringir el acceso.
Configuración de una ACL	Configure este elemento cuando necesite usar el filtrado de direcciones IP para restringir el acceso.
Configuración de una lista negra o una lista blanca de User-Agent	Configure este elemento cuando necesite usar el filtrado User-Agent para restringir el acceso.
Configuración de la firma de URL	Configure este elemento cuando necesite proteger los recursos de su sitio web de ser descargados por usuarios malintencionados.

Configuración avanzada

Asegúrese de que el nombre de dominio está en el estado **Enabled** o **Configuring** y no está bloqueado o prohibido por CDN antes de configurar la configuración.

Artículo	Descripción
Configuración de encabezado HTTP (solicitudes de origen cruzado)	Puede personalizar los valores de los encabezados de respuesta HTTP para su sitio web.
Páginas de error personalizadas	Puede personalizar las páginas de error devueltas a los clientes de usuario.
Compresión inteligente	Puede comprimir contenido estático en sus sitios web reduciendo el tamaño del archivo. Esto acelera la transferencia de archivos y le ahorra mucho ancho de banda.

2.2 Configuración básica

2.2.1 Modificación de los detalles del servidor de origen

Un servidor de origen es un servidor de sitio web, que es la fuente de los datos acelerados por CDN. Si los detalles del servidor de origen, como la dirección IP, el nombre de dominio, el nombre de dominio del bucket OBS, o el puerto de origen, deben modificarse en la página de configuración del servidor de origen.

Fondo

- Al agregar un nombre de dominio, CDN considera el servidor de origen configurado como el servidor de origen principal de forma predeterminada. También puede agregar un servidor de origen en espera para reducir la tasa de errores de recuperación.
- El mecanismo de sondeo se utiliza si los servidores de origen primario y en espera tienen varias direcciones IP.
 - Si la conexión a una dirección IP se agota, CDN espera dos segundos y luego intenta conectarse a la siguiente dirección IP.
 - Si CDN recibe un código de estado 5xx, CDN comienza inmediatamente a conectarse a la siguiente dirección IP.

Precauciones

- Asegúrese de que la configuración del servidor de origen sea correcta. La configuración incorrecta del servidor de origen provoca errores de recuperación.
- Si ha modificado contenido en el servidor de origen, actualice la caché de CDN.
- No puede agregar un servidor de origen en espera para nombres de dominio cuyo tipo de servicio sea aceleración de sitio completo.
- Si el nuevo servidor de origen se conecta a CDN por primera vez, se requiere una verificación. Para obtener más información, consulte [Verificación del servidor de origen](#).

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Basic Settings**.
5. En el área **Origin Server Settings**, haga clic en **Edit**.
Aparece el cuadro de diálogo **Modify Origin Server**.
6. Modifique los parámetros del servidor de origen principal en función de sus requisitos de servicio. [Tabla 2-1](#) describe los parámetros.

Figura 2-1 Modificación de los detalles del servidor de origen

Modify Origin Server

Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur.
If your primary origin is an OBS bucket, adding a standby origin is not supported. If you change the OBS bucket domain name or static website hosting settings below, Private Bucket Retrieval on the Retrieval tab page will be automatically disabled.

Primary Origin Server

Type IP address Domain name OBS bucket

Origin

Origin Port HTTP port HTTPS port

Retrieval Host
Domain name of the site accessed by CDN nodes when retrieving content. Learn more. Ensure that the domain name above is the actual retrieval site. If it is not, update the name.

Standby Origin Server

Switch

Add Standby Origin Server

OK Cancel

Tabla 2-1 Parámetros del servidor de origen

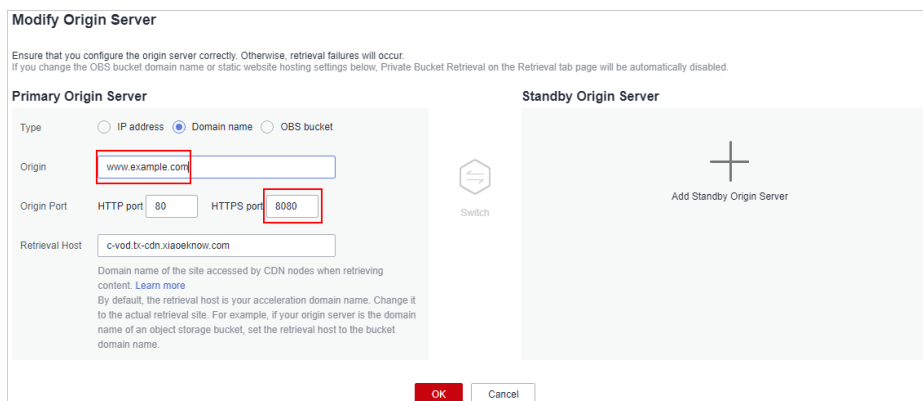
Parámetro	Descripción
IP address	Puede introducir hasta 15 direcciones IP separadas por punto y coma (;).
Domain name	Solo puede introducir un nombre de dominio.
OBS bucket	Tiene que comprar un bucket de Huawei Cloud OBS como servidor de origen. NOTA <ul style="list-style-type: none"> ● Si el bucket OBS es un bucket privado, habilite la recuperación del bucket privado. De lo contrario, la recuperación de contenido de CDN falla. Para obtener más información sobre cómo habilitar la recuperación de bucket privado, consulte Recuperación de bucket privado de OBS. ● Para usar un custom OBS private bucket como servidor de origen, configure una política para el bucket privado. Para obtener más información, consulte Configuración de una política para un bucket privado de OBS personalizado.
Origin port	CDN admite puertos personalizados. Si configura un bucket OBS como servidor de origen, no puede utilizar un puerto personalizado.
Retrieval Host	Para más detalles, consulte Host de recuperación .

 **NOTA**

- Si los buckets de OBS están configurados como servidores de origen para CDN, el tráfico para recuperar contenido de los depósitos de OBS es facturado por OBS.
 - La configuración tarda de 5 a 10 minutos.
7. (Opcional) Haga clic en **Add Standby Origin Server**.
 8. (Opcional) Agregue o modifique los parámetros del servidor de origen en espera según sus requisitos de servicio. Los métodos y parámetros para agregar o modificar un servidor de origen en espera son los mismos que aquellos para agregar o modificar un servidor de origen primario.
 9. Haga clic en **OK**.
 10. Haga clic en la flecha de arriba **Switch** para cambiar entre servidores de origen primarios y en espera.

Ejemplos

Supongamos que desea migrar recursos de un nombre de dominio de aceleración a un servidor cuyo nombre de dominio sea `www.example.com` y el número de puerto HTTPS para la recuperación sea 8080. Puede modificar la configuración del servidor de origen en CDN de la siguiente manera:



2.2.2 Cambio del área de servicio

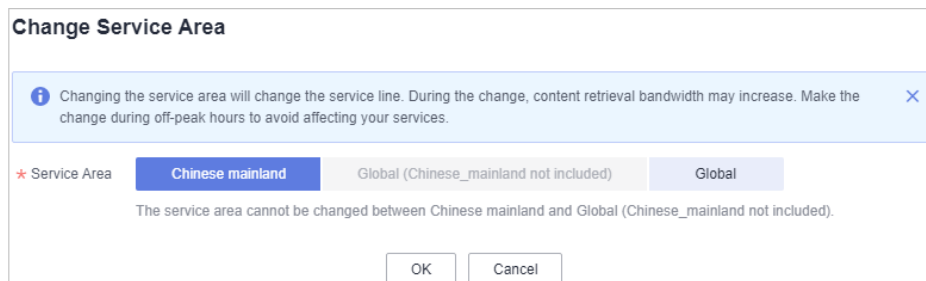
Puede cambiar el área de servicio de un nombre de dominio de aceleración en la consola de CDN.

Notas importantes

- Si desea cambiar el área de servicio entre **Chinese mainland** y **Global (Chinese_mainland not included)**, cambie el área de servicio primero a **Global** y luego a la deseada para evitar que sus servicios se vean afectados.
- El área de servicio de nombres de dominio para la aceleración de sitios completos no se puede cambiar.

Procedimiento

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de nombres de dominio, haga clic en el nombre de dominio que desea modificar o haga clic en **Configure** en la fila que contiene el nombre de dominio.
4. En la página de la pestaña **Basic Settings**, haga clic en **Edit** junto a **Service Area**. Aparece el cuadro de diálogo **Change Service Area**.



NOTA

El área de servicio de un nombre de dominio de aceleración con configuraciones especiales no se puede cambiar.

5. Seleccione el área de servicio deseada y haga clic en **OK**.

2.2.3 Configuración de IPv6

Puede habilitar IPv6 para permitir que los clientes accedan a los nodos de CDN mediante el protocolo IPv6 y permitir que CDN lleve direcciones IP de cliente IPv6 para acceder a su servidor de origen.

Precauciones

- La mayoría de los nodos chinos soportan IPv6. Después de que IPv6 está habilitado, si un usuario usa IPv6 para acceder a CDN pero el nodo óptimo no admite IPv6, el usuario todavía puede usar IPv4 para acceder al nodo.
- Para un nombre de dominio cuya área de servicio es global, puede enviar un ticket de servicio para habilitar IPv6 para nodos en China continental.
- IPv6 no es compatible con nombres de dominio cuya área de servicio está fuera de China continental.
- IPv6 no se puede habilitar para nombres de dominio con configuraciones especiales.

Procedimiento

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, seleccione **Domains**.
3. En la lista de nombres de dominio, haga clic en el nombre de dominio que desea modificar o haga clic en **Configure** en la fila que contiene el nombre de dominio.



4. Active **IPv6**.

2.3 Configuración de recuperación

2.3.1 Descripción general

Cuando un usuario solicita contenido en un nombre de dominio de aceleración y el contenido no se almacena en caché en los nodos de CDN, los nodos de CDN recuperarán el contenido del servidor de origen. Puede establecer parámetros de recuperación en función de sus necesidades para acelerar el acceso.

En la siguiente tabla se describe la configuración de recuperación:

Función	Descripción
Host de recuperación	Si el nombre de dominio que desea que CDN recupere el contenido no es su nombre de dominio de aceleración, establezca un host de recuperación. CDN considera un nombre de dominio de aceleración como el host de recuperación de forma predeterminada.

Función	Descripción
Protocolo de origen	Puede configurar el protocolo de solicitud utilizado por CDN para la recuperación de contenido.
Reescritura de URL de solicitud de recuperación	Si las direcciones URL de las solicitudes de recuperación de contenido no coinciden con las direcciones URL del servidor de origen, puede volver a escribir las direcciones URL de solicitud para mejorar la relación de aciertos de recuperación de contenido.
Recuperación basada en rango	Puede configurar la recuperación basada en rangos para acelerar la distribución de archivos de gran tamaño durante la recuperación de contenido y reducir el consumo de ancho de banda.
Recuperación de redireccionamiento	Si su servidor de origen utiliza una redirección 301/302, puede habilitar la recuperación de redirección para almacenar en caché los recursos redirigidos en nodos CDN para una distribución acelerada.
Recuperación de bucket privado de OBS	Si configura un bucket privado de Huawei Cloud OBS como servidor de origen, habilite la recuperación de bucket privado para que CDN pueda acceder a su servidor de origen y acelerar su sitio. NOTA Si su servidor de origen es un bucket OBS público, no habilite la recuperación de bucket privado.
Encabezados de solicitud de recuperación	Puede establecer encabezados de solicitud de recuperación para reescribir la información de encabezado en las URL de solicitud de recuperación de los usuarios.
Intervalo de tiempo de espera de recuperación	Puede ajustar el intervalo de tiempo de espera de recuperación en función de las características y los escenarios de servicio del servidor de origen.

2.3.2 Host de recuperación

Un host de recuperación es el host especificado en el encabezado de solicitud HTTP. Es el nombre de dominio al que acceden los nodos CDN al recuperar contenido del servidor de origen. Después de configurar el anfitrión de recuperación, CDN obtiene recursos del sitio correspondiente basándose en la información del anfitrión durante la recuperación de contenido.

Fondo

Las diferencias entre el servidor de origen y el host de recuperación son las siguientes:

- El servidor de origen decide la dirección a la que se accede durante la recuperación de contenido.
- El host de recuperación decide el sitio que está asociado con el contenido solicitado.

Supongamos que su servidor de origen es un servidor Nginx. Su dirección IP es x.x.x.x, y su nombre de dominio es www.test.com. Los siguientes sitios se implementan en el servidor de origen.

```
server {
    listen 80;
    server_name www.a.com;

    location / {
        root html;
    }
}

server {
    listen 80;
    server_name www.b.com;

    location / {
        root html;
    }
}
```

Si desea que CDN recupere contenido de este servidor Nginx, establezca la dirección del servidor de origen en **x.x.x.x** o **www.test.com** en CDN. Dado que hay varios sitios en el servidor de origen, debe especificar el sitio específico para recuperar el contenido. Si desea que la CDN recupere contenido del sitio **www.a.com** establezca el host de recuperación en **www.a.com** en la CDN. Si desea que la CDN recupere contenido del sitio **www.b.com** establezca el host de recuperación en **www.b.com** en la CDN.

Precauciones

- Después de agregar un nombre de dominio, CDN lo considera como el host de recuperación por defecto. Si no desea que CDN recupere el contenido del nombre de dominio de aceleración, establezca un host de recuperación para especificar la ubicación del contenido solicitado.
- Si la dirección del servidor de origen es una dirección IP o un nombre de dominio, el tipo de host de recuperación es el nombre de dominio de aceleración de forma predeterminada.
- Si se utiliza un bucket de Huawei Cloud OBS como servidor de origen, el nombre de dominio del bucket se utiliza como host de recuperación de forma predeterminada y no se puede cambiar.
- Si establece la dirección del servidor de origen como nombre de dominio y especifica el nombre de dominio como el de un bucket de almacenamiento de objetos de Huawei Cloud OBS u otro proveedor, establezca el host de recuperación en el nombre de dominio de su bucket de almacenamiento de objetos. De lo contrario, la recuperación falla.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. En el área **Origin Server Settings**, haga clic en **Edit**. Aparece el cuadro de diálogo **Modify Origin Server**.

Modify Origin Server

Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur.
If your primary origin is an OBS bucket, adding a standby origin is not supported. If you change the OBS bucket domain name or static website hosting settings below, Private Bucket Retrieval on the Retrieval tab page will be automatically disabled.

Primary Origin Server

Type IP address Domain name OBS bucket

Origin

Origin Port HTTP port HTTPS port

Retrieval Host **zfpcomtest01.com**
Domain name of the site accessed by CDN nodes when retrieving content.
Learn more
Ensure that the domain name above is the actual retrieval site. If it is not, update the name.

Standby Origin Server

+
Add Standby Origin Server

Switch

OK Cancel

5. Introduzca el nombre de dominio del host de recuperación y haga clic en **OK**.

NOTA

La configuración tarda unos 5 minutos.

Ejemplos

Supongamos que tiene un nombre de dominio de aceleración **www.example.com**. Su nombre de dominio del servidor de origen es de **www.origin.com**, y el host de recuperación es de **www.example01.com**.

Modify Origin Server

Ensure that you configure the origin server correctly. Otherwise, retrieval failures will occur.
If your primary origin is an OBS bucket, adding a standby origin is not supported. If you change the OBS bucket domain name or static website hosting settings below, Private Bucket Retrieval on the Retrieval tab page will be automatically disabled.

Primary Origin Server

Type IP address Domain name OBS bucket

Origin

Origin Port HTTP port HTTPS port

Retrieval Host **www.example01.com**
Domain name of the site accessed by CDN nodes when retrieving content.
Learn more
Ensure that the domain name above is the actual retrieval site. If it is not, update the name.

Standby Origin Server

+
Add Standby Origin Server

Switch

OK Cancel

Cuando un usuario solicita el archivo **http://www.example.com/test.jpg** el archivo no se almacena en caché en CDN, y CDN recupera ese archivo del servidor de origen **www.origin.com** cuya dirección IP es 192.168.1.1. El archivo se encuentra en el sitio **www.example01.com** del servidor de origen. A continuación, CDN devuelve el archivo al usuario y almacena el archivo en caché en los nodos.

2.3.3 Protocolo de origen

Puede configurar el protocolo utilizado para la recuperación de contenido.

Precauciones

De forma predeterminada, el protocolo utilizado para la recuperación de contenido es el mismo que el protocolo de las solicitudes de usuario.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Retrieval Settings**.
5. Haga clic en **Edit** junto a **Origin Protocol**. Aparece el cuadro de diálogo **Origin Protocol**.

Origin Protocol

Protocol HTTP HTTPS Same as user

If you select HTTP for Origin Protocol, make sure that Force HTTPS is disabled for your origin server. If Force HTTPS is enabled, content retrieval will fail.

OK Cancel

Protocolo de origen	Descripción
Same as user	El protocolo utilizado para la recuperación de contenido es el mismo que el protocolo de las solicitudes de usuario.
HTTP	CDN utiliza HTTP para la recuperación de contenido.
HTTPS	CDN utiliza HTTPS para la recuperación de contenido.

6. Seleccione un protocolo utilizado para la recuperación de contenido y haga clic en **OK**.

2.3.4 Reescritura de URL de solicitud de recuperación

Si las direcciones URL de las solicitudes de recuperación de contenido no coinciden con las direcciones URL del servidor de origen, la recuperación de contenido falla. Puede reescribir las URL de solicitud de recuperación en aquellas que coincidan con el servidor de origen, lo que mejora la relación de aciertos de recuperación de contenido.

Notas importantes

- Puede agregar hasta 20 reglas de reescritura de URL.
- Las URL de solicitud de recuperación no se pueden reescribir para nombres de dominio con configuraciones especiales.

Procedimiento

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Retrieval Settings**.
5. En el área **Retrieval Request URL Rewrite**, haga clic en **Edit**.

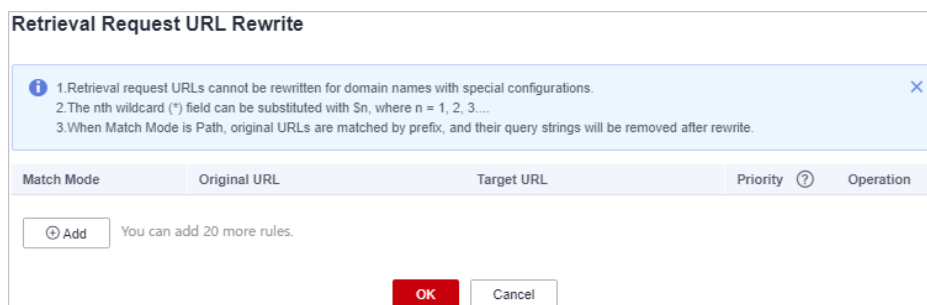


Tabla 2-2 Descripción del parámetro

Parámetro	Descripción
All files	Reescribe las URL de todas las solicitudes de recuperación al nombre de dominio.
Path	Reescribe las URL de solicitud con una ruta específica.
Wildcard	Se admite la coincidencia con carácter comodín.
Original URL	URL que se va a reescribir. <ul style="list-style-type: none"> ● Una URL comienza con una barra (/) y no contiene http://, https://, ni el nombre de dominio. ● Una URL contiene hasta 512 caracteres. ● Se admiten comodines (*), por ejemplo, /test/*/*.mp4. ● Cuando Match Mode es Path, las cadenas de consulta de la URL original se eliminarán después de reescribir.
Target URL	URL después de reescribir. <ul style="list-style-type: none"> ● Una URL comienza con una barra (/) y no contiene http://, https://, ni el nombre de dominio. ● Una URL contiene hasta 256 caracteres. ● El campo <i>n</i>th wildcard (*) se puede sustituir con \$n, donde <i>n</i> = 1, 2, 3..., por ejemplo, /newtest/\$1/\$2.jpg.

Parámetro	Descripción
Priority	<p>Prioridad de una regla de reescritura de URL.</p> <ul style="list-style-type: none"> ● La prioridad de una regla es obligatoria y debe ser única. ● La regla con la prioridad más alta se usará primero para hacer coincidir. ● La prioridad es un entero que oscila entre 1 y 100. Un número mayor indica una prioridad más alta.

Ejemplos

Ejemplo 1: Suponga que ha configurado la siguiente regla de reescritura para el nombre de dominio `www.example.com`:

Match Mode	Original URL	Target URL	Priority
Path	/test/a.txt	/test/b.txt	1

Solicitud de recuperación original: <https://www.example.com/test/a.txt>

Solicitud de recuperación reescrita: <https://www.example.com/test/b.txt>

Ejemplo 2: Suponga que ha configurado la siguiente regla de reescritura para el nombre de dominio `www.example.com`:

Match Mode	Original URL	Target URL	Priority
Wildcard	/test/*.*mp4	/newtest/\$1/\$2.mp4	1

Solicitud de recuperación original: <https://www.example.com/test/aaa/bbb.mp4?pr1>

Solicitud de recuperación reescrita: <https://www.example.com/newtest/aaa/bbb.mp4>

Ejemplo 3: Suponga que ha configurado la siguiente regla de reescritura para el nombre de dominio `www.example.com`:

Match Mode	Original URL	Target URL	Priority
All files		/new.jpg	1

Solicitud de recuperación original: <https://www.example.com/test/aaa/bbb.txt>

Solicitud de recuperación reescrita: <https://www.example.com/new.jpg>

2.3.5 Recuperación basada en rango

En la recuperación basada en rango, el servidor de origen envía datos de un rango específico a un nodo CDN basándose en la información de rango en el encabezado de solicitud HTTP.

Fondo

- La información de rango especifica las posiciones del primer y último bytes para los datos que se van a devolver. Por ejemplo, **Range: bytes=0-100** indica que se requieren los primeros 101 bytes del archivo.

- La recuperación basada en rango acorta el tiempo de distribución de archivos de gran tamaño, mejora la eficiencia de la recuperación y reduce el consumo de recuperación de contenido.

Precauciones

- Para habilitar la recuperación basada en rango, el servidor de origen debe admitir solicitudes de rango, es decir, solicitudes con el campo Rango en los encabezados. De lo contrario, la recuperación de contenido puede fallar.
- La recuperación basada en rango no es válida para los nombres de dominio cuyo tipo de servicio es la aceleración de todo el sitio.
- De forma predeterminada, la recuperación basada en rango está habilitada para la aceleración de descarga de archivos y la aceleración de servicio bajo demanda.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Retrieval Settings**.
5. En el área **Range-based Retrieval**, active o desactive **Range-based Retrieval** según los requisitos de servicio.



Ejemplos

Supongamos que ha habilitado la recuperación basada en rango para el nombre de dominio **www.example.com**.



- Si el usuario A solicita `www.example.com/cdn.mp4`, y los nodos CDN no almacenan en caché el contenido o el contenido almacenado en caché en los nodos CDN ha expirado, el nodo CDN óptimo inicia una solicitud basada en rango para recuperar rangos del contenido del servidor de origen. Los rangos del contenido se almacenan en caché en el nodo.
- Cuando el contenido solicitado del usuario A está siendo almacenado en caché, si el usuario B envía una solicitud basada en rango a este nodo, y la memoria caché en el nodo ya contiene el rango del contenido solicitado por el usuario B, el nodo devuelve inmediatamente el rango solicitado.

2.3.6 Recuperación de redireccionamiento

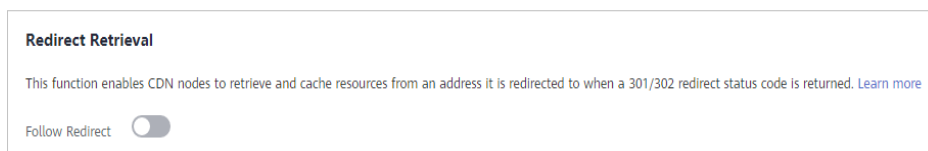
Fondo

Si un servidor de origen utiliza un redireccionamiento 301/302, cuando un nodo CDN envía una solicitud para recuperar contenido solicitado por un usuario desde el servidor de origen, se devuelve un código de estado 301/302. A continuación, CDN toma medidas en función de si está habilitada la recuperación de redirección.

- **Recuperación de redireccionamiento deshabilitada**
Un nodo CDN devuelve la dirección de redireccionamiento al usuario y deja que el usuario termine el proceso de solicitud. Si el nombre de dominio de la dirección de redireccionamiento no se agrega a CDN, el proceso de solicitud posterior no se acelerará por CDN.
- **Recuperación de redireccionamiento habilitada**
Un nodo CDN recupera contenido de la dirección de redirección y almacena en caché el contenido, que luego se devuelve al usuario. Cuando otro usuario solicita el mismo contenido, la caché de nodo se devuelve directamente.

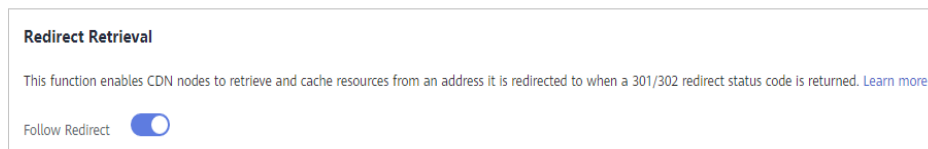
Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Retrieval Settings**.
5. En el área **Redirect Retrieval**, active o desactive **Follow Redirect** según los requisitos de servicio.



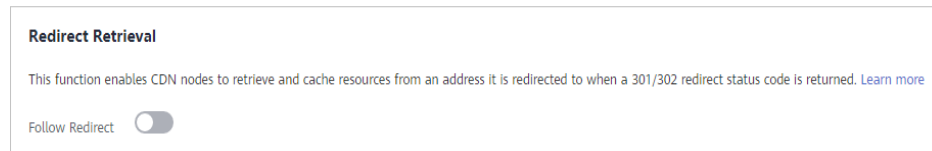
Ejemplos

- La recuperación de redirección está **enabled** para el nombre de dominio `www.example.com`.



Si un usuario solicita el archivo `www.example.com/cdn.jpg` y el nodo CDN no almacena en caché el contenido, el nodo recupera el contenido del servidor de origen. El servidor de origen devuelve el código de estado HTTP 301 o 302 y la dirección de redireccionamiento `www.example.com/test/cdn.jpg`.

- a. El nodo envía directamente una solicitud a la dirección de redirección.
 - b. Después de obtener el contenido solicitado, el nodo devuelve el contenido al usuario y almacena en caché el contenido.
 - c. Cuando otro usuario solicita el mismo archivo, el nodo devuelve directamente el contenido almacenado en caché.
- La recuperación de redireccionamiento está **disabled** para el nombre de dominio `www.example.com`.



Si un usuario solicita el archivo `www.example.com/cdn.jpg` y el nodo CDN no almacena en caché el contenido, el nodo recupera el contenido del servidor de origen. El servidor de origen devuelve el código de estado HTTP 301 o 302 y la dirección de redireccionamiento `www.example.com/test/cdn.jpg`.

- a. El nodo devuelve directamente el código de estado HTTP 301 o 302 al cliente de usuario. El cliente de usuario envía una solicitud a la dirección de redirección.
- b. Si el nombre de dominio de la dirección de redirección no se añade a CDN, los nodos CDN no almacenan en caché el contenido solicitado y el proceso de solicitud posterior no se acelerará.
- c. Si otro usuario solicita el mismo archivo, se repite el proceso anterior.

2.3.7 Recuperación de bucket privado de OBS

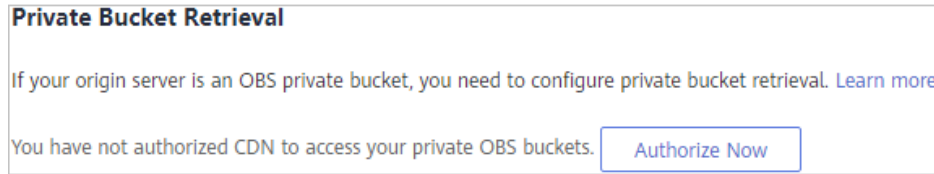
Si configura un bucket privado de Huawei Cloud OBS como servidor de origen, debe habilitar la recuperación de bucket privado para que CDN pueda recuperar contenido de su bucket privado.

Precauciones

- La recuperación de bucket privado solo se admite cuando el servidor de origen del nombre de dominio de aceleración es un bucket OBS.
- Antes de habilitar la recuperación de bucket privado, debe autorizar a CDN para acceder a los recursos de la nube de OBS. Después de que la autorización se haya realizado correctamente, CDN tiene el permiso para acceder a todos los recursos de bucket privados de su cuenta.

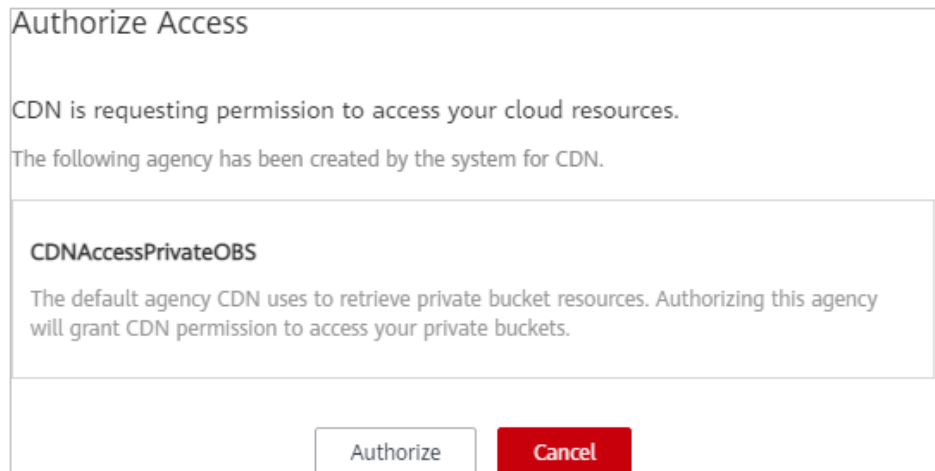
Procedimiento

1. Inicie sesión en la **Consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Retrieval Settings**.
5. Si configura la recuperación de bucket privado por primera vez, se muestra la página que se muestra en la siguiente figura.



El procedimiento de configuración correcto es el siguiente:

- a. Haga clic en **Authorize Now**. Aparece el cuadro de diálogo **Authorize Access**.

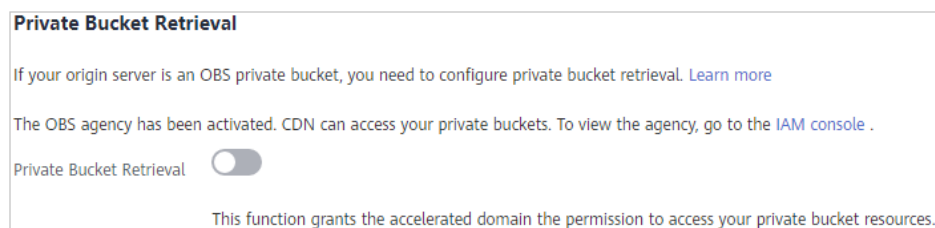


- b. Haga clic en **Authorize**. El sistema crea una agencia llamada **CDNAccessPrivateOBS** para usted en la [consola de IAM](#). CDN ahora tiene el permiso para acceder a sus depósitos OBS privados.

