

CDN

Guia de usuário

Edição 01
Data 18-07-2023



Copyright © Huawei Technologies Co., Ltd. 2023. Todos os direitos reservados.

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Technologies Co., Ltd.

Marcas registadas e permissões



HUAWEI e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd.

Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Índice

1 Gerenciamento de nomes de domínio.....	1
1.1 Funções.....	1
1.2 Ativação/desativação de CDN para um nome de domínio.....	2
1.3 Remoção de um nome de domínio.....	5
1.4 Cópia de configurações de domínio.....	6
1.5 Revisão de um nome de domínio.....	8
1.6 Política de encerramento de serviço.....	9
1.7 Gerenciamento de cotas de nomes de domínio.....	12
2 Configurações de nome de domínio.....	14
2.1 Visão geral.....	14
2.2 Configurações básicas.....	17
2.2.1 Modificação de detalhes do servidor de origem.....	17
2.2.2 Alteração de área de serviço.....	20
2.2.3 Configuração do IPv6.....	21
2.3 Configurações de recuperação.....	21
2.3.1 Visão geral.....	21
2.3.2 Host de recuperação.....	22
2.3.3 Protocolo de origem.....	24
2.3.4 Reescrita dos URLs de solicitação de recuperação.....	25
2.3.5 Recuperação de intervalo.....	27
2.3.6 Recuperação redirecionada.....	29
2.3.7 Recuperação de bucket privado do OBS.....	30
2.3.8 Cabeçalhos de solicitação de recuperação.....	33
2.3.9 Intervalo de tempo limite de recuperação.....	38
2.3.10 Perguntas frequentes.....	39
2.4 Configurações de HTTPS.....	40
2.4.1 Visão geral.....	41
2.4.2 Certificados de HTTPS.....	41
2.4.3 Requisitos do certificado HTTPS.....	46
2.4.4 Conversão de formato de certificado de HTTPS.....	49
2.4.5 Grampeamento de OCSP.....	50
2.4.6 Redirecionamento forçado.....	50
2.4.7 HTTP/2.....	51


2.4.8 Versões de TLS.....	52
2.4.9 Perguntas frequentes.....	53
2.5 Configurações de cache.....	54
2.5.1 Visão geral.....	54
2.5.2 Regras de cache.....	55
2.5.3 Filtragem de parâmetros de URL.....	60
2.5.4 Controle de cache de origem.....	62
2.5.5 Idade de cache de código de estado.....	64
2.6 Controle de acesso.....	65
2.6.1 Visão geral.....	66
2.6.2 Configuração de validação do referenciador.....	66
2.6.3 Configuração de uma ACL.....	70
2.6.4 Configuração de uma lista negra ou lista branca do agente de usuário.....	72
2.6.5 Configuração de assinatura de URL.....	73
2.6.5.1 Método de assinatura A.....	73
2.6.5.2 Método de assinatura B.....	78
2.6.5.3 Método de assinatura C1.....	82
2.6.5.4 Método de assinatura C2.....	86
2.6.6 Configuração de autenticação remota.....	91
2.7 Configurações avançadas.....	96
2.7.1 Configurações de cabeçalho HTTP (solicitações de origem cruzada).....	96
2.7.2 Páginas de erro personalizadas.....	102
2.7.3 Compressão inteligente.....	103
3 Atualização e pré-aquecimento de cache.....	105
3.1 Visão geral.....	105
3.2 Atualização de cache.....	105
3.3 Pré-aquecimento de cache.....	107
3.4 Exibição de progressos de tarefa.....	109
3.5 Perguntas frequentes.....	109
4 Análise de estatísticas.....	113
4.1 Descrição de estatística.....	113
4.2 Estatísticas de utilização.....	114
4.3 Estatísticas de acesso.....	116
4.4 Estatísticas do servidor de origem.....	117
4.5 Hotspots.....	119
4.6 Estatísticas de região & de operadora.....	119
4.7 Códigos de estado.....	122
4.8 Estatísticas de utilização para aceleração de todo o site.....	123
4.9 Perguntas frequentes.....	124
5 Gerenciamento de pacotes.....	126
6 Gerenciamento de log.....	127

7 Gerenciamento de certificados.....	131
8 Verificação de endereços IP de nó.....	137
9 Gerenciamento de permissões.....	138
9.1 Criação de um usuário e concessão de permissões de CDN.....	138
9.2 Criação de uma política personalizada.....	139
10 Projetos empresariais.....	142
11 Auditoria.....	143

1 Gerenciamento de nomes de domínio

1.1 Funções

Depois que um nome de domínio é adicionado, você pode habilitar, desabilitar, remover e revisar o nome de domínio no console da CDN. Você também pode configurar a política de terminação do nome de domínio.

Você pode clicar em  no canto superior direito da página **Domains** para exportar configurações básicas de nomes de domínio para um arquivo do Excel.

Cenários

A tabela a seguir descreve as funções.

Tabela 1-1 Cenários

Item	Descrição	API
Ativação/ desativação de CDN para um nome de domínio	Enable: você pode habilitar um nome de domínio no estado Disabled . Disable: você pode desabilitar um nome de domínio no estado Enabled ou Error .	Ativação de CDN para um nome de domínio Desativação de CDN para um nome de domínio
Remoção de um nome de domínio	Você pode remover um nome de domínio no estado Disabled ou Rejected . NOTA Depois que um nome de domínio é removido, o sistema exclui automaticamente a configuração correspondente do nome de domínio. Se você quiser usar CDN para o nome de domínio removido novamente, adicione novamente e configure o nome de domínio.	Exclusão de um nome de domínio

Item	Descrição	API
Cópia de configurações de domínio	Você pode copiar a configuração de um nome de domínio para outros nomes de domínio.	-
Revisão de um nome de domínio	Se um nome de domínio for banido devido à expiração da licença ICP, você pode solicitar que ele seja revisado depois que o nome de domínio for novamente licenciado. Depois que a revisão for aprovada, a CDN desbanirá o nome de domínio.	-
Política de encerramento de serviço	O serviço CDN da HUAWEI CLOUD é encerrado com base em uma política predefinida. Você pode selecionar Redirect to origin server ou Disable domain name para a política de encerramento.	-
Gerenciamento de cotas de nomes de domínio	As cotas são impostas para recursos de serviço na plataforma para evitar picos imprevistos no uso de recursos. As cotas podem limitar o número ou a quantidade de recursos disponíveis para os usuários. Se a cota de nome de domínio existente não puder atender aos seus requisitos de serviço, envie um tíquete de serviço para solicitar uma cota mais alta.	-

1.2 Ativação/desativação de CDN para um nome de domínio

Cenários

Você pode habilitar ou desabilitar a CDN para seus nomes de domínio na página **Domains** no console da CDN.

Exibição de informações básicas do domínio

Na página **Domains** do **console de CDN**, clique em **Configure** na linha que contém o nome de domínio de destino. Na página de guia **Basic Settings**, exiba as informações básicas sobre o nome de domínio.

Os status do domínio incluem **Enabled**, **Disabled**, **Configuring**, **Error**, **Reviewing**, **Rejected**, e **Removing**.

Desativação de CDN para nomes de domínio

Você pode desativar a CDN para um nome de domínio cujo status é **Enabled** ou **Error**. Depois que a CDN for desabilitada, a CDN não fornecerá mais serviços de aceleração para seu nome de domínio, mas as configurações de domínio permanecerão. Para restaurar o serviço de aceleração, habilite o CDN novamente.

Para manter seu site acessível, aponte seu nome de domínio para um registro CNAME que não esteja alocado pela CDN da Huawei Cloud em sua provedor de DNS antes de desabilitar o CDN.

NOTA

Os serviços de CDN para nomes de domínio que não foram acessados por mais de 180 dias serão automaticamente desativados.


Desativação de CDN para um único nome de domínio

Na página **Domains** do **console de CDN**, escolha **More > Disable** na linha que contém o nome de domínio para o qual a CDN deve ser desabilitada.

Domain Name	Status	CNAME	Service T...	Modified	Operation
exa...	Enabled	exa...aw...	File downlo...	Sep 16, 20...	Monitor Settings Copy Configuration More
exa...	Enabled	exa...hu...	File downlo...	Sep 16, 20...	Monitor Settings Copy Configuration Review
exa...	Enabled	exa...ia...	File downlo...	Aug 10, 2...	Monitor Settings Copy Configuration Disable
ww...	Enabled	ww...31...	Whole site	Apr 06, 20...	Monitor Settings Copy Configuration Remove

Confirme as informações sobre o nome de domínio e clique em **Yes**.

Disable CDN

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

Domain Name	Status	Service Type
exa...ei.com	Enabled	File download

Desativação de CDN para vários nomes de domínio

Na página **Domains** do **console de CDN**, selecione os nomes de domínio para os quais a CDN será desabilitada e clique em **Disable** acima da lista de nomes de domínio.

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

1. Na página **Domains** do console CDN, escolha **More > Disable** na linha que contém o nome de domínio para o qual a CDN deve ser desabilitada. (Para desativar a CDN para

vários nomes de domínio, selecione os nomes de domínio e clique em **Disable** acima da lista de nomes de domínio.)

2. Confirme as informações sobre o nome de domínio e clique em **Yes**.

Ativação de CDN para nomes de domínio

Você pode habilitar o CDN para um nome de domínio cujo status é **Disabled**.

1. Na página **Domains** do console de CDN, escolha **More > Enable** na linha que contém o nome de domínio para o qual a CDN deve ser habilitada. (Para habilitar o CDN para vários nomes de domínio, selecione os nomes de domínio e clique em **Enable** acima da lista de nomes de domínio.)
2. Confirme as informações sobre o nome de domínio e clique em **Yes**.


Ativação de CDN para um único nome de domínio

Na página **Domains** do [console de CDN](#), escolha **More > Enable** na linha que contém o nome de domínio para o qual a CDN deve ser habilitada.

Domain Name	Status	CNAME	Service T...	Modified	Operation
exa...en...	Disabled	exa...en...	File downlo...	Sep 16, 2021 ...	Monitor Settings Copy Configuration More
exa...h...	Disabled	exa...hu...	File downlo...	Sep 16, 2021 ...	Monitor Settings Copy Configur... Review Enable Disable
exa...h...	Enabled	exa...h...	File downlo...	Aug 10, 2021...	Monitor Settings Copy Configura...
ww...l...	Enabled	ww...ple...	Whole site	Apr 06, 2021 ...	Monitor Settings Copy Configura...

Confirme as informações sobre o nome de domínio e clique em **Yes**.

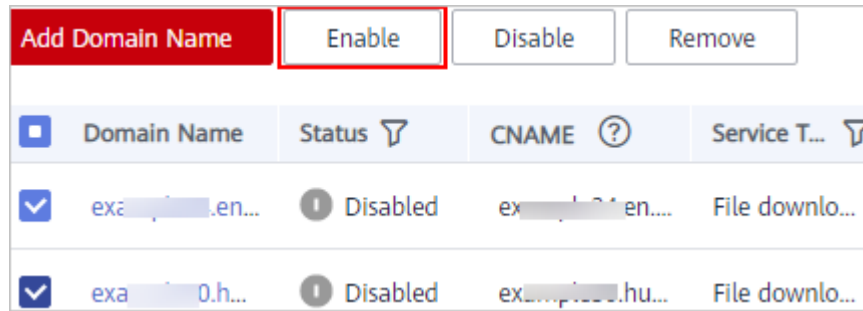
Enable CDN

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

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

Ativação de CDN para vários nomes de domínio

Na página **Domains** do [console de CDN](#), selecione os nomes de domínio para os quais a CDN deve ser habilitada e clique em **Enable** acima da lista de nomes de domínio.



1.3 Remoção de um nome de domínio

Cenários

Se você não quiser mais acelerar um nome de domínio, poderá removê-lo da página **Domains** do console de CDN. O sistema eliminará automaticamente a configuração correspondente do nome de domínio. Se você quiser acelerar o nome de domínio removido novamente, adicione novamente e reconfigure o nome de domínio.

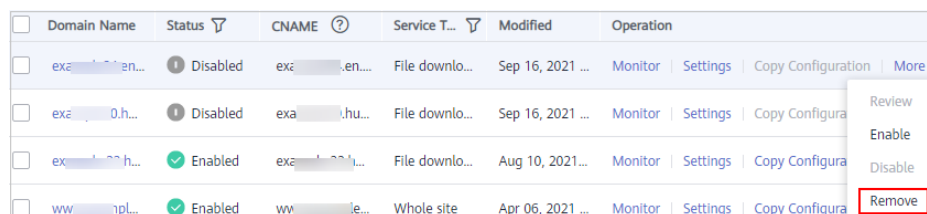
Somente os nomes de domínio que estão no estado **Disabled** ou **Rejected** podem ser removidos.

NOTA

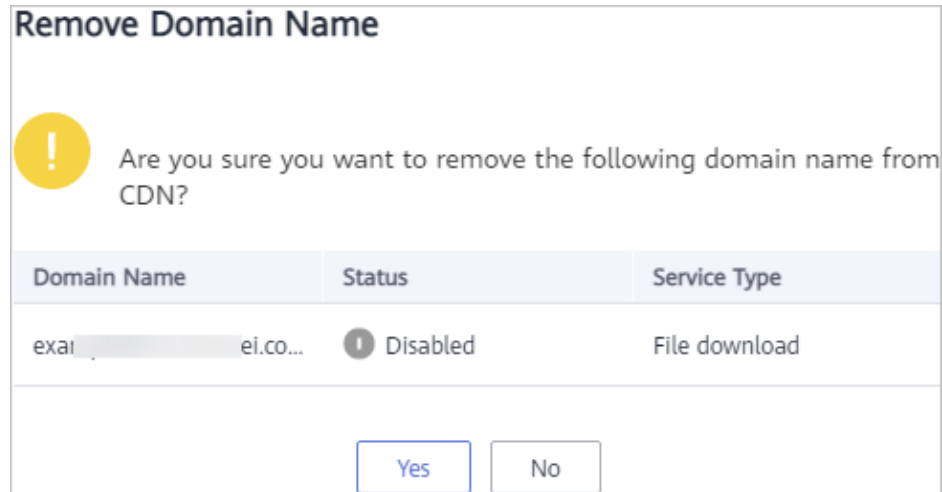
Se um nome de domínio estiver no estado **Disabled** ou **Rejected** por mais de 120 dias, o sistema removerá automaticamente esse nome de domínio. Se a aceleração de CDN for necessária para o nome de domínio, adicione o nome de domínio novamente.

Remoção de um único nome de domínio

Na página **Domains** do [console de CDN](#), escolha **More > Remove** na linha que contém o nome de domínio a ser removido.

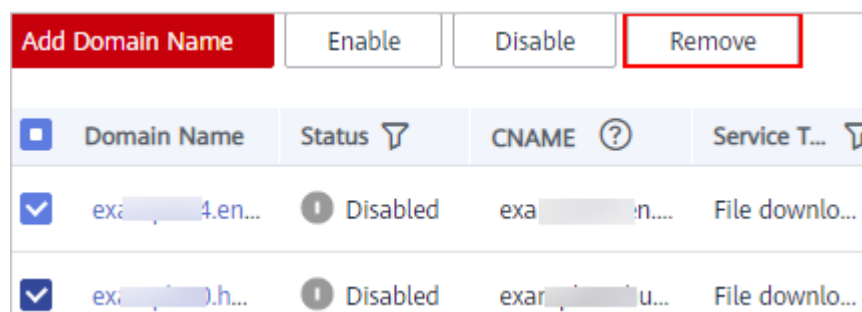


Confirme as informações sobre o nome de domínio e clique em **Yes**.



Remoção de vários nomes de domínio

Na página **Domains** do [console de CDN](#), selecione os nomes de domínio a serem removidos e clique em **Remove** acima da lista de nomes de domínio.



1.4 Cópia de configurações de domínio

Você pode copiar a configuração de um nome de domínio para outros nomes de domínio.

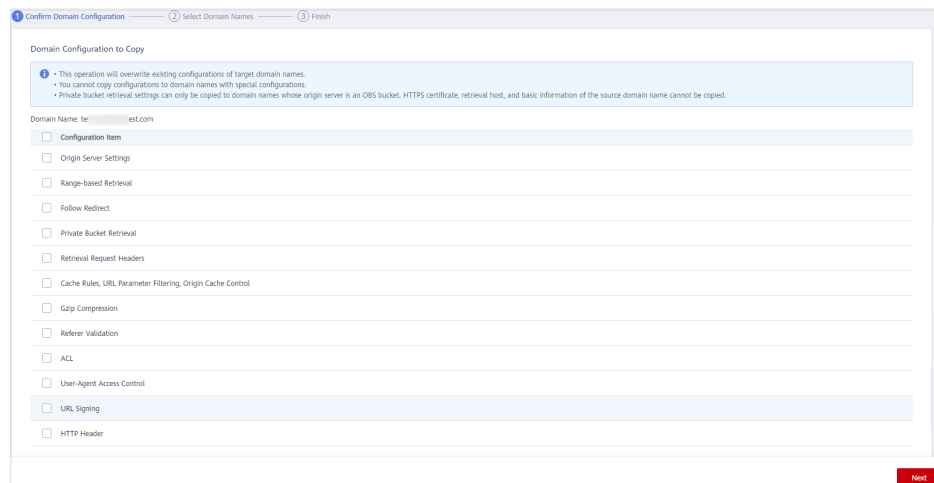
Precauções

- Somente a configuração de um nome de domínio no estado **Enabled** pode ser copiada.
- A cópia de configuração não pode ser desfeita. Antes de copiar a configuração de um nome de domínio, verifique se a configuração está correta.
- Configurações especiais de domínio não podem ser copiadas.
- Para um nome de domínio com alto tráfego ou largura de banda, tenha cuidado ao copiar sua configuração para evitar perdas econômicas.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.