 **NOTA**

- No elimine la agencia CDNAccessPrivateOBS. De lo contrario, CDN no puede recuperar recursos de los depósitos privados de OBS.
- Si su servidor de origen es un bucket OBS público, no habilite la recuperación de bucket privado.

- c. La siguiente figura muestra la página después de la autorización.



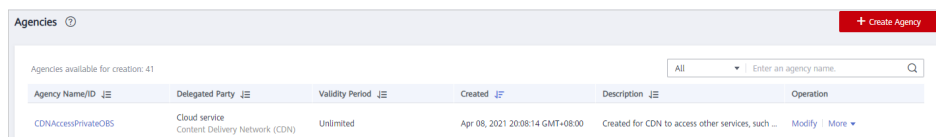
- d. Active **Private Bucket Retrieval**.

6. Espere unos 5 minutos para que la configuración entre en vigor. Cuando el estado del nombre de dominio cambia de **Configuring** a **Enabled**, la configuración ha tenido efecto.

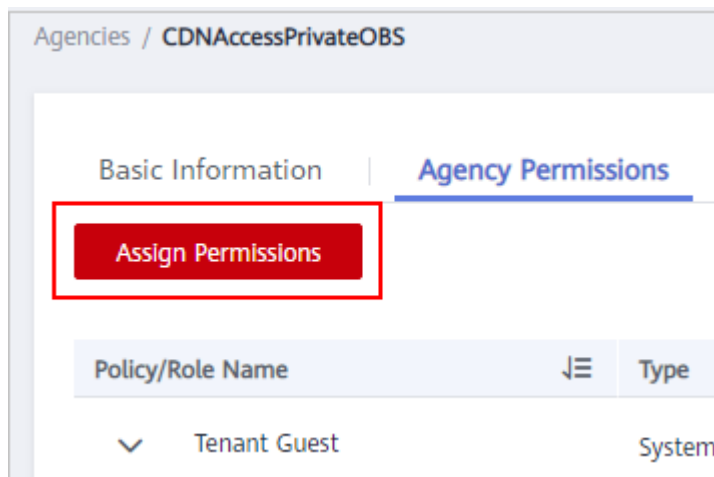
<input type="checkbox"/>	Domain Name	Status
<input type="checkbox"/>	ex. [redacted] .ei.com	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/>	ex. [redacted] .ei.com	<input checked="" type="checkbox"/> Enabled

Si CDN solo recupera archivos no cifrados del bucket privado de OBS, solo necesita completar la configuración anterior. Si los archivos de su bucket OBS están cifrados mediante KMS, debe asignar los permisos de **KMS Administrator** a la agencia CDNAccessPrivateOBS para que CDN pueda leer y acelerar los archivos cifrados.

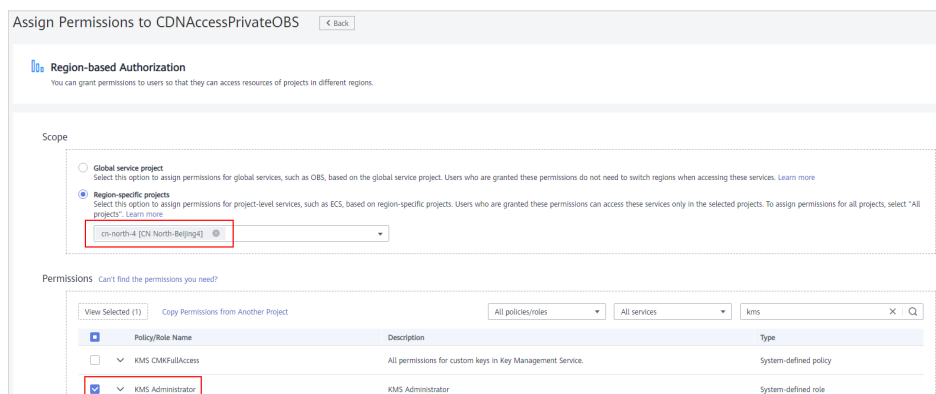
7. **(Optional)** Asigne los permisos de **KMS Administrator** a la agencia CDNAccessPrivateOBS.
 - a. Inicie sesión en la **Consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Management & Government > Identity and Access Management**.
Se muestra la consola IAM.
 - b. En el panel de navegación, elija **Agencies**.
 - c. En la página **Agencies**, elija **More > Manage Permissions** en la columna **Operation** de la fila que contiene la agencia CDNAccessPrivateOBS.



- d. Se muestra la pestaña **Agency Permissions**.



- e. Haga clic en **Assign Permissions**.
 - Establezca **Scope** en **Region-specific projects** y seleccione la región en la que se encuentra el bucket OBS.
 - En el área **Permissions**, seleccione **KMS Administrator**.



- f. Haga clic en **OK**.

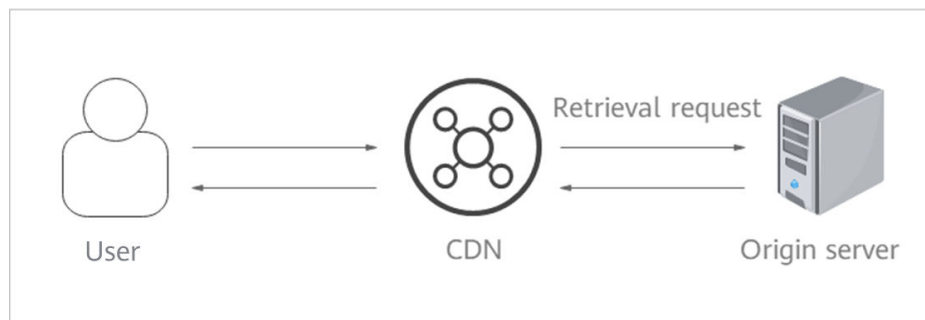
2.3.8 Encabezados de solicitud de recuperación

Puede configurar el encabezado de solicitud de recuperación en una URL de solicitud de recuperación.

Fondo

Si el contenido solicitado no se almacena en caché en los nodos de CDN, los nodos de CDN recuperan ese contenido de un servidor de origen. Puede configurar los encabezados de solicitud de recuperación en la consola de CDN para reescribir los detalles del encabezado de las URL de solicitud de recuperación.

Los encabezados HTTP forman parte de un mensaje de solicitud o respuesta HTTP que define los parámetros operativos de una transacción HTTP.



Precauciones

- Esta configuración solo modifica los encabezados de solicitud de recuperación en los mensajes HTTP para la recuperación de contenido a través de CDN. No modifica los de un mensaje HTTP que los nodos CDN devuelven a los usuarios.
- Un encabezado de solicitud no puede tener dos valores diferentes al mismo tiempo.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Retrieval Settings**.
5. En el área **Retrieval Request Headers**, haga clic en **Add**.
6. Configure los detalles del encabezado de la solicitud de recuperación.
 - **Add**: Agregar un encabezado de solicitud de recuperación a CDN para reescribir los detalles del encabezado en las URL de solicitud de usuario.

Tabla 2-3 Parámetros

Parámetro	Ejemplo	Descripción
Request Header Operation	Set	<p>Agregar un encabezado de solicitud específico a una solicitud HTTP de recuperación.</p> <ul style="list-style-type: none"> ● Si una URL de solicitud contiene el parámetro de X-test y la X-test se establece en 111, CDN establecerá la X-test en aaa en la URL de solicitud de recuperación. ● Si una URL de solicitud no contiene el parámetro X-test, CDN agregará el parámetro X-test a la URL de solicitud de recuperación y establecerá su valor en aaa.
	Delete	<p>Eliminar el encabezado que existe en una URL de solicitud de usuario.</p> <ul style="list-style-type: none"> ● Si una URL de solicitud contiene el parámetro X-test, este parámetro se eliminará de la URL de solicitud de recuperación.
Name	X-test	<ul style="list-style-type: none"> ● Ingrese entre 1 y 64 caracteres. ● Ingrese solo letras, dígitos o guiones (-).
Value	aaa	<ul style="list-style-type: none"> ● Introduzca de 1 a 512 caracteres. ● Escriba solo letras, dígitos, asteriscos (*), puntos (.), guiones (-) y guiones bajos (_). ● Las variables, como <i>\$client_ip</i> y <i>\$remote_port</i>, no están permitidas.

– **Edit:** Modifica el valor u operación de un encabezado de solicitud de recuperación.

Haga clic en **Edit** en la columna **Operation**. El siguiente cuadro de diálogo aparecerá en pantalla.

Parámetro	Ejemplo	Descripción
Request Header Operation	Set	Agregar un encabezado de solicitud específico a una solicitud HTTP de recuperación. <ul style="list-style-type: none"> ● Si una URL de solicitud contiene el parámetro de X-test y la X-test se establece en 111, CDN establecerá la X-test en aaa en la URL de solicitud de recuperación. ● Si una URL de solicitud no contiene el parámetro X-test, CDN agregará el parámetro X-test a la URL de solicitud de recuperación y establecerá su valor en aaa.
	Delete	Eliminar el encabezado que existe en una URL de solicitud de usuario. <ul style="list-style-type: none"> ● Si una URL de solicitud contiene el parámetro X-test, este parámetro se eliminará de la URL de solicitud de recuperación.
Name	X-test	Este parámetro no se puede modificar.
Value	aaa	<ul style="list-style-type: none"> ● Introduzca de 1 a 512 caracteres. ● Escriba solo letras, dígitos, asteriscos (*), puntos (.), guiones (-) y guiones bajos (_). ● Las variables, como <i>\$client_ip</i> y <i>\$remote_port</i>, no están permitidas.

7. Click **OK**.

NOTA

Si el área de servicio de su nombre de dominio es global o fuera de China continental y el encabezado **Accept-Encoding** en las solicitudes de usuario contiene varios valores, solo **Gzip** se pasa de forma transparente durante la recuperación de contenido.

Ejemplos

Supongamos que ha configurado los siguientes encabezados de solicitud de recuperación para el nombre de dominio `www.example.com`:

Retrieval Request Headers

You can modify header details in a retrieval request URL.

Request Header Operation ?	Name	Value	Operation
Set	X-cdn	aaa	Edit Delete
Delete	X-test		Edit Delete

Cuando un usuario solicita el archivo `http://www.example.com/abc.jpg` el archivo no se almacena en caché en CDN, y CDN recupera ese archivo del servidor de origen. El encabezado **X-cdn** se agregará a la solicitud de recuperación y el encabezado **X-test** se eliminará.

Restricciones

- Si su nombre de dominio tiene configuraciones especiales, no se pueden configurar Content-Type, Cache-Control, Expires, Content-Language, y Content-Disposition.
- No se pueden reescribir los siguientes encabezados estándares.

Origin	accept-ch	clear-site-data	push-policy
WsTag	Tcp-Retrans	access-control-allow-methods	access-control-max-age
vary	Date	X-Forward-Type	width
Age	ETag	Purge-Extra	X-Cacheable
access-control-allow-headers	Front-End-Https	ping-to	content-range
cross-origin-opener-policy	Location	viewport-width	Mime-Version
Proxy-Support	X-Resp-Time	If-Range	sec-fetch-dest
device-memory	X-Mem-Url	Cdn-Src-Ip	ping-from
Allow	X-Url-Blackwhite-List	early-data	Sec-WebSocket-Extensions
if-unmodified-since	X-Forward-Uri	Conf-File	x-download-options
X-Error-Status	Negotiate	x-permitted-cross-domain-policies	service-worker-allowed
X-Appa	x-firefox-spdy	content-dpr	X-Miss-Times-Limit
X-Bwctrl-Limit	X-Bwctrl-Para	X-Max-Conns	nel

public-key-pins-report-only	X-MAA-Alias	Sec-WebSocket-Location	X-Cache-2
Authorization	Expect	last-event-id	Sec-WebSocket-Key
X-Refresh-Pattern	forwarded	X-Local-Ip	Sec-WebSocket-Protocol
feature-policy	cross-origin-resource-policy	Request-Range	Conf-Other
strict-transport-security	signed-headers	Cdn-Server-Ip	Sec-WebSocket-Version
accept	X-Black-List	content-location	sourcemap
Partition-Block-Size	Proxy-Authentication-Info	cross-origin-embedder-policy	X-Request-Id
x-dns-prefetch-control	if-none-match	If-Non-Match	Public
X-White-List	x-ua-compatible	Keep-Alive	Transfer-Encoding
alt-svc	max-age	Last-Modified	x-xss-protection
Sec-WebSocket-Nonce	dnt	Link	x-robots-tag
Key	expect-ct	sec-fetch-site	access-control-request-headers
X-Error-URL	X-Log-Url	content-encoding	X-Times-Limit
X-Appa-Origin	X-Miss-Rate-Limit	X-IP-Region	Dynamic
X-Squid-Error	From	accept-ch-lifetime	X-MAA-Auth
Connection	X-Via-CDN	Max-Forwards	Upgrade
sec-fetch-user	content-security-policy-report-only	Pragma	save-data
X-Client-Ip	Cdn-Qos	x-powered-by	X-Forward-Measured
accept-push-policy	server	large-allocation	X-Request-Uri
X-Forward-Ip	Host	Proxy-Authenticate	X-Request-Url
X-Cache-Lookup	Conf-Option	X-Forward-Host	upgrade-insecure-requests
X-Accelerator-Vary	signature	X-Ip-Blackwhite-List	X-Cdn-Src-Port
Sec-WebSocket-Draft	Sec-WebSocket-Origin	X-IP-Region-CN	public-key-pins

Ws-Hdr	If-Match	Proxy-Authorization	X-Rate-Limit
sec-fetch-mode	trailer	X-Rewrite-Url	Via
X-Cache	X-Mgr-Traffic	accept-signature	Warning
x-forwarded-proto	If-Modified-Since	Authentication-Info	access-control-request-method
Content-Length	x-frame-options(xfo)	Range	A_Dynamic
te	x-forwarded-host	Title	WWW-Authenticate
tk	X-Query-Key	accept-charset	access-control-allow-origin
accept-ranges	report-to	access-control-expose-headers	x-content-type-options
Proxy-Connection	server-timing	Retry-After	x-requested-with
X-No-Referer	X-Forward-Peer	Sec-WebSocket-Accept	X-Forwarded-For
Conf-Err-Host	Sec-WebSocket-Key2	access-control-allow-credentials	X-Denyattack-Dynconf
referer-policy	Sec-WebSocket-Key1	content-security-policy	timing-allow-origin
X-DNS-Time	Conf-File-List	X-expireURL	x-pingback
Purge-Domain	dpr	-	-

2.3.9 Intervalo de tiempo de espera de recuperación

Si el contenido solicitado por un usuario no se almacena en caché en los nodos de CDN, CDN recupera el contenido del servidor de origen. El intervalo de tiempo de espera predeterminado de una solicitud de recuperación es 30s. Si la solicitud supera el tiempo de espera, la solicitud falla. Puede ajustar el intervalo de tiempo de espera de recuperación en función de las características del servicio y el estado de la red del servidor de origen para garantizar la recuperación normal del contenido.

Precauciones

- Para modificar el intervalo de tiempo de espera de recuperación de nombres de dominio con configuraciones especiales, envíe un ticket de servicio.
- El intervalo de tiempo de espera de recuperación no se puede configurar para nombres de dominio que sirven a usuarios fuera de China continental.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Retrieval Settings**.
5. En el área **Retrieval Timeout Interval**, haga clic en **Edit**.

Configure Retrieval Timeout Interval

To configure the retrieval timeout interval for domain names with special configurations, submit a service ticket.

Retrieval Timeout Interval seconds

Default value: 30s. Value range: 5s to 60s.

OK Cancel

6. Introduzca el intervalo de tiempo de espera de recuperación y haga clic en **OK**.

2.3.10 Preguntas Frecuentes

¿En qué escenarios CDN recupera contenido de un servidor de origen?

- El contenido deseado no se almacena en caché en los nodos de CDN.
- El contenido almacenado en caché en los nodos CDN ha caducado.

¿Cuál es la diferencia entre un host de recuperación y un servidor de origen?

- El servidor de origen decide la dirección a la que se accede durante la recuperación de contenido.
- El host de recuperación decide el sitio que está asociado con el contenido solicitado.

Supongamos que su servidor de origen es un servidor Nginx. Su dirección IP es x.x.x.x y su nombre de dominio es www.test.com. Los siguientes sitios se implementan en el servidor de origen:

```
server {
    listen 80;
    server_name www.a.com;

    location / {
        root html;
    }
}
server {
    listen 80;
    server_name www.b.com;

    location / {
        root html;
    }
}
```

Si desea que CDN recupere contenido de este servidor Nginx, establezca la dirección del servidor de origen en **x.x.x.x** o **www.test.com** en CDN. Dado que hay varios sitios en el servidor de origen, debe especificar el sitio específico para recuperar el contenido. Si desea que la CDN recupere contenido del sitio **www.a.com** establezca el host de recuperación en **www.a.com** en la CDN. Si desea que la CDN recupere contenido del sitio **www.b.com** establezca el host de recuperación en **www.b.com** en la CDN.

¿Huawei Cloud CDN admite la recuperación directa de contenido a través del acceso de rastreador?

No.

Huawei Cloud CDN no puede distinguir el acceso normal del usuario del acceso del rastreador. Si el rastreador registra la dirección IP de un nodo, el rastreador puede acceder directamente a esa dirección IP la próxima vez. Si el nodo no funciona correctamente o se somete a mantenimiento de rutina, el rastreador no podrá recuperar el contenido de esa dirección IP.

¿Cómo configuro el servidor de origen si un bucket de almacenamiento de objetos que no es de Huawei sirve como servidor de origen?

1. Obtenga el nombre de dominio del bucket de almacenamiento de objetos.
Al agregar un nombre de dominio en la consola de CDN, seleccione **Domain name** para **Origin Server Address** e introduzca el nombre de dominio del bucket de almacenamiento de objetos en el cuadro de texto.
2. Modifique las configuraciones de recuperación de contenido.
De forma predeterminada, el host de recuperación es el nombre de dominio de aceleración. Si configura un bucket de almacenamiento de objetos como servidor de origen, cambie el host de recuperación por el nombre de dominio de ese bucket de almacenamiento de objetos. De lo contrario, la recuperación de contenido falla.

2.4 Configuración de HTTPS

2.4.1 Descripción general

HTTPS garantiza una transmisión segura a través de la encriptación y la autenticación de identidad. Es ampliamente utilizado en comunicaciones sensibles a la seguridad en la World Wide Web, como el pago en línea.

En la siguiente tabla se describe la configuración HTTPS:

Función	Descripción
Certificados HTTPS	Puede agregar un certificado para la aceleración de HTTPS.
Versiónes de TLS	Puede habilitar o deshabilitar las versiones de TLS según sea necesario.

Función	Descripción
Requisitos del certificado HTTPS	Describe la combinación y la secuencia de carga de certificados emitidos por diferentes autoridades
Conversión de formato de certificado HTTPS	Puede convertir certificados en otros formatos al formato PEM que admite CDN.
OCSF Stapling	Puede permitir que CDN almacene el estado de los certificados en línea con antelación y devuelva el estado a los navegadores. Los navegadores no necesitan consultar el estado de las autoridades de certificación (CA), lo que acelera la verificación.
Forzar redireccionamiento	Puede forzar la redirección a HTTP o HTTPS.
HTTP/2	Describe los antecedentes y ventajas de HTTP/2.

2.4.2 Certificados HTTPS

Puede configurar un certificado HTTPS para un nombre de dominio de aceleración en la consola CDN para habilitar la aceleración HTTPS.

Fondo

- **HTTP**
 HTTP transfiere contenido en texto plano sin ninguna encriptación de datos. Si un atacante intercepta paquetes transmitidos entre el navegador y los servidores del sitio web, el contenido transmitido se puede leer directamente.
- **HTTPS**
 Basado en HTTP, HTTPS utiliza Secure Sockets Layer (SSL) para cifrar la transmisión de datos. Con SSL, los servidores se autentican mediante certificados y las comunicaciones entre navegadores y servidores se cifran.

Prerrequisitos

Puede utilizar su propio certificado o un certificado alojado por Huawei Cloud SSL Certificate Manager (SCM) para configurar HTTPS.

- Su propio certificado
 El formato del certificado debe cumplir con los requisitos descritos en [Requisitos del certificado HTTPS](#).
- Un certificado alojado por Huawei Cloud SCM en la consola Cloud Certificate Manager (CCM)
 Debe enviar el certificado a CDN en la consola CCM antes de habilitar la aceleración HTTPS en CDN. Para obtener más información sobre cómo enviar un certificado, consulte [Enviar un certificado SSL a otros servicios en la nube](#).

Precauciones

- Solo se admiten certificados y claves privadas en formato PEM. Si un certificado no está en formato PEM, convierta el certificado haciendo referencia a [Requisitos del certificado HTTPS](#).
- Un nombre de dominio de aceleración tiene su certificado asociado. Deben coincidir. Si su nombre de dominio es un dominio carácter comodín, configure un certificado para él haciendo referencia a [¿Cómo configuro un certificado si mi nombre de dominio es un dominio comodín?](#)
- La configuración del certificado se eliminará automáticamente una vez que la aceleración segura HTTPS esté deshabilitada. Es necesario volver a configurar el certificado si la aceleración segura HTTPS está habilitada de nuevo.
- Si el certificado ha cambiado, actualice la información del certificado en la consola de CDN de manera oportuna.

Configuración de certificados HTTPS

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **HTTPS Settings**.
5. En la página de la pestaña **HTTPS Settings**, haga clic en **Edit**. Aparece el cuadro de diálogo **Configure HTTPS Secure Acceleration**.

6. Active **Status** para habilitar este elemento de configuración.
7. Configure los parámetros correspondientes.

Parámetro	Descripción
Certificate Type	Seleccione My certificate o Huawei-managed certificate .
Certificate Name	<ul style="list-style-type: none"> ● My certificate: : Introduzca el nombre del certificado. Un nombre de certificado puede tener hasta 32 caracteres. ● Huawei-managed certificate: Ve a la consola CCM para enviar un certificado a CDN y luego selecciona el certificado en la lista desplegable junto a Certificate Name en la consola CDN. Para obtener más información, consulte Cómo enviar un certificado SSL a otros servicios en la nube.

Parámetro	Descripción
Certificate Body	<ul style="list-style-type: none"> ● My certificate: Utilice un editor de texto local para abrir el certificado y copiar el contenido del certificado en el cuadro de texto. ● Huawei-managed certificate: El contenido se rellena automáticamente. <p>NOTA El cuerpo del certificado no puede contener espacios ni líneas en blanco. De lo contrario, se muestra un mensaje que indica que los parámetros del certificado son incorrectos.</p>
Private Key	<ul style="list-style-type: none"> ● My certificate: Utilice un editor de texto local para abrir la clave privada y copiar el contenido en el cuadro de texto. ● Huawei-managed certificate: El contenido se rellena automáticamente.

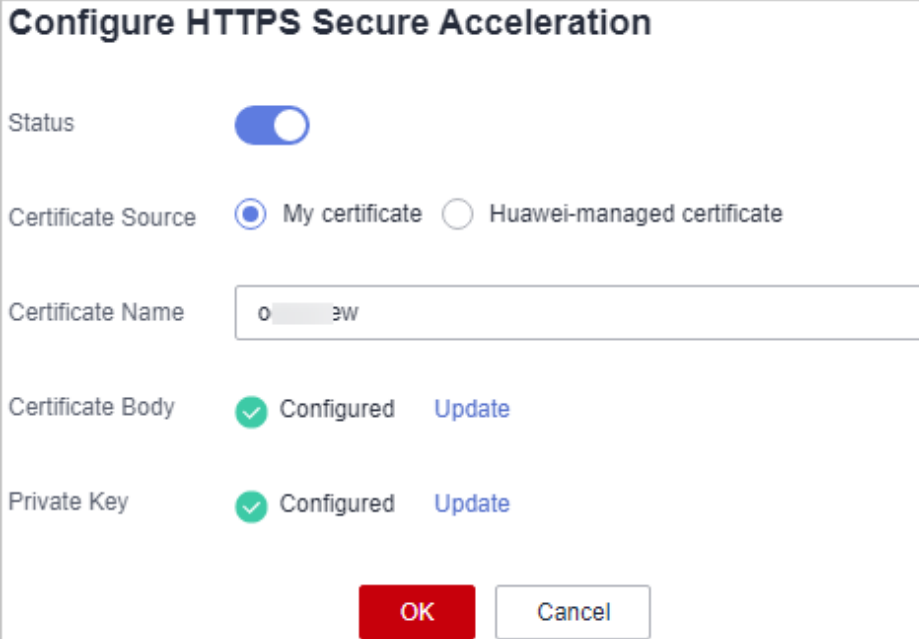
8. Haga clic en **OK**.
9. Compruebe si el certificado HTTPS ha entrado en vigor.

Si el certificado ha entrado en vigor, puede acceder a los recursos del sitio web del nombre de dominio de aceleración a través de HTTPS y ver la información de autenticación del sitio web haciendo clic en el icono de candado en el cuadro de dirección del navegador.

Actualización del certificado HTTPS

Si se actualiza el certificado de nombre de dominio, debe actualizar los detalles del certificado en el elemento de configuración HTTPS.

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
 Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **HTTPS Settings**.
5. En la página de la pestaña **HTTPS Settings**, haga clic en **Edit**. Aparece el cuadro de diálogo **Configure HTTPS Secure Acceleration**.



Configure HTTPS Secure Acceleration

Status

Certificate Source My certificate Huawei-managed certificate

Certificate Name

Certificate Body Configured [Update](#)

Private Key Configured [Update](#)

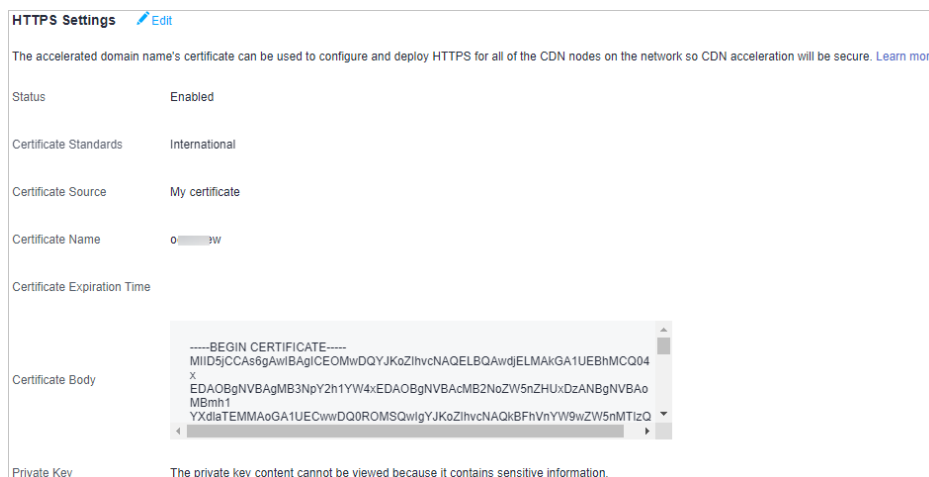
[OK](#) [Cancel](#)

6. Haga clic en **Update** para actualizar el certificado y la clave privada configurados. La actualización tarda aproximadamente de 5 a 10 minutos en surtir efecto.

Consulta de la información del certificado HTTPS

En la página de configuración del certificado HTTPS, puede ver detalles sobre el certificado HTTPS configurado para los nombres de dominio de aceleración.

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **HTTPS Settings**.
5. En la página que se muestra, puede ver detalles sobre el certificado HTTPS configurado para el nombre de dominio, como el tiempo de caducidad del certificado. También puede ver el contenido del certificado. Sin embargo, el contenido de clave privada no se puede ver, por razones de seguridad.



El valor del **Certificate Expiration Time** depende del tiempo de caducidad del certificado que caduca por primera vez en la cadena de certificados.

2.4.3 Requisitos del certificado HTTPS

La configuración HTTPS solo admite certificados o claves privadas en formato PEM. Para diferentes agencias emisoras de certificados, hay diferentes requisitos de carga.

Certificados emitidos por Root CA

Un certificado emitido por la Root CA es un certificado completo. Al configurar HTTPS, solo necesita cargar el certificado.

Utilice un editor de texto para abrir el certificado. El contenido del certificado debe ser algo similar a lo que está dentro en **Figura 2-2**.

Un certificado PEM:

- El certificado comienza con la instrucción **-----BEGIN CERTIFICATE-----** y termina con la instrucción **-----END CERTIFICATE-----**.
- Cada línea del certificado tiene 64 caracteres, pero la última línea puede ser más corta.
- No se permiten espacios en el contenido del certificado.

Figura 2-2 Certificado PEM

```
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIEAJGCTANBgkqhkiG9w0BAQUFADBUMQswCQYDVQGEwJj
bjELMAkGA1UECAwCZ2QxZCZAJBgNVBACMAmN6MQswCQYDVQKDAJodzELMAkGA1UE
CwwCaHcxGDAwBgNVBAMMD21OT0MgUm9vdCBDQSBWMjERMA8GCSqGSIb3DQEJARYC
aHcwHhcNMTYwNTE3MDEyODQ2WhcNMjEwNTE2MDEyODQ2WjBdMQswCQYDVQGEwJj
bjELMAkGA1UECBMCZ2QxZCZAJBgNVBAcTAmh3MQswCQYDVQQLLEwJodzEUMBIGA1UE
AxQLKi5vd3Nnby5jb20xETAPBgkqhkiG9w0BCQEWAmh3MIIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAXDKJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909e
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
HRMEAjAAMCwGCWGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbnVvYXR1ZCB2ZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQUmNstyLA+uGec0xx8f+XPLs3AiEUwHwYDVR0jBBgwFoAU
PRaAjcivt51G+7642KLZ+GbJTIQwDQYJKoZIhvcNAQEFBQADggEBABkMxMrUMhEH
ZNhb19blt90NKQJpi7ugy7rj+vft4fUYeTvapsRwNutjWGVmnWB3HV85tnbIgvsa
OpP6yKbJ+mJhL5AB/crDMDMgGhywUEoG80kzEQJSeUHJ/R/iTaksmkqSPyDrbvaN
1DpIf5Sa7YA9VbWYpIZDuOhyk07HSZc8kcSmD+0K9gOke7QS1L3FKAvdqqJepeL6
A137VUmYtdh2mqS78LcpSs+SofippOGgi5AuimZqp5xrn8Od6GjQqEc7nGH5foQ
lJq8ekhn07Aqd7chFbDfW4qLSY7nEHT3uLzGME8Y9QQ4zs5H7lCaJVGXtoTQfpXR
nuMo/2NXiA0=
-----END CERTIFICATE-----
```

Certificados emitidos por agencias intermedias

Un expediente de certificado emitido por una agencia intermediaria contiene varios certificados. Es necesario combinar los certificados en un único certificado completo para cargarlos al configurar la aceleración de seguridad HTTPS. Un certificado combinado se muestra como [Figura 2-3](#).

Utilice un editor de texto para abrir todos los certificados. Comience con el certificado de servidor y añada el contenido de los certificados intermedios al archivo. Generalmente, se emitirá una instrucción junto con el certificado. Tenga en cuenta las reglas de la instrucción. Las reglas generales son las siguientes:

- No hay líneas vacías entre los certificados.
- Los formatos de las cadenas de certificados son los siguientes:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Figura 2-3 Certificado combinado

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj41j5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmVmcxETAPBgNVBACM
CFNoZW56aGVuMQ8wDQYDVQQKDAZidWF3ZWkxZCzAJBgNVBAsMAk1UMS4wLWYDVQ
DCVidWF3ZWkxZDViIFN1Y3V5ZSBjbnR1cm5ldCBHYXR1d2F5IENBMB4XDTE3MTAx
ODAwNDA0N1oXDTE4MTAxODAwNDA0N1owGZoxCzAJBgNVBAYTAKNOMRAwDgYDVQQI
DAdqaWZ3N1MRAwDgYDVQQHDAduYW5qaW5nMS4wLWYDVQQKDCVidWF3ZWkxZDViIFN5
dHdhcmUgVGVjaG5vbG9naWVzIENvLiV2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3f5hC6J20XSF/Y7Wb8o6l30yzgaUYWGLEX8t
ldQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPFLT/IV6UnvMLnxJQBavqauykCskadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhrfmR4owS/3w1wxdpwy5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccYlufuqr3v0TToaNN4c37kwjJeKf+b2F/IqO/KF+9zF
AgWgMBMGA1UdJQQMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuWQ3st8axvhDD9jZGoninzW
JSGpdm04NEshlvSfdeHpy/xKSLCIqg5Ue8tTI8zOf13U0RonMeHKSXsJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21dj1qQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2CCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemh1bjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDLDAJVVDEuMCAwGA1UEAw1SHVhd2VpIFd1
YiBTZWN1cmUgSW50ZXJuzXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemh1bjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDLDAJ
VDEuMCAwGA1UEAw1SHVhd2VpIFd1YiBTZWN1cmUgSW50ZXJuzXQgR2F0ZXdheSBD
rG0CAwEAAaNQME4wHQYDVR0OBBYEFDB6DZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9ksjRX56yw2Ku5Mm3gZu/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqilLlBcPxo/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpWJW3duj1FuRjGsvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhrAHezyfLrvimxIOky
2KZWitN+M1UwvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu671liddt7zzzzqW+U
QLU0ewUmUHQsV5mk62v1e8sRViHB1B2HJ3DU5gE=
-----END CERTIFICATE-----
```

Clave privada RSA

Los archivos PEM pueden contener certificados o claves privadas. Si un archivo PEM contiene solo claves privadas, el sufijo del archivo puede ser reemplazado por KEY.

Utilice un editor de texto para abrir el archivo de clave privada en formato PEM o KEY. A continuación, puede ver el contenido de la clave privada, como se muestra en [Figura 2-4](#).

Contenido de una clave privada RSA:

- La clave privada comienza con la instrucción `-----BEGIN RSA PRIVATE KEY-----` y termina con la instrucción `-----END RSA PRIVATE KEY-----`.
- Cada línea de la clave privada tiene 64 caracteres, pero la última línea puede ser más corta.
- No se permiten espacios en el contenido de la clave privada.

Figura 2-4 Clave privada RSA

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eYlvLCgow
wEPqs6vvyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oBl2AeAvbzKxWwRqf4JTLa3136B415yZVoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof00yp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlur1/Z9s8ytj3124AQY7NE1t1iL9wA47k
0EumxTaLz8H/vHB1fLMouyYfsSDEr3Snf6eSSwIDAQABAoIBAQCDCNmxC3qHXPgvI
EzB0tIPV11PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcm
-----END RSA PRIVATE KEY-----
```

Si la cadena de certificados de un archivo de clave privada contiene las siguientes information: `-----BEGIN PRIVATE KEY-----` y `-----END PRIVATE KEY-----`, o `-----BEGIN ENCRYPTED PRIVATE KEY-----` y `-----END ENCRYPTED PRIVATE KEY-----`, necesita usar la herramienta OpenSSL para ejecutar el siguiente comando para convertir el formato.

```
openssl rsa -in old_key.key -out new_key.key
```

Preguntas Frecuentes

[¿Qué puedo hacer si falla la configuración del certificado HTTPS y aparece el mensaje "Cadena de certificados incompleta"?](#)

2.4.4 Conversión de formato de certificado HTTPS

La configuración HTTPS solo admite certificados o claves privadas en formato PEM. Se recomienda utilizar [OpenSSL](#) para convertir certificados en otros formatos al formato PEM. Los siguientes ejemplos ilustran algunos métodos de conversión populares.

En los siguientes ejemplos, el nombre de los certificados antes de la conversión es **old_certificate** de forma predeterminada, y el de las claves privadas antes de la conversión es **old_key** de forma predeterminada. El nuevo certificado y los nombres de clave privada son **new_certificate** y **new_key** respectivamente.

- **Converting DER to PEM**

```
openssl x509 -inform der -in old_certificate.cer -out new_certificate.pem  
openssl rsa -inform DER -outform pem -in old_key.der -out new_key.key
```

- **Converting P7B to PEM**

```
openssl pkcs7 -print_certs -in old_certificate.p7b -out new_certificate.cer
```

- **Converting PFX to PEM**

```
openssl pkcs12 -in old_certificate.pfx -nokeys -out new_certificate.pem  
openssl pkcs12 -in old_certificate.pfx -nocerts -out new_key.key
```

También puede utilizar una herramienta de conversión de certificados de terceros en línea para convertir certificados en diferentes formatos.

2.4.5 OCSP Stapling

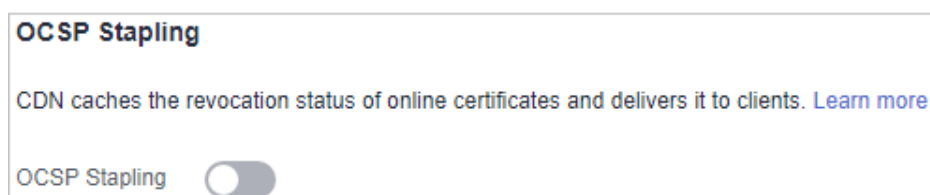
Cuando Online Certificate Status Protocol (OCSP) stapling está habilitado, CDN consulta y almacena en caché el estado de los certificados en línea por adelantado y devuelve el estado a un navegador al establecer una conexión TLS con el navegador. Esto significa que el navegador no necesita consultar el estado de las CA, lo que acelera la verificación.

Prerrequisitos

- Se ha configurado un certificado HTTPS. Para más detalles, consulte [Certificados HTTPS](#).
- El OCSP stapling no se puede aplicar a la aceleración de sitios completos o a nombres de dominio que también requieren servicios de aceleración fuera de China continental.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **HTTPS Settings**.



5. Active **OCSP Stapling**.

2.4.6 Forzar redireccionamiento

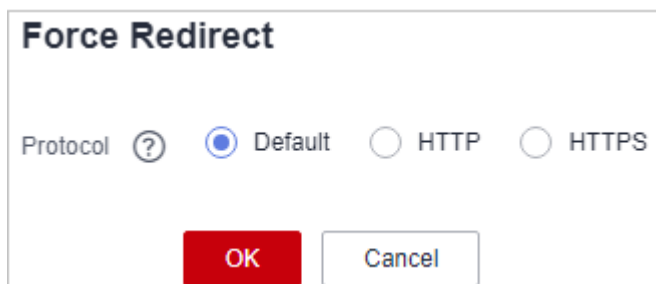
Las solicitudes de los clientes a los nodos CDN se pueden redirigir a la fuerza a HTTP o HTTPS.

Restricciones

Se ha configurado un certificado HTTPS para su nombre de dominio. Para más detalles, consulte [Certificados HTTPS](#).

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **HTTPS Settings**.
5. Haga clic en **Edit** junto a **Force Redirect**. Aparece el cuadro de diálogo **Force Redirect**.



Protocolo	Descripción
Default	Se soportan las solicitudes HTTP y HTTPS de los clientes.
HTTP	Las solicitudes de los clientes a los nodos CDN se redirigen a la fuerza a HTTP.
HTTPS	Las solicitudes de los clientes a los nodos CDN se redirigen a la fuerza a HTTPS.

6. Seleccione un protocolo y haga clic en **OK**.

2.4.7 HTTP/2

Fondo

HTTP/2 es un protocolo de transferencia de hipertexto de próxima generación. Reduce el retardo de establecimiento de enlace TCP, reduce el volumen de transmisión de cabecera de paquete y mejora la eficiencia de transmisión. Las direcciones en el formato de **http://url** solo pueden usar el protocolo HTTP/1.x, y las en el formato de **https://url** soportan HTTP/2.

Restricciones

Se ha configurado un certificado HTTPS. Para más detalles, consulte [Certificados HTTPS](#).

Ventajas del protocolo

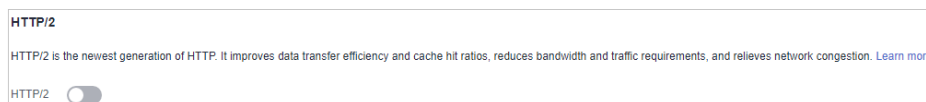
Actualmente, HTTP/1.1 es el protocolo para Internet. HTTP/2 supera a HTTP/1.1 y mantiene la sintaxis de HTTP/1.1.

HTTP/2 supera a HTTP/1.1 en los siguientes aspectos:

- **Encuadre binario**
HTTP/2 usa formato binario para transferir datos, mientras que HTTP/1.1 es un protocolo basado en texto. El formato binario es más ventajoso en la resolución y optimización del protocolo, y aumenta la eficiencia de la transferencia de datos.
- **Compresión de campo de encabezado**
HTTP/2 comprime y transfiere encabezados de mensaje usando HPACK. Estos encabezados se trazan y se almacenan en una tabla de encabezados. Una vez que un encabezado de mensaje ha sido enviado por una vez, es almacenado en caché y puede ser obtenido por otros encabezados de mensaje idénticos automáticamente.
Las solicitudes que usan HTTP1.1 llevan una gran cantidad de información de encabezado redundante, lo que causa desperdicio en el ancho de banda. Con la compresión del campo de encabezado, HTTP/2 ahorra el ancho de banda y el tráfico.
- **Multiplexación**
HTTP/2 multiplexa múltiples solicitudes o respuestas a través de una única conexión TCP. Mientras que HTTP/1.1 establece una conexión TCP para cada solicitud o respuesta en orden. Al enviar solicitudes simultáneamente, HTTP/2 disminuye la presión sobre la conexión al servidor y alivia el problema de bloqueo de red.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **HTTPS Settings**.
5. Active **HTTP/2**.



2.4.8 Versiones de TLS

Puede configurar las versiones TLS según sea necesario.

Fondo

Transport Layer Security (TLS) es un protocolo de seguridad utilizado para garantizar la seguridad y la integridad de los datos para la comunicación por Internet. La aplicación más

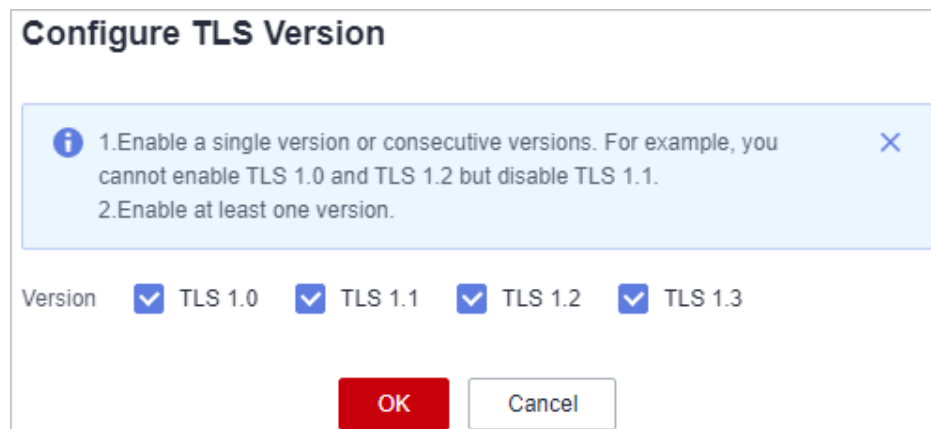
típica es HTTPS. TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3 están disponibles. Una versión posterior es más segura, pero es menos compatible con los navegadores de versiones anteriores.

Restricciones

- Se ha configurado un certificado HTTPS. Para más detalles, consulte [Certificados HTTPS](#).
- Las versiones TLS no se pueden configurar para nombres de dominio con configuraciones especiales.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **HTTPS Settings**.
5. En el área **TLS Version**, haga clic en **Edit**.



NOTA

- Puede habilitar una sola versión o versiones consecutivas. Por ejemplo, no puede habilitar TLS 1.0 y TLS 1.2 pero deshabilitar TLS 1.1.
 - Debe habilitar al menos una versión.
 - De forma predeterminada, TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3 están habilitados.
6. Seleccione una o más versiones de TLS y haga clic en **OK**.

2.4.9 Preguntas Frecuentes

¿Cómo puedo solucionarlo si se muestra la "Incomplete certificate chain"?

Esto es tal vez porque:

- Formato de certificado no válido

- Los certificados están mal llenados.
- Los certificados se instalan en el orden equivocado.

Ordene los certificados con el certificado root al final. Por ejemplo, si tiene tres certificados, A, B y C; y el certificado root, el orden debe ser: certificado C - certificado B - certificado A - certificado root.

Para obtener más información sobre cómo obtener la cadena de certificados correcta, consulte [Requisitos de certificado HTTPS](#).

Alternativamente, puede utilizar una herramienta de cadena de certificados en línea para corregir la cadena de certificados incompleta.

¿Cómo puedo solucionarlo si el sistema muestra un mensaje que indica que el formato del certificado es incorrecto?

La configuración HTTPS solo admite certificados y claves privadas en formato PEM. Diferentes autoridades de certificación tienen diferentes requisitos sobre la carga del organismo de certificación. Para obtener más información acerca de los requisitos de formato, consulte [Requisitos de certificado HTTPS](#). Si el formato de certificado no es PEM, utilice una herramienta de terceros en línea para convertir el certificado antes de cargarlo.

2.5 Configuración de caché

2.5.1 Descripción general

CDN almacena en caché el contenido de origen en nodos periféricos de todo el mundo para que los usuarios puedan obtener contenido de nodos cercanos. Puede modificar la configuración de caché para cambiar el estado de caché de los recursos en los nodos de CDN.

En la siguiente tabla se describe la configuración de caché.

Función	Descripción
Cache Rules	Puede establecer la edad y la prioridad máximas de la caché para diferentes recursos para aumentar la proporción de aciertos y reducir la tasa de retorno al origen.
URL Parameter Filtering	Puede filtrar los parámetros de URL para permitir que los nodos CDN ignoren los parámetros siguiendo un signo de interrogación (?) al almacenar recursos en caché, mejorando la relación de aciertos de caché y acelerando la distribución.
Origin Cache Control	Puede establecer que el tiempo de caducidad de la caché en los nodos CDN sea el mismo que el de su servidor de origen.
Tiempo de la caché del código de estado	Puede configurar la vigencia de la caché de los códigos de estado para permitir que la CDN almacene en caché y devuelva los códigos de estado a los usuarios, reduciendo la relación de recuperación y la presión sobre el servidor de origen.

NOTA

- Si ha modificado las reglas de caché y la configuración de control de caché de origen, preste atención a lo siguiente:
 - La nueva regla no se aplica al contenido que se ha almacenado en caché, sino que solo se aplica al contenido nuevo.
 - Después de modificar las reglas de caché, **actualice la caché** para que la modificación surta efecto.

2.5.2 Reglas de caché

Puede configurar la edad máxima para uno o más recursos almacenados en caché en los nodos de CDN. Si se ha alcanzado la edad máxima de un archivo almacenado en caché en nodos CDN, CDN solicita el contenido más reciente del archivo desde el servidor de origen cuando un usuario solicita el archivo. CDN devuelve el contenido al usuario y lo almacena en caché en los nodos CDN. Puede almacenar en caché todos los archivos y la página de inicio, o almacenar en caché el contenido deseado por directorio, tipo de archivo y ruta completa.

Antecedentes

Las políticas de caché en los nodos CDN cumplen con HTTP. Puede controlar la antigüedad de la caché configurando el campo **Cache-Control: max-age** en un encabezado de respuesta HTTP. Al aprovechar las reglas de caché, puede optimizar los períodos de caché para diferentes servicios. Las políticas de caché adecuadas pueden aumentar el índice de aciertos y reducir la tasa de recuperación, lo que reduce la utilización del ancho de banda.

Después de recibir una solicitud, un nodo CDN comprobará si el contenido solicitado ha expirado en la memoria caché. Si el contenido solicitado es válido en la caché, se devolverá directamente desde ese nodo CDN al usuario, acelerando la respuesta del sitio. Si el contenido solicitado en la memoria caché ha expirado, el nodo CDN enviará una solicitud para recuperar contenido nuevo desde un servidor de origen para que pueda actualizar su memoria caché local y servir contenido nuevo al usuario.

Precauciones

- Se pueden agregar hasta 60 reglas de caché a cada nombre de dominio.
- La vigencia máxima de la caché afecta directamente a la tasa de recuperación. Si la vigencia máxima de la memoria caché es corta, el contenido almacenado en la memoria caché en los nodos CDN se vuelve inválido en poco tiempo, lo que resulta en recuperaciones frecuentes, lo que aumenta la carga del servidor de origen y prolonga la latencia de acceso. Sin embargo, si la edad máxima de la caché es demasiado larga, el contenido almacenado en caché puede estar obsoleto como resultado.
- Si la vigencia máxima de la memoria caché se establece en 0, CDN recupera el contenido del servidor de origen para todas las solicitudes de usuario, lo que puede interrumpir el servicio de aceleración.
- Los recursos almacenados en caché en los nodos pueden eliminarse debido al acceso poco frecuente.
- Si ha modificado la regla de caché,
 - La nueva regla no se aplica al contenido que se ha almacenado en caché, sino que solo se aplica al contenido nuevo.
 - Puede actualizar la caché para que la modificación surta efecto inmediatamente para el contenido nuevo y el contenido que se ha almacenado en caché.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Cache Settings**.
5. En el área **Cache Rules**, haga clic en **Edit**. Aparece el cuadro de diálogo **Configure Cache Rule**.
6. Haga clic en **Add** para agregar reglas de caché. Consulte [Figura 2-5](#). [Tabla 2-4](#) describe los parámetros. Puede hacer clic en **Suggested Rules** para ver la configuración recomendada.

Figura 2-5 Configuración de una regla de caché

The screenshot shows the 'Configure Cache Rule' dialog box. At the top, there is a message: 'Modified rules are effective for new content cache. For existing cache, refresh to apply the modifications.' Below this is a table with the following data:

Type	Content	Priority	Maximum Age	Operation
File type	.php;.jsp;.asp;.aspx	2	0 days	Delete
All files		1	30 days	Delete

Below the table, there are two buttons: 'Add' and 'Suggested Rules'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Tabla 2-4 Parámetros de regla de caché

Parámetro	Descripción	Regla de configuración
All files	Todos los recursos almacenados en caché en nodos CDN	Por defecto, CDN tiene una regla para cada nuevo nombre de dominio. La regla especifica que la edad máxima de la caché para All files es de 30 días. Puede modificar esta regla, pero no puede eliminarla.

Parámetro	Descripción	Regla de configuración
File type	Archivos de un tipo específico Si el tipo de servicio de un nuevo nombre de dominio es Website , File download , o On-demand service y su servidor de origen es privado, CDN le agrega una regla de forma predeterminada. La regla especifica que vigencia máxima de la caché es 0 para los archivos dinámicos comunes, como los archivos.php.jsp.asp y.aspx. CDN recupera dichos archivos del servidor de origen para cada solicitud. Puede modificar y eliminar esta regla.	<ul style="list-style-type: none"> ● Se admiten todos los tipos de archivo. ● Inicie cada extensión de nombre de archivo con un punto (.), y extensiones de nombre de archivo separadas con punto y coma (;). ● Ingrese un máximo de 20 extensiones de nombre de archivo. ● Ingrese 255 caracteres como máximo. ● Las extensiones de nombre de archivo no distinguen entre mayúsculas y minúsculas. Example: .JPG;.zip;.exe
Directory	Archivos en un directorio	Iniciar un directorio con una barra diagonal (/), y separar varios directorios con punto y coma (;). Introduzca un máximo de 20 directorios con un máximo de 255 caracteres en total. Ejemplo: /test/folder01;/test/folder02
Full path	Un archivo específico	Una ruta completa debe comenzar con una barra diagonal (/) y no puede terminar con un asterisco (*). Un archivo en el directorio o archivo especificado con el comodín * puede ser coincidente. Introduzca sólo una ruta completa. Ejemplos: /test/index.html o /test/*.jpg
Homepage	Directorio root	El directorio raíz de un sitio web es el directorio de nivel superior de la carpeta del sitio web, que contiene todas las subcarpetas del sitio web. Por ejemplo, para abc/file01/2.png , abc/ es el directorio raíz, y una regla de caché está configurada para abc/ .

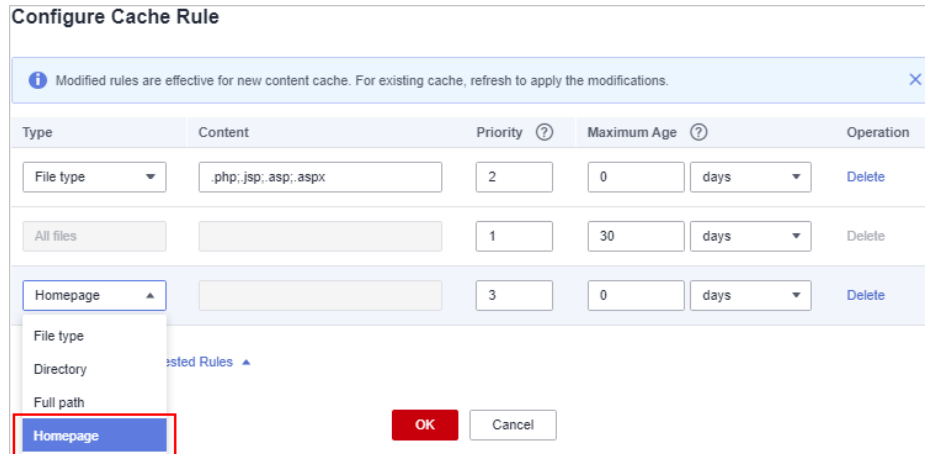
Parámetro	Descripción	Regla de configuración
Priority	Prioridad de una regla de caché Cada regla de caché debe tener una prioridad única. El establecimiento de prioridades es obligatorio. Si se especifica un recurso en varias reglas de caché, se aplica la regla con la prioridad más alta.	Escriba un número entero comprendido entre 1 y 100. Un número mayor indica una prioridad más alta.
Maximum Age	Duración en la que se puede almacenar un archivo en caché. Si se ha alcanzado la edad máxima del archivo, CDN solicita el contenido más reciente del archivo desde el servidor de origen cuando un usuario solicita el archivo desde un nodo CDN. Además, la CDN almacena en caché ese contenido en el nodo de CDN.	La vigencia de un archivo en caché no puede exceder los 365 días. Se recomienda establecer la hora de acuerdo con las siguientes reglas: <ul style="list-style-type: none"> ● Para los archivos estáticos (como los archivos.jpg y.zip) que no se actualizan con frecuencia, establezca la edad máxima en más de un mes. ● Para los archivos estáticos (como los archivos.js y.css) que se actualizan con frecuencia, establezca la edad máxima en función de los requisitos del servicio. ● Para archivos dinámicos (como archivos.php, .jsp y.asp), establezca la edad máxima en 0 segundos.

7. (Opcional) Eliminar una regla de caché si no la usa por mucho tiempo.
8. Haga clic en **OK**.

Ejemplos

Escenario 1: Suponga que ha agregado un portal web a Huawei Cloud CDN para la aceleración, pero no desea almacenarlo en caché.

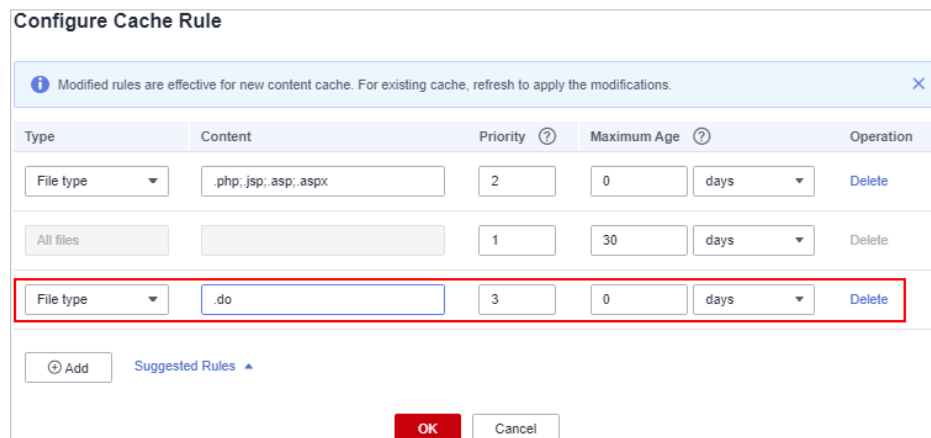
Puede agregar una regla de caché para este portal web en la consola de CDN, con **Type** establecido en **Homepage** y **Maximum Age** en **0**.



Escenario 2: Supongamos que no desea almacenar en caché archivos de un tipo específico o una página web específica.

1. Ha configurado la aceleración de CDN para su sitio web y establece la edad máxima de caché de los archivos.do en un día. Sin embargo, debido a los requisitos de servicio, ya no es necesario que los archivos cache.do.

Puede agregar una regla de caché para su sitio web en la consola de CDN, con **Type** establecido en **File type**, **Content** a **.do**, y **Maximum Age** en **0**.



NOTA

La nueva regla solo se aplica al contenido nuevo. Después de agregar la nueva regla, actualice la URL o el directorio en caché donde se encuentra el archivo.do en la consola de CDN para que la nueva regla pueda tener efecto para los archivos all.do.

2. Ha configurado la aceleración de CDN para su sitio web, la página de inicio de sesión de su sitio web se muestra cíclicamente y sus clientes no pueden iniciar sesión en el sitio web. Después de deshabilitar la aceleración de CDN, los clientes pueden iniciar sesión en el sitio web.

Esto se debe a que los nodos CDN han almacenado en caché la página de inicio de sesión. Para resolver el problema, agregue una regla de caché para su sitio web en la consola de CDN y establezca la edad máxima de caché de la página de inicio de sesión en 0 en la regla. Tome la página de inicio de sesión de la consola Huawei Cloud como ejemplo. La página de inicio de sesión de la consola Huawei Cloud es **https://auth.huaweicloud.com/authui/login.html#/login**. Puede agregar una regla de caché en la consola de CDN, con **Type** establecido en **Full path**, **Content** en **/authui/login.html#/login**, y **Maximum Age** en **0**.

Type	Content	Priority	Maximum Age	Operation
File type	.php;.jsp;.asp;.aspx	2	0 days	Delete
All files		1	30 days	Delete
Full path	/authui/login.html#/login	3	0 days	Delete

Escenario 3: Suponga que ha configurado las siguientes reglas de caché para su nombre de dominio de aceleración `www.example.com` pero no sabe qué regla tiene efecto.

Type	Content	Priority	Maximum Age
All files		1	30 days
File type	.jpg	2	1 days
Directory	/test/folder01	6	5 days
Full path	/test/*.jpg	8	3 days

Cuando un usuario solicita las reglas de `www.example.com/test/cdn.jpg`, de **All files**, **File type**, y **Full path** coinciden. La prioridad de la regla de **Full path** es 8, que es la más alta entre las tres reglas. Por lo tanto, se utiliza la regla del tipo de **Full path** (`/test/*.jpg`).

2.5.3 Filtrado de parámetros de URL

Fondo

La mayoría de las solicitudes de páginas web llevan parámetros de URL que comienzan con un signo de interrogación (?). Si los parámetros no contienen información importante (como la versión), puede habilitar el filtrado de parámetros de URL para mejorar la relación de aciertos de caché y acelerar la distribución de contenido. Al configurar el filtrado de parámetros de URL, puede conservar o ignorar parámetros específicos.

Habilitación del filtrado de parámetros de URL

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List** > **Storage** > **CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Cache Settings**.
5. Haga clic en **Edit** junto a **URL Parameter Filtering**.

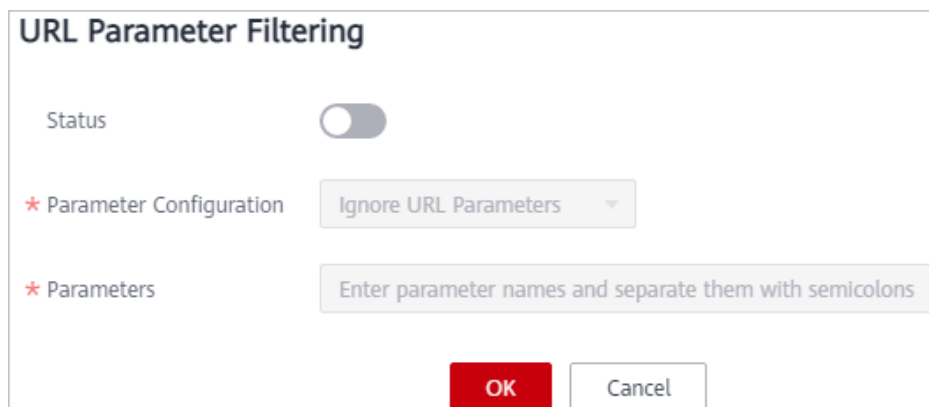


Tabla 2-5 Descripción del parámetro

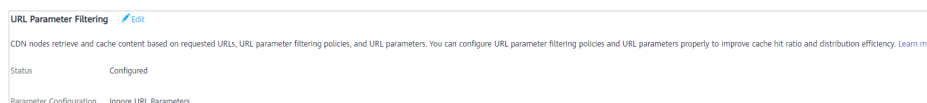
Parámetro	Descripción	Regla de configuración
Status	<p>Deshabilitado: (predeterminado) El filtrado de parámetros de URL está deshabilitado. CDN almacena en caché el recurso basándose en los parámetros que siguen al signo de interrogación (?) en una URL de solicitud.</p> <p>Habilitado: si el filtrado de parámetros de URL está habilitado, los siguientes elementos de configuración tienen efecto.</p>	-
Ignore URL parameters	CDN ignora todos los parámetros que siguen a los signos de interrogación (?) en las URL de solicitud, mejorando la relación de aciertos de caché.	N/A
Ignore specific parameters	CDN ignora los parámetros específicos en las URL de solicitud, pero conserva otros parámetros.	<ul style="list-style-type: none"> ● Ingrese hasta 10 nombres de parámetros separados por punto y coma (;). ● Solo se admiten letras, dígitos, puntos (.), guiones bajos y tildes (~).
Retain specific parameters	CDN conserva los parámetros específicos en las URL de solicitud, pero ignora otros parámetros.	<ul style="list-style-type: none"> ● Ingrese hasta 10 nombres de parámetros separados por punto y coma (;). ● Solo se admiten letras, dígitos, puntos (.), guiones bajos y tildes (~).

NOTA

- Si una regla de caché de su nombre de dominio tiene una configuración especial de parámetros de URL, no puede configurar el filtrado de parámetros de URL para el nombre de dominio en la consola de CDN. En este caso, puede enviar un ticket de servicio.
6. Active **Status** seleccione una operación de parámetro en la lista desplegable **Parameter Configuration**, establezca parámetros haciendo referencia a [Tabla 2-5](#) y haga clic en **OK**.