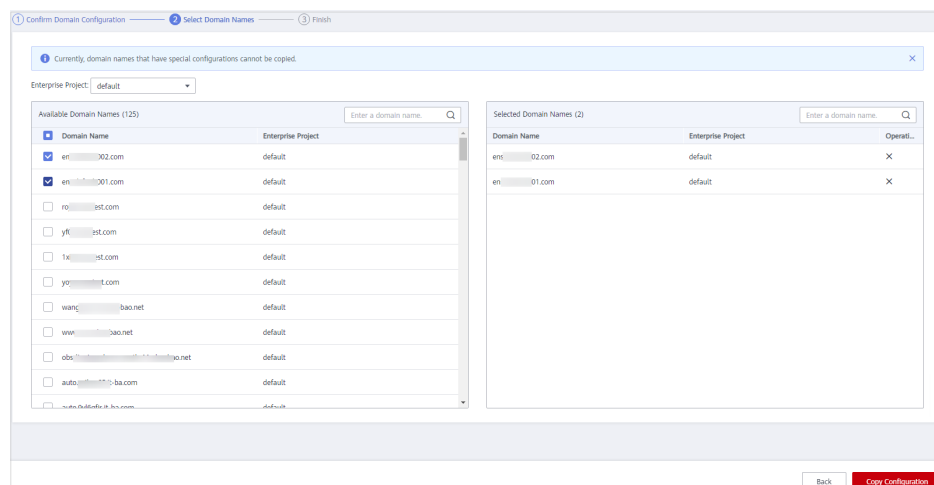
3. Na página **Domains**, clique em **Copy Configuration** na coluna **Operation** da linha que contém o nome de domínio de destino. A página **Confirm Domain Configuration** é exibida.



NOTA

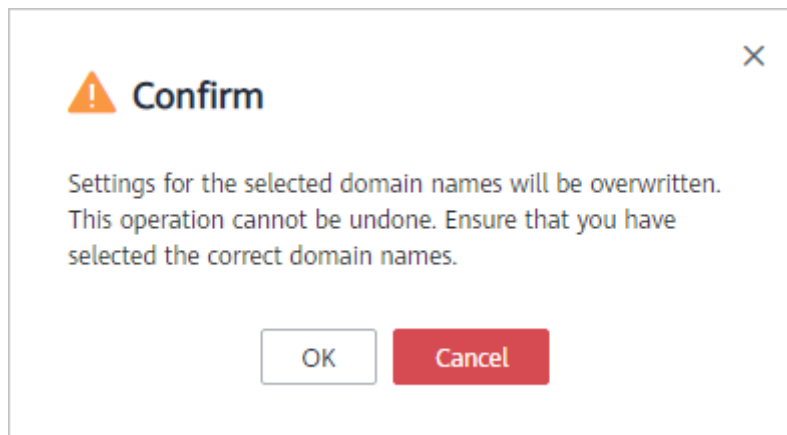
Se você copiar a configuração para outros nomes de domínio, as configurações originais desses nomes de domínio serão substituídas.

4. Selecione os itens de configuração a serem copiados e clique em **Next**.

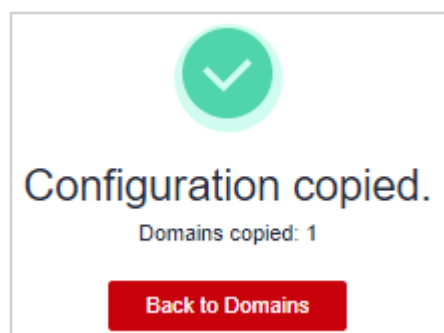


NOTA

- Se você ativou a função de projeto corporativo, os nomes de domínio disponíveis serão exibidos pelo projeto corporativo.
 - Você pode selecionar até 10 nomes de domínio de destino.
 - As configurações não podem ser copiadas para nomes de domínio com configurações especiais.
5. Selecione os nomes de domínio cujas configurações precisam ser sobregravadas e clique em **Copy Configuration**.



6. Clique em **OK**.



1.5 Revisão de um nome de domínio

Cenários

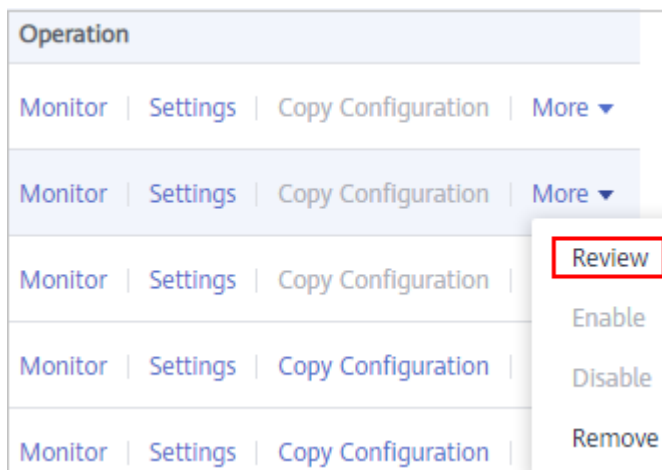
Se um nome de domínio for banido devido à expiração da licença ICP, você pode solicitar que ele seja revisado depois que o nome de domínio for novamente licenciado. Depois que a revisão for aprovada, a CDN desbanirá o nome de domínio.

NOTA

- Se um nome de domínio for banido por outros motivos, ele não poderá ser desbanido por meio de análises.
- Se um nome de domínio for banido devido a violações dos regulamentos de conteúdo (sexualmente explícito, drogas ilegais, jogos de azar ou conteúdo extremista) ou for atacado, ele será banido permanentemente.

Procedimento

Na página **Domains** do [console de CDN](#), escolha **More > Review** na linha que contém o nome de domínio a ser revisado.



Os resultados da revisão dependem se o nome de domínio foi banido porque a licença ICP expirou ou por algum outro motivo.

- Banido porque a licença ICP expirou:
 - Se o nome de domínio tiver sido novamente licenciado, o sistema exibirá uma mensagem indicando que o nome de domínio foi desbanido.
 - Se o nome de domínio ainda não tiver sido novamente licenciado, o sistema exibirá uma mensagem indicando que o nome de domínio não foi licenciado. Neste caso, obtenha a licença do Ministério da Indústria e Tecnologia da Informação (MIIT) e tente novamente.

- Proibido por outros motivos

Se o nome de domínio foi banido por razões diferentes ou para além de uma licença ICP expirada, é apresentada uma mensagem depois de clicar em **Review**, informando-o das razões. Resolva os problemas com base nos motivos e envie um tíquete de serviço para tentar novamente.

1.6 Política de encerramento de serviço

Se um nome de domínio atender às condições para o término do serviço, a CDN da Huawei Cloud deixará de fornecer serviços de aceleração para ele e você não poderá configurar as configurações para o nome de domínio.

Cenários

Huawei Cloud CDN encerrará os serviços de um nome de domínio no seguinte cenário:

Cenário	Descrição
Conta em atraso	Quando o período de retenção começar, a CDN da Huawei Cloud encerrará o nome de domínio até que você recarregue sua conta.

 **NOTA**

- Quando o serviço CDN for encerrado para um nome de domínio, a CDN enviará uma notificação por SMS ou e-mail para o seu número de telefone ou endereço de e-mail reservado. Você pode recarregar sua conta para restaurar o serviço CDN.
- Seu nome de domínio será banido se for atacado, sua licença de ICP tiver expirado ou tiver conteúdo inadequado. Seu serviço CDN não será encerrado.

Precauções

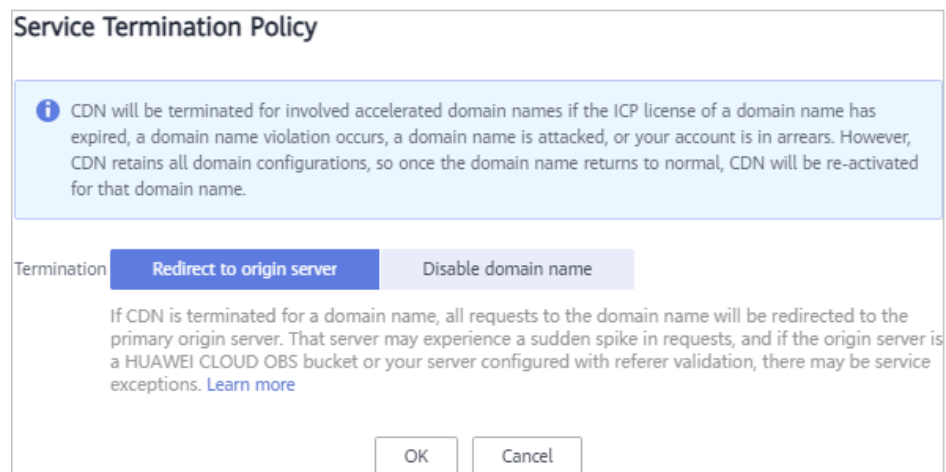
- A política de encerramento padrão é **Redirect to origin server**.
- A política de terminação do serviço CDN é uma política global. Isso entra em vigor para todos os nomes de domínio em sua conta.

Configuração de política de encerramento de serviço

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console da CDN é exibido.

2. Clique em **Service Termination Policy** no canto superior direito da página **Domains**. A página de configuração da política de encerramento do serviço é exibida.



3. Selecione uma política de rescisão de serviço.

O serviço CDN da Huawei Cloud é encerrado com base em uma política predefinida. Você pode selecionar **Redirect to origin server** ou **Disable domain name** para a política de encerramento. A tabela a seguir descreve as políticas.

Política	Descrição
Redirecionar para o servidor de origem	<p>Todas as solicitações para o seu nome de domínio de aceleração são redirecionadas para o servidor de origem principal. O status do nome de domínio torna-se Disabled. O serviço de aceleração CDN é interrompido para o nome de domínio. O CDN retém os detalhes de configuração desse nome de domínio. Depois que o problema do nome de domínio for resolvido, as solicitações do nome de domínio serão encaminhadas aos nós CDN para aceleração.</p> <p>NOTA</p> <ul style="list-style-type: none"> • Depois que um nome de domínio de aceleração é encerrado por 30 dias, Huawei Cloud CDN não fornece mais o serviço de recuperação e o nome de domínio de aceleração não pode ser acessado. • Se você selecionar Redirect to origin server, o nome de domínio ou o endereço IP do servidor de origem será exposto aos usuários. Se você não quiser expor o domínio de origem ou o endereço IP de origem, selecione Disable domain name. • Se o seu site funciona corretamente após as solicitações serem redirecionadas para o servidor de origem depende do servidor de origem.
Desativar nome de domínio	<p>CDN coloca seu nome de domínio de aceleração off-line cujo status se torna Disabled. O nome de domínio não pode ser acessado, mas sua configuração é mantida. Depois que o nome de domínio voltar ao normal, o CDN o ativará.</p>

4. Clique em **OK**.

Processo de encerramento de serviço

A tabela a seguir descreve o processo de desabilitação do serviço CDN para um nome de domínio.

Cenário	Processo de encerramento de serviço
Conta em atraso	<ul style="list-style-type: none"> • Seus recursos da HUAWEI CLOUD (como recursos de domínio CDN) entram em um período de retenção. Para obter detalhes sobre o período de retenção, consulte Período de retenção. • A CDN encerrará os serviços para o nome de domínio de aceleração com base na política de rescisão definida.

A CDN encerrará os serviços para o nome de domínio de aceleração com base na política de encerramento definida, **Redirect to origin server** ou **Disable domain name**.

- **Redirect to origin server**
 - As solicitações para o nome de domínio são redirecionadas para o servidor de origem primário.
 - CDN desativa o nome de domínio de aceleração.
 - A CDN altera o status do nome de domínio para **Disabled** e interrompe o serviço de aceleração.

- **Disable domain name**
 - CDN desativa o nome de domínio de aceleração.
 - A CDN altera o status do nome de domínio para **Disabled** e interrompe o serviço de aceleração.

1.7 Gerenciamento de cotas de nomes de domínio

Cota total de nomes de domínio

As cotas são impostas para recursos de serviço na plataforma para evitar picos imprevistos no uso de recursos. As cotas limitam a quantidade e a capacidade dos recursos disponíveis para os usuários. Se uma cota de recursos existente não puder atender aos requisitos de serviço, envie um tíquete de serviço para aumentar a cota. A tabela a seguir lista as cotas padrão para nomes de domínio CDN.

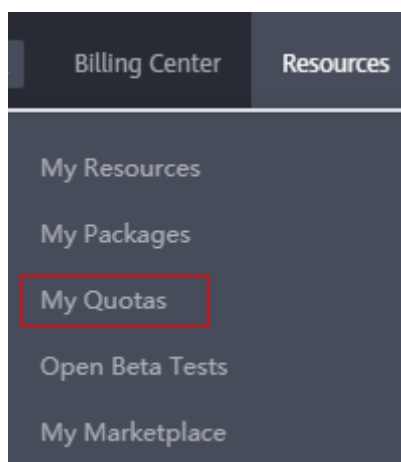
Recurso	Cota padrão
Nomes de domínio de aceleração	100
Arquivos a serem atualizados	2000 por dia
Diretórios a serem atualizados	100 por dia
Os URLs a serem pré-aquecidos	1000 por dia

NOTA

Se algum nome de domínio sob sua conta for banido devido a violação, você não poderá adicionar novos nomes de domínio de aceleração e executar atualização de cache ou pré-aquecimento.

Como faço para visualizar minha cota?

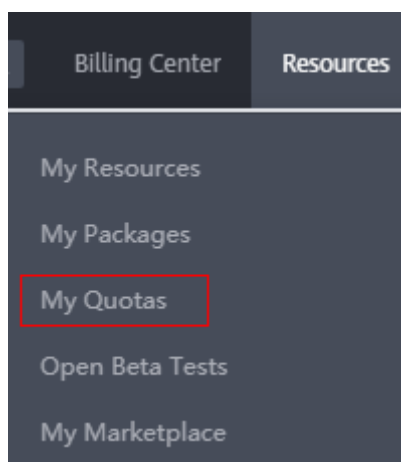
1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No canto superior direito da página, escolha **Resources > My Quotas**. A página **Service Quota** é exibida.



3. Visualize a cota usada e a cota total de cada tipo de recursos CDN na página exibida.

Como faço para solicitar uma cota mais alta?

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No canto superior direito da página, escolha **Resources > My Quotas**. A página **Service Quota** é exibida.



3. Clique em **Increase Quota**.
 4. Na página **Create Service Ticket**, configure os parâmetros conforme necessário.
Na área **Problem Description**, preencha o conteúdo e descreva por que você precisa do ajuste.
 5. Depois que todos os parâmetros obrigatórios estiverem configurados, selecione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** e clique em **Submit**.
- Você pode clicar em **My Service Ticket** para visualizar os tíquetes de serviço enviados.

2 Configurações de nome de domínio

2.1 Visão geral

Depois que um nome de domínio é adicionado para aceleração, você pode configurar o nome de domínio com base nos requisitos de serviço. Configurações personalizáveis incluem aquelas para servidores de origem, recuperação (host de recuperação, recuperação baseada em intervalo, recuperação de bucket privado do OBS e recuperação de redirecionamento) HTTPS, cache e controle de acesso (proteção de hotlink e lista negra/lista branca de endereços IP) e configurações avançadas (cabeçalhos HTTP).

Configurações básicas

Certifique-se de que o nome de domínio esteja no estado **Enabled** ou **Configuring** e não esteja bloqueado ou banido pela CDN antes de definir as configurações.

Item	Descrição
Modificação de detalhes do servidor de origem	Se o endereço IP ou o nome de domínio do servidor de origem for alterado, as informações do servidor de origem estiverem incorretas ou for necessário um servidor de origem em espera, modifique as configurações do servidor de origem.
Alteração de área de serviço	Se a região onde seus usuários estão localizados mudar, você poderá alterar a área de serviço do nome de domínio de aceleração para melhor corresponder aos seus serviços.
Configuração do IPv6	Para permitir que os usuários acessem nós CDN usando IPv6, habilite o IPv6 no console da CDN.

Configurações de recuperação

Certifique-se de que o nome de domínio esteja no estado **Enabled** ou **Configuring** e não esteja bloqueado ou banido pela CDN antes de definir as configurações.

Item	Descrição
Host de recuperação	Se você precisar especificar o nome de domínio do site em que o recurso está localizado, defina os parâmetros relacionados ao host de recuperação de conteúdo neste item de configuração.
Protocolo de origem	Você pode configurar o protocolo de solicitação usado pelo CDN para recuperação de conteúdo.
Reescrita dos URLs de solicitação de recuperação	Se os URLs das solicitações de recuperação de conteúdo não corresponderem aos URLs do servidor de origem, você poderá reescrever os URLs de solicitação para melhorar a taxa de acertos da recuperação de conteúdo.
Recuperação de intervalo	Se precisar melhorar a eficiência de distribuição de arquivos grandes, você pode habilitar a recuperação baseada em intervalo neste item de configuração.
Recuperação redirecionada	Suponha que o redirecionamento 302/301 seja realizado para o endereço do servidor de origem. Se você não deseja que a CDN envie diretamente um endereço de redirecionamento 302/301 aos usuários, mas, em vez disso, armazene em cache o conteúdo solicitado e encaminhe o conteúdo aos usuários, ative a recuperação de redirecionamento.
Recuperação de bucket privado do OBS	Se você configurar um bucket privado do OBS da HUAWEI CLOUD como servidor de origem, deverá ativar a recuperação de bucket privado para que a CDN possa recuperar conteúdo do seu bucket privado.
Cabeçalhos de solicitação de recuperação	Se você quiser reescrever o cabeçalho de uma solicitação de recuperação de conteúdo, será necessário definir o cabeçalho da solicitação de recuperação no console da CDN.
Intervalo de tempo limite de recuperação	Você pode ajustar o intervalo de tempo limite de recuperação com base nos recursos e cenários de serviço do servidor de origem.

Configurações de HTTPS

Certifique-se de que o nome de domínio esteja no estado **Enabled** ou **Configuring** e não esteja bloqueado ou banido pela CDN antes de definir as configurações.

Função	Descrição
Certificados de HTTPS	Você pode adicionar um certificado para aceleração HTTPS.
Versões de TLS	Você pode ativar ou desativar versões TLS conforme necessário.

Função	Descrição
Requisitos do certificado HTTPS	Descreve a combinação e a sequência de carregamento de certificados emitidos por diferentes autoridades
Conversão de formato de certificado de HTTPS	Você pode converter certificados em outros formatos para o formato PEM suportado pela CDN.
Grampeamento de OCSP	Se você ativar essa função, o CDN armazenará em cache o status dos certificados on-line antecipadamente e retornará o status aos navegadores. Os navegadores não precisam consultar o status das CAs, acelerando a verificação.
Redirecionamento forçado	Você pode forçar o redirecionamento para HTTP ou HTTPS.
HTTP/2	Descreve os antecedentes e as vantagens do HTTP/2.

Configurações de cache

Certifique-se de que o nome de domínio esteja no estado **Enabled** ou **Configuring** e não esteja bloqueado ou banido pela CDN antes de definir as configurações.

Item	Descrição
Regras de cache	Você pode definir a idade máxima do cache e a prioridade para diferentes recursos para aumentar a taxa de acertos e reduzir a taxa de retorno à origem.
Filtragem de parâmetros de URL	Você pode filtrar parâmetros de URL para permitir que os nós da CDN ignorem os parâmetros após um ponto de interrogação (?) ao armazenar recursos em cache, melhorando a taxa de acertos do cache e acelerando a distribuição.
Controle de cache de origem	Você pode definir o tempo de expiração do cache nos nós da CDN para ser o mesmo que o do servidor de origem.
Idade de cache de código de estado	Você pode configurar a idade do cache dos códigos de status para permitir que a CDN armazene em cache e devolva os códigos de status aos usuários, reduzindo a taxa de recuperação e a pressão sobre o servidor de origem.

Controle de acesso

Certifique-se de que o nome de domínio esteja no estado **Enabled** ou **Configuring** e não esteja bloqueado ou banido pela CDN antes de definir as configurações.

Item	Descrição
Configuração de validação do referenciador	Configure este item quando precisar identificar e filtrar visitantes para restringir o acesso.
Configuração de uma ACL	Configure este item quando precisar usar a filtragem de endereços IP para restringir o acesso.
Configuração de uma lista negra ou lista branca do agente de usuário	Configure este item quando precisar usar a filtragem do agente de usuário para restringir o acesso.
Configuração de assinatura de URL	Configure este item quando precisar proteger os recursos do seu site de serem baixados por usuários mal-intencionados.

Configurações avançadas

Certifique-se de que o nome de domínio esteja no estado **Enabled** ou **Configuring** e não esteja bloqueado ou banido pela CDN antes de definir as configurações.

Item	Descrição
Configurações de cabeçalho HTTP (solicitações de origem cruzada)	Você pode personalizar os valores dos cabeçalhos de resposta HTTP para o seu site.
Páginas de erro personalizadas	Você pode personalizar páginas de erro retornadas aos clientes do usuário.
Compressão inteligente	Você pode compactar o conteúdo estático em seus sites reduzindo o tamanho do arquivo. Isso acelera a transferência de arquivos e economiza muita largura de banda.

2.2 Configurações básicas

2.2.1 Modificação de detalhes do servidor de origem

Um servidor de origem é um servidor de site, que é a fonte dos dados acelerados pelo CDN. Se os detalhes do servidor de origem, como endereço IP, nome de domínio, nome de domínio do bucket do OBS ou porta de origem, precisarem ser modificados, modifique-os na página de configurações do servidor de origem.

Conhecimento de fundo

- Quando você adiciona um nome de domínio, o CDN considera o servidor de origem configurado como o servidor de origem principal por padrão. Você também pode adicionar um servidor de origem em espera para reduzir a taxa de falha de recuperação.
- O mecanismo de sondagem é usado se os servidores de origem primário e em espera tiverem vários endereços IP.
 - Se a conexão com um endereço IP expirar, o CDN aguardará dois segundos e tentará se conectar ao próximo endereço IP.
 - Se a CDN receber um código de status 5xx, a CDN começará imediatamente a se conectar ao próximo endereço IP.

Precauções

- Verifique se a configuração do servidor de origem está correta. A configuração incorreta do servidor de origem causa falhas de recuperação.
- Se você modificou o conteúdo no servidor de origem, atualize o cache da CDN.
- Não é possível adicionar um servidor de origem em espera para nomes de domínio cujo tipo de serviço é a aceleração de todo o site.
- Se o novo servidor de origem estiver conectado à CDN pela primeira vez, será necessária uma verificação. Para obter detalhes, consulte [Verificação do servidor de origem](#).

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List** > **Storage** > **CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Basic Settings**.
5. Na área **Origin Server Settings**, clique em **Edit**.
A caixa de diálogo **Modify Origin Server** é exibida.
6. Modifique os parâmetros do servidor de origem principal com base em seus requisitos de serviço. [Tabela 2-1](#) descreve os parâmetros.

Figura 2-1 Modificação de detalhes do servidor de origem

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

Tabela 2-1 Parâmetros do servidor de origem

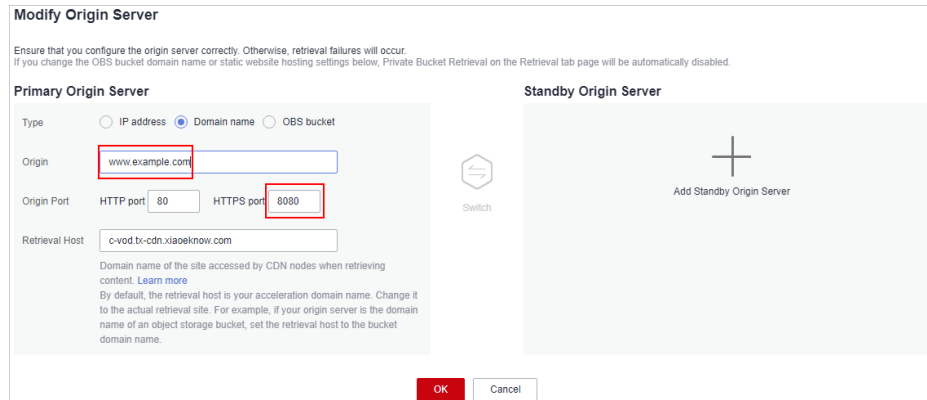
Parâmetro	Descrição
Endereço IP	Você pode inserir até 15 endereços IP separados por ponto e vírgula (;).
Nome de domínio	Você pode inserir apenas um nome de domínio.
Bucket do OBS	Você precisa comprar um bucket do OBS da HUAWEI CLOUD como servidor de origem. NOTA <ul style="list-style-type: none"> Se o bucket do OBS for um bucket privado, ative a recuperação do bucket privado. Caso contrário, a recuperação de conteúdo CDN falha. Para obter detalhes sobre como ativar a recuperação do bucket privado, consulte Recuperação de bucket privado do OBS. Para usar um custom OBS private bucket como servidor de origem, configure uma política para o intervalo privado. Para obter detalhes, consulte Configuração de uma política para um bucket privado do OBS personalizado.
Porta de origem	A CDN suporta portas personalizadas. Se você configurar um bucket do OBS como servidor de origem, não poderá usar uma porta personalizada.
Host de recuperação	Para mais detalhes, consulte Host de recuperação .

 **NOTA**

- Se os buckets do OBS estiverem configurados como servidores de origem para CDN, o tráfego para recuperação de conteúdo dos buckets do OBS será cobrado pelo OBS.
 - A configuração leva cerca de 5 a 10 minutos.
- (Opcional) Clique em **Add Standby Origin Server**.
 - (Opcional) Adicione ou modifique os parâmetros do servidor de origem em espera com base em seus requisitos de serviço. Os métodos e parâmetros para adicionar ou modificar um servidor de origem em espera são os mesmos que para adicionar ou modificar um servidor de origem principal.
 - Clique em **OK**.
 - Clique na seta acima de **Switch** para alternar entre os servidores de origem principal e em espera.

Exemplos

Suponha que pretende migrar recursos de um nome de domínio de aceleração para um servidor cujo nome de domínio é `www.example.com` e o número de porta HTTPS para recuperação é 8080. Você pode modificar as configurações do servidor de origem no CDN da seguinte maneira:



2.2.2 Alteração de área de serviço

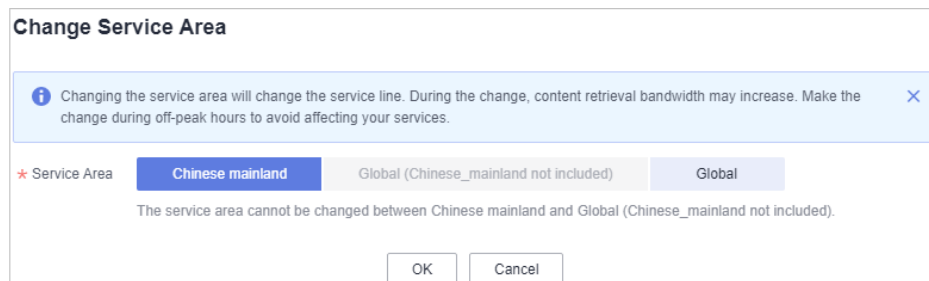
Você pode alterar a área de serviço de um nome de domínio de aceleração no console da CDN.

Avisos importantes

- Se você quiser alterar a área de serviço entre a **Chinese mainland** e **Global (Chinese_mainland not included)**, altere a área de serviço primeiro para **Global** e depois para a desejada para evitar afetar seus serviços.
- A área de serviço de nomes de domínio para a aceleração do site inteiro não pode ser alterada.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de nomes de domínio, clique no nome de domínio a ser modificado ou clique em **Configure** na linha que contém o nome de domínio.
4. Na página de guia **Basic Settings**, clique em **Edit** ao lado de **Service Area**. A caixa de diálogo **Change Service Area** é exibida.



NOTA

A área de serviço de um nome de domínio de aceleração com configurações especiais não pode ser alterada.

5. Selecione a área de serviço desejada e clique em **OK**.

2.2.3 Configuração do IPv6

Você pode habilitar o IPv6 para permitir que os clientes acessem os nós CDN usando o protocolo IPv6 e permitir que o CDN transporte endereços IP do cliente IPv6 para acessar seu servidor de origem.

Precauções

- A maioria dos nós da China continental suporta IPv6. Após a ativação do IPv6, se um usuário usar o IPv6 para acessar o CDN, mas o nó ideal não oferecer suporte ao IPv6, o usuário ainda poderá usar o IPv4 para acessar o nó.
- Para um nome de domínio cuja área de serviço é global, você pode enviar um tíquete de serviço para habilitar o IPv6 para nós na China continental.
- IPv6 não é suportado para nomes de domínio cuja área de serviço está fora da China continental.
- O IPv6 não pode ser ativado para nomes de domínio com configurações especiais.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de nomes de domínio, clique no nome de domínio a ser modificado ou clique em **Configure** na linha que contém o nome de domínio.



4. Ative o **IPv6**.

2.3 Configurações de recuperação

2.3.1 Visão geral

Quando um usuário solicita conteúdo em um nome de domínio de aceleração e o conteúdo não é armazenado em cache em nós CDN, os nós CDN recuperam o conteúdo do servidor de origem. Você pode definir parâmetros de recuperação com base em suas necessidades para acelerar o acesso.

A tabela a seguir descreve as configurações de recuperação:

Função	Descrição
Host de recuperação	Se o nome de domínio que você deseja que o CDN recupere o conteúdo não for seu nome de domínio de aceleração, defina um host de recuperação. A CDN considera um nome de domínio de aceleração como o host de recuperação por padrão.

Função	Descrição
Protocolo de origem	Você pode configurar o protocolo de solicitação usado pelo CDN para recuperação de conteúdo.
Reescrita dos URLs de solicitação de recuperação	Se os URLs das solicitações de recuperação de conteúdo não corresponderem aos URLs do servidor de origem, você poderá reescrever os URLs de solicitação para melhorar a taxa de acertos da recuperação de conteúdo.
Recuperação baseada em intervalo	Você pode configurar a recuperação baseada em intervalo para acelerar a distribuição de arquivos grandes durante a recuperação de conteúdo e reduzir o consumo de largura de banda.
Redirecionar recuperação	Se o servidor de origem usar um redirecionamento 301/302, você poderá ativar a recuperação de redirecionamento para armazenar em cache os recursos redirecionados em nós CDN para distribuição acelerada.
Recuperação de bucket privado do OBS	Se você configurar um bucket privado do OBS da HUAWEI CLOUD como servidor de origem, ative a recuperação de bucket privado para que a CDN possa acessar seu servidor de origem e acelerar seu site. NOTA Se o servidor de origem for um bucket do OBS público, não habilite a recuperação do bucket privado.
Cabeçalhos de solicitação de recuperação	Você pode definir cabeçalhos de solicitação de recuperação para reescrever as informações do cabeçalho nos URLs de solicitação de recuperação dos usuários.
Intervalo de tempo limite de recuperação	Você pode ajustar o intervalo de tempo limite de recuperação com base nos recursos e cenários de serviço do servidor de origem.

2.3.2 Host de recuperação

Um host de recuperação é o host especificado no cabeçalho da solicitação HTTP. É o nome de domínio acessado pelos nós CDN ao recuperar conteúdo do servidor de origem. Depois que o host de recuperação é configurado, o CDN obtém recursos do site correspondente com base nas informações do host durante a recuperação de conteúdo.

Conhecimento de fundo

As diferenças entre o servidor de origem e o host de recuperação são as seguintes:

- O servidor de origem decide o endereço a ser acessado durante a recuperação do conteúdo.
- O host de recuperação decide o site que está associado ao conteúdo solicitado.

Suponha que seu servidor de origem seja um servidor Nginx. Seu endereço IP é x.x.x.x, e seu nome de domínio é www.test.com. Os seguintes sites são implantados no servidor de origem.