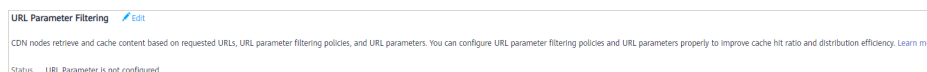
Ejemplos

- **Ejemplo 1:** Su nombre de dominio **www.example.com** tiene la siguiente configuración de filtrado de parámetros de URL:



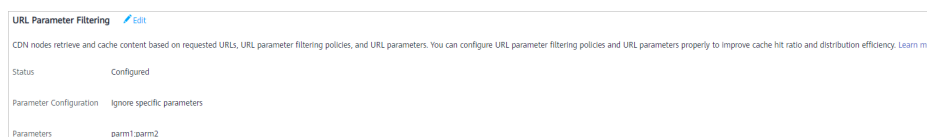
Cuando un usuario solicita **http://www.example.com/1.txt** por primera vez, el archivo no se almacena en caché en CDN, por lo que CDN necesita recuperar el archivo del servidor de origen. Cuando el usuario solicita **http://www.example.com/1.txt?test1**, el parámetro que sigue al signo de interrogación (?) será ignorado. Como resultado, **http://www.example.com/1.txt** es hit.

- **Example 2:** Su nombre de dominio **www.example.com** tiene la siguiente configuración de filtrado de parámetros de URL:



Cuando un usuario solicita **http://www.example.com/1.txt** por primera vez, el archivo no se almacena en caché en CDN, por lo que CDN necesita recuperar el archivo del servidor de origen. Cuando el usuario solicita **http://www.example.com/1.txt?test1**, la CDN buscará una coincidencia para la URL completa, incluyendo el parámetro que sigue al signo de interrogación (?) porque el filtrado de parámetros de URL está deshabilitado. Como resultado, CDN tiene que recuperar **http://www.example.com/1.txt?test1** del servidor de origen porque no se golpea la caché.

- **Example 3:** Su nombre de dominio **www.example.com** tiene la siguiente configuración de filtrado de parámetros de URL:



Cuando un usuario solicita **http://www.example.com/1.txt** por primera vez, el archivo no se almacena en caché en CDN, por lo que CDN necesita recuperar el archivo del servidor de origen. Cuando el usuario solicita **http://www.example.com/1.txt?parm1&parm2**, los parámetros **parm1** y **parm2** en la URL serán ignorados. Como resultado, **http://www.example.com/1.txt** es hit.

2.5.4 Control de caché de origen

Fondo

Si **Cache-Control: max-age** se ha configurado para el servidor de origen y desea que el tiempo de caducidad de la caché en el lado CDN sea el mismo que **Cache-Control: max-age**,

puede activar **Origin Cache Control**. A continuación, **Cache-Control: max-age** determina cuánto tiempo se almacena el contenido en caché en los nodos de CDN.

Activación del control de caché de origen

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Cache Settings**.
5. Vea la página siguiente.

Origin Cache Control

If this is disabled, custom cache rules determine how long content can be cached.

Origin Cache Control

6. Active **Origin Cache Control**.

Origin Cache Control

If this is enabled, Cache-Control: max-age determines how long content can be cached.

Origin Cache Control

Ejemplos

Supongamos que ha habilitado **Origin Cache Control** para el nombre de dominio **www.example.com**.

Origin Cache Control

If this is enabled, Cache-Control: max-age determines how long content can be cached.

Origin Cache Control

Cuando un usuario solicita el archivo **http://www.example.com/abc.jpg**:

- Si ha establecido **cache-control** en **max-age** en el servidor de origen, se utiliza la configuración **max-age** en el servidor de origen.
- Si ha establecido **cache-control** en **no-cache**, **private** o **no-store** en el servidor de origen, CDN no almacena en caché el archivo y la entrega de contenido no se puede acelerar.

- Si no ha establecido **cache-control** en el servidor de origen, se utiliza la edad máxima de caché configurada en CDN.

2.5.5 Tiempo de la caché del código de estado

Cuando un nodo CDN recupera un recurso del servidor de origen, el servidor de origen devuelve un código de estado de respuesta. Puede establecer el tiempo de la caché del código de estado en la consola de CDN. Cuando un cliente solicita el recurso de nuevo, la recuperación de contenido no se activará, lo que reduce la relación de recuperación y la presión sobre el servidor de origen.

Escenarios

Esta función se aplica al escenario en el que el servidor de origen devuelve un código de estado anormal. Cuando el servidor de origen se está ejecutando correctamente, CDN almacena en caché un recurso recuperado en los nodos según las reglas de caché que configure. Cuando un usuario accede al recurso, la recuperación de contenido no se activará. Si el servidor de origen responde de forma anormal y no desea que el servidor de origen responda a todas las solicitudes, puede establecer la antigüedad de la caché del código de estado para reducir la presión sobre el servidor de origen.

Aplicación: Si los usuarios acceden continuamente a la imagen **abc.jpg** que no está almacenada en caché en nodos CDN y que se ha eliminado del servidor de origen, Los nodos CDN recuperarán la imagen para cada solicitud de usuario y el servidor de origen devolverá un código de estado 4xx, aumentando la presión sobre el servidor de origen. En este caso, si configura el tiempo de la caché para el código de estado 4xx en CDN, los nodos CDN devolverán directamente el código de estado 4xx cuando los usuarios soliciten la imagen, y no se requiere la recuperación de contenido.

Precauciones

- El tiempo de la caché del código de estado no se puede configurar para nombres de dominio con configuraciones especiales.
- Puede configurar la edad de la caché para los siguientes códigos de estado:
 - 4XX: 400, 403, 404, 405, y 414
 - 5XX: 500, 501, 502, 503, y 504

Procedimiento

1. Inicie sesión en la **consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Cache Settings**.
5. Haga clic en **Add** en **Status Code Cache Age**.

Add Cache Rule

i To configure the status code cache age for domain names with special configurations, submit a service ticket.

* Status Code

* Cache Age seconds ▼

OK Cancel

Parámetro	Descripción	Ejemplo
Status Code	Código de estado que se almacenará en caché.	404
Cache Age	Duración para almacenar en caché los códigos de estado en los nodos CDN. <ul style="list-style-type: none"> ● Si se establece en 0, el código de estado no se almacena en caché. ● El valor máximo es de 365 días. 	3 días

6. Configure los parámetros y haga clic en **OK**.

Ejemplos

Supongamos que ha configurado las siguientes reglas de caché de código de estado para el nombre de dominio `www.example.com`:

Status Code Cache Age

You can customize the duration for caching status codes returned by the origin server on CDN nodes, reducing the retrieval ratio and relieving the pressure on the origin server. [Learn more](#)

Add

Status Code	Cache Age
404	30 days

Result: Cuando un usuario accede a un recurso que no está almacenado en caché en un nodo CDN, el nodo CDN recupera los recursos del servidor de origen. Sin embargo, el servidor de origen ha eliminado el recurso y devuelve un código de estado 404. La CDN transmite de forma transparente el código de estado al usuario y almacena en caché el código de estado en el nodo de CDN. Durante el período de validez del caché (30 días), cuando el usuario accede nuevamente al recurso, la CDN devuelve directamente el código de estado 404 al usuario sin volver al origen, lo que reduce la presión en el sitio de origen.

2.6 Control de acceso

2.6.1 Descripción general

Puede configurar la validación de referencia, la lista negra y la lista blanca de direcciones IP, la lista negra y la lista blanca de agentes de usuario y la autenticación de URL para identificar y filtrar usuarios no autorizados y mejorar la seguridad de la CDN.

Función	Descripción
Configuración de la validación de referencia	En este tema se describe cómo configurar una lista negra o una lista blanca de referencias. Los usuarios son identificados y filtrados de acuerdo con las políticas de filtro configuradas, con el fin de controlar las fuentes de acceso.
Configuración de una ACL	Esta sección describe cómo configurar una ACL. Al establecer una política de filtrado, puede filtrar solicitudes de direcciones IP específicas para restringir el acceso.
Configuración de una lista negra o una lista blanca de User-Agent	Esta sección describe cómo configurar el filtrado User-Agent para restringir el acceso.
Configuración de la firma de URL	Esta sección describe cómo configurar la autenticación de URL para proteger los recursos del sitio web de los usuarios malintencionados.

2.6.2 Configuración de la validación de referencia

En este tema se describe cómo configurar una lista negra o una lista blanca de referencias. Los usuarios son identificados y filtrados de acuerdo con las políticas de filtro configuradas, con el fin de controlar las fuentes de acceso.

Fondo

El campo de referencia en un encabezado de solicitud HTTP identifica la dirección de la página web desde la que se ha solicitado el recurso. Los nodos CDN pueden usar el campo de referencia para rastrear e identificar la fuente.

Cuando se reciben solicitudes de acceso de los usuarios, los nodos CDN identifican y comprueban a los usuarios con respecto a la lista negra o la lista blanca de referencia. Solo los usuarios que cumplan con los requisitos de listas negras y blancas pueden acceder al contenido. Los usuarios no calificados recibirán una respuesta de error 403.

Procedimiento

1. Inicie sesión en la **consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control**.

- En el área **Referer Validation**, haga clic en **Edit**. Aparece el cuadro de diálogo **Configure Referer Validation**.

- Active **Status** para habilitar este elemento de configuración.
- Seleccione un valor para **Type** y establezca parámetros de referencia en función de los requisitos de servicio. La tabla siguiente describe los parámetros.

Parámetro	Descripción	Regla de llenado
Include blank referer	Un referente en blanco es cuando el campo de referencia en una solicitud HTTP se deja en blanco o cuando una solicitud HTTP no contiene el campo de referencia. Si se selecciona esta opción, dichas solicitudes también se filtrarán en función de las listas blancas y negras configuradas.	/

Parámetro	Descripción	Regla de llenado
Referer whitelist	<ul style="list-style-type: none"> ● Si el campo de referencia de una solicitud de acceso coincide con las reglas de la lista blanca, el solicitante puede acceder al contenido solicitado. De lo contrario, CDN devuelve un código de respuesta de error 403, que indica que el acceso está prohibido. ● Si se selecciona Include blank referer y una solicitud de acceso contiene una referencia en blanco, el solicitante puede acceder al contenido solicitado. 	<ul style="list-style-type: none"> ● Introducir nombres de dominio o direcciones IP separadas por punto y coma (;). ● Se admiten nombres de dominio carácter comodín. ● Se admiten nombres de dominio con puertos. El número máximo de puerto es 65535. ● Ingrese hasta 400 nombres de dominio y direcciones IP. Ejemplo www.example.com:443;*.test.com;192.168.0.0
Referer blacklist	<ul style="list-style-type: none"> ● Si el campo de referencia en una solicitud de acceso coincide con las reglas de la lista negra, el solicitante no puede acceder al contenido solicitado, y 403 Forbidden será devuelto. De lo contrario, el solicitante puede acceder al contenido solicitado. ● Si se selecciona Include blank referer y una solicitud de acceso contiene una referencia en blanco, se rechazará la solicitud de acceso y se devolverá 403 Forbidden. 	<ul style="list-style-type: none"> ● Introducir nombres de dominio o direcciones IP separadas por punto y coma (;). ● Se admiten nombres de dominio carácter comodín. ● Se admiten nombres de dominio con puertos. El número máximo de puerto es 65535. ● Ingrese hasta 400 nombres de dominio y direcciones IP. Ejemplo www.example.com:443;*.test.com;192.168.0.0

8. En el cuadro de texto **Rule**, escriba los nombres de dominio.
9. Haga clic en **OK**.

Ejemplos

1. Supongamos que se configura una lista blanca de referencia **www.test.com** para el nombre de dominio **www.example.com** y que se selecciona **Include blank referer**.

Configure Referer Validation

Status

* Type Referer blacklist Referer whitelist

Include blank referer ?

* Rule

OK Cancel

- Si el usuario 1 solicita la URL **https://www.example.com/file.html** y el valor del campo de referencia en la solicitud está en blanco, CDN devuelve el contenido.
 - Si el usuario 2 solicita la URL **https://www.example.com/file.html** y el valor del campo de referencia en la solicitud es **www.test.com**, la CDN devuelve el contenido.
 - Si el usuario 3 solicita la URL **https://www.example.com/file.html** y el valor del campo de referencia en la solicitud es de **www.abc.com**, la CDN devuelve un código de respuesta de error 403.
2. Supongamos que se configura un **www.test01.com** de lista negra de referencia para el nombre de dominio **www.example01.com** y que se selecciona **Include blank referer**.

Configure Referer Validation

Status

* Type Referer blacklist Referer whitelist

Include blank referer ?

* Rule

OK Cancel

- Si el usuario 1 solicita el **https://www.example01.com/file.html** de URL y el valor del campo de referencia en la solicitud está en blanco, CDN devuelve un código de respuesta de error 403.

- Si el usuario 2 solicita la URL **https://www.example01.com/file.html** y el valor del campo de referencia en la solicitud es de **www.test01.com**, la CDN devuelve un código de respuesta de error 403.
- Si el usuario 3 solicita la URL **https://www.example01.com/file.html** y el valor del campo de referencia en la solicitud es **www.bcd.com**, la CDN devuelve el contenido.

2.6.3 Configuración de una ACL

En este tema se describe cómo configurar una ACL. Puede establecer una política de filtrado para filtrar las solicitudes de direcciones IP específicas para restringir el acceso y evitar el robo de contenido y los ataques.

Procedimiento

1. Inicie sesión en la **consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control**.
5. En el área **ACL**, haga clic en **Edit**. Aparece el cuadro de diálogo **Configure ACL**.

Configure ACL

1. Up to 150 blacklisted or whitelisted IP addresses and subnets are supported. Enter one IP address or subnet on each row.
2. Only 8, 16, 24 and 32 bit subnet masks are supported.
3. The IP address portion of the subnet must be the first IP address on that block.
4. Multiple duplicate IP/IP segments are combined into one.
5. Wildcards are not supported.
6. IPv6 addresses are allowed.

Status

* Type IP address blacklist IP address whitelist

* Rule

OK Cancel

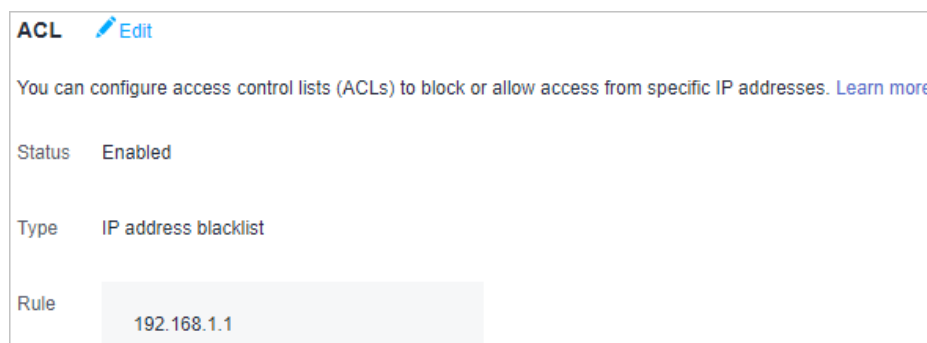
6. Active **Status** para habilitar este elemento de configuración.
7. Seleccione un tipo e introduzca reglas.

Parámetro	Descripción
Type	<ul style="list-style-type: none"> ● IP address blacklist: Si la dirección IP de un usuario está incluida en la lista negra de direcciones IP, el código de estado 403 se devolverá cuando el usuario acceda a un nodo CDN. ● IP address whitelist: Si la dirección IP de un usuario no está incluida en la lista blanca de direcciones IP, el código de estado 403 se devolverá cuando el usuario acceda a un nodo CDN. <p>NOTA</p> <ul style="list-style-type: none"> ● Puede configurarse una lista negra de direcciones IP o una lista blanca de direcciones IP.
Rule	<ul style="list-style-type: none"> ● Se admiten hasta 150 direcciones IP o subredes. Ingrese una dirección IP o subred en cada fila. ● Sólo se admiten máscaras de subred de 8, 16, 24 y 32 bits. ● La parte de la dirección IP de la subred debe ser la primera dirección IP de ese bloque. ● Se eliminarán las direcciones IP duplicadas y los segmentos de dirección IP. ● No se admiten comodines, por ejemplo, 192.168.0.*. ● Se permiten direcciones IPv6.

8. Haga clic en **OK**.

Ejemplos

Supongamos que ha configurado la siguiente ACL para el nombre de dominio **www.example.com**:



- Un usuario solicita **http://www.example.com/abc.jpg**. La dirección IP del cliente de usuario 192.168.1.1 se incluye en la lista negra, por lo que se devuelve el código de error 403.
- Un usuario solicita **http://www.example.com/abc.jpg**. La dirección IP del cliente del usuario 192.168.1.3 no está incluida en la lista negra, por lo que se devuelve el contenido solicitado.

2.6.4 Configuración de una lista negra o una lista blanca de User-Agent

Puede configurar una lista negra o blanca de User-Agent para su nombre de dominio para identificar y filtrar a los visitantes y mejorar la seguridad del nombre de dominio.

Fondo

Puede configurar una lista negra o blanca de User-Agent para filtrar las solicitudes a su nombre de dominio basándose en el campo User-Agent.

Lista negra: las solicitudes que incluyen campos en la lista negra no pueden acceder al contenido y 403 serán devueltos.

Lista blanca: Solo las solicitudes que incluyan campos en la lista blanca pueden acceder al contenido. Otras solicitudes fallarán y 403 serán devueltas.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control**.
5. En el área **User-Agent Access Control**, haga clic en **Edit**. Aparece el cuadro de diálogo **Configure User-Agent Access Control**.

Configure User-Agent Access Control

Status

* Type Blacklist Whitelist

You can configure either a blacklist or whitelist for your domain name.

* Rule

Only wildcard characters (*) can be used for regular expression matching. If no wildcard character is specified, exact matching will be performed. Enter up to 10 rules and enter them on separate rows.

OK Cancel

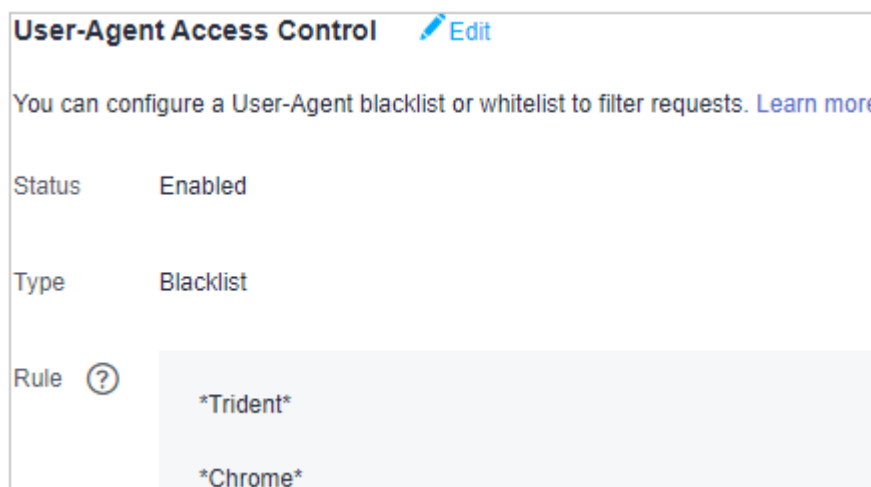
6. Active **Status**.
7. Seleccione un tipo e introduzca reglas.

Parámetro	Descripción
Type	<ul style="list-style-type: none"> ● Blacklist: Las solicitudes que incluyen campos en la lista negra no pueden acceder al contenido. ● Whitelist: Solo las solicitudes que incluyan campos en la lista blanca pueden acceder al contenido.
Rule	<ul style="list-style-type: none"> ● Solo se permiten letras, números, espacios y los siguientes caracteres especiales: *._- ();/. ● Sólo se pueden utilizar caracteres comodín (*) para la coincidencia de expresiones regulares. Si no se incluye ningún carácter comodín, se usará una coincidencia exacta. ● Ingrese hasta 100 caracteres para una regla. ● Ingrese hasta 10 reglas e introdúzcalas en filas separadas.

8. Haga clic en **OK**.

Ejemplos

Supongamos que ha configurado la siguiente lista negra del agente de usuario para el nombre de dominio **www.example.com**:



Si **User-Agent** en el encabezado de una solicitud HTTP es uno de los siguientes:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0)
like Gecko
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/95.0.4638.54 Safari/537.36
```

Trident o **Chrome** se incluyen en la lista negra, por lo que se devuelve 403.

2.6.5 Configuración de la firma de URL

2.6.5.1 Método de firma A

Por defecto, los recursos públicos son distribuidos por CDN. La firma de URL protege estos recursos de ser descargados y robados por usuarios malintencionados. Huawei Cloud CDN proporciona cuatro métodos de firma de URL. En este tema se describe el método de firma A.

NOTA

- Si su nombre de dominio tiene configuraciones especiales, no se puede configurar la firma de URL para este nombre de dominio en la consola de CDN.
- Cuando se configura la firma de URL, las solicitudes de usuario incluirán parámetros de autenticación. Si **Ignore specific parameters** no está configurado:
 - La recuperación de contenido se volverá frecuente.
 - Si su servidor de origen es un bucket OBS, se incurrirán en tarifas por el tráfico saliente del bucket.

Cómo funciona

Una URL firmada de ejemplo se ve así:

```
http://DomainName/Filename?auth_key=timestamp-rand-uid-md5hash
http://DomainName/Filename?auth_key=timestamp-rand-uid-sha256
```

En la siguiente tabla se describen los parámetros de una dirección URL firmada.

Parámetro	Descripción
DomainName	Nombre de dominio de aceleración.
timestamp	Hora de inicio de una solicitud válida. El valor es el número total de segundos que han transcurrido desde las 00:00:00 del 1 de enero de 1970. Es un entero decimal.
Validity Period	Cuánto tiempo permanece efectiva una URL firmada. El valor oscila entre 0s y 31,536,000s. Ejemplo: Si el período de validez se establece en 1800s, los usuarios pueden acceder a CDN dentro de 1800s desde la hora indicada por timestamp . La autenticación falla y la URL es inaccesible si los usuarios acceden a CDN 1800s más tarde.
rand	Número aleatorio. El valor recomendado es un UUID, que no puede contener guiones (-) por ejemplo, 202cb962ac59075b964b07152d234b70 .
uid	ID de usuario. Este parámetro no se utiliza ahora. Puede establecerlo en 0 .
md5hash	Una cadena de 32 caracteres calculada usando el algoritmo MD5. La cadena consta de dígitos (0 a 9) y letras minúsculas.
sha256	Una cadena de 32 caracteres calculada usando el algoritmo SHA256. La cadena consta de dígitos y letras minúsculas.
Filename	Back-to-origin URL. Su valor debe comenzar con una barra diagonal (/) y no incluye los parámetros que siguen al signo de interrogación (?).

Parámetro	Descripción
PrivateKey	Clave de firma, que se utiliza para generar una URL firmada, por ejemplo, huaweicloud123. La tecla contiene de 6 a 32 caracteres y solo puede contener letras y dígitos.
Authentication Parameter	Parámetro de autenticación incluido en una URL. El valor predeterminado es auth_key .

Método de verificación

Después de recibir una solicitud, un nodo CDN verifica la solicitud de la siguiente manera:

1. Comprueba si los parámetros de autenticación están incluidos en la solicitud. Si no es así, la solicitud se considera inválida y se devuelve un código de error HTTP 403.
2. Comprueba si la hora actual del sistema está dentro del rango [marca de tiempo, marca de tiempo + período válido]. Si el tiempo de sistema actual excede el intervalo, el nodo CDN considera que la solicitud expira y devuelve un código de error HTTP 403. Si el tiempo actual del sistema está dentro del intervalo, continúa el siguiente paso.
3. Construye una cadena de caracteres, calcula **HashValue** con la cadena usando el algoritmo MD5 y SHA256, y compara **HashValue** con el valor **md5hash** o **sha256** en la solicitud. Si el valor **md5hash** o **sha256** es el mismo que **HashValue**, la autenticación se realiza correctamente y se devuelve un archivo. De lo contrario, la autenticación falla y se devuelve un código de error HTTP 403. **HashValue** se calcula de la siguiente manera:

```
sstring = "Filename-Timestamp-rand-uid-PrivateKey"
HashValue = md5sum(sstring)
```

O

```
sstring = "Filename-Timestamp-rand-uid-PrivateKey"
HashValue = sha256sum(sstring)
```

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control** y haga clic en **Sign URL**.

Sign URL

Status

Signing Method Method A Method B Method C1 Method C2

Signed URL example:
 http://hwcdn.example.com/test/1.jpg?auth_key=1498752000-0-0-40e64d69aac7d15edfc6ec8a080042cb [Learn more](#)

Signing Key
 Enter 6 to 32 characters. Only letters and digits are allowed. [Automatically Generate](#)

Encryption Algorithm MD5 SHA256

Time Format **Decimal**

Validity Period (s)

OK Cancel

5. Establezca los parámetros de acuerdo con la siguiente tabla y haga clic en **OK**.

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos.
Encryption Algorithm	MD5 o SHA256 .
Validity Period (s)	Cuánto tiempo permanece efectiva la URL firmada. El valor oscila entre 0s y 31,536,000s.

URL Signing Calculator

Con URL signing calculator, puede generar una URL firmada para los usuarios. Establezca los parámetros según [Tabla 2-6](#), y haga clic en **Generate** para generar una URL firmada que caducará en un momento específico.

URL Signing Calculator

Signing Method Method A Method B Method C1 Method C2

Signing Key
Enter 6 to 32 characters. Only letters and digits are allowed. [Automatically Generate](#)

Access Path

Encryption Algorithm MD5 SHA256

Start Time

Time Format

Validity Period (s)

Signed URL `http://www...om/test?auth_key=1638762163-2ee4991dcf95460fb94800283ec548a3-0-225443abb6d0c7e0389a967d8c8d021a`

Expires `Dec 06, 2021 12:12:43 GMT+08:00`

NOTA

Escapar caracteres especiales en la URL firmada si hay alguno.

Tabla 2-6 Descripción del parámetro

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos. El valor debe ser el mismo que la clave de firma especificada en la configuración de firma de URL.
Access Path	Ruta de acceso del contenido, que comienza con una barra diagonal (/) y no lleva una cadena de consulta.
Encryption Algorithm	MD5 o SHA256 .
Start Time	Hora en la que la URL firmada tendrá efecto.
Validity Period (s)	Cuánto tiempo permanece efectiva la URL firmada. El valor oscila entre 0s y 31,536,000s. Si este valor es mayor que el período de validez establecido en la configuración de firma de URL, se utilizará este último. Ejemplo: Si establece este parámetro en 2000s, pero el período de validez establecido en la configuración de firma de URL es 1800s, el período de validez de las URL firmadas será 1800s.

Ejemplo

A continuación se utiliza el algoritmo MD5 como ejemplo:

1. Supongamos que la URL de regreso al origen es la siguiente:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Establecer **PrivateKey** en **huaweicloud123**.
3. La autenticación tiene efecto desde las 00:00:00 del 30 de junio de 2017. **Timestamp** es **1498752000**. Establezca el período de validez en 1800s.
4. El nodo de CDN construye una cadena para calcular las **HashValue**.
`/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3-1498752000-0-0-huaweicloud123`
5. El nodo CDN calcula **HashValue** de acuerdo con la cadena de caracteres con signo.
`HashValue = md5sum("/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3-1498752000-0-0-huaweicloud123") =
40e64d69aac7d15edfc6ec8a080042cb`
6. La URL de solicitud es la siguiente:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3?
auth_key=1498752000-0-0-40e64d69aac7d15edfc6ec8a080042cb`

Si la solicitud se encuentra dentro del período de validez , (desde las 00:00:00 del 30 de Junio de 2017 hasta las 00:30:00 del 30 de Junio de 2017) y el **HashValue** calculado es el mismo que el valor de **md5hash** (40e64d69aac7d15edfc6ec8a080042cb) llevado en la solicitud, la autenticación se realiza correctamente.

2.6.5.2 Método de firma B

Por defecto, los recursos públicos son distribuidos por CDN. La firma de URL protege estos recursos de ser descargados y robados por usuarios malintencionados. Huawei Cloud CDN proporciona cuatro métodos de firma de URL. En este tema se describe el método de firma B.

NOTA

- Si su nombre de dominio tiene configuraciones especiales, no se puede configurar la firma de URL para este nombre de dominio en la consola de CDN.
- Cuando se configura la firma de URL, las solicitudes de usuario incluirán parámetros de autenticación. Si **Ignore specific parameters** no está configurado:
 - La recuperación de contenido se volverá frecuente.
 - Si su servidor de origen es un bucket OBS, se incurrirán en tarifas por el tráfico saliente del bucket.

Cómo funciona

Una URL firmada de ejemplo se ve así:

```
http://DomainName/timestamp/sha256/FileName
```

```
http://DomainName/timestamp/md5hash/FileName
```

Si la autenticación se realiza correctamente, la back-to-origin URL es:

```
http://DomainName/FileName
```

En la siguiente tabla se describen los parámetros de una dirección URL firmada.

Parámetro	Descripción
DomainName	Nombre de dominio de aceleración.
timestamp	Hora de inicio de una solicitud válida. Está en el formato de YYYYMMDDHHMM, por ejemplo, 201706301000.
Validity Period	Cuánto tiempo permanece efectiva una URL firmada. El valor oscila entre 0s y 31,536,000s. Ejemplo: Si el período de validez se establece en 1800s y timestamp es 201706301000 , la URL caduca a las 10:30:00 a.m. el 30 de junio de 2017.
md5hash	Una cadena de 32 caracteres calculada usando el algoritmo MD5. La cadena consta de dígitos (0 a 9) y letras minúsculas.
sha256	Una cadena de 32 caracteres calculada usando el algoritmo SHA256. La cadena consta de dígitos y letras minúsculas.
Filename	Back-to-origin URL. Su valor debe comenzar con una barra diagonal (/) y no incluye los parámetros que siguen al signo de interrogación (?).
PrivateKey	Clave de firma, que se utiliza para generar una URL firmada, por ejemplo, huaweicloud123. La tecla contiene de 6 a 32 caracteres y solo puede contener letras y dígitos.

Método de verificación

Después de recibir una solicitud, un nodo CDN verifica la solicitud de la siguiente manera:

1. Comprueba si los parámetros de autenticación están incluidos en la solicitud. Si no es así, la solicitud se considera inválida y se devuelve un código de error HTTP 403.
2. Comprueba si la hora actual del sistema está dentro del rango [marca de tiempo, marca de tiempo + período válido]. Si el tiempo de sistema actual excede el intervalo, el nodo CDN considera que la solicitud expira y devuelve un código de error HTTP 403. Si el tiempo actual del sistema está dentro del intervalo, continúa el siguiente paso.
3. Construye una cadena de caracteres, calcula **HashValue** con la cadena usando el algoritmo MD5 y SHA256, y compara **HashValue** con el valor **md5hash** o **sha256** en la solicitud. Si el valor **md5hash** o **sha256** es el mismo que **HashValue**, la autenticación se realiza correctamente y se devuelve un archivo. De lo contrario, la autenticación falla y se devuelve un código de error HTTP 403. **HashValue** se calcula de la siguiente manera:

```
sstring = "PrivateKeytimestampFilename"
HashValue = sha256sum(sstring)
```

O

```
sstring = "PrivateKeytimestampFilename"
HashValue = md5sum(sstring)
```

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.

2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control** y haga clic en **Sign URL**.

5. Establezca los parámetros de acuerdo con la siguiente tabla y haga clic en **OK**.

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos.
Encryption Algorithm	MD5 o SHA256 .
Validity Period (s)	Cuánto tiempo permanece efectiva una URL firmada. El valor oscila entre 0s y 31,536,000s.

URL Signing Calculator

Con URL signing calculator, puede generar una URL firmada para los usuarios. Establezca los parámetros según [Tabla 2-7](#), y haga clic en **Generate** para generar una URL firmada que caducará en un momento específico.

URL Signing Calculator

Signing Method Method A Method B Method C1 Method C2

Signing Key
Enter 6 to 32 characters. Only letters and digits are allowed. [Automatically Generate](#)

Access Path

Encryption Algorithm MD5 SHA256

Start Time

Time Format

Validity Period (s)

Signed URL `http://www. .com/202112061142/7c21604fbacd9f99f830674e83c5743e/test`

Expires `Dec 06, 2021 12:12:43 GMT+08:00`

Tabla 2-7 Descripción del parámetro

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos. El valor debe ser el mismo que la clave de firma especificada en la configuración de firma de URL.
Access Path	Ruta de acceso del contenido, que comienza con una barra diagonal (/) y no lleva una cadena de consulta.
Encryption Algorithm	MD5 o SHA256 .
Start Time	Hora en la que la URL firmada tendrá efecto.
Validity Period (s)	Cuánto tiempo permanece efectiva la URL firmada. El valor oscila entre 0s y 31,536,000s. Si este valor es mayor que el período de validez establecido en la configuración de firma de URL, se utilizará este último. Ejemplo: Si establece este parámetro en 2000s, pero el período de validez establecido en la configuración de firma de URL es 1800s, el período de validez de las URL firmadas será 1800s.

 **NOTA**

Escapar caracteres especiales en la URL firmada si hay alguno.

Ejemplo

A continuación se utiliza el algoritmo MD5 como ejemplo:

1. Supongamos que la URL de regreso al origen es la siguiente:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Establecer **PrivateKey** en **huaweicloud123**.
3. **timestamp** es **201706301000**.
4. El nodo CDN construye una cadena para calcular **md5hash**.
`huaweicloud123201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
5. El nodo CDN calcula **md5hash** de acuerdo con la cadena de caracteres con signo.
`md5hash = md5sum("huaweicloud123201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3") = 51415b2256b64a9772a30edf69c00b08`
6. La URL de solicitud es:
`http://hwcdn.example.com/201706301000/51415b2256b64a9772a30edf69c00b08/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`

Si la solicitud se encuentra dentro del período de validez , (desde 10:00:00 el 30 de junio de 2017 hasta 10:30:00 el 30 de junio de 2017) y el **md5hash** calculado es el mismo que el valor de **md5hash** (51415b2256b64a9772a30edf69c00b08) transportado en la solicitud, la autenticación es satisfactoria.

2.6.5.3 Método de firma C1

Por defecto, los recursos públicos son distribuidos por CDN. La firma de URL protege estos recursos de ser descargados y robados por usuarios malintencionados. Huawei Cloud CDN proporciona cuatro métodos de firma de URL. En este tema se describe el método de firma C1.

 **NOTA**

- Si su nombre de dominio tiene configuraciones especiales, no se puede configurar la firma de URL para este nombre de dominio en la consola de CDN.
- Cuando se configura la firma de URL, las solicitudes de usuario incluirán parámetros de autenticación. Si **Ignore specific parameters** no está configurado:
 - La recuperación de contenido se volverá frecuente.
 - Si su servidor de origen es un bucket OBS, se incurrirán en tarifas por el tráfico saliente del bucket.

Cómo funciona

Una URL firmada de ejemplo se ve así:

```
http://DomainName/{<sha256>/{<timestamp>}/FileName
http://DomainName/{<md5hash>/{<timestamp>}/FileName
```

En la siguiente tabla se describen los parámetros de una dirección URL firmada.

Parámetro	Descripción
DomainName	Nombre de dominio de aceleración.

Parámetro	Descripción
timestamp	Hora de inicio de una solicitud válida. El valor es el número total de segundos que han transcurrido desde las 00:00:00 del 1 de enero de 1970. Es un entero hexadecimal.
Validity Period	Cuánto tiempo permanece efectiva una URL firmada. El valor oscila entre 0s y 31,536,000s. The default value is 1800s. Ejemplo: Si el período de validez se establece en 1800s, los usuarios pueden acceder a CDN dentro de 1800s desde la hora indicada por timestamp . La autenticación falla y la URL es inaccesible si los usuarios acceden a CDN 1800s más tarde.
md5hash	Una cadena de 32 caracteres calculada usando el algoritmo MD5. La cadena consta de dígitos (0 a 9) y letras minúsculas.
sha256	Una cadena de 32 caracteres calculada usando el algoritmo SHA256. La cadena consta de dígitos y letras minúsculas.
Filename	Back-to-origin URL. Su valor debe comenzar con una barra diagonal (/) y no incluye los parámetros que siguen al signo de interrogación (?).
PrivateKey	Clave de firma, que se utiliza para generar una URL firmada, por ejemplo, huaweicloud123. La tecla contiene de 6 a 32 caracteres y solo puede contener letras y dígitos.

Método de verificación

Después de recibir una solicitud, un nodo CDN verifica la solicitud de la siguiente manera:

1. Comprueba si los parámetros de autenticación están incluidos en la solicitud. Si no es así, la solicitud se considera inválida y se devuelve un código de error HTTP 403.
2. Comprueba si la hora actual del sistema está dentro del rango [marca de tiempo, marca de tiempo + período válido]. Si el tiempo de sistema actual excede el intervalo, el nodo CDN considera que la solicitud expira y devuelve un código de error HTTP 403. Si el tiempo actual del sistema está dentro del intervalo, continúa el siguiente paso.
3. Construye una cadena de caracteres, calcula **HashValue** con la cadena usando el algoritmo MD5 y SHA256, y compara **HashValue** con el valor **md5hash** o **sha256** en la solicitud. Si el valor **md5hash** o **sha256** es el mismo que **HashValue**, la autenticación se realiza correctamente y se devuelve un archivo. De lo contrario, la autenticación falla y se devuelve un código de error HTTP 403. **HashValue** se calcula de la siguiente manera:

```
sstring = "PrivateKey-Filename-Timestamp"
HashValue = md5sum(sstring)
```

O

```
sstring = "PrivateKey-Filename-Timestamp"
HashValue = sha256sum(sstring)
```

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.

2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control** y haga clic en **Sign URL**.

Sign URL

Status

Signing Method Method A Method B Method C1 Method C2

Signed URL example:
<http://hwcdn.example.com/aecf1b07f481bbb8122eef5cd52a4bc1/5955b0a0/test/1.jpg> [Learn more](#)

Signing Key
Enter 6 to 32 characters. Only letters and digits are allowed. [Automatically Generate](#)

Encryption Algorithm MD5 SHA256

Time Format Hexadecimal

Validity Period (s)

5. Establezca los parámetros de acuerdo con la siguiente tabla y haga clic en **OK**.

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos.
Encryption Algorithm	MD5 o SHA256 .
Validity Period (s)	Cuánto tiempo permanece efectiva la URL firmada. El valor oscila entre 0s y 31,536,000s.

URL Signing Calculator

Con URL signing calculator, puede generar una URL firmada para los usuarios. Establezca los parámetros según [Tabla 2-8](#), y haga clic en **Generate** para generar una URL firmada que caducará en un momento específico.

URL Signing Calculator

Signing Method Method A Method B Method C1 Method C2

Signing Key
Enter 6 to 32 characters. Only letters and digits are allowed. [Automatically Generate](#)

Access Path

Encryption Algorithm MD5 SHA256

Start Time

Time Format **Hexadecimal**

Validity Period (s)

Signed URL **http://ww[redacted].com/e2d6fa501a9544a9f00bb5334e4a25eb/61ad86b3/test**

Expires **Dec 06, 2021 12:12:43 GMT+08:00**

NOTA

Escapar caracteres especiales en la URL firmada si hay alguno.

Tabla 2-8 Descripción del parámetro

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos. El valor debe ser el mismo que la clave de firma especificada en la configuración de firma de URL.
Access Path	Ruta de acceso del contenido, que comienza con una barra diagonal (/) y no lleva una cadena de consulta.
Encryption Algorithm	MD5 o SHA256 .
Start Time	Hora en la que la URL firmada tendrá efecto.

Parámetro	Descripción
Validity Period (s)	<p>Cuánto tiempo permanece efectiva la URL firmada. El valor oscila entre 0s y 31,536,000s. Si este valor es mayor que el período de validez establecido en la configuración de firma de URL, se utilizará este último.</p> <p>Ejemplo: Si establece este parámetro en 2000s, pero el período de validez establecido en la configuración de firma de URL es 1800s, el período de validez de las URL firmadas será 1800s.</p>

Ejemplo

A continuación se utiliza el algoritmo MD5 como ejemplo:

- Supongamos que la URL de regreso al origen es la siguiente:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
- Establecer **PrivateKey** en **huaweicloud123**.
- La autenticación entra en vigor desde las 10:00:00 del 30 de junio de 2017. **Timestamp** es **5955b0a0**. Establezca el período de validez en 1800s.
- El nodo CDN construye una cadena para calcular **md5hash**.
`huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0`
- El nodo CDN calcula **md5hash** de acuerdo con la cadena de caracteres con signo.
`md5hash = md5sum(huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0) = aecf1b07f481bbb8122eef5cd52a4bc1`
- La URL de solicitud es:
`http://hwcdn.example.com/aecf1b07f481bbb8122eef5cd52a4bc1/5955b0a0/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`

Si la solicitud se encuentra dentro del período de validez, (desde 10:00:00 el 30 de junio de 2017 hasta 10:30:00 el 30 de junio de 2017) y el **md5hash** calculado es el mismo que el valor **md5hash** (aecf1b07f481bbb8122eef5cd52a4bc1) transportado en la solicitud, la autenticación se realiza correctamente.

2.6.5.4 Método de firma C2

Por defecto, los recursos públicos son distribuidos por CDN. La firma de URL protege estos recursos de ser descargados y robados por usuarios malintencionados. Huawei Cloud CDN proporciona cuatro métodos de firma de URL. En este tema se describe el método de firma C2.

NOTA

- Si su nombre de dominio tiene configuraciones especiales, no se puede configurar la firma de URL para este nombre de dominio en la consola de CDN.
- Cuando se configura la firma de URL, las solicitudes de usuario incluirán parámetros de autenticación. Si **Ignore specific parameters** no está configurado:
 - La recuperación de contenido se volverá frecuente.
 - Si su servidor de origen es un bucket OBS, se incurrirán en tarifas por el tráfico saliente del bucket.

Cómo funciona

Una URL firmada de ejemplo se ve así:

```
http://DomainName/FileName?auth_key=<sha256>&timestamp=<timestamp>
http://DomainName/FileName?auth_key=<md5hash>&timestamp=<timestamp>
```

En la siguiente tabla se describen los parámetros de una dirección URL firmada.

Parámetro	Descripción
DomainName	Nombre de dominio de aceleración.
timestamp	Hora de inicio de una solicitud válida. El valor es el número total de segundos que han transcurrido desde las 00:00:00 del 1 de enero de 1970. Es un entero decimal o hexadecimal.
Validity Period	Cuánto tiempo permanece efectiva una URL firmada. El valor oscila entre 0s y 31,536,000s. El valor predeterminado es 1800s. Ejemplo: Si el período de validez se establece en 1800s, los usuarios pueden acceder a CDN dentro de 1800s desde la hora indicada por timestamp . La autenticación falla y la URL es inaccesible si los usuarios acceden a CDN 1800s más tarde.
md5hash	Una cadena de 32 caracteres calculada usando el algoritmo MD5. La cadena consta de dígitos (0 a 9) y letras minúsculas.
sha256	Una cadena de 32 caracteres calculada usando el algoritmo SHA256. La cadena consta de dígitos y letras minúsculas.
Filename	URL de regreso al origen. Su valor debe comenzar con una barra diagonal (/) y no incluye los parámetros que siguen al signo de interrogación (?).
PrivateKey	Clave de firma, que se utiliza para generar una URL firmada, por ejemplo, huaweicloud123. La clave contiene de 6 a 32 caracteres y solo puede contener letras y dígitos.
Authentication Parameter	Parámetro de autenticación incluido en una URL. El valor predeterminado es auth_key .
Timestamp	Nombre del parámetro de marca de tiempo incluido en la URL de solicitud.

Método de verificación

Después de recibir una solicitud, un nodo CDN verifica la solicitud de la siguiente manera:

1. Comprueba si los parámetros de autenticación están incluidos en la solicitud. Si no es así, la solicitud se considera inválida y se devuelve un código de error HTTP 403.
2. Comprueba si la hora actual del sistema está dentro del rango [marca de tiempo, marca de tiempo + período válido]. Si el tiempo de sistema actual excede el intervalo, el nodo CDN considera que la solicitud expira y devuelve un código de error HTTP 403. Si el tiempo actual del sistema está dentro del intervalo, continúa el siguiente paso.
3. Construye una cadena de caracteres, calcula **HashValue** con la cadena usando el algoritmo MD5 y SHA256, y compara **HashValue** con el valor **md5hash** o **sha256** en la

solicitud. Si el valor **md5hash** o **sha256** es el mismo que **HashValue**, la autenticación se realiza correctamente y se devuelve un archivo. De lo contrario, la autenticación falla y se devuelve un código de error HTTP 403. **HashValue** se calcula de la siguiente manera:

```
sstring = "PrivateKey-Filename-Timestamp"
HashValue = md5sum(sstring)
```

O

```
sstring = "PrivateKey-Filename-Timestamp"
HashValue = sha256sum(sstring)
```

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control** y haga clic en **Sign URL**.

5. Establezca los parámetros de acuerdo con la siguiente tabla y haga clic en **OK**.

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos.
Time Format	Formato de la hora en la URL firmada.
Encryption Algorithm	MD5 o SHA256 .

Parámetro	Descripción
Validity Period (s)	Cuánto tiempo permanece efectiva la URL firmada. El valor oscila entre 0s y 31,536,000s.

URL Signing Calculator

Con URL signing calculator, puede generar una URL firmada para los usuarios. Establezca los parámetros según **Método de firma C2**, y haga clic en **Generate** para generar una URL firmada que caducará en un momento específico.

URL Signing Calculator

Signing Method Method A Method B Method C1 Method C2

Signing Key
Enter 6 to 32 characters. Only letters and digits are allowed. [Automatically Generate](#)

Access Path

Encryption Algorithm MD5 SHA256

Start Time

Time Format Decimal Hexadecimal

Validity Period (s)

Signed URL `http://www. :?auth_key=4c80143fc4da3076c56d77f8427b3883×tamp=1638762163`

Expires Dec 06, 2021 12:12:43 GMT+08:00

NOTA

Escapar caracteres especiales en la URL firmada si hay alguno.

Tabla 2-9 Descripción del parámetro

Parámetro	Descripción
Signing Key	Contraseña de autenticación. Introduzca de 6 a 32 caracteres. Solo se permiten letras y dígitos. El valor debe ser el mismo que la clave de firma especificada en la configuración de firma de URL.
Access Path	Ruta de acceso del contenido, que comienza con una barra diagonal (/) y no lleva una cadena de consulta.
Encryption Algorithm	MD5 o SHA256 .

Parámetro	Descripción
Start Time	Hora en la que la URL firmada tendrá efecto.
Time Format	Formato de la hora en la URL firmada. Formato de hora de la URL firmada, que debe ser el mismo que el especificado en la configuración de firma de URL.
Validity Period (s)	Cuánto tiempo permanece efectiva la URL firmada. El valor oscila entre 0s y 31,536,000s. Si este valor es mayor que el período de validez establecido en la configuración de firma de URL, se utilizará este último. Ejemplo: Si establece este parámetro en 2000s, pero el período de validez establecido en la configuración de firma de URL es 1800s, el período de validez de las URL firmadas será 1800s.

Ejemplo

A continuación se utiliza el algoritmo MD5 como ejemplo:

- Supongamos que la URL de regreso al origen es la siguiente:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
- Establecer **PrivateKey** en **huaweicloud123**.
- La autenticación entra en vigor desde las 10:00:00 del 30 de junio de 2017. **Timestamp** es **5955b0a0**. Establezca el período de validez en 1800s.
- El nodo CDN construye una cadena para calcular **md5hash**.
`huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0`
- El nodo CDN calcula **md5hash** de acuerdo con la cadena de caracteres con signo.
`md5hash = md5sum(huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0) = aecf1b07f481bbb8122eef5cd52a4bc1`
- La URL de solicitud es:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3?auth_key=aecf1b07f481bbb8122eef5cd52a4bc1×tamp=5955b0a0`

Si la solicitud se encuentra dentro del período de validez , (desde 10:00:00 el 30 de junio de 2017 hasta 10:30:00 el 30 de junio de 2017) y el **md5hash** calculado es el mismo que el valor **md5hash** (aecf1b07f481bbb8122eef5cd52a4bc1) transportado en la solicitud, la autenticación se realiza correctamente.

2.6.6 Configuración de la autenticación remota

Huawei Cloud CDN admite autenticación remota. Cuando un usuario solicita un recurso desde un nodo de CDN, CDN reenvía la solicitud de usuario a un servidor de autenticación específico y determina si devolver el recurso al usuario basándose en el resultado devuelto por el servidor de autenticación.

Fondo

La autenticación remota es similar a la firma de URL. Las diferencias son las siguientes:

- Firma de URL: Los nodos CDN realizan la autenticación.
- Autenticación remota: los nodos CDN reenvían las solicitudes de usuario a un servidor de autenticación específico para la autenticación.

El proceso de autenticación remota es el siguiente.

Figura 2-6 Proceso de autenticación remota

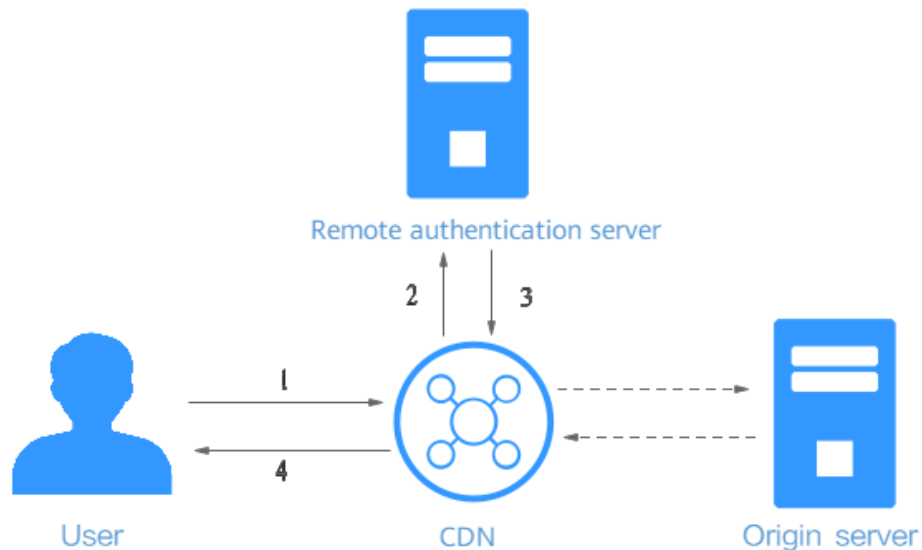


Tabla 2-10 Descripción del proceso

Paso	Descripción
1	Un usuario lleva parámetros de autenticación para acceder a un nodo de CDN.
2	CDN reenvía la solicitud a un servidor de autenticación remoto.
3	El servidor de autenticación remoto verifica la solicitud y devuelve un código de estado al nodo de CDN.
4	El nodo CDN determina si devolver el recurso solicitado al usuario basándose en el código de estado recibido.

Restricciones

Los nombres de dominio con configuraciones especiales no admiten autenticación remota.

Procedimiento

1. Inicie sesión en la **consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Access Control** y haga clic en **Remote Authentication**.

Figura 2-7 Configuración de la autenticación remota

Configure Remote Authentication

Status

* Authentication Server Address

* Request Method GET POST HEAD

* File Type All Specific

URL Signing Parameters

* Parameters to Retain All Specific None

Custom URL Signing Parameters	Type	Parameter	Value	Operation
<input type="button" value="+ Add"/>				

Request Header Authentication Parameters

* Request Headers to Retain All Specific None

Custom Request Header Authentication Parameters	Type	Parameter	Value	Operation
<input type="button" value="+ Add"/>				

Authentication Status Codes

* Success Status Code

* Failure Status Code

Action After Failure

* Custom Response Status Code

Authentication Timeout

* Timeout Interval ms

* Action After Timeout Accept Reject

Tabla 2-11 Parámetros

Parámetro	Descripción	Ejemplo
Authentication Server Address	Dirección IP de un servidor accesible. <ul style="list-style-type: none"> ● La dirección debe incluir http:// o https://. ● La dirección no puede ser una dirección local como localhost o 127.0.0.1. ● La dirección no puede ser un nombre de dominio de aceleración agregado en CDN. 	https://example.com/auth
Request Method	Método de solicitud admitido por el servidor de autenticación. GET, POST y HEAD son compatibles.	GET
File Type	<ul style="list-style-type: none"> ● All: Se autentican las solicitudes de todos los archivos. ● Specific: Requests for files of specific types are authenticated. Ejemplo: jpg MP4 ● Los tipos de archivo no distinguen entre mayúsculas y minúsculas. Por ejemplo, jpg y JPG indican el mismo tipo de archivo. Tipos de archivo separados por barras verticales (). 	All
Parameters to Retain	Parámetros que necesitan ser autenticados en las solicitudes de usuario. Puede conservar o ignorar todos los parámetros de URL o conservar parámetros de URL específicos. <ul style="list-style-type: none"> ● Los parámetros son insensibles a mayúsculas y minúsculas. Usa barras verticales () para separarlas. 	All
Custom URL Signing Parameters	Parámetros que se agregarán cuando los nodos CDN reenvían solicitudes de usuario al servidor de autenticación remoto. Puede seleccionar parámetros preestablecidos o personalizar parámetros (los parámetros y valores no distinguen entre mayúsculas y minúsculas).	Seleccione http_host . Valor: \$http_host .

Parámetro	Descripción	Ejemplo
Request Headers to Retain	Encabezados que se autenticarán en las solicitudes de usuario. Puede conservar o ignorar todos los encabezados de solicitud o conservar encabezados de solicitud específicos. Los encabezados son insensibles a mayúsculas y minúsculas. Usa barras verticales () para separarlas.	All
Custom Request Header Authentication Parameters	Los encabezados de solicitud que se agregarán cuando los nodos CDN reenvían las solicitudes de usuario al servidor de autenticación remoto. Puede seleccionar encabezados de solicitud preestablecidos o personalizar los encabezados de solicitud (los encabezados y los valores no distinguen entre mayúsculas y minúsculas).	Seleccione http_referer . Valor: \$http_referer .
Success Status Code	Código de estado devuelto por el servidor de autenticación remota a los nodos CDN cuando la autenticación se realiza correctamente. ● Rango de valores: 2xx y 3xx.	200
Código de estado de falla	Código de estado devuelto por el servidor de autenticación remota a los nodos CDN cuando la autenticación falla. ● Rango de valores: 4xx y 5xx.	403
Custom Response Status Code	Código de estado devuelto por los nodos CDN a los usuarios cuando la autenticación falla. ● Rango de valores: 2xx, 3xx, 4xx, y 5xx.	403
Timeout Interval	Duración desde el momento en que un nodo CDN reenvía una solicitud de autenticación al momento en que el nodo CDN recibe el resultado devuelto por el servidor de autenticación remoto. Introduzca 0 o un valor comprendido entre 50 y 3000. La unidad es milisegundo.	60

Parámetro	Descripción	Ejemplo
Action After Timeout	<p>Cómo los nodos CDN procesan una solicitud de usuario después de que la autenticación se agote.</p> <ul style="list-style-type: none"> ● Accept: Se aceptará la solicitud del usuario y se devolverá el recurso solicitado. ● Reject: Se rechazará la solicitud del usuario y se devolverá el código de estado de respuesta personalizado configurado. 	Reject

5. Configure los parámetros según se le solicite y haga clic en **OK**.

2.7 Configuración avanzada

2.7.1 Configuración de encabezado HTTP (solicitudes de origen cruzado)

Los encabezados HTTP forman parte de un mensaje de solicitud o respuesta HTTP que define los parámetros operativos de una transacción HTTP.

Si la configuración de encabezado HTTP está habilitada, puede agregar encabezados personalizados en los mensajes de respuesta devueltos al solicitante e implementar funciones como el uso compartido de recursos entre orígenes.

Precauciones

La configuración de encabezado HTTP es específica del nombre de dominio. Cuando una nueva configuración entra en vigor, los mensajes de respuesta se agregarán a los encabezados utilizados para cualquier recurso dentro de todo el dominio. Sin embargo, la configuración de encabezado HTTP solo afecta al comportamiento de respuesta de los clientes (navegadores). No afectan al comportamiento de la caché de los nodos CDN.

Fondo

Huawei Cloud CDN le permite personalizar los siguientes encabezados de respuesta HTTP:

- **Content-Disposition**

El encabezado Content-Disposition puede iniciar una descarga en el lado del cliente y especificar el nombre del archivo que se va a descargar.

Cuando un servidor envía un archivo a un navegador, siempre y cuando el formato de archivo sea compatible (por ejemplo, TXT o JPG), el archivo se abre mediante el navegador de forma predeterminada. Si el archivo debe tratarse como un archivo adjunto y guardarse con un nombre de archivo específico, puede utilizar el campo de encabezado Content-Disposition para especificar este requisito.

 **NOTA**

Si utiliza un bucket OBS creado después del 1 de enero de 2022 como servidor de origen y desea habilitar la vista previa en línea, establezca Content-Disposition en línea. Para obtener más información, consulte [¿Cómo previsualizo objetos en OBS a través de un explorador?](#)

- **Content-Language**

El encabezado Content-Language especifica el idioma o la combinación de idiomas preferidos del navegador. El contenido se puede personalizar para diferentes usuarios.

- **Access-Control-Allow-Origin**

El encabezado Access-Control-Allow-Origin incluye los nombres de dominio permitidos para CORS después de la autenticación del servidor. Para una solicitud CORS simple, el navegador determina si devolver el contenido de recursos solicitado al cliente basándose en este encabezado de mensaje. Para una solicitud de comprobación previa, el navegador determina si iniciar una solicitud CORS real al servidor basándose en este encabezado de mensaje.

 **NOTA**

Para evitar errores entre dominios causados por la caché del navegador, borre la caché del navegador después de configurar Access-Control-Allow-Origin.

- **Access-Control-Allow-Methods**

El encabezado Access-Control-Allow-Methods incluye los métodos que se permiten para el acceso CORS después de la autenticación del servidor. Para una solicitud CORS simple, el navegador determina si devolver el contenido de recursos solicitado al cliente basándose en este encabezado de mensaje. Para una solicitud de comprobación previa, el navegador determina si iniciar una solicitud CORS real al servidor basándose en este encabezado de mensaje.

- **Access-Control-Max-Age**

El encabezado Access-Control-Max-Age determina cuánto tiempo se pueden almacenar en caché los resultados de precomprobación para las solicitudes CORS permitidas por el servidor. El navegador determina la edad máxima de la caché para los resultados de la solicitud de comprobación previa basándose en este encabezado de mensaje. Mientras el periodo definido por esta cabecera no haya expirado, el navegador puede determinar si iniciar una solicitud CORS al servidor basándose en los resultados. Una vez que este periodo expira, el navegador debe enviar otra solicitud de comprobación previa al servidor.

- **Access-Control-Expose-Headers**

Access-Control-Expose-Headers especifica los encabezados de respuesta que el navegador puede exponer al cliente. Puede utilizar este campo para definir los encabezados de respuesta visibles para el cliente. Los siguientes encabezados de respuesta son visibles por defecto para el cliente: Cache-Control, Content-Language, Content-Type, Caduca, Last-Modified y Pragma.

- **Custom**

Si los encabezados de respuesta anteriores no pueden satisfacer sus necesidades, puede crear encabezados de respuesta. Un encabezado de respuesta personalizado puede contener de 1 a 100 caracteres, comenzando con una letra y constando de letras, dígitos y guiones (-).

Procedimiento

1. Inicie sesión en la [Consola de CDN](#).
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Advanced Settings**.
5. En el área **HTTP Header**, haga clic en **Edit**. Aparece el cuadro de diálogo **Configure HTTP Header**.

6. Haga clic en **Add** y seleccione una operación de encabezado de respuesta en la lista desplegable.

Operación del encabezado o de respuesta	Descripción
Set	<ul style="list-style-type: none"> ● Si el encabezado ya existe en la respuesta, el valor del encabezado que configure sobrescribirá el original. ● Si el encabezado no existe en la respuesta, el encabezado se agregará a la respuesta.
Delete	El encabezado se eliminará de la respuesta.

NOTA

- Algunos encabezados no se pueden establecer ni eliminar. Para más detalles, consulte [Restricciones](#).
 - Puede agregar hasta 10 configuraciones de encabezado de respuesta HTTP.
7. Establezca el parámetro y el valor del encabezado.

Parámetro	Descripción	Valor de ejemplo
Content-disposition	<p>Inicia una descarga en el lado del cliente y especifica el nombre del archivo que se va a descargar.</p> <p>Value requirements: Para una configuración típica, vea el ejemplo de la derecha.</p>	attachment;filename=FileName.xls

Parámetro	Descripción	Valor de ejemplo
Content-Language	Especifica el idioma de la página de respuesta del cliente. Value requirements: Para una configuración típica, vea el ejemplo de la derecha.	zh-CN en-US
Access-Control-Allow-Origin	Especifica las direcciones URL de dominio externo (origen de solicitud) a los que se permite acceder al recurso en el uso compartido de recursos entre orígenes (CORS). Value requirements: <ul style="list-style-type: none"> ● Ingrese hasta 256 caracteres para una URL. ● Una URL debe comenzar con http:// o https://. ● Si se establece en *, no se permiten direcciones URL después del comodín (*). 	Ejemplo 1: https:// www.example.com Ejemplo 2: * NOTA No se admiten nombres de dominio carácter comodín.
Access-Control-Allow-Methods	Especifica los métodos de solicitud HTTP que se pueden utilizar en una solicitud CORS. Value requirements: Se pueden configurar varios métodos al mismo tiempo. Separar con comas (,).	GET, POST, HEAD
Access-Control-Max-Age	Especifica cuánto tiempo se almacenarán en caché los resultados de la comprobación previa de las solicitudes CORS en recursos específicos. Value requirements: Este valor se expresa en segundos. El rango de valores es 1-1000000000.	86400
Access-Control-Expose-Headers	Especifica la información del encabezado de respuesta visible para el cliente para una solicitud CORS. Value requirements: Se pueden configurar varios encabezados al mismo tiempo. Separar con comas (,).	Content-Length, Content-Encoding

Parámetro	Descripción	Valor de ejemplo
Custom	Especifica el encabezado de respuesta personalizado para una solicitud CORS. Value requirements: Ingrese hasta 256 caracteres, que pueden contener letras, dígitos, espacios y caracteres especiales (. _ *#! %&+ ^-'"/:;=@?).	x-testcdn

- Haga clic en **OK**.

Restricciones

- Si su nombre de dominio tiene configuraciones especiales, no se pueden configurar Content-Type, Cache-Control, y Expires.
- Los siguientes encabezados de respuesta se pueden modificar pero no se pueden eliminar.

Content-Base	Content-Disposition
Server	Content-Language

- CDN no admite los siguientes encabezados de respuesta:

A_Dynamic	If-None-Match	Sec-WebSocket-Origin	X-Forward-Peer
Accept-Ranges	If-Range	Sec-WebSocket-Protocol	X-Forward-Type
Age	Keep-Alive	Sec-WebSocket-Version	X-Forward-Uri
Allow	Key	Set-Cookie	X-Forwarded-For
Authentication-Info	Last-Modified	Tcp-Retrans	X-IP-Region
Authorization	Link	Title	X-IP-Region-CN
X-Forward-Measured	Location	Transfer-Encoding	X-Ip-Blackwhite-List
Cdn-Qos	Max-Forwards	Upgrade	X-Local-Ip
Cdn-Server-Ip	Meter	Vary	X-Log-Url
Cdn-Src-Ip	Mime-Version	Via	X-MAA-Alias
Conf-Err-Host	Negotiate	WWW-Authenticate	X-MAA-Auth

Conf-File	Origin	Warning	X-Max-Conns
Conf-File-List	Partition-Block-Size	Ws-Hdr	X-Mem-Url
Conf-Option	Pragma	WsTag	X-Mgr-Traffic
Conf-Other	Proxy-Authenticate	X-Accelerator-Vary	X-Miss-Rate-Limit
Connection	Proxy-Authentication-Info	X-Appa	X-Miss-Times-Limit
Content-Encoding	Proxy-Authorization	X-Appa-Origin	X-No-Referer
Content-Length	Proxy-Connection	X-Black-List	X-Query-Key
Content-Location	Proxy-Support	X-Bwctrl-Limit	X-Rate-Limit
Content-MD5	Public	X-Bwctrl-Para	X-Refresh-Pattern
Content-Range	Purge-Domain	X-Cache	X-Request-Id
Sec-WebSocket-Nonce	Purge-Extra	X-Cache-2	X-Request-Uri
Date	Range	X-Cache-Lookup	X-Request-Url
Dynamic	Request-Range	X-Cacheable	X-Resp-Time
Etag	Retry-After	X-Cdn-Src-Port	X-Rewrite-Url
Error	Sec-WebSocket-Accept	X-Client-Ip	X-Squid-Error
Expect	Sec-WebSocket-Draft	X-DNS-Time	X-Times-Limit
If-Modified-Since	Sec-WebSocket-Extensions	X-Denyattack-Dynconf	X-Url-Blackwhite-List
From	Sec-WebSocket-Key	X-Error-Status	X-Via-CDN
Front-End-Https	Sec-WebSocket-Key1	X-Error-URL	X-White-List
Host	Sec-WebSocket-Key2	X-Forward-Host	-
If-Match	Sec-WebSocket-Location	X-Forward-Ip	-

2.7.2 Páginas de error personalizadas

Cuando se informa de un error durante el acceso del usuario, se muestra una página de error en el cliente de usuario. Puede personalizar la página de error en la consola de CDN para optimizar la experiencia del usuario.

Precauciones

- Puede personalizar las páginas de error para los códigos de estado 4xx y 5xx.
- Si la aceleración de CDN está habilitada para las páginas de error personalizadas, CDN le facturará.
- Las páginas de error no se pueden personalizar para nombres de dominio con configuraciones especiales.

Procedimiento

1. Inicie sesión en la [consola de CDN](#).
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Advanced Settings**.
5. En el área **Custom Error Pages**, haga clic en **Add**.

Parámetro	Descripción	Ejemplo
Error Code	Código de error cuya página de error debe ser personalizada.	404
Redirect Mode	Modo de redirigir la página de código de error a una nueva página. Las opciones son 301 y 302 .	301
Destination URL	Nueva página a la que se redirige la página de código de error. El valor debe comenzar con http:// o https://.	https://example.com/error404.html

6. Configure los parámetros y haga clic en **OK**.

Ejemplos

La imagen **abc.jpg** se ha eliminado del servidor de origen y la caché en los nodos CDN ha caducado. Cuando un usuario accede a <https://example.com/abc.jpg>, se devuelve un código de estado 404. Supongamos que configura la siguiente configuración en la consola de CDN:



Error Code	Redirect Mode	Destination URL
404	301	https://example.com/error404.html

Result: Cuando otro usuario accede a <https://example.com/abc.jpg>, el usuario será redirigido a <https://example.com/error404.html>.

2.7.3 Compresión inteligente

Fondo

Si la compresión inteligente está activada, CDN comprime automáticamente los archivos estáticos. Esto puede ahorrarle una gran cantidad de ancho de banda al reducir el tamaño del archivo y acelerar la transferencia de archivos. La compresión inteligente incluye compresión gzip y compresión Brotli. El rendimiento de la compresión de Brotli es del 15% al 25% mayor que el de la compresión gzip.

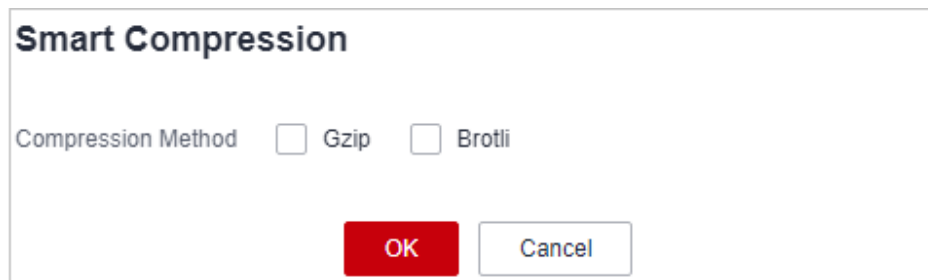
Restricciones

- La compresión inteligente se aplica a los archivos JS, HTML, CSS, XML, JSON, SHTML y HTM. Solo comprime archivos estáticos de 256 bytes a 2 MB.
- No habilite esta función si se ha configurado la verificación MD5 para su servidor de origen. Cuando CDN comprime archivos estáticos, se cambia el valor MD5. Como resultado, el valor MD5 del archivo comprimido es diferente al del archivo en el servidor de origen.
- Algunos navegadores no soportan la compresión de Brotli. Comprueba los navegadores compatibles en [este sitio web](#).
- No puede habilitar la compresión inteligente para nombres de dominio con configuraciones especiales.
- Si tanto la compresión gzip como la de Brotli están habilitadas, la compresión de Brotli se realiza preferentemente.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.

4. Haga clic en la pestaña **Advanced Settings**.
5. Haga clic en **Edit** junto a **Smart Compression**.



The image shows a dialog box titled "Smart Compression". It contains a label "Compression Method" followed by two radio button options: "Gzip" and "Brotli". At the bottom of the dialog, there are two buttons: a red "OK" button and a white "Cancel" button with a grey border.

6. Seleccione un método de compresión y haga clic en **OK**.

2.8 Configuración de vídeo

2.8.1 Búsqueda de vídeo

Antecedentes

La búsqueda de vídeo se utiliza principalmente en escenarios VOD. Permite a los usuarios buscar una cierta posición en un vídeo.

- Si se configura la búsqueda de vídeo, un cliente de usuario envía una solicitud similar a la siguiente al servidor cuando el usuario arrastra la barra de progreso durante la reproducción de vídeo:

```
http://www.example.com/test.flv?start=50
```

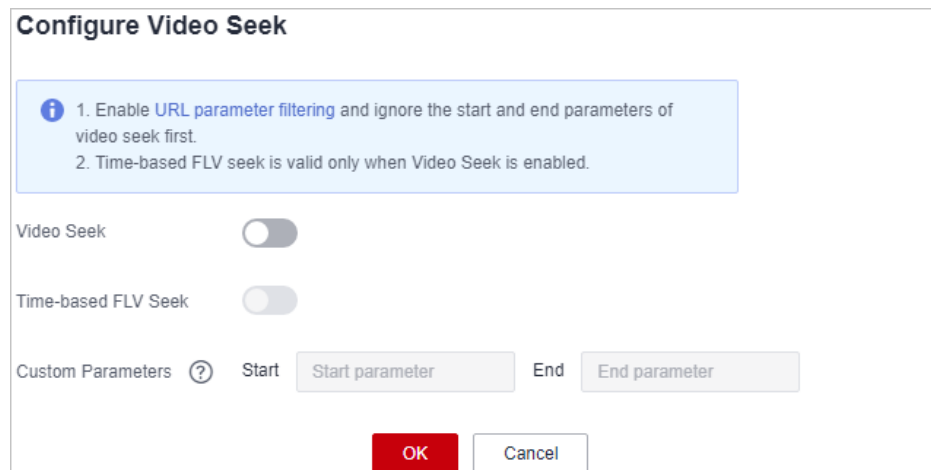
Los datos que comienzan desde el byte 50 se devuelven al cliente. Si el vídeo se ha almacenado en caché en un nodo CDN, el nodo CDN devuelve directamente los datos al usuario.

- La búsqueda de vídeo sólo es válida cuando el filtrado de parámetros de URL se establece en **Ignore URL Parameters**.
- La búsqueda de vídeo solo es válida cuando el servidor de origen admite solicitudes de rango.
- Solo se admiten vídeos MP4 y FLV.

Formato de archivos	Meta Información	Parámetro de inicio	Ejemplo
MP4	La metainformación del vídeo en el servidor de origen debe estar contenida en el encabezado del archivo.	El parámetro start indica un tiempo. CDN localiza automáticamente el fotograma clave antes de la hora especificada por el parámetro de inicio si la hora especificada no es un fotograma clave. La unidad es segunda y se admiten decimales. Por ejemplo, start=1.01 indica que la hora de inicio es de 1.01 segundos.	<code>http://www.example.com/test.mp4?start=50</code> La reproducción comienza a partir del segundo 50.
FLV	El vídeo en el servidor de origen debe contener información de metadatos.	El parámetro start indica un byte. CDN localiza automáticamente el fotograma clave antes del byte especificado por el parámetro start si el byte especificado no es un fotograma clave.	<code>http://www.example.com/test.flv?start=500</code> La reproducción comienza desde el byte 500.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Domains**.
3. En la lista de dominios, haga clic en el nombre del dominio de destino o haga clic en **Configure** en la columna **Operation**.
4. Haga clic en la pestaña **Video Settings**.
5. Haz clic en el botón de edición junto a **Video Seek**.



6. (Opcional) Habilite la búsqueda de FLV basada en el tiempo.
Active **Time-based FLV Seek**, por lo que los videos FLV pueden ser buscados por el tiempo.

 **NOTA**

Si habilita **Time-based FLV Seek**, solo es válida cuando **Video Seek** está habilitada.

7. (Opcional) Configure los parámetros inicial y final.
 - De forma predeterminada, el parámetro **start** es start y la hora de finalización es **end**.
 - Un parámetro puede contener hasta 64 caracteres, incluyendo letras, dígitos y guiones bajos (_).
8. Haga clic en **OK**.

3 Actualización y precalentamiento de caché

3.1 Descripción general

CDN puede actualizar y precalentar el contenido.

- **Actualización de caché**

Después de enviar una solicitud de actualización de caché, el contenido almacenado en caché en los nodos CDN caducará a la fuerza. Si un usuario solicita ese contenido, CDN tendrá que recuperar contenido nuevo del servidor de origen y luego almacenar en caché ese contenido nuevo.

- **Precalentamiento de caché**

Después de enviar una solicitud de precalentamiento de caché, el servidor de origen envía de forma proactiva el contenido más actual a un nodo CDN para almacenar en caché. Si un usuario solicita el contenido, el nodo CDN devuelve inmediatamente el contenido almacenado en caché. No necesita recuperar ningún contenido nuevo.

Prerrequisitos

La actualización de caché y el precalentamiento solo se pueden configurar para nombres de dominio en el estado **Enabled** o **Configuring**. Para obtener más información sobre el estado del dominio, consulte [Consulta de información básica del dominio](#).

3.2 Actualización de caché

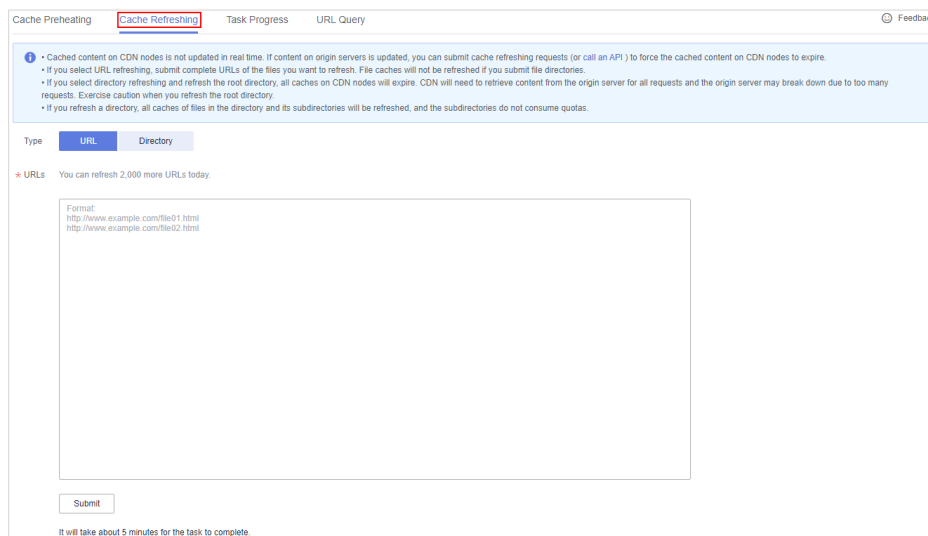
Escenarios típicos

New content release: Después de que el contenido nuevo sobrescribe el contenido antiguo con el mismo nombre en los servidores de origen, para permitir que todos los usuarios accedan al contenido más reciente, puede enviar solicitudes para actualizar las URL o directorios correspondientes del contenido, lo que obliga a que caduque el contenido almacenado en caché en los nodos.

Non-compliant content clearing: Cuando se detecta contenido no conforme y se elimina de los servidores de origen, todavía se puede acceder al contenido almacenado en caché en los nodos. Puede actualizar las direcciones URL para eliminar el contenido almacenado en caché.

Procedimiento

1. Inicie sesión en la **consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Preheating & Refresh**.
3. Haga clic en la pestaña **Cache Refreshing**, seleccione el tipo de actualización e introduzca las direcciones URL o directorios que se van a actualizar.



Tipo	Descripción
actualización de URL <ul style="list-style-type: none"> ● CDN actualiza un archivo específico. 	<ul style="list-style-type: none"> ● Cada cuenta puede actualizar un máximo de 2000 URL por día y un máximo de 1000 URL por tarea. ● Se debe incluir la parte http:// o https:// de la URL. ● Introduce una URL por fila. Ejemplo: http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk
Actualización de directorios <ul style="list-style-type: none"> ● CDN actualiza todos los archivos de un directorio. 	<ul style="list-style-type: none"> ● Cada cuenta puede actualizar un máximo de 100 directorios por día a la vez. ● Una URL debe contener http o https y terminar con una barra diagonal (/). ● Introduce una URL por fila. Ejemplo: http://www.example01.com/folder01/ http://www.example01.com/folder02/

NOTA

- Al elegir la actualización de directorios, se actualizan todos los recursos del directorio, incluidos los recursos de los subdirectorios.
- Si se reescribe una dirección URL, debe utilizar la ruta de recurso real de la nueva dirección URL para actualizar la caché.
- Algunos recursos pueden almacenarse en caché en los navegadores. Actualice la caché del navegador después de actualizar la caché del nodo.

4. Haga clic en **Submit**.

Después de enviar una tarea de actualización, puede ver el estado de la tarea en la pestaña **Task Progress**.

NOTA

- También puede crear una tarea de actualización de caché para un nombre de dominio llamando a una API. Para obtener más información, consulte [Descripción general de API](#).
- Se tarda unos 5 minutos para que una tarea de actualización de caché tenga efecto.

3.3 Precalentamiento de caché

Escenarios típicos

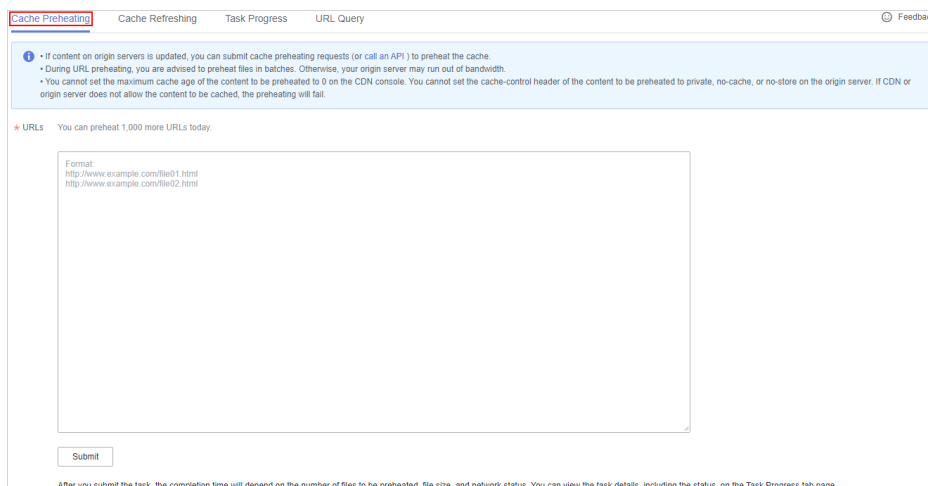
Initial access: Cuando conecta un nombre de dominio a CDN por primera vez, puede precalentar archivos de gran tamaño, incluidos vídeos, para mejorar la experiencia del usuario.

Installation package release: Antes de lanzar un paquete de instalación de software o un paquete de actualización, puede precalentar el contenido a los nodos CDN distribuidos globalmente. Después de que se inicie el software o la actualización, los nodos CDN responden directamente a las solicitudes de descarga de un gran número de usuarios, lo que mejora la velocidad de descarga y reduce en gran medida la presión sobre su servidor de origen.

Promotional activity: Antes de lanzar una campaña promocional, puede precalentar el contenido estático involucrado en la página de actividad a los nodos de CDN. Una vez iniciada la actividad, los nodos CDN responden a las solicitudes de los usuarios para acceder a todo el contenido estático, lo que garantiza la disponibilidad del servicio y mejora la experiencia del usuario.

Procedimiento

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Preheating & Refresh**.
3. Haga clic en la pestaña **Cache Preheating** e introduzca las direcciones URL que desea precalentar.



Tipo	Descripción
<p>Precalentamiento de URL</p> <ul style="list-style-type: none"> ● CDN precalienta un archivo específico. 	<ul style="list-style-type: none"> ● Se debe incluir la parte <code>http://</code> o <code>https://</code> de la URL. ● Introduce una URL por fila. ● Cada cuenta puede precalentar un máximo de 1000 URL por día o por tarea. Ejemplo: <code>http://www.example.com/file01.html</code> <code>http://www.example.com/file02.html</code> <code>https://example.huawei.com/download/app/abc.apk</code>

4. Haga clic en **Submit**.

Después de enviar una tarea de precalentamiento, puede ver el estado de la tarea en la pestaña **Task Progress**.

NOTA

- También puede crear una tarea de precalentamiento de caché para un nombre de dominio llamando a una API. Para obtener más información, consulte [Descripción general de API](#).
- El tiempo necesario para completar una tarea de precalentamiento depende del número y tamaño de los archivos que se van a precalentar, y de las condiciones de la red.
- Si el estado de precalentamiento de caché de una URL es **Completed**, el precalentamiento es completado.
- El precalentamiento de un gran número de archivos puede ocupar completamente los recursos de ancho de banda del servidor de origen. Por lo tanto, se recomienda precalentar los archivos en lotes.
- Los archivos dinámicos, como los archivos ASP, JSP y PHP, no se pueden precalentar.

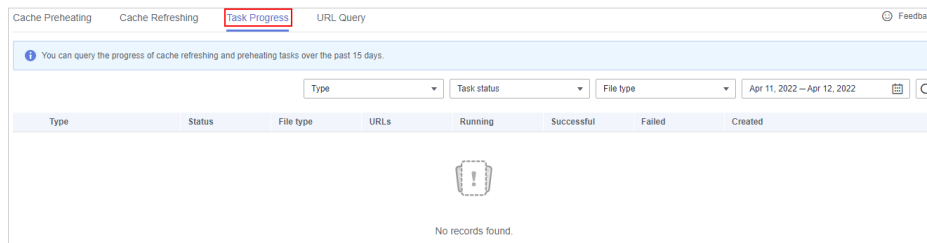
3.4 Consulta de Progresos de Tareas

Después de enviar una tarea de actualización o precalentamiento de caché, puede ver el estado de la tarea en la página de pestaña **Task Progress**.

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, elija **Preheating & Refresh**.
3. Seleccione la pestaña **Task Progress** para comprobar el estado de las tareas de actualización y precalentamiento.



NOTA

- En la página de la pestaña **Task Progress**, puede ver el estado de las tareas de actualización y precalentamiento de caché durante los últimos 15 días.
- También puede consultar los registros de actualización y precalentamiento de caché de los últimos 15 días en la página de pestaña **URL Query**.

3.5 Preguntas Frecuentes

¿Cuáles son las diferencias entre la actualización de caché y el precalentamiento de caché?

Las diferencias entre actualizar y precalentar la caché son:

- **Actualización de caché**
Después de enviar una solicitud de actualización de caché, el contenido almacenado en caché en los nodos CDN caducará a la fuerza. Si un usuario solicita ese contenido, CDN tendrá que recuperar contenido nuevo del servidor de origen y luego almacenar en caché ese contenido nuevo.
- **Precalentamiento de caché**
Después de enviar una solicitud de precalentamiento de caché, el servidor de origen envía de forma proactiva el contenido más actual a un nodo CDN para almacenar en caché. Si un usuario solicita el contenido, el nodo CDN devuelve inmediatamente el contenido almacenado en caché. No necesita recuperar ningún contenido nuevo.

Para obtener más información, consulte [Actualización y precalentamiento de caché](#).

¿Hay una secuencia entre la actualización de caché de CDN y el precalentamiento?

Si desea actualizar el contenido en caché en los nodos de CDN después de actualizar el contenido de origen, preste atención a lo siguiente:

- Primero debe actualizar la caché. Se tarda unos 5 minutos para que una tarea de actualización de caché tenga efecto. A continuación, ejecute la tarea de precalentamiento de caché.
- Si omite la actualización de caché y realiza directamente el precalentamiento de caché, el contenido almacenado en caché en los nodos de CDN no se actualizará.

- Si accede a CDN por primera vez y no se almacena contenido en caché en los nodos de CDN, puede realizar directamente el precalentamiento de caché para almacenar contenido en caché en los nodos de CDN.

¿La actualización de caché actualiza el contenido almacenado en caché en todos los nodos?

Sí.

¿Por qué es una tarea de precalentamiento particular en el estado de procesamiento durante tanto tiempo?

Entre las causas comunes se incluyen las siguientes:

- La tarea de precalentamiento se envió durante una hora pico, por lo que todavía está en la cola.
- Está precalentando un gran número de archivos. El precalentamiento recuperará el contenido del servidor de origen, por lo que el precalentamiento de un gran número de archivos puede consumir todo el ancho de banda disponible para el servidor de origen. Se recomienda que:
 - Divida las tareas de precalentamiento en lotes.
 - Precaliente los archivos durante las horas no pico, por ejemplo, por la noche.
 - Aumente el ancho de banda del servidor de origen.
- La tarea de precalentamiento se ha completado pero el estado no se actualiza en la consola. Actualice la página de la consola y vuelva a comprobarlo.

¿Cómo actualizo la caché de CDN donde el nombre de dominio incluye un carácter comodín?

Cuando actualice la caché de un nombre de dominio que incluya un comodín, introduzca las direcciones URL o directorios de los nombres de dominio de nivel 2. No introduzca una URL que contenga un comodín, como **https://*.example.com/file01.html** o **https://*.example.com/file02/**.

Example:

- Un nombre de dominio de aceleración es ***.example.com**.
- El nombre de dominio de nivel 2 que contiene el contenido que se va a actualizar es **abc.example.com**.
 - Ingrese la URL que desea actualizar: **https://abc.example.com/file01.html**.
 - Ingrese el directorio que desea actualizar: **https://abc.example.com/file02/**.

¿Por qué es que incluso después de precalentar o actualizar la caché, el contenido no se ha actualizado?

Es posible que el intervalo entre la actualización de la memoria caché y el precalentamiento sea demasiado corto. Como resultado, la actualización falla. Si una caché acaba de actualizarse o precalentarse, se recomienda que espere al menos 5 minutos antes de repetir esta acción.

¿Qué puedo hacer si falla una operación de precalentamiento de caché?

Es posible que:

- Un gran número de archivos están siendo precalentados al mismo tiempo, y esta operación ha ocupado todo el ancho de banda del servidor de origen. En este caso, se recomienda realizar operaciones de precalentamiento en lotes. También puede aumentar el ancho de banda del servidor de origen para mejorar la eficiencia del precalentamiento.
- La edad máxima de caché del contenido solicitado es 0. En este caso, cambie la configuración de edad máxima de la caché.
- **Cache-Control** es **private**, **no-cache**, o **no-store**. Si **Cache-Control** no está configurado, se utiliza el valor predeterminado **private**.
- Ha solicitado precalentar directorios, contenido dinámico o URL cuya antigüedad máxima de caché esté establecida en 0.

¿CDN soporta el precalentamiento del directorio?

No. Solo se pueden precalentar las URL completas. No se admiten directorios de precalentamiento. Para obtener más información, consulte [Actualización y precalentamiento de caché](#).

¿Necesito precalentar/actualizar las URL de HTTP y HTTPS por separado?

No. Solo necesita precalentar/actualizar URLs de HTTP o HTTPS.

Si la CDN está habilitada dentro y fuera de China continental, ¿necesita diferenciarse al actualizar y al precalentar?

No. Puede actualizar o precalentar directamente las URL correspondientes.

¿Puedo precalentar archivos M3U8?

Sí.

¿Por qué el sistema informa de un error que indica que no tengo permiso para actualizar la caché?

Es posible que su nombre de dominio de aceleración haya sido deshabilitado. Habilitar la CDN para el nombre de dominio de nuevo. Si su cuenta está en mora, CDN puede haber sido deshabilitado para su nombre de dominio de aceleración. Asegúrese de que el saldo de la cuenta sea suficiente.

¿Se puede actualizar automáticamente la caché después de actualizar un archivo estático en el servidor de origen?

No. Sin embargo, puede llamar a las API para forzar la expiración del contenido actual y, a continuación, precalentar contenido nuevo. Para obtener más información, consulte [Descripción general de API](#).

¿Por qué no se admite el precalentamiento de directorios y cómo la CDN solicita contenido del servidor de origen?

Puede considerar CDN como un usuario, que descarga contenido desde el servidor de origen. Si CDN soporta el precalentamiento de directorio, el servidor de origen no sabe qué archivos en el directorio se van a descargar cuando CDN envía una solicitud de acceso a directorio al servidor de origen. Si solicita un archivo, el servidor de origen sabe exactamente qué es.

¿Son obligatorias las actualizaciones y el precalentamiento de la CDN?

Eso depende.

- Si un archivo se actualiza en un servidor de origen, el archivo también debe actualizarse en nodos CDN.
- Se recomienda precalentar archivos de gran tamaño, especialmente archivos de vídeo, para mejorar la experiencia del usuario.
- No se recomienda el precalentamiento para archivos pequeños.

Actualmente, CDN no admite la actualización y el precalentamiento automáticos. Es necesario realizar estas operaciones manualmente.

4 Análisis estadístico

4.1 Descripción de estadísticas

Tabla 4-1 describe seis tipos de informes de análisis estadísticos proporcionados por CDN. Usted puede aprender:

Tabla 4-1 Descripción de estadísticas

Indicador	Descripción
Estadísticas de utilización	Puede consultar las estadísticas de utilización de tráfico/ancho de banda y el índice de aciertos de tráfico para todos sus nombres de dominio, y exportar las estadísticas.
Estadísticas de acceso	Puede consultar el total de solicitudes, la relación de aciertos de caché y las consultas por segundo para todos sus nombres de dominio, y exportar las estadísticas.
Estadísticas de servidor original	Puede consultar el tráfico de recuperación, el ancho de banda de recuperación y la tasa de errores de recuperación de todos los nombres de dominio y exportar las estadísticas.
Hotspots	Puede consultar las 100 direcciones URL principales según el uso del tráfico o el total de solicitudes de todos los nombres de dominio y exportar los detalles de estas 100 direcciones URL principales.
Estadísticas de región & operador	Puede consultar el uso del tráfico/ancho de banda y las solicitudes totales de todos los nombres de dominio por región o operador, y exportar estadísticas por región o operador.
Códigos de estado	Puede consultar los códigos de estado de las solicitudes a todos los nombres de dominio y exportar los detalles de estos códigos de estado.

Indicador	Descripción
Estadísticas de utilización para la aceleración de todo el sitio	Puede consultar el tráfico o el ancho de banda consumidos por los nombres de dominio cuyo tipo de servicio es la aceleración de todo el sitio.

 **NOTA**

- CDN le permite consultar estadísticas sobre nombres de dominio eliminados.
- Si ha habilitado la función de proyecto de empresa, no se pueden consultar estadísticas de nombres de dominio eliminados.
- En la consola de CDN, hay un retraso de aproximadamente 1 hora para los datos en las páginas de **Statistics Analysis** y **Dashboard**.

También puede consultar la siguiente información en la página **Dashboard**:

- Tráfico, ancho de banda máximo, número de solicitudes y porcentaje de visitas por mes
- Tráfico, ancho de banda máximo, número de solicitudes y ratio de aciertos por día
- Tendencia de tráfico de los 5 nombres de dominio principales en el día actual
- Tendencia de ancho de banda máximo de los 5 nombres de dominio principales en el día actual
- Solicitar tendencia de los 5 mejores nombres de dominio
- Número total de nombres de dominio añadidos
- Cuota restante en sus paquetes de tráfico

Preguntas Frecuentes

- [¿Por qué no hay datos en el análisis estadístico?](#)
- [¿Cuánto tiempo es el retraso de la API de las 100 URL principales en CDN Hotspot Statistics?](#)
- [¿Qué podría caer en la categoría "otro" en las estadísticas de la región de visitantes?](#)

4.2 Estadísticas de utilización

Puede consultar las estadísticas de utilización del tráfico/ancho de banda y el índice de aciertos de tráfico de todos sus nombres de dominio (excluyendo aquellos eliminados si ha habilitado la función de proyecto de empresa).

- Los últimos 90 días de datos se pueden consultar, y cada consulta puede incluir hasta 31 días de datos.
- Si no hay datos disponibles dentro del intervalo de tiempo consultado, no se muestran datos en los gráficos de tendencias de tráfico/ancho de banda y ratio de aciertos de tráfico o en la lista de utilización de tráfico/ancho de banda de nombres de dominio.
- La granularidad estadística mínima predeterminada es de 5 minutos. Si el lapso de tiempo de consulta es de 8 días o más, la granularidad estadística mínima es de 4 horas.
- Hay un retraso de aproximadamente una hora para los datos mostrados en la página **Utilization Statistics**.

- Puede exportar los resultados de la consulta.
- Se admite la comparación de datos.

Restricciones

Si el área de servicio de su nombre de dominio es **Global**, debe consultar las estadísticas de este nombre de dominio eligiendo **Chinese mainland** y **Global (Chinese mainland not included)** respectivamente. Consultar por **Global** no está disponible.

Procedimiento


1. Inicie sesión en la **Consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

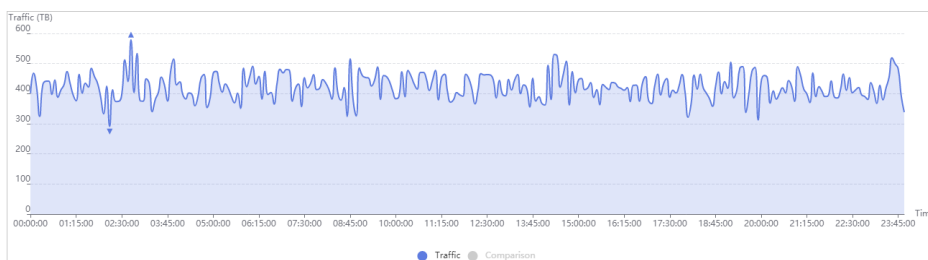
Se muestra la consola de CDN.

2. En el panel de navegación, elija **Statistical Analysis > Utilization Statistics**.


3. Establezca los criterios de búsqueda para consultar los siguientes datos:

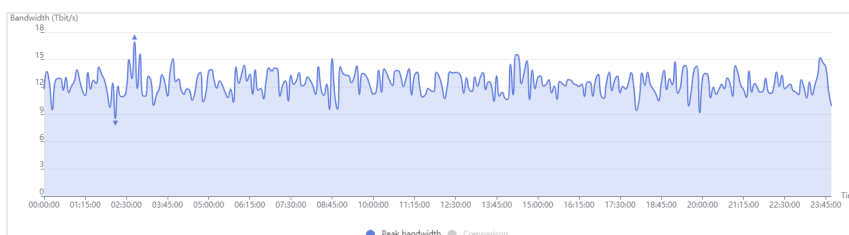
- **Traffic Monitoring:** muestra el tráfico de nombres de dominio específicos a lo largo del tiempo. Puede hacer clic en las entradas de leyenda, por ejemplo,

 **Traffic**, para ocultar o mostrar las estadísticas correspondientes.



- **Peak Bandwidth Monitoring:** muestra el ancho de banda máximo de nombres de dominio específicos a lo largo del tiempo. Puede hacer clic en las entradas de

leyenda, por ejemplo,  **Peak bandwidth**, para ocultar o mostrar las estadísticas correspondientes.



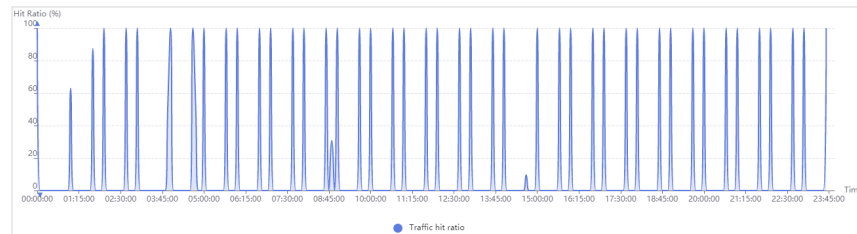
NOTA

El ancho de banda del percentil 95 y el ancho de banda pico diario promedio se muestran para el mismo período de tiempo. Si no se monitorizan estadísticas de ancho de banda dentro del intervalo de tiempo consultado, la línea de ancho de banda o la línea de ancho de banda de pico diario promedio no se visualizan.

- **Traffic Hit Ratio:** muestra el ratio de aciertos de tráfico de nombres de dominio específicos a lo largo del tiempo.

Ratio de aciertos de tráfico = Tráfico generado cuando se acierta en la memoria caché/Tráfico total de solicitudes

El tráfico total de solicitudes es la suma del tráfico generado cuando se golpea la memoria caché de nodo CDN y el tráfico generado durante la recuperación de contenido.



- **Domain Name Traffic/Bandwidth Utilization:** muestra el tráfico y el ancho de banda de nombres de dominio específicos.

Domain Name	Traffic	Peak Bandwidth	Traffic Hit Ratio
tx- api.com	110.50 MB	41.91 kbit/s	100.00 %
ww- .ite	10.69 KB	0.05 kbit/s	36.02 %

Puede hacer clic en **Traffic**, **Peak Bandwidth**, o **Traffic Hit Ratio** en el encabezado de la tabla para ver las estadísticas de utilización en orden descendente o ascendente.

4.3 Estadísticas de acceso

Puede consultar el número total de solicitudes, la relación de aciertos de caché y las consultas por segundo de todos los nombres de dominio (excluyendo los eliminados si ha habilitado la función de proyecto de empresa).

- Los últimos 90 días de datos se pueden consultar, y cada consulta puede incluir hasta 31 días de datos.
- La información de acceso se muestra en función de las estadísticas de registro. Los datos se sincronizan una vez por hora.
- Si no hay datos disponibles dentro del intervalo de tiempo consultado, no se muestran datos sobre el total de solicitudes, la relación de aciertos de caché y los gráficos de tendencias de consultas por segundo o en la lista de detalles de acceso de nombres de dominio.
- Puede exportar los resultados de la consulta.
- La granularidad estadística mínima predeterminada es de 5 minutos. Si el lapso de tiempo de consulta es de 8 días o más, la granularidad estadística mínima es de 4 horas.

Restricciones

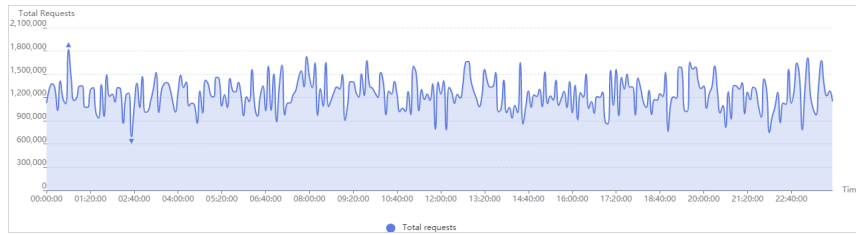
Si el área de servicio de su nombre de dominio es **Global**, debe consultar las estadísticas de este nombre de dominio eligiendo **Chinese mainland** y **Global (Chinese mainland not included)** respectivamente. Consultar por **Global** no está disponible.

Procedimiento

1. Inicie sesión en la **Consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Statistical Analysis > Access Statistics**.

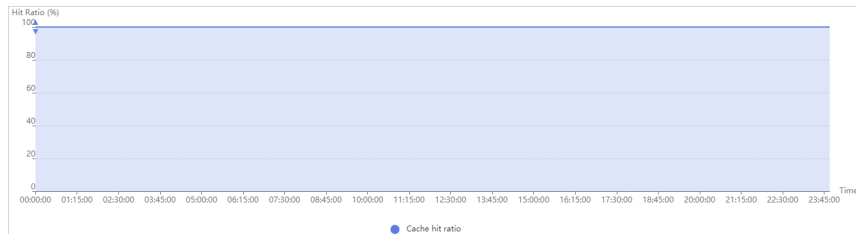
3. Establezca los criterios de búsqueda para consultar los siguientes datos:

- **Total Requests:** muestra el número de solicitudes a nombres de dominio específicos a lo largo del tiempo.



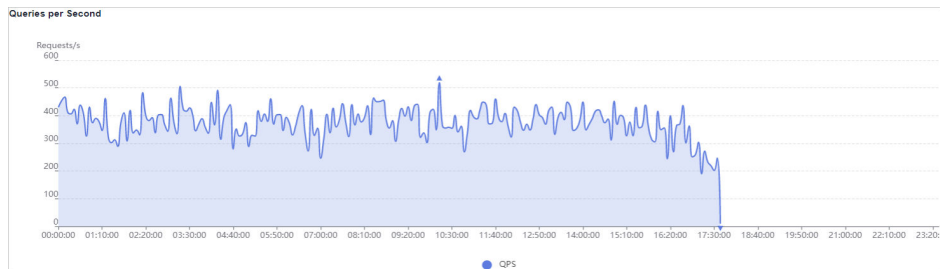
- **Cache Hit Ratio:** muestra la relación de aciertos de caché de nombres de dominio específicos a lo largo del tiempo.

Proporción de aciertos de caché = Número de solicitudes que llegan al caché/
 Número de solicitudes totales



- **Queries per Second:** muestra las consultas por segundo de nombres de dominio específicos a lo largo del tiempo.

Las consultas por segundo son una medida común del número de consultas que reciben los nombres de dominio durante un segundo.



- **Domain Name Access:** muestra el número de solicitudes a nombres de dominio específicos, la relación de aciertos de caché y las consultas por segundo.

Puede hacer clic en **Total Requests**, **Cache Hit Ratio**, o **Queries per Second** en el encabezado de la tabla para ver las estadísticas de acceso en orden descendente o ascendente.

Domain Name	Total Requests	Cache Hit Ratio	Queries per Second
ca:ao.net	2,975,387	100.00 %	34
1.c:op	1,547,309	100.00 %	18
o:p	1,547,309	100.00 %	18

4.4 Estadísticas de servidor original

Puede consultar el tráfico de recuperación, el ancho de banda de recuperación y la tasa de errores de recuperación de todos los nombres de dominio . (excluyendo aquellos eliminados si ha habilitado la función de proyecto de empresa).

- Los últimos 90 días de datos se pueden consultar, y cada consulta puede incluir hasta 31 días de datos.
- Si no hay datos disponibles dentro del intervalo de tiempo consultado, no se muestran datos en los gráficos de tendencia de la tasa de error de recuperación de tráfico/ancho de banda ni en la lista de detalles de recuperación de nombres de dominio.
- La granularidad estadística mínima predeterminada es de 5 minutos. Si el lapso de tiempo de consulta es de 8 días o más, la granularidad estadística mínima es de 4 horas.
- Puede exportar los resultados de la consulta.

Procedimiento

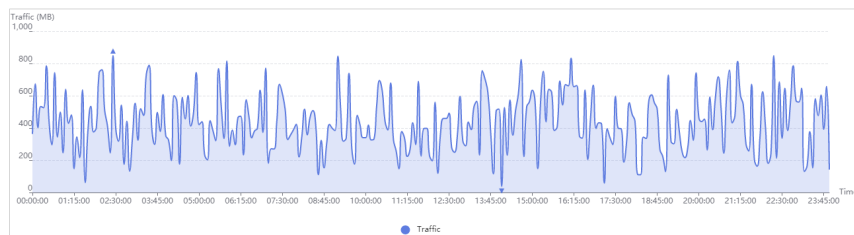
1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

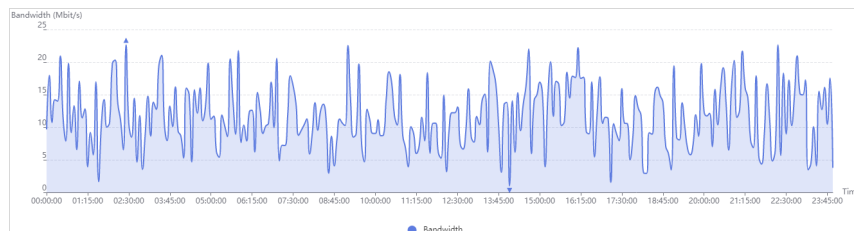
2. En el panel de navegación, elija **Statistical Analysis > Origin Server Statistics**.

3. Establezca los criterios de búsqueda para consultar los siguientes datos:

- **Retrieval Traffic:** muestra el tráfico de recuperación de contenido de nombres de dominio específicos a lo largo del tiempo.



- **Retrieval Bandwidth:** muestra el ancho de banda de recuperación de contenido de nombres de dominio específicos a lo largo del tiempo.



- **Retrieval Failure Rate:** muestra la tasa de fallas de recuperación a lo largo del tiempo.

Tasa de errores de recuperación = $\frac{\text{Número de solicitudes de recuperación fallidas}}{\text{Número de solicitudes de recuperación totales}}$



NOTA

Los errores de recuperación pueden ser causados por errores de configuración del host de recuperación, desconexión entre CDN y el host de recuperación, incompatibilidad HTTP y errores del host de recuperación.

- **Domain Name Retrieval Details:** muestra el tráfico de recuperación, el ancho de banda de recuperación y las tasas de errores de recuperación de nombres de dominio específicos.

Puede hacer clic en **Retrieval Traffic**, **Retrieval Bandwidth**, o **Retrieval Failure Rate** en el encabezado de la tabla para ver las estadísticas de recuperación en orden descendente o ascendente.

Domain Name	Retrieval Traffic	Retrieval Bandwidth	Retrieval Failure Rate
brc :2.com	1.87 GB	2.61 Mbit/s	0.00 %
ww .site	6.84 KB	0.04 kbit/s	76.47 %

4.5 Hotspots

Puede consultar las 100 URL que consumen más tráfico y las 100 URL más solicitadas.

- Los últimos 90 días de datos se pueden consultar, y cada consulta puede incluir hasta 31 días de datos.
- Las 100 mejores URLs se actualizan todos los días.
- Si no hay datos disponibles dentro del intervalo de tiempo consultado, no se muestran datos en la lista de las 100 URL principales.
- Puede exportar los resultados de la consulta.
- Las 100 URL principales se muestran en función de las estadísticas de registro. El retardo de datos es de 4 a 6 horas.

Restricciones

Si el área de servicio de su nombre de dominio es **Global**, debe consultar las estadísticas de este nombre de dominio eligiendo **Chinese mainland** y **Global (Chinese mainland not included)** respectivamente. Consultar por **Global** no está disponible.

Procedimiento

1. Inicie sesión en la **Consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Statistical Analysis > Hotspots**.
3. Configure los criterios de búsqueda.

Parameter

Traffic Total requests

Top 100 URLs (Traffic Usage)

URL	Traffic
www. .site/	1.08 KB

Puede consultar las 100 URL que consumen más tráfico y las 100 URL más solicitadas. Puede hacer clic en **Traffic** o **Total Requests** en los encabezados de tabla para ordenar las 100 direcciones URL principales en orden ascendente o descendente.

 **NOTA**

El tráfico que se muestra en la tabla es solo para referencia. Obtener los datos reales de otras páginas de análisis estadístico.

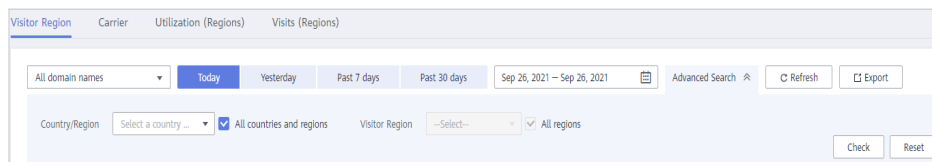
4.6 Estadísticas de región & operador

Puede consultar el uso del tráfico/ ancho de banda, el número de solicitudes y la distribución de visitantes de todos los nombres de dominio . (excluyendo aquellos eliminados si ha habilitado la función de proyecto de empresa) por región o operador.

- Los últimos 90 días de datos se pueden consultar, y cada consulta puede incluir hasta 31 días de datos.
- Si no hay datos disponibles dentro del intervalo de tiempo consultado, no se muestran datos en la lista de detalles estadísticos del índice de portador.
- La granularidad estadística mínima es de 5 minutos.
- Puede exportar los resultados de la consulta.

Procedimiento

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Statistical Analysis**.
3. Seleccione **Region & Carrier Statistics** under **Statistical Analysis**.



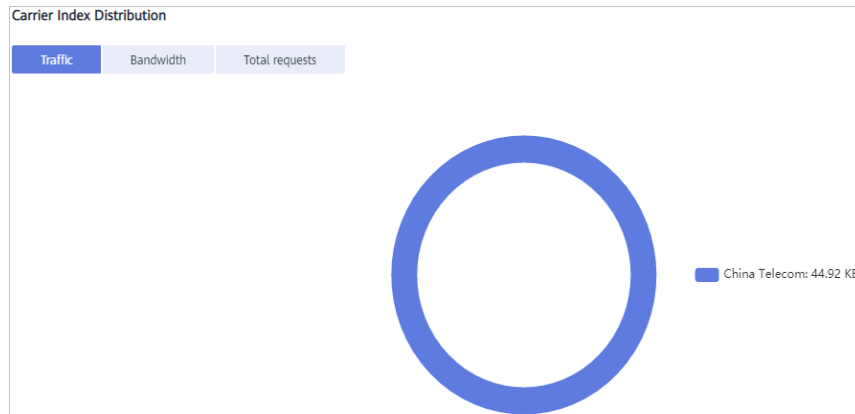
4. Seleccione una pestaña y establezca criterios de búsqueda para consultar los siguientes datos:

- **Visitor Region:** muestra la región donde se encuentran los visitantes.

Si selecciona **China** en la lista desplegable **Country and Region**, puede consultar los detalles de los visitantes de 34 regiones administrativas provinciales de China.

Visitor Region	Traffic (Percentage)	Peak Bandwidth	Total Requests (Percentage)
China	1.02 MB (100.00%)	0.05 kbit/s	1,066,000 (100.00%)

- **Carrier:** incluye China Mobile, China Telecom, China Unicom, China Education and Research Network (CERNET), Dr. Peng, y China Mobile Tietong.
 - i. **Carrier Index Distribution:** muestra la proporción que ocupa cada portadora en diferentes estadísticas de índice.



- ii. **Carrier Index Statistical Details:** muestra el tráfico, el ancho de banda máximo y el número de solicitudes por operador. Puede hacer clic en **Traffic**, **Peak Bandwidth** o **Total Requests** en el encabezado de la tabla **Carrier Index Statistical Details** para ver los datos en orden ascendente o descendente.

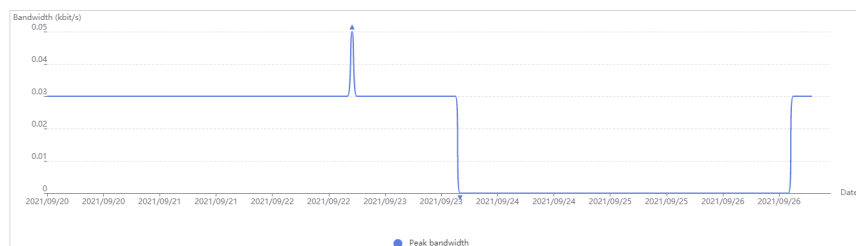
Carrier	Traffic (Percentage)	Peak Bandwidth (Percentage)	Total Requests (Percentage)
Other	110.64 MB (93.75%)	85.04 kbit/s (98.35%)	228 (1.19%)
China Mobile	7.03 MB (5.96%)	1.26 kbit/s (1.46%)	18,035 (94.12%)
China Mobile Tietong	349.32 KB (0.29%)	0.07 kbit/s (0.08%)	893 (4.66%)
China Telecom	5.07 KB (0.00%)	0.07 kbit/s (0.08%)	5 (0.03%)
China Unicom	0.75 KB (0.00%)	0.02 kbit/s (0.02%)	1 (0.01%)

– **Utilization (Regions)**

- i. **Traffic:** muestra el tráfico de nombres de dominio específicos por país/región o operadores.



- ii. **Peak bandwidth:** muestra el ancho de banda máximo de nombres de dominio específicos por país/región o operadores.



- iii. **Domain Name Traffic/Bandwidth Utilization:** muestra el tráfico y el ancho de banda de nombres de dominio específicos.

Domain Name	Traffic	Peak Bandwidth
1m...t.com	1.02 MB	0.05 kbit/s

- **Visits (Regions):** muestra el número de solicitudes de nombres de dominio específicos en un país o región específicos.

- i. **Total Requests:** muestra el número de solicitudes a nombres de dominio específicos en un país o región específicos.



- ii. **Domain Name Access:** muestra los detalles de acceso de nombres de dominio específicos en un país o región específicos.

Domain Name	Total Requests
1mi st.com	106.80 Ten Thousands

4.7 Códigos de estado

Puede consultar los códigos de estado devueltos a las solicitudes a todos los nombres de dominio (excluido los eliminados si ha habilitado la función de proyecto de empresa).

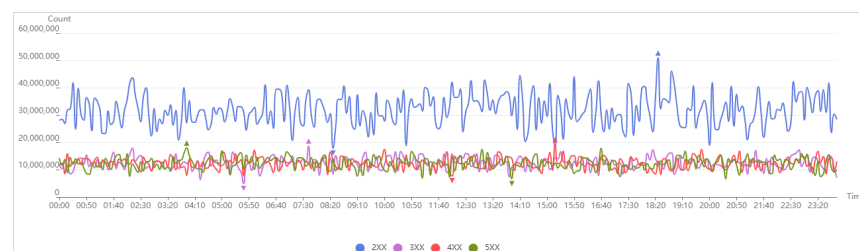
- Los últimos 90 días de datos se pueden consultar, y cada consulta puede incluir hasta 31 días de datos.
- Si no hay datos disponibles dentro del intervalo de tiempo consultado, no se muestran datos en la lista de códigos de estado.
- La granularidad estadística mínima predeterminada es de 5 minutos. Si el lapso de tiempo de consulta es de 8 días o más, la granularidad estadística mínima es de 4 horas.
- Puede exportar los resultados de la consulta a un equipo local.

Restricciones

Si el área de servicio de su nombre de dominio es **Global**, debe consultar las estadísticas de este nombre de dominio eligiendo **Chinese mainland** y **Global (Chinese mainland not included)** respectivamente. Consultar por **Global** no está disponible.

Procedimiento

1. Inicie sesión en la **Consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Statistical Analysis > Status Codes**.
3. Establezca los criterios de búsqueda para consultar los siguientes datos:
 - **Status Codes Overview:** muestra el número de cada código de estado a lo largo del tiempo.



Puede hacer clic en las entradas de leyenda, por ejemplo, ● 2XX, para ocultar o mostrar las estadísticas de códigos específicos. Las estadísticas se recopilan en los códigos de estado, incluidos 2XX, 3XX, 4XX, y 5XX..

Código de estado	Descripción
2XX	Códigos de respuesta de éxito. Estos indican que una solicitud ha sido aceptada y procesada por el servidor.
3XX	Redirección de mensajes. Estos indican que el cliente necesita realizar operaciones adicionales para completar la solicitud.
4XX	Códigos de respuesta de error del cliente. Estos indican que hubo un error en el lado del cliente, incluyendo pero no limitado a errores de sintaxis o fallo al completar la solicitud.
5XX	Códigos de respuesta de error del servidor. Estos indican que hubo un error cuando el servidor estaba procesando la solicitud.

- **Status Code Statistics:** muestra el número y la proporción de diferentes códigos de estado para nombres de dominio específicos.

Puede hacer clic en **Count** o **Percentage** en el encabezado de la tabla de la lista de detalles de estadísticas para ver los datos correspondientes en orden ascendente o descendente.

Sum		Details	
Status Code	Count	Percentage	
2XX	9,182,562,128	46.21 %	
3XX	3,581,136,478	18.02 %	
4XX	3,564,608,990	17.94 %	
5XX	3,543,929,339	17.83 %	

4.8 Estadísticas de utilización para la aceleración de todo el sitio

Puede consultar las estadísticas de utilización de todos los nombres de dominio cuyo tipo de servicio es la aceleración de todo el sitio (excluyendo los eliminados si ha habilitado la función de proyecto de empresa).

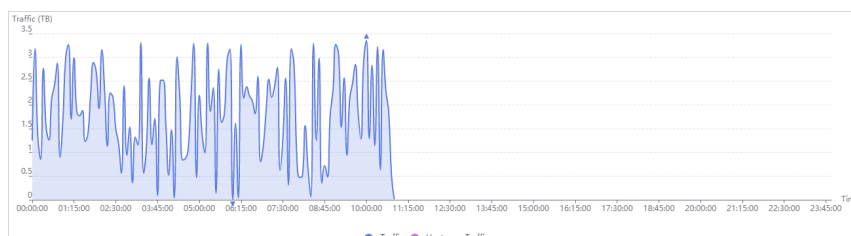
- Los últimos 90 días de datos se pueden consultar, y cada consulta puede incluir hasta 31 días de datos.
- La granularidad estadística mínima predeterminada es de 5 minutos. Si el lapso de tiempo de consulta es de 8 días o más, la granularidad estadística mínima es de 4 horas.

Procedimiento

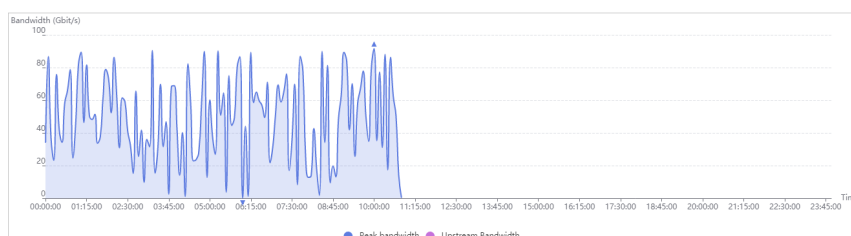
1. Inicie sesión en la **Consola de Huawei Cloud**. En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, elija **Statistical Analysis > Utilization Statistics for Whole Site Acceleration**.
3. Establezca los criterios de búsqueda para consultar los siguientes datos:
 - **Traffic**: muestra el tráfico y el tráfico ascendente utilizado para la aceleración de todo el sitio.



- **Bandwidth**: muestra el ancho de banda máximo y el ancho de banda ascendente utilizados para la aceleración de todo el sitio.



4.9 Preguntas Frecuentes

¿Por qué no hay datos en el análisis estadístico?

- El registro CNAME configurado para su nombre de dominio es incorrecto.
- Las estadísticas de CDN en la página **Statistical Analysis** son una hora más tarde que los datos en tiempo real.

Si el problema no es causado por ninguna de las razones anteriores, [envíe un ticket de servicio](#).

¿Qué podría caer en la categoría "Other" en las estadísticas de la región de visitantes?

Other se refiere a aquellos cuya región no se puede identificar porque sus direcciones IP no están registradas en la biblioteca de direcciones IP o sus direcciones IP no se pueden obtener por CDN.

¿Cuánto tiempo es el retraso de la API de las 100 URL principales en las estadísticas de puntos de acceso de CDN?

Llamar a la API de las 100 URL principales tiene un retraso de aproximadamente 6 horas. Esta situación vuelve a la normalidad a las 12:00 del día siguiente.

¿Cuáles son los significados de HEAD, HIT y MISS en los registros de CDN?

- **HEAD**

El método HEAD es el mismo que el método GET, excepto que el servidor no devuelve el cuerpo del mensaje HEAD. En una respuesta a una solicitud HEAD, los metadatos contenidos en la cabecera HTTP son los mismos que en una respuesta a una solicitud GET. HEAD se puede usar para obtener los metadatos ocultos en una solicitud, en lugar de transmitir la propia entidad. También se utiliza a menudo para probar la validez, la disponibilidad y los cambios recientes de los hipervínculos.

- **HIT**

Esto indica un acierto de caché. Un nodo de borde sirve directamente el contenido.

- **MISS**

Esto indica una falta de memoria caché. Un nodo perimetral necesita recuperar contenido del servidor de origen.

¿Cuánto tiempo se pueden consultar los datos?

Puede consultar los datos de la CDN en los últimos 90 días. El intervalo de tiempo máximo de consulta es de 31 días.

¿Por qué se devuelve el mensaje "Fine-grained Authentication Failed" cuando llamo a una API para descargar registros de CDN?

Es posible que no se encuentre el proyecto de empresa. Puede agregar **enterprise_project_id=ALL** a la ruta de la solicitud.

Ejemplo:

```
GET https://cdn.myhuaweicloud.com/v1.0/cdn/logs?  
query_date=1502380500000&domain_name=www.example.com&page_size=10&page_number=1&en  
terprise_project_id=ALL
```

¿Qué significa el OkHttp de User-Agent en los registros de CDN?

OkHttp es un protocolo de solicitud utilizado por el marco de red de Android para procesar solicitudes de red.

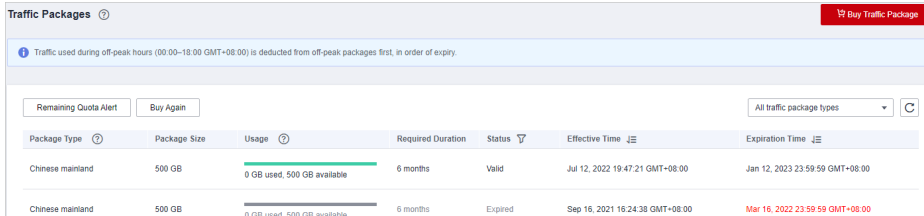
5 Gestión de paquetes

Si el tráfico te factura, puedes ahorrar dinero comprando un paquete de tráfico en la página **Traffic Packages**. También puede ver la información básica sobre los paquetes de tráfico y gestionarlos en la página **Traffic Packages**.

Procedimiento

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Traffic Packages**.

Figura 5-1 Paquetes de tráfico



Package Type	Package Size	Usage	Required Duration	Status	Effective Time	Expiration Time
Chinese mainland	500 GB	0 GB used, 500 GB available	6 months	Valid	Jul 12, 2022 19:47:21 GMT+08:00	Jan 12, 2023 23:59:59 GMT+08:00
Chinese mainland	500 GB	0 GB used, 500 GB available	6 months	Expired	Sep 16, 2021 19:24:38 GMT+08:00	Mar 16, 2022 23:59:59 GMT+08:00

3. Puede realizar las siguientes operaciones:
 - Ver información básica sobre un paquete de tráfico: Obtenga información sobre el consumo de su paquete de tráfico en cualquier momento.
 - Configuración de la alerta de cuota restante: Haga clic en **Remaining Quota Alert** para establecer una alerta para las cuotas restantes de paquetes de tráfico válidos. Compre un nuevo paquete de tráfico o recargue su cuenta de manera oportuna para evitar pérdidas de servicio causadas por atrasos.
 - Comprar paquetes de tráfico de nuevo: Haga clic en **Buy Again** y compre paquetes según sus requisitos de servicio. Para obtener más información, consulte [Comprar de nuevo](#).
 - Comprar paquetes de tráfico: Haga clic en **Buy Traffic Package** y compre paquetes según sus requisitos de servicio.

6 Gestión de registros

CDN registra las solicitudes a todos los nombres de dominio, incluidos los eliminados. Si ha habilitado la función de proyecto de empresa, la gestión de registros no está disponible para estos nombres de dominio eliminados. Puede descargar registros de un período específico durante los últimos 30 días, o puede usar la [herramienta de combinación de registros](#) para combinar y descargar registros de diferentes días durante los últimos 30 días. A continuación, puede analizar el acceso a sus recursos de servicio en detalle.

Descripción del registro

Latencia del archivo de registro: puede consultar los archivos de registro generados durante las últimas seis horas en la página **Logs**.

Las reglas de nombres de registro son las siguientes: *Log time span-acceleration domain name-Service area.gz*. El área de servicio está representada por una abreviatura de dos letras. Los registros que terminan en **cn** son para áreas en el continente chino, y los que terminan en **ov** son para áreas fuera de China continental. Por lo tanto, un nombre de registro típico podría ser, **2018021123-www.example01.com-ov.gz**.

De forma predeterminada, se genera un archivo de registro para cada nombre de dominio cada hora, y se generan 24 archivos de registro cada día.

Ejemplo de contenido del archivo de registro