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

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

    location / {
        root html;
    }
}
```

Se você quiser que a CDN recupere o conteúdo desse servidor Nginx, defina o endereço do servidor de origem como **x.x.x.x** ou **www.test.com** na CDN. Como há vários sites no servidor de origem, você precisa especificar o site específico para recuperar o conteúdo. Se você quiser que a CDN recupere o conteúdo do site do **www.a.com**, defina o host de recuperação como **www.a.com** na CDN. Se você quiser que a CDN recupere o conteúdo do site do **www.b.com**, defina o host de recuperação como **www.b.com** na CDN.

Precauções

- Depois que um nome de domínio é adicionado, o CDN o considera como o host de recuperação por padrão. Se você não quiser que a CDN recupere o conteúdo do nome de domínio de aceleração, defina um host de recuperação para especificar o local do conteúdo solicitado.
- Se o endereço do servidor de origem for um endereço IP ou um nome de domínio, o tipo de host de recuperação será o nome de domínio de aceleração por padrão.
- Se um bucket do OBS da HUAWEI CLOUD for usado como um servidor de origem, o nome de domínio do bucket será usado como o host de recuperação por padrão e não poderá ser alterado.
- Se você definir o endereço do servidor de origem como um nome de domínio e especificar o nome de domínio como o de um intervalo de armazenamento de objetos do Huawei Cloud OBS ou de outro fornecedor, defina o host de recuperação como o nome de domínio do intervalo de armazenamento de objetos. Caso contrário, a recuperação falha.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Na área **Origin Server Settings**, clique em **Edit**. A caixa de diálogo **Modify Origin Server** é exibida.

5. Digite o nome de domínio do host de recuperação e clique em **OK**.

NOTA

A configuração leva cerca de 5 minutos.

Exemplos

Suponha que você tenha um nome de domínio de aceleração **www.example.com**. Seu nome de domínio do servidor de origem é **www.origin.com**, e o host de recuperação é **www.example01.com**.

Quando um usuário solicita o arquivo **http://www.example.com/test.jpg**, o arquivo não é armazenado em cache na CDN e o recupera do servidor de origem **www.origin.com** cujo endereço IP é 192.168.1.1. O arquivo é encontrado no site do **www.example01.com** do servidor de origem. Em seguida, a CDN retorna o arquivo para o usuário e armazena o arquivo em cache nos nós.

2.3.3 Protocolo de origem

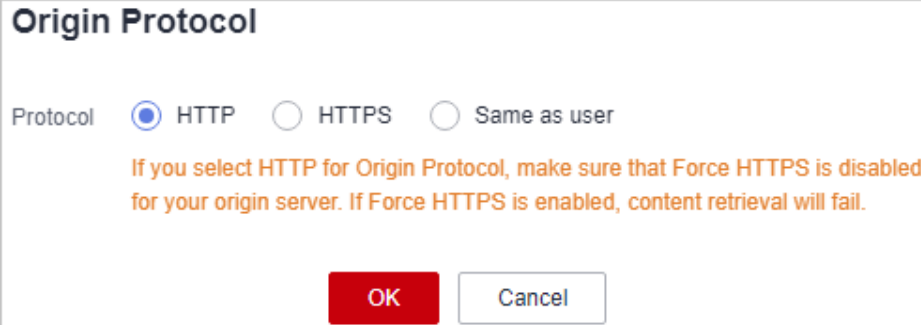
Você pode configurar o protocolo usado para a recuperação de conteúdo.

Precauções

Por padrão, o protocolo usado para recuperação de conteúdo é o mesmo que o protocolo de solicitações do usuário.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Retrieval Settings**.
5. Clique em **Edit** ao lado de **Origin Protocol**. A caixa de diálogo **Origin Protocol** é exibida.



The image shows a dialog box titled "Origin Protocol". It contains three radio button options: "HTTP" (selected), "HTTPS", and "Same as user". Below the options is a warning message in orange text: "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." At the bottom of the dialog are two buttons: "OK" (red) and "Cancel" (white).

Protocolo de origem	Descrição
Igual ao usuário	O protocolo usado para recuperação de conteúdo é o mesmo que o protocolo de solicitações do usuário.
HTTP	A CDN usa HTTP para recuperação de conteúdo.
HTTPS	O CDN usa HTTPS para recuperação de conteúdo.

6. Selecione um protocolo usado para recuperação de conteúdo e clique em **OK**.

2.3.4 Reescrita dos URLs de solicitação de recuperação

Se os URLs das solicitações de recuperação de conteúdo não corresponderem aos URLs do servidor de origem, a recuperação de conteúdo falhará. Você pode reescrever os URLs de solicitação de recuperação para aqueles que correspondem ao servidor de origem, melhorando a taxa de acertos de recuperação de conteúdo.

Avisos importantes

- Você pode adicionar até 20 regras de reescrita de URL.
- Os URLs de solicitação de recuperação não podem ser reescritos para nomes de domínio com configurações especiais.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console da CDN é exibido.

2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Retrieval Settings**.
5. Na área **Retrieval Request URL Rewrite**, clique em **Edit**.

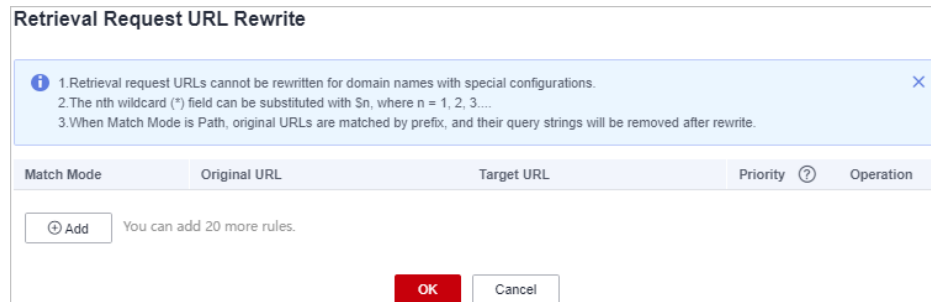


Tabela 2-2 Descrição do parâmetro

Parâmetro	Descrição
Todos os arquivos	Reescreve os URLs de todas as solicitações de recuperação para o nome de domínio.
Caminho	Reescreve os URLs de solicitação com um caminho específico. Correspondência de prefixo é usada.
Wildcard	Caracteres curinga são suportados. Correspondência de caminho completo é usado.
URL original	<p>URL a ser reescrita.</p> <ul style="list-style-type: none"> ● Um URL começa com uma barra (/) e não contém http://, https://, nem o nome do domínio. ● Um URL contém até 512 caracteres. ● Os curingas (*) são suportados, por exemplo, /test/*/*.mp4. ● Quando Match Mode for Path, as strings de consulta no URL original serão removidas após a reescrita. ● Quando o Match Mode é Wildcard e uma barra (/) é inserida, o diretório raiz é correspondido.
URL de destino	<p>URL após reescrita.</p> <ul style="list-style-type: none"> ● Um URL começa com uma barra (/) e não contém http://, https://, nem o nome do domínio. ● Um URL contém até 256 caracteres. ● O <i>n</i>-ésimo campo curinga (*) pode ser substituído por \$n, onde <i>n</i> = 1, 2, 3..., por exemplo, /newtest/\$1/\$2.jpg.

Parâmetro	Descrição
Prioridade	<p>Prioridade de uma regra de reescrita de URL.</p> <ul style="list-style-type: none"> ● A prioridade de uma regra é obrigatória e deve ser única. ● A regra com a prioridade mais alta será usada para combinar primeiro. ● A prioridade é um número inteiro que varia de 1 a 100. Um número maior indica uma prioridade maior.

Exemplos

Exemplo 1: suponha que configurou a seguinte regra de reescrita para o nome de domínio `www.example.com`:

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

Solicitação de recuperação original: <https://www.example.com/test/a.txt>

Solicitação de recuperação reescrita: <https://www.example.com/test/b.txt>

Exemplo 2: suponha que configurou a seguinte regra de reescrita para o nome de domínio `www.example.com`:

Match Mode	Original URL	Target URL	Priority
Wildcard	/test/*'.mp4	/newtest/S1/S2.mp4	1

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

Solicitação de recuperação reescrita: <https://www.example.com/newtest/aaa/bbb.mp4>

Exemplo 3: suponha que configurou a seguinte regra de reescrita para o nome de domínio `www.example.com`:

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

Solicitação de recuperação original: <https://www.example.com/test/aaa/bbb.txt>

Solicitação de recuperação reescrita: <https://www.example.com/new.jpg>

2.3.5 Recuperação de intervalo

Na recuperação baseada em intervalo, o servidor de origem envia dados de um intervalo específico para um nó CDN com base nas informações de intervalo no cabeçalho da solicitação de HTTP.

Conhecimento de fundo

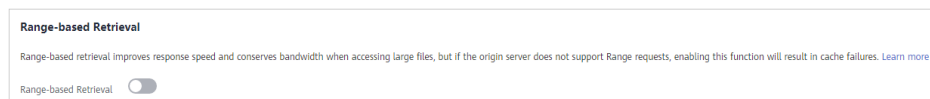
- Informações de intervalo especificam as posições do primeiro e último bytes para os dados a serem retornados. Por exemplo, **Range: bytes=0-100** indica que os primeiros 101 bytes do arquivo são necessários.
- A recuperação baseada em intervalo reduz o tempo de distribuição de arquivos grandes, melhora a eficiência de recuperação e reduz o consumo de recuperação de conteúdo.

Precauções

- Para ativar a recuperação baseada em intervalo, o servidor de origem deve suportar solicitações de intervalo, ou seja, solicitações com o campo intervalo nos cabeçalhos. Caso contrário, a recuperação de conteúdo pode falhar.
- A recuperação baseada em intervalo é inválida para nomes de domínio cujo tipo de serviço é a aceleração de todo o site.
- Por padrão, a recuperação baseada em intervalo está habilitada para aceleração de download de arquivos e aceleração de serviço sob demanda.

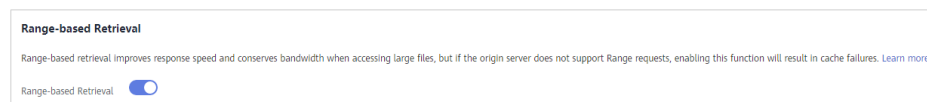
Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Retrieval Settings**.
5. Na área **Range-based Retrieval**, ative ou desative **Range-based Retrieval** com base nos requisitos de serviço.



Exemplos

Suponha que tenha activado a recuperação baseada em intervalo para o nome de domínio **www.example.com**.



- Se o usuário A solicitar que o **www.example.com/cdn.mp4**, e os nós CDN não armazenem em cache o conteúdo ou o conteúdo armazenado nos nós CDN tiver expirado, o nó CDN ideal iniciará uma solicitação baseada em intervalo para recuperar intervalos do conteúdo do servidor de origem. Os intervalos do conteúdo são então armazenados em cache no nó.
- Quando o conteúdo solicitado pelo usuário A está sendo armazenado em cache, se o usuário B enviar uma solicitação baseada em intervalo para esse nó e o cache no nó já

contiver o intervalo do conteúdo solicitado pelo usuário B, o nó retornará imediatamente o intervalo solicitado.

2.3.6 Recuperação redirecionada

Conhecimento de fundo

Se um servidor de origem usar um redirecionamento 301/302, quando um nó CDN enviar uma solicitação para recuperar o conteúdo solicitado por um usuário do servidor de origem, um código de status 301/302 será retornado. O CDN, em seguida, toma medidas com base em se a recuperação de redirecionamento está habilitada.

- Redirecionar recuperação desativada

Um nó CDN retorna o endereço de redirecionamento para o usuário e deixa o usuário concluir o processo de solicitação. Se o nome de domínio do endereço de redirecionamento não for adicionado à CDN, o processo de solicitação subsequente não será acelerado pela CDN.

- Redirecionar recuperação ativada

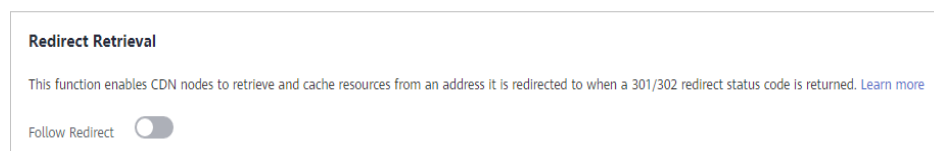
Um nó CDN recupera o conteúdo do endereço de redirecionamento e armazena em cache o conteúdo, que é retornado ao usuário. Quando outro usuário solicita o mesmo conteúdo, o cache de nó é retornado diretamente.

Precauções

Se o tipo de serviço for aceleração de todo o site, a recuperação de redirecionamento não terá efeito para conteúdo dinâmico que não esteja armazenado em cache em nós CDN.

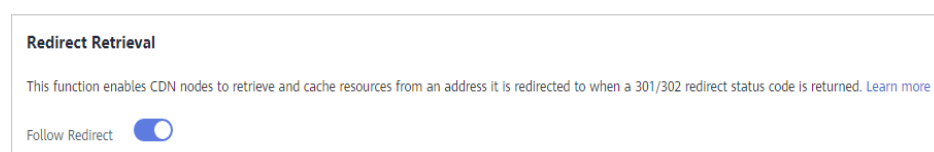
Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Retrieval Settings**.
5. Na área **Redirect Retrieval**, ative ou desative **Follow Redirect** com base nos requisitos de serviço.



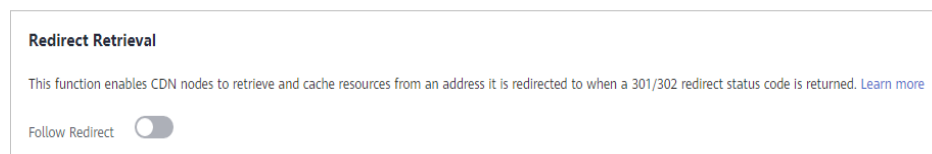
Exemplos

- A recuperação de redirecionamento está **enabled** para o nome de domínio [www.example.com](#).



Se um usuário solicitar o arquivo **www.example.com/cdn.jpg** e o nó CDN não armazenar o conteúdo em cache, o nó recuperará o conteúdo do servidor de origem. O servidor de origem retorna o código de status de HTTP 301 ou 302 e o endereço de redirecionamento **www.example.com/test/cdn.jpg**.

- a. O nó envia diretamente uma solicitação para o endereço de redirecionamento.
 - b. Depois de obter o conteúdo solicitado, o nó retorna o conteúdo para o usuário e armazena o conteúdo em cache.
 - c. Quando outro usuário solicita o mesmo arquivo, o nó retorna diretamente o conteúdo em cache.
- A recuperação de redirecionamento está **disabled** para o nome de domínio **www.example.com**.



Se um usuário solicitar o arquivo **www.example.com/cdn.jpg** e o nó CDN não armazenar o conteúdo em cache, o nó recuperará o conteúdo do servidor de origem. O servidor de origem retorna o código de status de HTTP 301 ou 302 e o endereço de redirecionamento **www.example.com/test/cdn.jpg**.

- a. O nó retorna diretamente o código de status de HTTP 301 ou 302 para o cliente do usuário. O usuário cliente envia uma solicitação para o endereço de redirecionamento.
- b. Se o nome de domínio do endereço de redirecionamento não for adicionado à CDN, os nós da CDN não armazenarão em cache o conteúdo solicitado e o processo de solicitação subsequente não será acelerado.
- c. Se outro usuário solicitar o mesmo arquivo, o processo anterior será repetido.

2.3.7 Recuperação de bucket privado do OBS

Se você configurar um bucket privado do OBS da HUAWEI CLOUD como servidor de origem, deverá ativar a recuperação de bucket privado para que a CDN possa recuperar conteúdo do seu bucket privado.

Precauções

- A recuperação de intervalo privado só é suportada quando o servidor de origem do nome de domínio de aceleração é um intervalo OBS.
- Antes de ativar a recuperação de intervalo privado, você deve autorizar a CDN a acessar os recursos de nuvem do OBS. Depois que a autorização for bem-sucedida, a CDN terá permissão para acessar todos os recursos do bucket privado em sua conta.

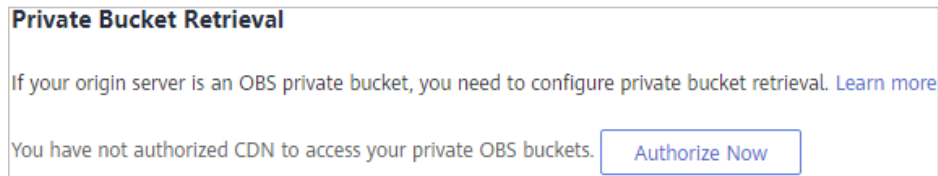
Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console da CDN é exibido.

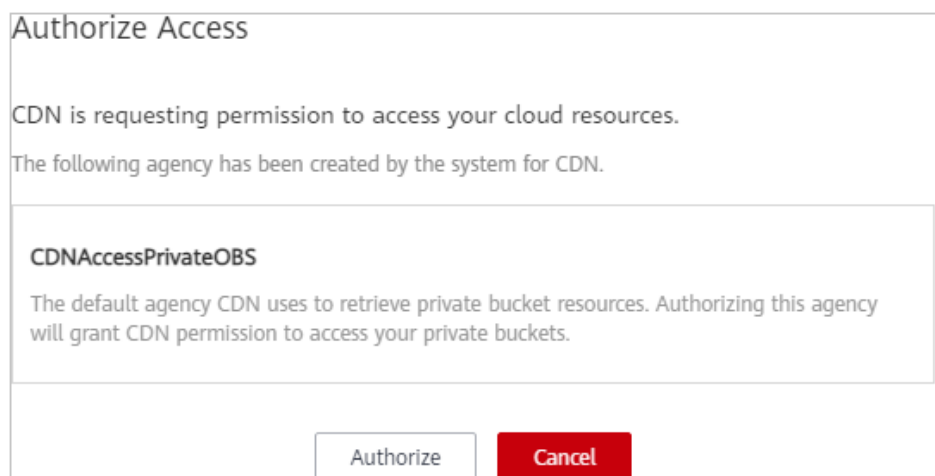
2. No painel de navegação, escolha **Domains**.

3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Retrieval Settings**.
5. Se você configurar a recuperação do bucket privado pela primeira vez, a página mostrada na figura a seguir será exibida.



O procedimento de configuração correto é o seguinte:

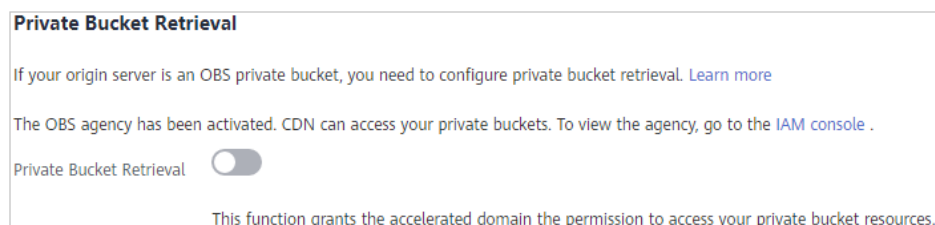
- a. Clique em **Authorize Now**. A caixa de diálogo **Authorize Access** é exibida.



- b. Clique em **Authorize**. O sistema cria uma agência denominada **CDNAccessPrivateOBS** para você no **console do IAM**. A CDN agora tem permissão para acessar seus buckets privados do OBS.

NOTA

- Não exclua a agência **CDNAccessPrivateOBS**. Caso contrário, a CDN não pode recuperar recursos de intervalos privados do OBS.
 - Se o servidor de origem for um bucket do OBS público, não habilite a recuperação do bucket privado.
- c. A figura a seguir mostra a página após a autorização.



- d. Ative o **Private Bucket Retrieval**.
6. Aguarde cerca de 5 minutos para que a configuração entre em vigor. Quando o status do nome de domínio muda de **Configuring** para **Enabled**, a configuração tem efeito.

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

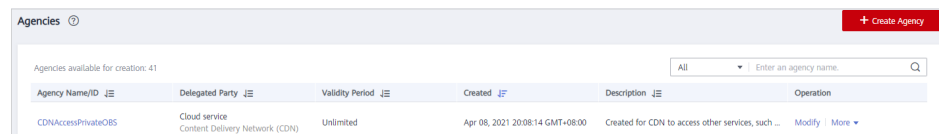
Se a CDN recuperar somente arquivos não criptografados do intervalo privado do OBS, você só precisará concluir a configuração anterior. Se os arquivos em seu bucket do OBS forem criptografados usando o KMS, será necessário atribuir as permissões de **KMS Administrator** à agência CDNAccessPrivateOBS para que a CDN possa ler e acelerar os arquivos criptografados.

7. **(Opcional)** Atribua as permissões de **KMS Administrator** à agência CDNAccessPrivateOBS.

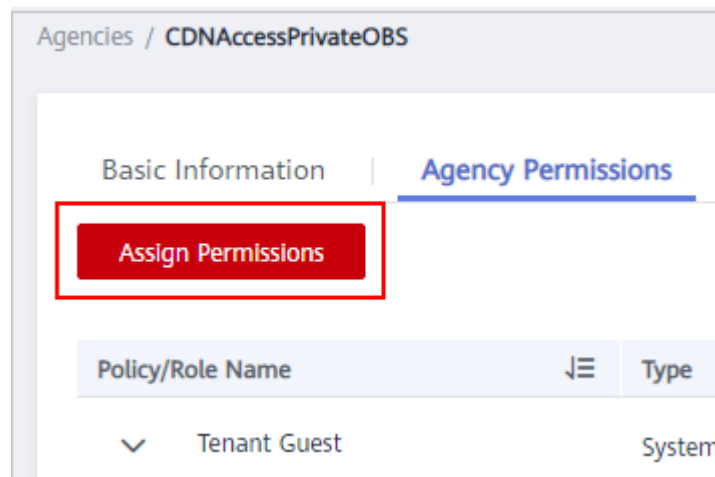
- a. Faça login em **console da Huawei Cloud**. Na página inicial do console de gerenciamento, escolha **Service List > Management & Government > Identity and Access Management**.

O console do IAM é exibido.

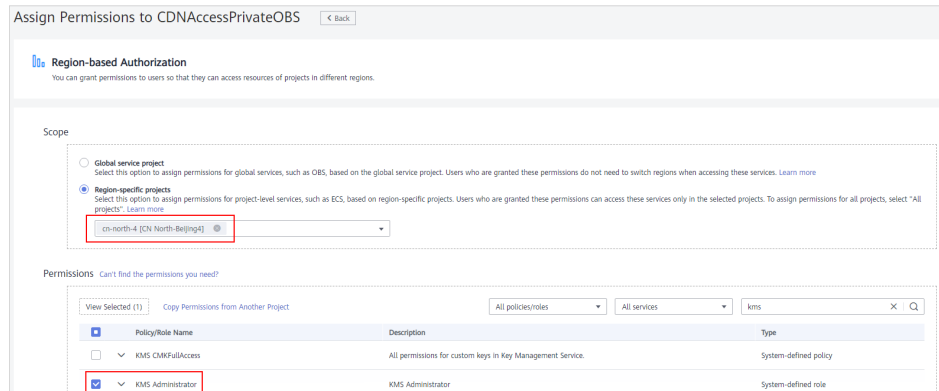
- b. No painel de navegação, escolha **Agencies**.
- c. Na página **Agencies**, escolha **More > Manage Permissions** na coluna **Operation** da linha que contém a agência CDNAccessPrivateOBS.



- d. A guia **Agency Permissions** é exibida.



- e. Clique em **Assign Permissions**.
 - Defina **Scope** para **Region-specific projects** e selecione a região onde o intervalo do OBS está localizado.
 - Na área **Permissions**, selecione **KMS Administrator**.



f. Clique em **OK**.

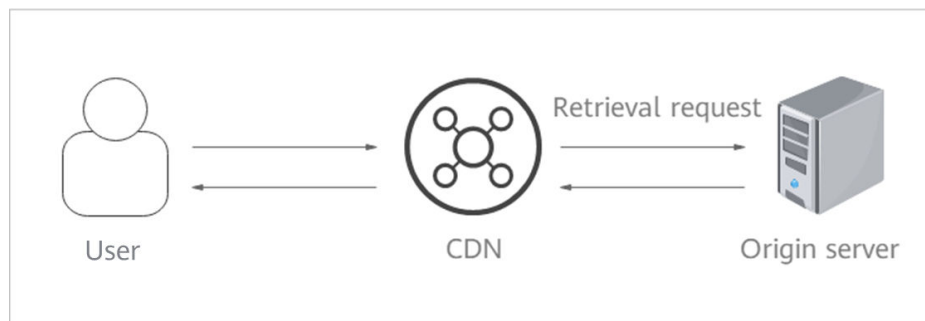
2.3.8 Cabeçalhos de solicitação de recuperação

Você pode configurar o cabeçalho da solicitação de recuperação em um URL de solicitação de recuperação.

Conhecimento de fundo

Se o conteúdo solicitado não estiver armazenado em cache em nós CDN, os nós CDN recuperam esse conteúdo de um servidor de origem. Você pode configurar cabeçalhos de solicitação de recuperação no console da CDN para reescrever detalhes de cabeçalho dos URLs de solicitação de recuperação.

Cabeçalhos HTTP são parte de uma solicitação HTTP ou mensagem de resposta que definem os parâmetros operacionais de uma transação HTTP.



Precauções

- Essa configuração modifica apenas os cabeçalhos de solicitação de recuperação em mensagens HTTP para recuperação de conteúdo por meio de CDN. Ele não modifica aqueles em uma mensagem HTTP que os nós CDN retornam aos usuários.
- Um cabeçalho de solicitação não pode ter dois valores diferentes ao mesmo tempo.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.

3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Retrieval Settings**.
5. Na área **Retrieval Request Headers**, clique em **Add**.
6. Configure os detalhes do cabeçalho da solicitação de recuperação.
 - **Add**: adicione um cabeçalho de solicitação de recuperação ao CDN para reescrever os detalhes do cabeçalho nos URLs de solicitação do usuário.

Add Retrieval Request Header

* Request Header Operation Set Delete

* Name

* Value

Tabela 2-3 Parâmetros

Parâmetro	Exemplo	Descrição
Operação de cabeçalho de solicitação	Definir	Adicione um cabeçalho de solicitação específico a uma solicitação HTTP de recuperação. <ul style="list-style-type: none"> ● Se uma URL de solicitação contiver o parâmetro X-test e X-test estiver definido como 111, a CDN definirá X-test como aaa na URL de solicitação de recuperação. ● Se um URL de solicitação não contiver o parâmetro X-test, a CDN adicionará o parâmetro X-test ao URL de solicitação de recuperação e definirá seu valor como aaa.
	Excluir	Exclua o cabeçalho que existe em um URL de solicitação do usuário. <ul style="list-style-type: none"> ● Se uma URL de solicitação contiver o parâmetro X-test, esse parâmetro será excluído da URL de solicitação de recuperação.
Nome	X-test	<ul style="list-style-type: none"> ● Insira de 1 a 64 caracteres. ● Insira apenas letras, dígitos ou hífen (-).

Parâmetro	Exemplo	Descrição
Valor	aaa	<ul style="list-style-type: none"> ● Digite de 1 a 512 caracteres. ● Digite apenas letras, dígitos, asteriscos (*), pontos (.), hífen (-) e sublinhados (_). ● Variáveis, como <i>\$client_ip</i> e <i>\$remote_port</i>, não são permitidas.

- **Edit:** modificar o valor ou a operação de um cabeçalho de solicitação de recuperação.

Clique em **Edit** na coluna **Operation**. A seguinte caixa de diálogo é exibida.

Parâmetro	Exemplo	Descrição
Operação de Cabeçalho de Solicitação	Definir	<p>Adicione um cabeçalho de solicitação específico a uma solicitação HTTP de recuperação.</p> <ul style="list-style-type: none"> ● Se uma URL de solicitação contiver o parâmetro X-test e X-test estiver definido como 111, a CDN definirá X-test como aaa na URL de solicitação de recuperação. ● Se um URL de solicitação não contiver o parâmetro X-test, a CDN adicionará o parâmetro X-test ao URL de solicitação de recuperação e definirá seu valor como aaa.
	Excluir	<p>Exclua o cabeçalho que existe em um URL de solicitação do usuário.</p> <ul style="list-style-type: none"> ● Se uma URL de solicitação contiver o parâmetro X-test, esse parâmetro será excluído da URL de solicitação de recuperação.

Parâmetro	Exemplo	Descrição
Nome	X-test	Este parâmetro não pode ser modificado.
Valor	aaa	<ul style="list-style-type: none"> ● Digite de 1 a 512 caracteres. ● Digite apenas letras, dígitos, asteriscos (*), pontos (.), hífen (-) e sublinhados (_). ● Variáveis, como <i>\$client_ip</i> e <i>\$remote_port</i>, não são permitidas.

7. Clique em **OK**.

NOTA

Se a área de serviço do seu nome de domínio for global ou estiver fora da China continental e o cabeçalho **Accept-Encoding** nas solicitações do usuário contiver vários valores, apenas o **Gzip** será transmitido de forma transparente durante a recuperação do conteúdo.

Exemplos

Suponha que você configurou os seguintes cabeçalhos de solicitação de recuperação para o nome de domínio `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

Quando um usuário solicita o arquivo `http://www.example.com/abc.jpg`, o arquivo não é armazenado em cache no CDN e o recupera do servidor de origem. O cabeçalho **X-cdn** será adicionado ao pedido de recuperação e o cabeçalho **X-test** será excluído.

Restrições

- Se o seu nome de domínio tiver configurações especiais, Content-Type, Cache-Control, Expires, Content-Language e Content-Disposition não poderão ser configurados.
- Os seguintes cabeçalhos padrão não podem ser reescritos.

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 tempo limite de recuperação

Se o conteúdo solicitado por um usuário não estiver armazenado em cache em nós CDN, a CDN recuperará o conteúdo do servidor de origem. O intervalo de tempo limite padrão de

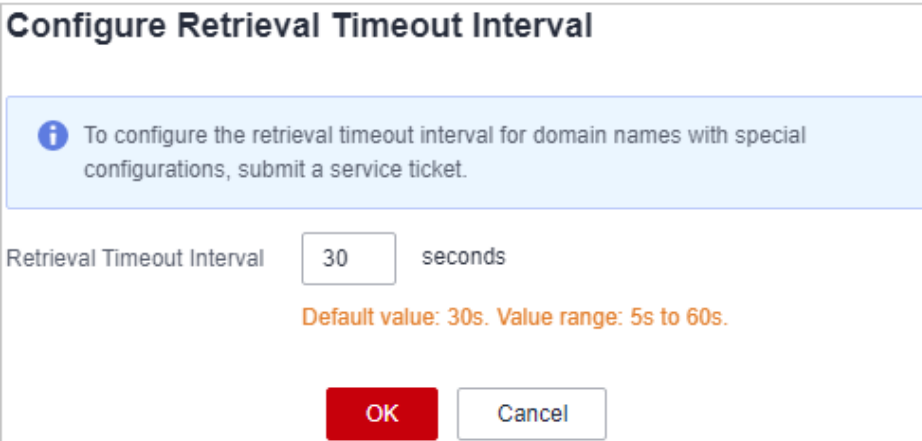
uma solicitação de recuperação é de 30s. Se a solicitação expirar, a solicitação falhará. Você pode ajustar o intervalo de tempo limite de recuperação com base nos recursos de serviço e no status da rede do servidor de origem para garantir a recuperação normal do conteúdo.

Precauções

- Para modificar o intervalo de tempo limite de recuperação para nomes de domínio com configurações especiais, envie um tíquete de serviço.
- O intervalo de tempo limite de recuperação não pode ser configurado para nomes de domínio que servem utilizadores fora da China continental.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Retrieval Settings**.
5. Na área **Retrieval Timeout Interval**, clique em **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. Digite o intervalo de timeout de recuperação e clique em **OK**.

2.3.10 Perguntas frequentes

Em quais cenários a CDN recupera conteúdo de um servidor de origem?

- O conteúdo desejado não é armazenado em cache nos nós CDN.
- O conteúdo armazenado em cache nos nós CDN expirou.

Qual é a diferença entre um host de recuperação e um servidor de origem?

- O servidor de origem decide o endereço a ser acessado durante a recuperação do conteúdo.
- O host de recuperação decide o site que está associado ao conteúdo solicitado.

Suponha que seu servidor de origem seja um servidor Nginx. Seu endereço IP é x.x.x.x, e seu nome de domínio é www.test.com. Os seguintes sites são implantados no servidor de origem:

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

  location / {
    root html;
  }
}

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

  location / {
    root html;
  }
}
```

Se você quiser que a CDN recupere o conteúdo desse servidor Nginx, defina o endereço do servidor de origem como **x.x.x.x** ou **www.test.com** na CDN. Como há vários sites no servidor de origem, você precisa especificar o site específico para recuperar o conteúdo. Se você quiser que a CDN recupere o conteúdo do site do **www.a.com**, defina o host de recuperação como **www.a.com** na CDN. Se você quiser que a CDN recupere o conteúdo do site do **www.b.com**, defina o host de recuperação como **www.b.com** na CDN.

A CDN da HUAWEI CLOUD oferece suporte à recuperação direta de conteúdo por meio do acesso ao rastreador?

Não.

A CDN da HUAWEI CLOUD não consegue distinguir o acesso normal do usuário do acesso do rastreador. Se o crawler registrar o endereço IP de um nó, ele poderá acessar diretamente esse endereço IP na próxima vez. Se o nó estiver com defeito ou passando por manutenção de rotina, o rastreador não poderá recuperar o conteúdo desse endereço IP.

Como faço para configurar o servidor de origem se um bucket de armazenamento de objetos que não seja da Huawei funciona como um servidor de origem?

1. Obtenha o nome de domínio do intervalo de armazenamento de objetos.

Ao adicionar um nome de domínio no console da CDN, selecione **Domain name** para **Origin Server Address** e digite o nome do domínio do intervalo de armazenamento de objetos na caixa de texto.

2. Modificar configurações de recuperação de conteúdo.

Por padrão, o host de recuperação é seu nome de domínio de aceleração. Se você configurar um intervalo de armazenamento de objetos como seu servidor de origem, altere o host de recuperação para o nome de domínio desse intervalo de armazenamento de objetos. Caso contrário, a recuperação de conteúdo falhará.

2.4 Configurações de HTTPS

2.4.1 Visão geral

O HTTPS garante a transmissão segura por meio de criptografia e autenticação de identidade. É amplamente utilizado em comunicações sensíveis à segurança na World Wide Web, como o pagamento on-line.

A tabela a seguir descreve as definições de HTTPS:

Função	Descrição
Certificados de HTTPS	Você pode adicionar um certificado para aceleração HTTPS.
Versões de TLS	Você pode ativar ou desativar versões TLS conforme necessário.
Requisitos do certificado HTTPS	Descreve a combinação e a sequência de carregamento de certificados emitidos por diferentes autoridades
Conversão de formato de certificado de HTTPS	Você pode converter certificados em outros formatos para o formato PEM suportado pela CDN.
Grampeamento de OCSP	Você pode permitir que a CDN armazene em cache o status dos certificados on-line com antecedência e retorne o status aos navegadores. Os navegadores não precisam consultar o status de autoridades de certificação (CAs), acelerando a verificação.
Redirecionamento forçado	Você pode forçar o redirecionamento para HTTP ou HTTPS.
HTTP/2	Descreve os antecedentes e as vantagens do HTTP/2.