```
[05/Feb/2018:07:54:52 +0800] x.x.x.x 1 "-" "HTTP/1.1" "GET" "www.test.com" "/test/1234.apk" 206 720 HIT "Mozilla/5.0 (Linux; U; Android 6.0; en-us; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1 (KHTML, like Gecko) Mobile Safari/533.1"
"bytes=-256"
```

Tabla 6-1 describe cada campo (de izquierda a derecha) en el registro.

Tabla 6-1 Descripción de un archivo de registro CDN

No.	Descripción del campo	Ejemplo
1	Tiempo de generación de registros	[05/Feb/2018:07:54:52 +0800]
2	Dirección IP de acceso	x.x.x.x
3	Latencia (ms)	1

No	Descripción del campo	Ejemplo
4	Información de referencia	-
5	Identificador de protocolo HTTP	HTTP/1.1
6	Método de solicitud HTTP	GET
7	nombre de dominio de aceleración	www.test.com
8	Ruta de acceso solicitada	/test/1234.apk
9	Código de estado de HTTP	206
10	Tamaño de la respuesta (en bytes)	720
11	Estado de aciertos en caché	HIT
12	Información del User-Agent, que ayuda a los servidores a reconocer el sistema operativo, la versión del sistema operativo, la CPU, el navegador y la información de la versión del navegador	Mozilla/5.0 (Linux; U; Android 6.0; zh-cn; EVA-AL10 Build/HUAWEIEVA-AL10) AppleWebKit/533.1 (KHTML, like Gecko) Mobile Safari/533.1
13	<p>La información de rango especifica las posiciones del primer y último bytes para los datos que se van a devolver.</p> <p>bytes pueden expresarse mediante los tres métodos siguientes:</p> <ul style="list-style-type: none"> ● bytes=x-y: solicitar contenido del x-ésimo al y-ésimo byte. ● bytes=-y: solicitar contenido de los últimos y bytes. ● bytes=x-: solicitar contenido desde el xésimo hasta el último byte. 	bytes=-256

Descarga de registros

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, seleccione **Logs**.
3. Seleccione el nombre de dominio de aceleración y especifique el intervalo de tiempo para la consulta.
Todos los registros del intervalo de tiempo especificado se muestran en la lista de registros. Si no se reciben solicitudes dentro del período consultado, no se generan registros y no se muestran datos en la página.

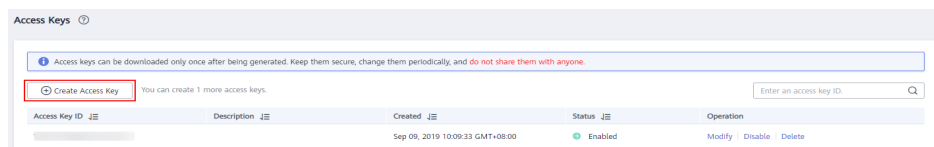
Figura 6-1 Gestión de registros

Name	Size	Start Time	End Time	Operation
2020	428.00 Byte	Nov 19, 2020 03:00:00 GMT+08:00	Nov 19, 2020 04:00:00 GMT+08:00	Download

- Haga clic en **Download** en la fila del registro deseado para descargar el archivo de registro en un equipo local.
- Descargue la **herramienta de combinación de registros** y utilice la herramienta para descargar los registros de un día específico en los últimos 30 días.

Antes de utilizar la herramienta de combinación de registros, **obtenga las claves de acceso**.

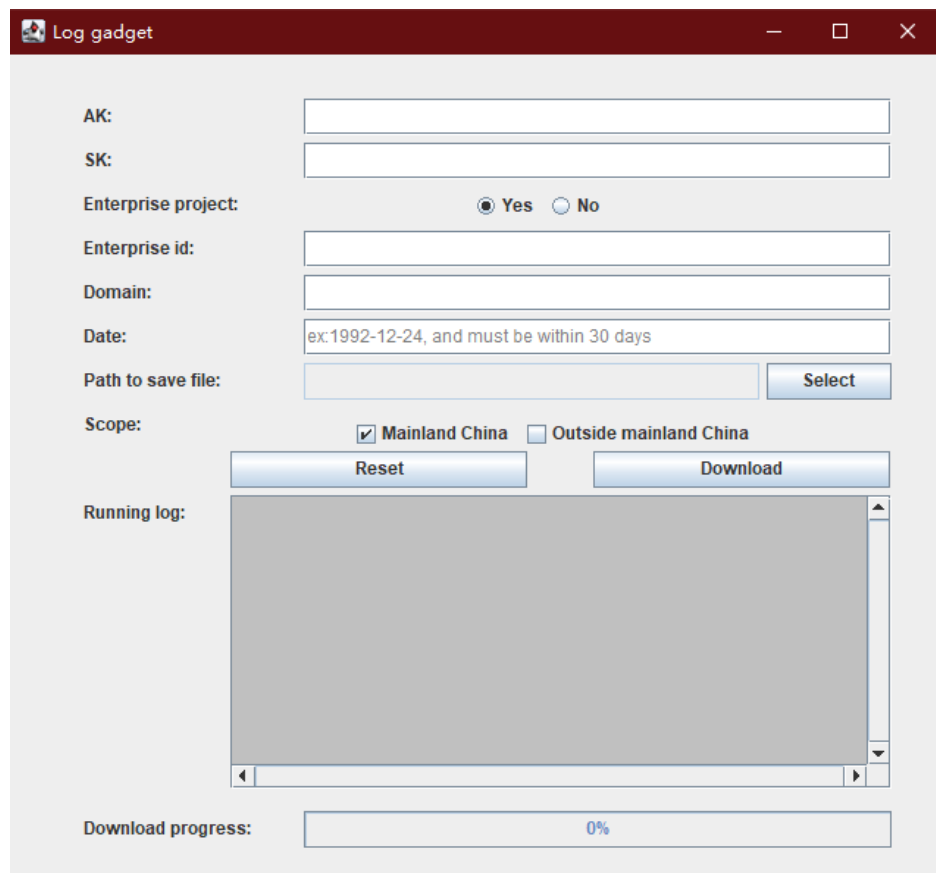
Figura 6-2 Obtención de claves de acceso



Haga clic en **Create Access Key** para obtener las claves de acceso. Las claves de acceso solo se pueden descargar una vez. Para la seguridad de la cuenta, se le aconseja cambiar periódicamente sus claves de acceso y mantenerlas seguras.

Uso de la herramienta Combinación de registros

- Descargue la herramienta de combinación de registros.
- Haga doble clic en logMerge.exe.



Parámetro	Descripción
AK/SK	Para obtener detalles sobre cómo obtener un par AK/SK, consulte Descarga de registros .
Enterprise project	Si selecciona Yes , introduzca un ID de empresa.
Enterprise id	Para obtener más información sobre cómo obtener un ID de proyecto empresarial, consulte ¿Cómo obtengo un ID de proyecto empresarial?
Domain	Nombre de dominio de aceleración cuyos registros se van a ver.
Date	Seleccione un día en los últimos 30 días, por ejemplo, 2022-03-21.
Path to save file	Ruta de acceso para almacenar archivos de registro.
Scope	China continental. Fuera de la China continental.
Running log	Se muestra el número de archivos descargados y los nombres de archivo originales. Si se produce un error, se muestra un mensaje de error.

- Haga clic en **Download** para descargar los registros del nombre de dominio seleccionado en el día especificado.

7 Gestión de certificados

Fondo

En este tema se describe cómo establecer un certificado HTTPS de un nombre de dominio e implementar la configuración HTTPS en todos los nodos de CDN para implementar la aceleración segura.

- **HTTP**
HTTP transfiere contenido en texto plano sin ninguna encriptación de datos. Si un atacante intercepta paquetes transmitidos entre el navegador y los servidores del sitio web, el contenido transmitido se puede leer directamente.
- **HTTPS**
Basado en HTTP, HTTPS utiliza Secure Sockets Layer (SSL) para cifrar la transmisión de datos. Con SSL, los servidores se autentican mediante certificados y las comunicaciones entre navegadores y servidores se cifran.

Escenarios

- Si tiene un certificado, puede subirlo directamente. También puede ver y eliminar certificados existentes.
- Puede comprar certificados o gestionar certificados existentes en el [SCM](#).

Configuración de un certificado

1. Inicie sesión en la [consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.
Se muestra la consola de CDN.
2. En el panel de navegación, elija **Certificates**.
3. Haga clic en **Configure Certificate** en la esquina superior izquierda.

Figura 7-1 Configuración de un certificado de propiedad propia

The screenshot shows a 'Configure Certificate' dialog box with a progress indicator at the top showing three steps: 1. Upload Certificate (active), 2. Associate Domain, and 3. Finish. The main content area contains several configuration options:

- Certificate Type:** Radio buttons for 'My certificate' (selected) and 'Huawei-managed certificate'.
- Certificate Name:** A text input field with the placeholder 'Enter your certificate name.'
- Certificate Body:** A text area containing 'PEM-encoded' with an 'Example' link below it.
- Private Key:** A text area containing 'PEM-encoded' with an 'Example' link below it.
- Origin Protocol:** Radio buttons for 'Retain the original value' (selected), 'HTTP', 'HTTPS', and 'Same as user'. A red warning message below states: 'If you have previously configured an origin protocol, all retrieval requests will comply with that setting. If you have not, the default protocol, HTTP, will be used.'
- Force Redirect:** Radio buttons for 'Retain the original value' (selected), 'Default', 'HTTP', and 'HTTPS'. A red warning message below states: 'If you have previously configured the redirection, all user requests will comply with that setting. If you have not, Force Redirect is disabled by default.'
- HTTP/2:** Radio buttons for 'Retain the original value' (selected), 'Enable', and 'Disable'. A red warning message below states: 'If you have previously configured the access protocol, all user requests will comply with that setting. If you have not, HTTP/2 is disabled by default.'

At the bottom, there are 'Next' and 'Cancel' buttons. A vertical toolbar on the right side of the dialog includes a close button (X), a help icon, and a refresh icon.

Figura 7-2 Configuración de un certificado gestionado por Huawei

The screenshot shows a 'Configure Certificate' dialog box with three steps: 1. Upload Certificate, 2. Associate Domain, and 3. Finish. Step 1 is currently active. The configuration options are as follows:

- Certificate Type:** Radio buttons for 'My certificate' and 'Huawei-managed certificate'. 'Huawei-managed certificate' is selected.
- Certificate Name:** A dropdown menu with the text 'Select a certificate.' Below it, a link says 'View certificate details or buy a new certificate on the [SCM console](#).'
- Certificate Body:** Unconfigured.
- Private Key:** Unconfigured.
- Origin Protocol:** Radio buttons for 'Retain the original value' (selected), 'HTTP', and 'HTTPS'. A note below states: 'If you have previously configured an origin protocol, all retrieval requests will comply with that setting. If you have not, the default protocol, HTTP, will be used.'
- Force Redirect:** Radio buttons for 'Retain the original value' (selected), 'Default', and 'HTTP'. A note below states: 'If you have previously configured the redirection, all user requests will comply with that setting. If you have not, Force Redirect is disabled by default.'
- HTTP/2:** Radio buttons for 'Retain the original value' (selected), 'Enable', and 'Disable'. A note below states: 'If you have previously configured the access protocol, all user requests will comply with that setting. If you have not, HTTP/2 is disabled by default.'

At the bottom, there are 'Next' and 'Cancel' buttons.

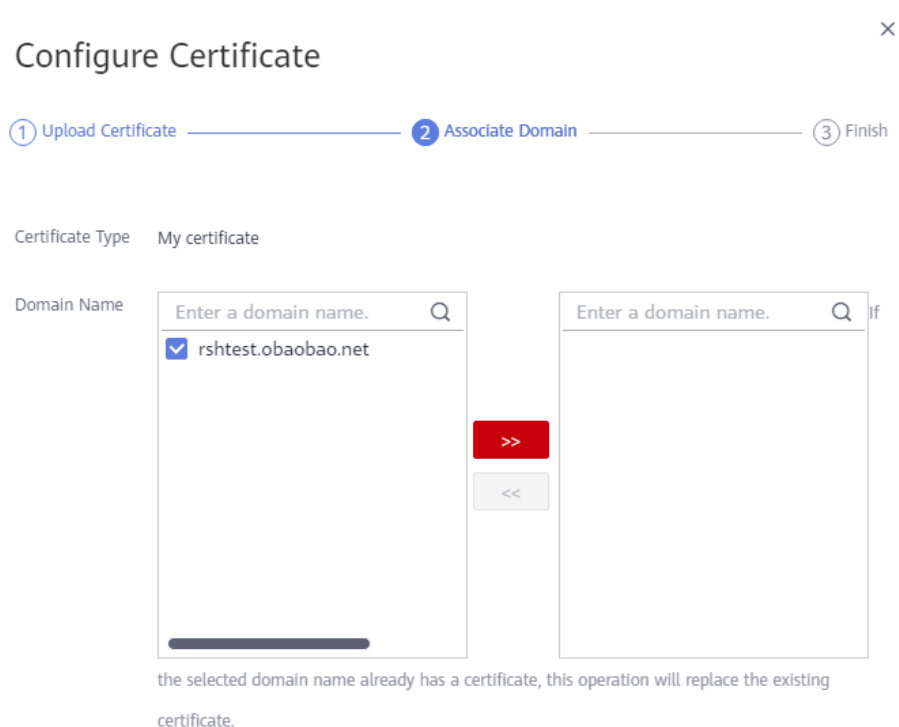
4. Configure los parámetros correspondientes.

Parámetro	Descripción
Certificate Type	My certificate o Huawei-managed certificate
Certificate Name	<ul style="list-style-type: none"> ● Si selecciona My certificate, introduzca el nombre del certificado. Un nombre de certificado puede tener hasta 32 caracteres. ● Si selecciona Huawei-managed certificate, vaya a la consola CCM para enviar un certificado a CDN y, a continuación, seleccione el certificado de la lista desplegable junto a Certificate Name en la consola CDN. Para obtener más información, consulte Cómo enviar un certificado SSL a otros servicios en la nube.

Parámetro	Descripción
Certificate Body	<ul style="list-style-type: none"> ● Si selecciona My certificate, utilice un editor de texto local para abrir el certificado y copiar el contenido del certificado en el cuadro de texto. Para obtener más información sobre el formato de certificado, consulte Requisitos del certificado HTTPS. ● Si selecciona Huawei-managed certificate, el contenido se completa automáticamente. <p>NOTA El cuerpo del certificado no puede contener espacios ni líneas en blanco. De lo contrario, se muestra un mensaje que indica que los parámetros del certificado son incorrectos.</p>
Private Key	<ul style="list-style-type: none"> ● Si selecciona My certificate, utilice un editor de texto local para abrir la clave privada y copiar el contenido en el cuadro de texto. Para obtener más información acerca de los requisitos de formato de clave privada, consulte RSA Private Key. ● Si selecciona Huawei-managed certificate, el contenido se completa automáticamente.
Origin Protocol	<ul style="list-style-type: none"> ● Retain the original value: Si ha configurado previamente un protocolo de origen, todas las solicitudes de recuperación cumplirán con esa configuración. Si no se ha configurado ningún protocolo de origen, se utilizará el protocolo predeterminado, HTTP. ● HTTP: Las solicitudes de recuperación cumplirán con el protocolo HTTP. ● HTTPS: Las solicitudes de recuperación cumplirán con el protocolo HTTPS. ● Same as user: Las solicitudes de recuperación cumplirán con el protocolo HTTP o HTTPS, dependiendo del utilizado por las solicitudes de usuario.
Force Redirect	<ul style="list-style-type: none"> ● Retain the original value: Si ha configurado previamente la redirección, todas las solicitudes de usuario cumplirán con esa configuración. Si no se ha configurado ninguna redirección, Force Redirect está deshabilitado de forma predeterminada. ● Default: Las solicitudes de usuario enviadas a los nodos CDN admiten tanto HTTP como HTTPS. ● HTTPS: Todas las solicitudes de usuario enviadas a los nodos CDN serán redirigidas a la fuerza a HTTPS. ● HTTP: Todas las solicitudes de usuario enviadas a los nodos CDN se redirigirán a la fuerza a HTTP.

Parámetro	Descripción
HTTP/2	<ul style="list-style-type: none"> ● Retain the original value: Si ha configurado previamente el protocolo de acceso, todas las solicitudes de usuario cumplirán con esa configuración. Si no se ha configurado ningún protocolo de acceso, HTTP/2 está deshabilitado de forma predeterminada. ● Enable: HTTP/2 estará habilitado. Todas las solicitudes de usuario enviadas a los nodos CDN cumplirán con HTTP/2. ● Disable: HTTP/2 será deshabilitado.

5. Haga clic en **Next** para asociar el certificado con su nombre de dominio.



6. Seleccione un nombre de dominio que se asociará a la izquierda, haga clic en el icono para asociar el nombre de dominio y haga clic en **Next**.

NOTA

Si el nombre de dominio seleccionado ya utiliza un certificado, esta operación reemplazará al certificado existente.

7. Haga clic en **Finish** para implementar la aceleración segura HTTPS para el nombre de dominio asociado.

Configure Certificate

① Upload Certificate — ② Associate Domain — ③ Finish

Domain Name	Status
rshtest.obaobao.net	Certificate associated successfully

Eliminación de un certificado administrado

- Al eliminar un certificado se eliminará del servidor, pero no se eliminarán los datos asociados con el certificado.
- Deshabilite HTTPS antes de eliminar un certificado asociado a su dominio.
- Para volver a usar el certificado, vuelva a presionarlo de SCM a CDN.

Procedimiento

1. Haga clic en **Delete Huawei-managed Certificate** en la esquina superior izquierda.
2. En la página mostrada, seleccione el certificado que desea eliminar y haga clic en **OK**.

Delete Huawei-managed Certificate

i • Deleting a certificate will remove it from the server but will not delete any data associated with the certificate.
• Disable HTTPS before deleting a certificate associated with your domain.
• If you want to use a Huawei-managed certificate again, you will need to re-push it to CDN.

Certificate Only display certificates that can be deleted.

<input checked="" type="checkbox"/> Certificate Name	Certificate Status	Valid Until
<input checked="" type="checkbox"/> test	Normal	2021/01/08 16:21:18 GM...

3. En el cuadro de diálogo mostrado, haga clic en **OK**.

NOTA

Para volver a usar el certificado, vuelva a presionarlo de SCM a CDN.

8 Comprobación de direcciones IP de nodo

Si el contenido que se muestra en la página de acceso del nombre de dominio de aceleración es anormal, puede utilizar la herramienta de comprobación de direcciones IP de nodo para comprobar si la dirección IP especificada es la dirección IP de un nodo de Huawei Cloud CDN. De esta manera, usted puede saber si la anomalía es causada por la red del operador u otras razones.

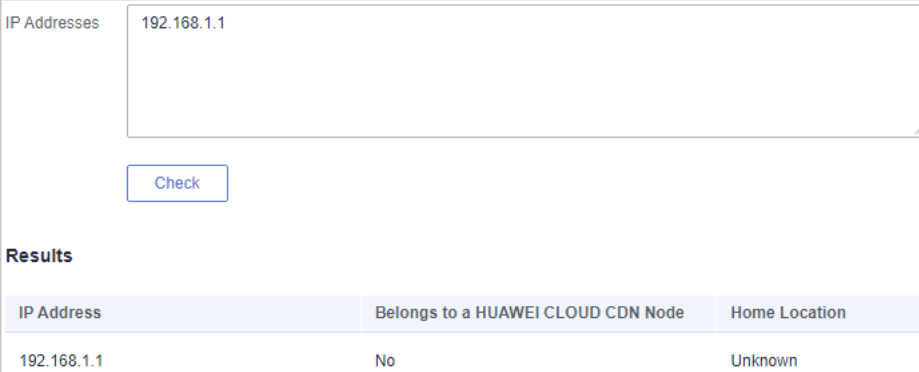
- Si el resultado de la comprobación muestra que la dirección IP no es la de un nodo de CDN de Huawei Cloud, el problema puede estar en la red del operador. En este caso, póngase en contacto con su operador.
- Si la dirección IP pertenece a un nodo de CDN de Huawei Cloud, corrija el error haciendo referencia a [Troubleshooting](#).

Procedimiento

1. Inicie sesión en la [Consola de Huawei Cloud](#). En la página principal de la consola de gestión, elija **Service List > Storage > CDN**.

Se muestra la consola de CDN.

2. En el panel de navegación, elija **Diagnosis > IP Address Check** para ir a la página de comprobación de dirección IP del nodo,



The screenshot shows the 'IP Address Check' interface. At the top, there is a text input field labeled 'IP Addresses' containing the IP address '192.168.1.1'. Below the input field is a blue 'Check' button. Underneath the button is a section titled 'Results' which contains a table with the following data:

IP Address	Belongs to a HUAWEI CLOUD CDN Node	Home Location
192.168.1.1	No	Unknown

3. Introduzca las direcciones IP que desea seleccionar en el cuadro de texto **IP Addresses**. Introduzca cada dirección IPv4 o IPv6 en líneas separadas. Se puede comprobar un máximo de 20 direcciones IP a la vez.
4. Haga clic en **Check**.

Una vez completado el diagnóstico, el sistema muestra los resultados en la lista.

9 Gestión de permisos

9.1 Creación de un usuario y concesión de permisos de CDN

Este capítulo describe cómo usar **IAM** para implementar un control de permisos detallado para sus recursos de CDN. Con IAM, usted puede:

- Cree usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tendrá sus propias credenciales de seguridad para acceder a los recursos de CDN.
- Conceder sólo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confíe una cuenta o servicio en la nube en Huawei Cloud para realizar operaciones profesionales y eficientes en sus recursos de CDN.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM, omita este capítulo.

En esta sección se describe el procedimiento para conceder permisos.

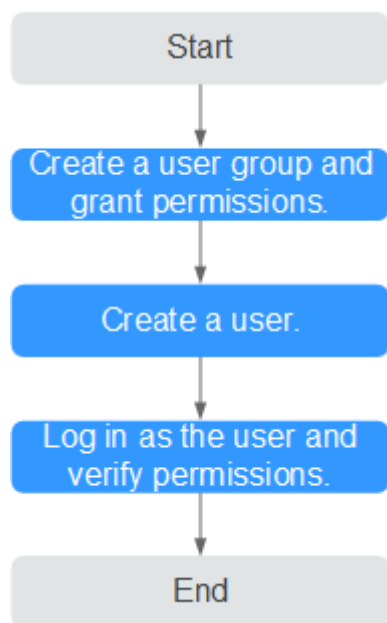
Prerrequisitos

Obtenga información sobre los permisos (consulte **Gestión de permisos**) admitidos por CDN y elija políticas o roles de acuerdo con sus requisitos. Para ver las políticas del sistema de otros servicios, consulte **Permisos del sistema**.

Flujo del proceso

Figura 9-1 muestra el proceso de concesión de permisos de CDN.

Figura 9-1 Proceso de concesión de permisos de CDN



1. **Crear un grupo de usuarios y asignar permisos.**

Cree un grupo de usuarios en la consola de IAM y asigne la política **CDN DomainReadOnlyAccess** al grupo.

2. **Crear un usuario de IAM.**

Cree un usuario en la consola IAM y agregue el usuario al grupo creado en 1.

3. **Iniciar sesión** y verificar los permisos.

Inicie sesión en la consola de CDN como usuario creado y verifique que solo tenga permisos de lectura para nombres de dominio de CDN.

- Habilitar o deshabilitar un nombre de dominio de aceleración. Si aparece un mensaje que indica que no tiene permisos suficientes para realizar la operación, la política **CDN DomainReadOnlyAccess** ya ha entrado en vigor.

Domain Name	Status	CNAME	Service Type	Modified	Operation
<input type="checkbox"/> www.def.huawei.com	Enabled	www.def.huawei.com.cdnhw1.com	Website	2019/05/29 16:15:36 GMT+08:00	Monitor Settings More
<input type="checkbox"/> example5.huawei.com	Enabled	example5.huawei.com.cdnhw1.com	Website	2019/05/22 15:27:48 GMT+08:00	Monitor Settings More
<input type="checkbox"/> example4.huawei.com	Enabled	example4.huawei.com.cdnhw1.com	Website	2019/05/22 10:06:18 GMT+08:00	Monitor Settings More

- Elija cualquier otro servicio en **Service List**. Si aparece un mensaje que indica que no tiene permisos suficientes para acceder al servicio, la política **CDN DomainReadOnlyAccess** ya ha entrado en vigor.

9.2 Creación de una política personalizada

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de CDN. Para ver las acciones que se pueden agregar a las directivas personalizadas, consulte **Políticas de permisos y acciones admitidas**.

Puede crear directivas personalizadas de cualquiera de las dos formas siguientes:

- Editor visual: Seleccione los servicios en la nube, acciones, recursos y condiciones de solicitud sin la necesidad de conocer la sintaxis de la política.

- JSON: Editar las políticas JSON desde cero o basándose en una política existente.

Para obtener más información, consulte [Creación de una política personalizada](#). Esta sección proporciona ejemplos de políticas de CCE personalizadas comunes.

Ejemplo de políticas personalizadas

- Ejemplo 1: Permitir a los usuarios crear nombres de dominio de aceleración

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cdn:configuration:createDomains"
      ]
    }
  ]
}
```

- Ejemplo 2: Permitir a los usuarios establecer una lista negra de IP

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "cdn:configuration:modifyIpAcl"
      ],
      "Effect": "Allow"
    }
  ]
}
```

- Ejemplo 3: Negar a los usuarios que eliminen nombres de dominio de aceleración.

Una política con solo permisos "Deny" debe usarse junto con otras políticas para que surtan efecto. Si los permisos asignados a un usuario contienen acciones Allow y Deny, las acciones Deny tienen prioridad sobre las acciones Allow.

El siguiente método se puede utilizar si necesita asignar permisos de la política de **CDN Admin** a un usuario, pero también prohibir que el usuario elimine los nombres de dominio de aceleración. Crear una política personalizada para denegar la eliminación de nombres de dominio de aceleración y asigne ambas políticas al grupo al que pertenece el usuario. A continuación, el usuario puede realizar todas las operaciones en CDN excepto la eliminación de nombres de dominio de aceleración. El siguiente se muestra un ejemplo de política de denegación:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "cdn:configuration:deleteDomains"
      ],
      "Effect": "Deny"
    }
  ]
}
```

- Ejemplo 4: Definición de permisos para varios servicios en una política

Una política personalizada puede contener las acciones de varios servicios que son de tipo global o de nivel de proyecto. A continuación se muestra una política de ejemplo que contiene acciones de varios servicios:

```
{
  "Version": "1.1",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [  
      "cdn:configuration:enableDomains",  
      "cdn:configuration:createDomains",  
      "scm:cert:get",  
      "scm:certProduct:get",  
      "scm:certType:get"  
    ]  
  }  
]
```

10 Proyectos empresariales

Huawei Cloud Enterprise Management permite la gestión unificada de recursos en la nube por proyecto empresarial. Puede gestionar recursos y personal en proyectos de empresa y asignar uno o más grupos de usuarios para gestionar proyectos de empresa. Puede crear proyectos empresariales de CDN en la consola de Enterprise Management para gestionar sus recursos de dominio de manera centralizada.

Creación de un proyecto de empresa

Para crear un proyecto de empresa de CDN:

1. En la consola de Enterprise Management, cree un proyecto de empresa basado en los requisitos de su empresa. Por ejemplo, puede crear proyectos empresariales basados en los tipos de servicio de los nombres de dominio de aceleración de CDN. Para más detalles, consulte [Creación de un Proyecto empresarial](#).
2. Después de crear un proyecto de empresa, puede migrar los recursos de nombre de dominio a un proyecto de empresa especificado. Para obtener más información, consulte [Servicios en la nube admitidos por EPS](#).

NOTA

- De forma predeterminada, se crea un proyecto de empresa denominado **default**. Este proyecto se utiliza para gestionar los recursos que no están asignados a un proyecto de empresa específico.
- La migración de un nombre de dominio de aceleración entre proyectos de empresa no afecta al servicio de aceleración.

Autorización de proyecto empresarial

Después de crear un proyecto de empresa y migrar los recursos de CDN al proyecto de empresa, puede agregar grupos de usuarios existentes y establecer directivas de permisos de grupo de usuarios para el proyecto de empresa en función de los requisitos del sitio. Sin estas directivas, los miembros del grupo de usuarios no podrán acceder ni operar los recursos de dominio de CDN en el proyecto de empresa. Para obtener más información acerca de cómo establecer directivas de permisos de grupo de usuarios, vea [Gestión de permisos](#).

11 Auditoría

Cloud Trace Service (CTS) registra las operaciones en los recursos de la nube en su cuenta. Puede utilizar los registros para realizar análisis de seguridad, realizar un seguimiento de los cambios de recursos, auditar el cumplimiento y localizar fallos.

Habilitación de CTS

Un rastreador se creará automáticamente después de que CTS esté habilitado. Todas las seguimientos grabadas por CTS están asociadas con un rastreador. Actualmente, solo se puede crear un rastreador para cada cuenta.

Para obtener más información sobre cómo habilitar el servicio de auditoría en la nube, consulte [Habilitación de CTS](#).

Operaciones de CDN grabadas por CTS

Tabla 11-1 Operaciones de CDN que pueden ser grabadas por CTS

Operación	Descripción
createDomain	Creación de un nombre de dominio
updateDomain	Actualización de un nombre de dominio
deleteDomain	Eliminación de un nombre de dominio
enableDomain	Habilitación de nombres de dominio
disableDomain	Deshabilitación de nombres de dominio
updateOrigin	Configuración de un servidor de origen
updateOriginHost	Configuración de un host de recuperación
createRefer	Creación de una regla de referencia
createCertificate	Configuración de un certificado de dominio
createCacheRule	Creación de una regla de caché

Operación	Descripción
createRefreshTask	Creación de una tarea de actualización de caché
createPreheatingTask	Creación de una tarea de precalentamiento de caché

Consulta de trazas CTS

Después de habilitar CTS, el sistema comienza a grabar las operaciones de CDN. Puede ver las operaciones de los últimos siete días en la consola CTS. Para obtener más información, consulte [Consulta de seguimientos en tiempo real](#)

Desactivación de CTS

Puede desactivar los rastreadores en la consola CTS. Después de deshabilitar un rastreador, el sistema detendrá las operaciones de grabación, pero aún puede ver los registros históricos. Para obtener más información sobre cómo deshabilitar un rastreador, consulte [Desactivación o Habilitación de un Tracker](#).