2.4.2 Certificados de HTTPS

Você pode configurar um certificado HTTPS para um nome de domínio de aceleração no console CDN para habilitar a aceleração HTTPS.

Conhecimento de fundo

- **HTTP**

HTTP transfere conteúdo em texto simples sem qualquer criptografia de dados. Se um invasor interceptar pacotes transmitidos entre navegadores e servidores de sites, o conteúdo transmitido pode ser lido diretamente.

- **HTTPS**

Baseado em HTTP, o HTTPS usa Secure Sockets Layer (SSL) para criptografar a transmissão de dados. Com SSL, os servidores são autenticados usando certificados e as comunicações entre navegadores e servidores são criptografadas.

Pré-requisitos

Você pode usar seu próprio certificado ou um certificado hospedado pelo SSL Certificate Manager (SCM) da Huawei Cloud para configurar HTTPS.

- Seu próprio certificado
O formato do certificado deve satisfazer os requisitos descritos em [Requisitos do certificado HTTPS](#).
- Um certificado hospedado pelo Huawei Cloud SCM no console do Cloud Certificate Manager (CCM)
Você deve enviar o certificado para a CDN no console do CCM antes de habilitar a aceleração HTTPS na CDN. Para obter detalhes sobre como enviar um certificado, consulte [Como enviar um certificado SSL para outros serviços de nuvem](#).

Precauções

- Apenas certificados e chaves privadas no formato PEM são suportados. Se um certificado não estiver no formato PEM, converta o certificado consultando [Requisitos do certificado HTTPS](#).
- Um nome de domínio de aceleração tem seu certificado associado. Eles devem corresponder. Se o seu nome de domínio é um domínio curinga, configure um certificado para ele, referindo-se [Como faço para configurar um certificado se meu nome de domínio é um domínio curinga?](#)
- As configurações de certificado serão excluídas automaticamente quando a aceleração segura HTTPS for desativada. Você precisa de reconfigurar o certificado se a aceleração segura de HTTPS é permitida outra vez.
- Se o seu certificado tiver sido alterado, atualize as informações do certificado no console da CDN em tempo hábil.

Configuração de certificados de HTTPS

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **HTTPS Settings**.
5. Na página de guia **HTTPS Settings**, clique em **Edit**. A caixa de diálogo **Configure HTTPS Secure Acceleration** é exibida.

Configure HTTPS Secure Acceleration

Status

Certificate Source My certificate Huawei-managed certificate

Certificate Name

Certificate Body
[Example](#)

Private Key
[Example](#)

6. Ative o **Status** para habilitar este item de configuração.
7. Definir parâmetros relacionados.

Parâmetro	Descrição
Tipo de certificado	Selecione My certificate ou Huawei-managed certificate .
Nome do certificado	<ul style="list-style-type: none">● My certificate: insira o nome do certificado. Um nome de certificado pode ter até 32 caracteres.● Huawei-managed certificate: vá para o console do CCM para enviar um certificado para a CDN e, em seguida, selecione o certificado na lista suspensa ao lado de Certificate Name no console da CDN. Para obter detalhes, consulte Como enviar um certificado SSL para outros serviços de nuvem.

Parâmetro	Descrição
Organismo de certificação	<ul style="list-style-type: none"> ● My certificate: use um editor de texto local para abrir o certificado e copiar o conteúdo do certificado para a caixa de texto. ● Huawei-managed certificate: o conteúdo é preenchido automaticamente. <p>NOTA O corpo do certificado não pode conter espaços ou linhas em branco. Caso contrário, será exibida uma mensagem indicando que os parâmetros do certificado estão incorretos.</p>
Chave privada	<ul style="list-style-type: none"> ● My certificate: use um editor de texto local para abrir a chave privada e copiar o conteúdo para a caixa de texto. ● Huawei-managed certificate: o conteúdo é preenchido automaticamente.

8. Clique em **OK**.
9. Verifique se o certificado HTTPS entrou em vigor.
 Se o certificado tiver entrado em vigor, você poderá acessar os recursos do site do nome de domínio de aceleração por meio de HTTPS e exibir as informações de autenticação do site clicando no ícone de cadeado na caixa de endereço do navegador.

Atualizando o certificado HTTPS

Se o certificado de nome de domínio for atualizado, você precisará atualizar os detalhes do certificado no item de configuração HTTPS.

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
 O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **HTTPS Settings**.
5. Na página de guia **HTTPS Settings**, clique em **Edit**. A caixa de diálogo **Configure HTTPS Secure Acceleration** é exibida.

Configure HTTPS Secure Acceleration

Status

Certificate Source My certificate Huawei-managed certificate

Certificate Name

Certificate Body Configured [Update](#)

Private Key Configured [Update](#)

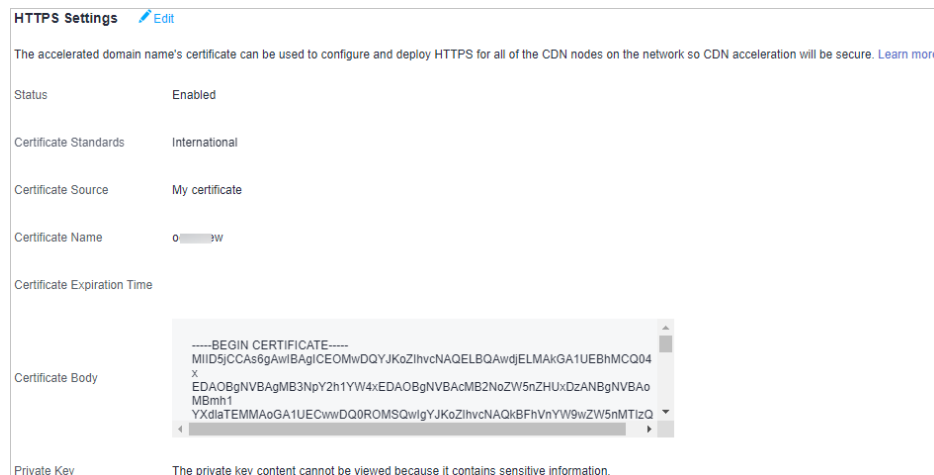
[OK](#) [Cancel](#)

6. Clique em **Update** para atualizar o certificado configurado e a chave privada. Demora aproximadamente 5 a 10 minutos para que a atualização entre em vigor.

Exibição de informações do certificado de HTTPS

Na página de configuração do certificado de HTTPS, você pode exibir detalhes sobre o certificado HTTPS configurado para os nomes de domínio de aceleração.

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **HTTPS Settings**.
5. Na página exibida, você pode exibir detalhes sobre o certificado HTTPS configurado para o nome de domínio, como o tempo de expiração do certificado. Você também pode exibir o conteúdo do certificado. No entanto, o conteúdo da chave privada não pode ser visualizado, por razões de segurança.



O valor de **Certificate Expiration Time** depende do tempo de expiração do certificado que expira primeiro na cadeia de certificados.

2.4.3 Requisitos do certificado HTTPS

A configuração HTTPS suporta apenas certificados ou chaves privadas no formato PEM. Para diferentes agências emissoras de certificados, existem diferentes requisitos de carregamento.

Certificados emitidos pela CA raiz

Um certificado emitido pela CA raiz é um certificado completo. Ao configurar o HTTPS, você só precisa fazer o carregamento do certificado.

Use um editor de texto para abrir o certificado. O conteúdo do certificado deve ser algo semelhante ao que está em [Figura 2-2](#).

Um certificado PEM:

- O certificado começa com a instrução **-----BEGIN CERTIFICATE-----** e termina com a instrução **-----END CERTIFICATE-----**.
- Cada linha do certificado tem 64 caracteres, mas a última linha pode ser mais curta.
- Não são permitidos espaços no conteúdo do certificado.

Figura 2-2 Certificado PEM

```

-----BEGIN CERTIFICATE-----
MIIDxCCAqygAwIBAgIEAJGCTANBgkqhkiG9w0BAQUFADBUMQswCQYDVQQGEwJj
bjELMAkGA1UECAwCZ2QxZCZAJBgNVBACMAN6MQswCQYDVQQKDAJodzeELMAkGA1UE
CwwCaHcxGDAwBgNVBAMMD21OT0MgUm9vdCBDQSBWmjERMA8GCSqGSIb3DQEJARYC
aHcwHhcNMTYwNTE3MDEyODQ2WhcNMjEwNTE2MDEyODQ2WjBdMQswCQYDVQQGEwJj
bjELMAkGA1UECBMCZ2QxZCZAJBgNVBAcTAmh3MQswCQYDVQQLEwJodzeEUMBGA1UE
AxQLKi5vd3Nnby5jb20xETAPBgkqhkiG9w0BCQEWAzh3MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAXDKJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909e
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
HRMEAjAAMCwGCWGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbnVvYXR1ZCBZDZlZ0aWZp
Y2F0ZTA0BgNVHQ4EFgQUmNstyLA+uGec0xx8f+XPLs3AiEUwHwYDVR0jBBgwFoAU
PRaAjcivt51G+7642KLZ+GbJTIQwDQYJKoZIhvcNAQEFBQADggEBABkMXMrUMhEH
ZNhb19blt90NKQJpi7ugy7rj+vft4fUYeTvapsRwNutjWGVmnWB3HV85tnbIgvsa
OpP6yKbJ+mJhL5AB/crDMDMqGhywUEoG80kzEQJSeUHJ/R/iTaksmkqSPyDrbvaN
1DpIf5Sa7YA9VbWYpIZDuOhyk07HSZc8kcSmD+0K9gOke7QS1L3FKAvdggJepel6
A137VUmYtdh2mqS78LcpSs+SofippOGgi5AuimZqp5xrn8Od6GjQqEc7nGH5foQ
lJq8ekhn07Aqd7chFbDfW4qLSY7nEHT3uLzGME8Y9QQ4zs5H71CaJVGXtoTQfpXR
nuMo/2NXiA0=
-----END CERTIFICATE-----
  
```

Certificados emitidos por agências intermediárias

Um arquivo de certificado emitido por uma agência intermediária contém vários certificados. Você precisa combinar os certificados em um único certificado completo para carregamento ao configurar a aceleração de segurança HTTPS. Um certificado combinado é mostrado como [Figura 2-3](#).

Use um editor de texto para abrir todos os certificados. Comece com o certificado do servidor e acrescente o conteúdo dos certificados intermediários ao arquivo. Geralmente, uma instrução será emitida juntamente com o certificado. Esteja ciente das regras na instrução. As regras gerais são as seguintes:

- Não há linhas vazias entre os certificados.
- Os formatos das cadeias de certificados são os seguintes:

```

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

Figura 2-3 Certificado combinado

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj41j5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmVmcxETAPBgNVBAcM
CFNoZW56aGVuMQ8wDQYDVQQKDAZlZWF3ZWkxZCZAJBgNVBAsMAk1UMS4wLWVhZDQw
DCVldWF3ZWkxZCZAJBgNVBAsMAk1UMS4wLWVhZDQwDQYJKoZIhvcNAQELBQAw
ODAwNDA0N1oXDTE4MTAxODAwNDA0N1owGZoxCzAJBgNVBAYTAKNOMRAwDgYDVQQI
DAdqWVhZ3N1MRAwDgYDVQQHDAduYW5qaW5nMS4wLWVhZDQwDQYJKoZIhvcNAQEL
dHdhcmUgVGVjaG5vbG9naWVzIENvbiwvZXRkMRkwFwYDVQQLDBBDbG91ZGJlIFNS
RSBEZXBOMRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE3f5hC6J20XSF/Y7Wb8o6l30yzgaUYWGLEX8t
ldQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPFLT/IV6UnvMLnxJQBavqauykCskadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhrfmR4owS/3w1wxdpw5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccYlufuqr3v0TToaNN4c37kwjJeKf+b2F/IqO/KF+9zF
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdm04NEshlvSFdEHpjy/xKSLCIqg5Ue8tTI8zOF13U0ROnMeHKSXsJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2CCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemh1bjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAlJVVDEuMCwGA1UEAw1SHVhd2VpIFd1
YiBTZWN1cmUgSW50ZXJlZCZAJBgNVBAsMAk1UMS4wLWVhZDQwDQYJKoZIhvcNAQEL
BQAwNjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemh1bjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAlJVV
DEuMCwGA1UEAw1SHVhd2VpIFd1YiBTZWN1cmUgSW50ZXJlZCZAJBgNVBAsMAk1UMS4w
LWVhZDQwDQYJKoZIhvcNAQELBQAw
rG0CAwEAAaNQME4wHQYDVRO0BBYEFDB6DZXX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZXX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9ksjRX56yw2Ku5Mm3gZu/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqilLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpwJW3duj1FuRjGsvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhrAHezyfLrvimxIOky
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu671liddt7zzzzqW+U
QLU0ewUmUHqsV5mk62v1e8sRViHB1B2HJ3DU5gE=
-----END CERTIFICATE-----
```

Chave privada de RSA

Os arquivos PEM podem conter certificados ou chaves privadas. Se um arquivo PEM contiver apenas chaves privadas, o sufixo do arquivo pode ser substituído por KEY.

Use um editor de texto para abrir o arquivo de chave privada no formato PEM ou KEY. Em seguida, você pode visualizar o conteúdo da chave privada, conforme mostrado na [Figura 2-4](#).

Conteúdo de uma chave privada RSA:

- A chave privada começa com a instrução `-----BEGIN RSA PRIVATE KEY-----` e termina com a instrução `-----END RSA PRIVATE KEY-----`.
- Cada linha da chave privada tem 64 caracteres, mas a última linha pode ser mais curta.
- Não são permitidos espaços no conteúdo da chave privada.

Figura 2-4 chave privada de RSA

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAXDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eY1vLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oB12AeAvbzKxWwRqf4JTLa3136B415yZVoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlurl/Z9s8ytj3124AQY7NE1t1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvyfSDEr3Snf6eSSwIDAQABAoIBAQCDCNmx3qHXPGvI
EzB0tIPV11PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcm
[...blurred content...
xxrq/vizzNh6K1dBrZKmrWrAqGifkHqx2M3wsssfSzG3WhS0UT1nrUnONg9XLb15
WeBd2Zp/Fn+tk2T9SsTotAgJAoGAOvmo5APBVRLILHwungLno8ZOYJopOtePGFDp
v0bHNFgGIRfMcoKlx2xuX5cUe9MihRdyPV8aHYvd4ciE6yOGGq2ypVat0SSS+TSL
GXJpezX9AjeWtQV8iWoEojIKKPs9FAHftS2aCbXXVJxwR1kbp8c1yDxQ9yNNCr7o
OBG9XHECgYEA0xuJhoD8HMmoLJockHeMvHY9DqjcncFLwXyuKORKzRT5SiUy7tDJ
VV8cqljV95gNbae6tUp9zNO7mw1wD2ztjyjDc1gtW+Kpfj7VXImtURHrxKFzflNx
uQ/fbf/zaVpJ7QPcL7y671BGevC/JIZ/i2jBGQkQtn8d4rhk72C1kyw=
-----END RSA PRIVATE KEY-----
```

Se a cadeia de certificados de um ficheiro de chave privada contiver as seguintes informações: `-----BEGIN PRIVATE KEY-----` e `-----END PRIVATE KEY-----`, ou `-----BEGIN ENCRYPTED PRIVATE KEY-----` e `-----END ENCRYPTED PRIVATE KEY-----`, você precisa usar a ferramenta OpenSSL para executar o seguinte comando para converter o formato.

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

2.4.4 Conversão de formato de certificado de HTTPS

A configuração de HTTPS suporta apenas certificados ou chaves privadas no formato PEM. Recomenda-se que [OpenSSL](#) seja usado para converter certificados em outros formatos para o formato PEM. Os exemplos a seguir ilustram alguns métodos populares de conversão.

Nos exemplos a seguir, o nome dos certificados antes da conversão é **old_certificate** por padrão, e o nome das chaves privadas antes da conversão é **old_key** por padrão. Os novos nomes de certificado e chave privada são **new_certificate** e **new_key**, respectivamente.

- **Câmbio de DER em 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
```

- **Câmbio de P7B para PEM**

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

- **Câmbio de PFX por PEM**

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

Você também pode usar uma ferramenta de conversão de certificados de terceiros on-line para converter certificados em formatos diferentes.

2.4.5 Grampeamento de OCSP

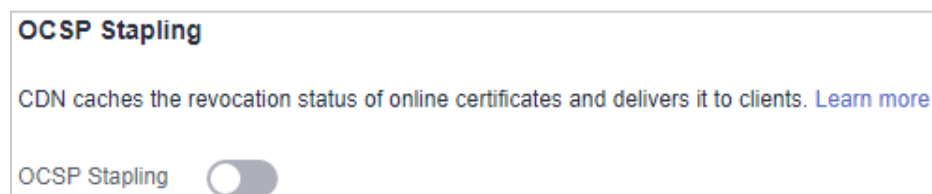
Quando o grampeamento do Protocolo de estado de certificado online (OCSP) está habilitado, a CDN consulta e armazena em cache o status dos certificados online antecipadamente e retorna o status para um navegador ao estabelecer uma conexão TLS com o navegador. Isso significa que o navegador não precisa consultar o status das CAs, acelerando a verificação.

Pré-requisitos

- Um certificado HTTPS foi configurado. Para mais detalhes, consulte [Certificados de HTTPS](#).
- O grampeamento OCSP não pode ser aplicado a toda a aceleração do site ou nomes de domínio que também exigem serviços de aceleração fora da China continental.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **HTTPS Settings**.



5. Ative o **OCSP Stapling**.

2.4.6 Redirecionamento forçado

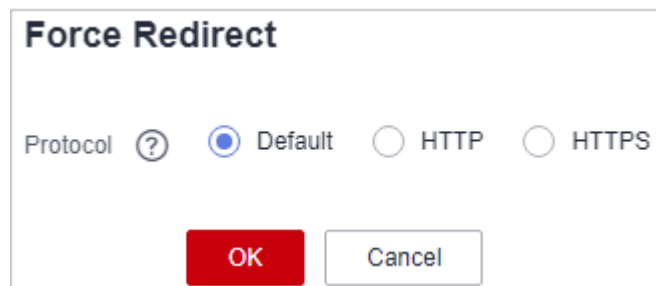
As solicitações de clientes para nós CDN podem ser forçadamente redirecionadas para HTTP ou HTTPS.

Restrições

Um certificado HTTPS foi configurado para o seu nome de domínio. Para mais detalhes, consulte [Certificados de HTTPS](#).

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **HTTPS Settings**.
5. Clique em **Edit** ao lado de **Force Redirect**. A caixa de diálogo **Force Redirect** é exibida.



Protocolo	Descrição
Padrão	As solicitações HTTP e HTTPS de clientes são suportadas.
HTTP	Solicitações de clientes para nós CDN são forçadamente redirecionadas para HTTP.
HTTPS	Solicitações de clientes para nós CDN são forçadamente redirecionadas para HTTPS.

6. Selecione um protocolo e clique em **OK**.

2.4.7 HTTP/2

Conhecimento de fundo

HTTP/2 é um protocolo de transferência de hipertexto de próxima geração. Ele reduz o atraso do handshake de TCP, reduz o volume de transmissão do cabeçalho do pacote e melhora a eficiência da transmissão. Endereços no formato **http://url** podem usar apenas o protocolo HTTP/1.x, e aqueles no formato **https://url** suportam HTTP/2.

Restrições

Um certificado HTTPS foi configurado. Para mais detalhes, consulte [Certificados de HTTPS](#).

Vantagens do protocolo

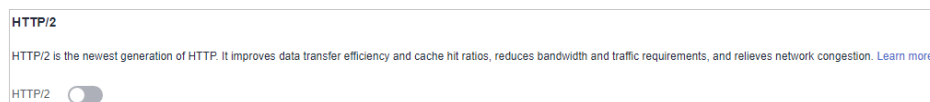
Atualmente, o HTTP/1.1 é o protocolo para a Internet. O HTTP/2 supera o HTTP/1.1 e mantém a sintaxe do HTTP/1.1.

O HTTP/2 supera o HTTP/1.1 nos seguintes aspectos:

- **Framing binário**
O HTTP/2 usa o formato binário para transferir dados, enquanto o HTTP/1.1 é um protocolo baseado em texto. O formato binário é mais vantajoso na resolução e otimização do protocolo, e aumenta a eficiência da transferência de dados.
- **Compressão de campo de cabeçalho**
HTTP/2 comprime e transfere cabeçalhos de mensagens usando HPACK. Esses cabeçalhos são rastreados e armazenados em uma tabela de cabeçalho. Uma vez que um cabeçalho de mensagem foi enviado por uma vez, ele é armazenado em cache e pode ser obtido por outros cabeçalhos de mensagem idênticos automaticamente.
Solicitações usando HTTP1.1 carregam uma grande quantidade de informações de cabeçalho redundantes, o que causa desperdício na largura de banda. Com a compactação de campo de cabeçalho, o HTTP/2 economiza a largura de banda e o tráfego.
- **Multiplexação**
O HTTP/2 multiplexa várias solicitações ou respostas em uma única conexão TCP. Enquanto o HTTP/1.1 estabelece uma conexão TCP para cada solicitação ou resposta em ordem. Ao enviar solicitações simultaneamente, o HTTP/2 diminui a pressão sobre a conexão do servidor e alivia o problema de bloqueio da rede.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **HTTPS Settings**.
5. Ative o **HTTP/2**.



2.4.8 Versões de TLS

Você pode configurar versões TLS conforme necessário.

Conhecimento de fundo

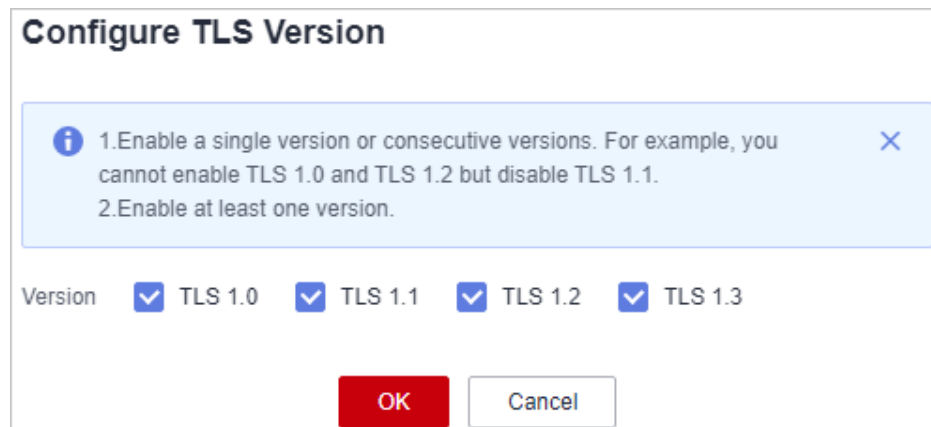
Transport Layer Security (TLS) é um protocolo de segurança usado para garantir a segurança e a integridade dos dados para comunicação na Internet. A aplicação mais comum é o HTTPS. TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3 estão disponíveis. Uma versão posterior é mais segura, mas é menos compatível com navegadores de versões anteriores.

Restrições

- Um certificado HTTPS foi configurado. Para mais detalhes, consulte [Certificados de HTTPS](#).
- As versões TLS não podem ser configuradas para nomes de domínio com configurações especiais.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List** > **Storage** > **CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **HTTPS Settings**.
5. Na área **TLS Version**, clique em **Edit**.



NOTA

- Você pode ativar uma única versão ou versões consecutivas. Por exemplo, você não pode habilitar o TLS 1.0 e o TLS 1.2, mas desabilitar o TLS 1.1.
 - Você precisa habilitar pelo menos uma versão.
 - Por padrão, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3 estão habilitados.
6. Selecione uma ou mais versões de TLS e clique em **OK**.

2.4.9 Perguntas frequentes

Como fazer para corrigi-lo se "Incomplete certificate chain" é exibido?

Isto é talvez porque:

- Formato de certificado inválido
- Os certificados são preenchidos errados.
- Os certificados são instalados na ordem errada.

Classifique os certificados com o certificado raiz no final. Por exemplo, se você tiver três certificados, A, B e C; e o certificado raiz, a ordem deve ser: certificado C - certificado B - certificado A - certificado raiz.

Para obter detalhes sobre como obter a cadeia de certificados correta, consulte [Requisitos de certificado de HTTPS](#).

Em alternativa, pode utilizar uma ferramenta de cadeia de certificados online para corrigir a cadeia de certificados incompleta.

Como fazer para corrigi-lo se o sistema exibe uma mensagem indicando que o formato do certificado está incorreto?

A configuração de HTTPS suporta apenas certificados e chaves privadas no formato PEM. Autoridades de certificação diferentes têm requisitos diferentes no carregamento do organismo de certificação. Para obter detalhes sobre os requisitos de formato, consulte [Requisitos de certificado de HTTPS](#). Se o formato do seu certificado não for PEM, use uma ferramenta online de terceiros para converter o certificado antes de carregá-lo.

2.5 Configurações de cache

2.5.1 Visão geral

A CDN armazena em cache o conteúdo de origem em nós de borda em todo o mundo para que os usuários possam obter conteúdo de nós próximos. Você pode modificar as configurações de cache para alterar o status do cache de recursos em nós CDN.

A tabela a seguir descreve as configurações de cache.

Função	Descrição
Regras de cache	Você pode definir a idade máxima do cache e a prioridade para diferentes recursos para aumentar a taxa de acertos e reduzir a taxa de retorno à origem.
Filtragem de parâmetros de URL	Você pode filtrar parâmetros de URL para permitir que os nós CDN ignorem os parâmetros após um ponto de interrogação (?) ao armazenar recursos em cache, melhorando a taxa de acertos do cache e acelerando a distribuição.
Controle de cache de origem	Você pode definir o tempo de expiração do cache nos nós CDN para ser o mesmo que o do servidor de origem.
Idade de cache de código de estado	Você pode configurar a idade do cache dos códigos de status para permitir que a CDN armazene em cache e devolva os códigos de status aos usuários, reduzindo a taxa de recuperação e a pressão sobre o servidor de origem.

NOTA

- Se você modificou as regras de cache e as configurações de controle de cache de origem, preste atenção ao seguinte:
 - A nova regra não se aplica ao conteúdo que foi armazenado em cache, mas aplica-se apenas ao novo conteúdo.
 - Depois de modificar as regras de cache, [atualize o cache](#) para que a modificação entre em vigor.

2.5.2 Regras de cache

Você pode configurar a idade máxima para um ou mais recursos armazenados em cache em nós de CDN. Se a idade máxima de um arquivo armazenado em cache em nós de CDN tiver atingido, a CDN solicitará o conteúdo mais recente do arquivo do servidor de origem quando um usuário solicitar o arquivo. A CDN retorna o conteúdo para o usuário e o armazena em cache nos nós da CDN. Você pode armazenar em cache todos os arquivos e a página inicial ou armazenar em cache o conteúdo desejado por diretório, tipo de arquivo e caminho completo.

Conhecimento de fundo

As políticas de cache nos nós de CDN estão em conformidade com HTTP. Você pode controlar o envelhecimento do cache configurando o campo **Cache-Control: max-age** em um cabeçalho de resposta HTTP. Aproveitando as regras de cache, você pode otimizar os períodos de cache para diferentes serviços. Políticas de cache adequadas podem aumentar a taxa de acertos e reduzir a taxa de recuperação, o que reduz a utilização da largura de banda.

Depois de receber uma solicitação, um nó de CDN verificará se o conteúdo solicitado expirou no cache. Se o conteúdo solicitado for válido no cache, ele será retornado diretamente desse nó de CDN para o usuário, acelerando a resposta do site. Se o conteúdo solicitado no cache tiver expirado, o nó de CDN enviará uma solicitação para recuperar novo conteúdo de um servidor de origem para que ele possa atualizar seu cache local e fornecer novo conteúdo ao usuário.

Precauções

- Até 60 regras de cache podem ser adicionadas a cada nome de domínio.
- A idade máxima do cache afeta a taxa de recuperação diretamente. Se a idade máxima do cache for curta, o conteúdo em cache nos nós CDN se tornará inválido em pouco tempo, resultando em recuperações frequentes, o que aumenta a carga do servidor de origem e prolonga a latência de acesso. No entanto, se a idade máxima do cache for muito longa, o conteúdo em cache pode ficar desatualizado como resultado.
- Se a idade máxima do cache for definida como 0, a CDN recupera o conteúdo do servidor de origem para todas as solicitações do usuário, o que pode interromper o serviço de aceleração.
- Os recursos armazenados em cache nos nós podem ser excluídos devido ao acesso infrequente.
- Se você modificou a regra de cache,
 - A nova regra não se aplica ao conteúdo que foi armazenado em cache, mas aplica-se apenas ao novo conteúdo.
 - Você pode atualizar o cache para que a modificação entre em vigor imediatamente para o novo conteúdo e o conteúdo que foi armazenado em cache.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
 O console de CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Cache Settings**.
5. Na área **Cache Rules**, clique em **Edit**. A caixa de diálogo **Configure Cache Rule** é exibida.
6. Clique em **Add** para adicionar regras de cache. Consulte [Figura 2-5](#). [Tabela 2-4](#) descreve os parâmetros. Você pode clicar em **Suggested Rules** para exibir a configuração recomendada.

Figura 2-5 Configuração de uma regra de cache

The screenshot shows the 'Configure Cache Rule' dialog box. It features 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 buttons for 'Add' and 'Suggested Rules'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Tabela 2-4 Parâmetros de regra de cache

Parâmetro	Descrição	Regra de configuração
Todos os arquivos	Todos os recursos armazenados em cache nos nós CDN	Por padrão, a CDN tem uma regra para cada novo nome de domínio. A regra específica que a idade máxima do cache para All files é de 30 dias (a idade máxima do cache para o conteúdo em um nome de domínio com aceleração de site inteiro é 0). Você pode modificar, mas não pode excluir essa regra.

Parâmetro	Descrição	Regra de configuração
Tipo de arquivo	Arquivos de um tipo específico Se o tipo de serviço de um novo nome de domínio for Website , File download , ou On-demand service e seu servidor de origem for privado, a CDN adicionará uma regra a ele por padrão. A regra especifica que a idade máxima do cache é 0 para arquivos dinâmicos comuns, como arquivos .php .jsp .asp, e .aspx. A CDN recupera esses arquivos do servidor de origem para cada solicitação. Você pode modificar e excluir essa regra.	<ul style="list-style-type: none"> • Todos os tipos de arquivo são suportados. • Inicie cada extensão de nome de arquivo com um (.), de ponto e separe as extensões de nome de arquivo com ponto-e-vírgula (;). • Insira um máximo de 20 extensões de nome de arquivo. • Insira até 255 caracteres. • As extensões de nome de arquivo não diferenciam maiúsculas de minúsculas. <p>Exemplo: .JPG;.zip;.exe</p>
Diretório	Arquivos em um diretório	<p>Iniciar um diretório com uma barra (/), e separar vários diretórios com ponto-e-vírgula (;). Insira um máximo de 20 diretórios com um máximo de 255 caracteres no total.</p> <p>Exemplo: /test/folder01;/test/folder02</p>
Caminho completo	Um arquivo específico	<p>Um caminho completo deve começar com uma barra (/) e não pode terminar com um asterisco (*). Um arquivo no diretório especificado ou arquivo com o curinga * pode ser correspondido. Insira apenas um caminho completo.</p> <p>Exemplos: /test/index.html ou /test/*.jpg</p>
Página inicial	Diretório raiz	<p>O diretório raiz de um site é o diretório de nível superior da pasta do site, que contém todas as subpastas do site.</p> <p>Por exemplo, para abc/file01/2.png, abc/ é o diretório raiz e uma regra de cache é configurada para abc/.</p>

Parâmetro	Descrição	Regra de configuração
Prioridade	Prioridade de uma regra de cache. Cada regra de cache deve ter uma prioridade exclusiva. A definição de prioridade é obrigatória. Se um recurso for especificado em várias regras de cache, a regra com a prioridade mais alta será aplicada.	Insira um número inteiro de 1 a 100. Um número maior indica uma prioridade maior.
Idade máxima	Duração que um arquivo pode ser armazenado em cache. Se a idade máxima do arquivo tiver atingido, a CDN solicitará o conteúdo mais recente do arquivo do servidor de origem quando um usuário solicitar o arquivo de um nó da CDN. Além disso, a CDN armazena em cache esse conteúdo no nó CDN.	A idade de um arquivo em cache não pode exceder 365 dias. É aconselhável definir o tempo de acordo com as seguintes regras: <ul style="list-style-type: none"> ● Para arquivos estáticos (como arquivos .jpg e .zip) que não são atualizados com frequência, defina a idade máxima para mais de um mês. ● Para arquivos estáticos (como arquivos .js e .css) que são atualizados com frequência, defina a idade máxima com base nos requisitos de serviço. ● Para arquivos dinâmicos (como arquivos .php, .jsp e .asp), defina a idade máxima para 0 segundos.

7. (Opcional) Exclua uma regra de cache se você não a usar mais.
8. Clique em **OK**.

Exemplos

Cenário 1: suponha que você adicionou um portal da web ao HUAWEI CLOUD CDN para aceleração, mas não deseja armazená-lo em cache.

Você pode adicionar uma regra de cache para esse portal da web no console da CDN, com **Type** definido como **Homepage** e **Maximum Age** como **0**.

Cenário 2: suponha que você não deseja armazenar em cache arquivos de um tipo específico ou uma página da web específica.

1. Você configurou a aceleração de CDN para o seu site e definiu a idade máxima do cache dos arquivos .do para um dia. No entanto, devido a requisitos de serviço, você não precisa mais armazenar arquivos cache.do.

Você pode adicionar uma regra de cache para seu site no console da CDN, com **Type** definido como **File type**, **Content** para **.do** e Idade máxima como **0**.

📖 NOTA

A nova regra só vale para novos conteúdos. Depois que a nova regra for adicionada, atualize a URL em cache ou o diretório em que o arquivo .do está localizado no console da CDN para que a nova regra entre em vigor para todos os arquivos .do.

2. Você configurou a aceleração de CDN para o seu site, a página de login do seu site é exibida ciclicamente e seus clientes não podem fazer login no site. Depois que a aceleração da CDN é desativada, os clientes podem fazer login no site.

Isso ocorre porque os nós CDN armazenaram em cache a página de login. Para resolver o problema, adicione uma regra de cache para seu site no console da CDN e defina a idade máxima do cache da página de login como 0 na regra. Tome como exemplo a página de login do console da HUAWEI CLOUD. A página de login do console da HUAWEI CLOUD é <https://auth.huaweicloud.com/authui/login.html#/login>. Você pode adicionar uma regra de cache no console CDN, com **Type** definido como **Full path**, **Content** como **/authui/login.html#/login** e **Maximum Age** como **0**.

Cenário 3: suponha que você configurou as seguintes regras de cache para o nome de domínio de aceleração `www.example.com` mas não sabe qual regra tem efeito.

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

Quando um usuário solicita `www.example.com/test/cdn.jpg`, as regras de **All files**, **File type** e Tipo de **Full path** são todas correspondentes. A prioridade da regra **Full path** é 8, que é a mais alta entre as três regras. Portanto, a regra do tipo de **Full path** (`/test/*.jpg`) é usada.

2.5.3 Filtragem de parâmetros de URL

Conhecimento de fundo

A maioria das solicitações de páginas da web carrega parâmetros de URL que começam com um ponto de interrogação (?). Se os parâmetros não contiverem informações importantes (como versão), você poderá ativar a filtragem de parâmetros de URL para melhorar a taxa de acertos do cache e acelerar a distribuição de conteúdo. Ao configurar a filtragem de parâmetros de URL, você pode reter ou ignorar parâmetros específicos.

Ativação da filtragem de parâmetros de URL

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Cache Settings**.
5. Clique em **Edit** ao lado de **URL Parameter Filtering**.

Tabela 2-5 Descrição do parâmetro

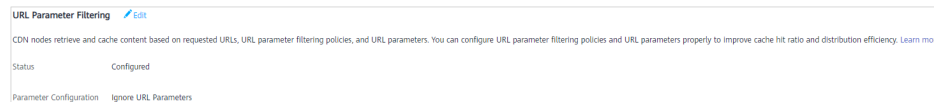
Parâmetro	Descrição	Regra de configuração
Estado	Desativado: (padrão) a filtragem de parâmetros de URL está desativada. A CDN armazena o recurso em cache com base nos parâmetros que seguem o ponto de interrogação (?) em uma URL de solicitação. Ativado: se a filtragem de parâmetros de URL estiver ativada, os seguintes itens de configuração entrarão em vigor.	-
Ignorar parâmetros de URL	CDN ignora todos os parâmetros após pontos de interrogação (?) em URLs de solicitação, melhorando a taxa de acertos do cache.	N/D
Ignorar parâmetros específicos	A CDN ignora os parâmetros específicos em URLs de solicitação, mas mantém outros parâmetros.	<ul style="list-style-type: none"> ● Insira até 10 nomes de parâmetros separados por ponto e vírgula (;). ● Somente letras, dígitos, pontos de (.), sublinhados (_), e til (~) são suportados.
Reten parâmetros específicos	A CDN retém os parâmetros específicos em URLs de solicitação, mas ignora outros parâmetros.	<ul style="list-style-type: none"> ● Insira até 10 nomes de parâmetros separados por ponto e vírgula (;). ● Somente letras, dígitos, pontos de (.), sublinhados (_), e til (~) são suportados.

 **NOTA**

- Se uma regra de cache do seu nome de domínio tiver configurações especiais de parâmetro de URL, não será possível configurar a filtragem de parâmetros de URL para o nome de domínio no console da CDN. Nesse caso, você pode enviar um tíquete de serviço.
6. Ative **Status**, selecione uma operação de parâmetro na lista suspensa **Parameter Configuration**, defina os parâmetros fazendo referência a **Tabela 2-5**, e clique em **OK**.

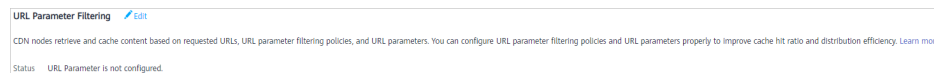
Exemplos

- **Exemplo 1:** seu nome de domínio **www.example.com** tem a seguinte configuração de filtragem de parâmetros de URL:



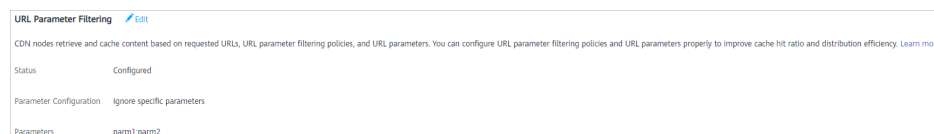
Quando um usuário solicita o **http://www.example.com/1.txt** pela primeira vez, o arquivo não é armazenado em cache no CDN, portanto o CDN precisa recuperá-lo do servidor de origem. Quando o usuário solicitar o **http://www.example.com/1.txt?test1**, o parâmetro que segue o ponto de interrogação (?) será ignorado. Como resultado, o **http://www.example.com/1.txt** é atingido.

- **Exemplo 2:** seu nome de domínio **www.example.com** tem a seguinte configuração de filtragem de parâmetros de URL:



Quando um usuário solicita o **http://www.example.com/1.txt** pela primeira vez, o arquivo não é armazenado em cache no CDN, portanto o CDN precisa recuperá-lo do servidor de origem. Quando o usuário solicitar o **http://www.example.com/1.txt?test1**, a CDN procurará uma correspondência para a URL completa, incluindo o parâmetro após o ponto de interrogação (?) porque a filtragem de parâmetros de URL está desativada. Como resultado, a CDN precisa recuperar **http://www.example.com/1.txt?test1** do servidor de origem porque nenhum cache é atingido.

- **Exemplo 3:** seu nome de domínio **www.example.com** tem a seguinte configuração de filtragem de parâmetros de URL:



Quando um usuário solicita o **http://www.example.com/1.txt** pela primeira vez, o arquivo não é armazenado em cache no CDN, portanto o CDN precisa recuperá-lo do servidor de origem. Quando o usuário solicitar **http://www.example.com/1.txt?parm1&parm2**, os parâmetros **parm1** e **parm2** na URL serão ignorados. Como resultado, o **http://www.example.com/1.txt** é atingido.

2.5.4 Controle de cache de origem

Conhecimento de fundo

Se **Cache-Control: max-age** tiver sido configurado para o servidor de origem e você quiser que o tempo de expiração do cache no lado da CDN seja o mesmo que **Cache-Control: max-**

age, você pode ativar o **Origin Cache Control**. Em seguida, **Cache-Control: max-age** determina por quanto tempo o conteúdo é armazenado em cache nos nós de CDN.

Habilitar o controle de cache de origem

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Cache Settings**.
5. Veja a página seguinte.

Origin Cache Control

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

Origin Cache Control

6. Ativar o **Origin Cache Control**.

Origin Cache Control

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

Origin Cache Control

Exemplos

Suponha que tenha ativado o **Origin Cache Control** para o nome de domínio **www.example.com**.

Origin Cache Control

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

Origin Cache Control

Quando um usuário solicita o arquivo **http://www.example.com/abc.jpg**

- Se você tiver definido **cache-control** como **max-age** no servidor de origem, a configuração **max-age** no servidor de origem será usada.
- Se você tiver definido o **cache-control** como **no-cache**, **private**, ou **no-store** no servidor de origem, a CDN não armazenará o arquivo em cache e a entrega de conteúdo não poderá ser acelerada.

- Se você não tiver definido o **cache-control** no servidor de origem, a idade máxima do cache configurada no CDN será usada.

2.5.5 Idade de cache de código de estado

Quando um nó CDN recupera um recurso do servidor de origem, o servidor de origem retorna um código de status de resposta. Você pode definir a idade do cache do código de status no console CDN. Quando um cliente solicitar o recurso novamente, a recuperação de conteúdo não será acionada, reduzindo a taxa de recuperação e a pressão sobre o servidor de origem.

Cenários

Esta função se aplica ao cenário em que o servidor de origem retorna um código de status anormal. Quando o servidor de origem está sendo executado corretamente, a CDN armazena em cache um recurso recuperado em nós com base nas regras de cache configuradas por você. Quando um usuário acessa o recurso, a recuperação de conteúdo não será acionada. Se o servidor de origem responder de forma anormal e você não quiser que o servidor de origem responda a todas as solicitações, você poderá definir a idade do cache do código de status para reduzir a pressão sobre o servidor de origem.

Aplicação: se os usuários estiverem acessando continuamente a imagem **abc.jpg** que não esteja armazenada em cache em nós CDN e que tenha sido excluída do servidor de origem, os nós CDN recuperarão a imagem para cada solicitação do usuário e o servidor de origem retornará um código de status 4xx, aumentando a pressão no servidor de origem. Nesse caso, se você configurar a idade do cache para o código de status 4xx na CDN, os nós da CDN retornarão diretamente o código de status 4xx quando os usuários solicitarem a imagem e a recuperação do conteúdo não será necessária.

Precauções

- A idade do cache do código de status não pode ser configurada para nomes de domínio com configurações especiais.
- Você pode configurar a idade do cache para os seguintes códigos de estado:
 - 4XX: 400, 403, 404, 405 e 414
 - 5XX: 500, 501, 502, 503 e 504

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Cache Settings**.
5. Clique em **Add** em **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

Parâmetro	Descrição	Exemplo
Código de estado	Código de estado a ser armazenado em cache.	404
Idade do cache	Duração para armazenar em cache os códigos de status nos nós CDN. <ul style="list-style-type: none"> ● Se for definido como 0, o código de status não será armazenado em cache. ● O valor máximo é de 365 dias. 	3 days

6. Configure os parâmetros e clique em **OK**.

Exemplos

Suponha que você configurou as seguintes regras de cache de código de status para o nome de domínio `www.example.com`:



Resultado: quando um usuário acessa um recurso que não está armazenado em cache em um nó CDN, o nó CDN recupera os recursos do servidor de origem. No entanto, o servidor de origem excluiu o recurso e retorna um código de estado 404. A CDN transmite de forma transparente o código de status para o usuário e armazena em cache o código de status no nó da CDN. Dentro da era do cache (30 dias), quando um usuário acessa o recurso novamente, a CDN retorna diretamente o código de status 404 para o usuário e não precisa recuperar o conteúdo do servidor de origem, reduzindo a pressão sobre o servidor de origem.

2.6 Controle de acesso

2.6.1 Visão geral

Você pode configurar validação de referência, lista negra e lista branca de endereços IP, lista negra e lista branca do agente de usuário e autenticação de URL para identificar e filtrar usuários não autorizados e melhorar a segurança da CDN.

Função	Descrição
Configuração da validação do referenciador	Este tópico descreve como configurar uma lista negra ou uma lista branca de referência. Os usuários são identificados e filtrados de acordo com as políticas de filtro configuradas, a fim controlar fontes de acesso.
Configuração de uma ACL	Esta seção descreve como configurar uma ACL. Ao definir uma política de filtragem, você pode filtrar solicitações de endereços IP específicos para restringir o acesso.
Configuração de uma lista negra ou lista branca do agente de usuário	Esta seção descreve como configurar a filtragem do agente de usuário para restringir o acesso.
Configuração da assinatura de URL	Esta seção descreve como configurar a autenticação de URL para proteger os recursos do site de serem baixados por usuários mal-intencionados.

2.6.2 Configuração de validação do referenciador

Este tópico descreve como configurar uma lista negra ou uma lista branca de referência. Os usuários são identificados e filtrados de acordo com as políticas de filtro configuradas, a fim controlar fontes de acesso.

Conhecimento de fundo

O campo de referência em um cabeçalho de solicitação HTTP identifica o endereço da página da Web da qual o recurso foi solicitado. Os nós CDN podem usar o campo de referência para rastrear e identificar a origem.

Ao receber solicitações de acesso de usuários, os nós da CDN identificam e verificam os usuários em relação à lista negra ou lista branca de referência. Somente os usuários que atendem aos requisitos de lista negra e lista branca podem acessar o conteúdo. Usuários não qualificados receberão uma resposta de erro 403.

Procedimento

1. Faça login em **console da Huawei Cloud**. Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Access Control**.

5. Na área **Referer Validation**, clique em **Edit**. A caixa de diálogo **Configure Referer Validation** é exibida.

Configure Referer Validation

Status

* Type Referer blacklist Referer whitelist

Include blank referer ?

* Rule
 Enter up to 100 domain names and IP addresses separated with semicolons (;).
 Wildcard domain names and domain names with ports are allowed. Maximum
 port number is 65535.
 Example:
 www.example.com:443;*.test.com;192.168.0.0

OK Cancel

6. Ative o **Status** para habilitar este item de configuração.
7. Selecione um valor para **Type** e defina parâmetros de referência com base nos requisitos de serviço. A tabela a seguir descreve os parâmetros.

Parâmetro	Descrição	Regra de preenchimento
Incluir referência em branco	Uma referência em branco é quando o campo de referência em uma solicitação HTTP é deixado em branco ou quando uma solicitação HTTP não contém o campo de referência. Se esta opção for selecionada, tais solicitações também serão filtradas com base em listas brancas e listas negras configuradas.	/

Parâmetro	Descrição	Regra de preenchimento
Lista branca do referenciador	<ul style="list-style-type: none"> ● Se o campo de referência de uma solicitação de acesso corresponder às regras da lista branca, o solicitante poderá acessar o conteúdo solicitado. Caso contrário, a CDN retornará um código de resposta de erro 403, indicando que o acesso é proibido. ● Se Include blank referer estiver selecionada e uma solicitação de acesso contiver uma referência em branco, o solicitante poderá acessar o conteúdo solicitado. 	<ul style="list-style-type: none"> ● Insira nomes de domínio ou endereços IP separados por ponto e vírgula (;). ● Nomes de domínio curinga são suportados. ● Nomes de domínio com portas são suportados. O número máximo de porta é 65535. ● Digite até 400 nomes de domínio e endereços IP. Exemplo: o www.example.com: 443;*.test.com; 192.168.0.0
Lista negra de referência	<ul style="list-style-type: none"> ● Se o campo de referência em uma solicitação de acesso corresponder às regras da lista negra, o solicitante não poderá acessar o conteúdo solicitado e 403 Forbidden será retornado. Caso contrário, o solicitante poderá acessar o conteúdo solicitado. ● Se Include blank referer for selecionado e uma solicitação de acesso contiver uma referência em branco, a solicitação de acesso será rejeitada e 403 Forbidden será retornada. 	<ul style="list-style-type: none"> ● Insira nomes de domínio ou endereços IP separados por ponto e vírgula (;). ● Nomes de domínio curinga são suportados. ● Nomes de domínio com portas são suportados. O número máximo de porta é 65535. ● Digite até 400 nomes de domínio e endereços IP. Exemplo: o www.example.com: 443;*.test.com; 192.168.0.0

8. Na caixa de texto **Rule**, insira os nomes de domínio.
9. Clique em **OK**.

Exemplos

1. Suponha que uma lista branca de referência **www.test.com** esteja configurada para o nome de domínio **www.example.com** e **Include blank referer** esteja selecionada.

Configure Referer Validation

Status

* Type Referer blacklist Referer whitelist

Include blank referer ?

* Rule

OK Cancel

- Se o usuário 1 solicitar o URL **https://www.example.com/file.html** e o valor do campo de referência na solicitação estiver em branco, a CDN retornará o conteúdo.
- Se o usuário 2 solicitar o URL **https://www.example.com/file.html** e o valor do campo de referência na solicitação for **www.test.com**, a CDN retornará o conteúdo.
- Se o usuário 3 solicitar o URL **https://www.example.com/file.html** e o valor do campo de referência na solicitação for **www.abc.com**, a CDN retornará um código de resposta de erro 403.

2. Suponha que uma lista negra de referência **www.test01.com** esteja configurada para o nome de domínio **www.example01.com** e **Include blank referer** esteja selecionada.

Configure Referer Validation

Status

* Type Referer blacklist Referer whitelist

Include blank referer ?

* Rule

OK Cancel

- Se o usuário 1 solicitar o URL **https://www.example01.com/file.html** e o valor do campo de referência na solicitação estiver em branco, a CDN retornará um código de resposta de erro 403.

- Se o usuário 2 solicitar o URL **https://www.example01.com/file.html** e o valor do campo de referência na solicitação for **www.test01.com**, a CDN retornará um código de resposta de erro 403.
- Se o usuário 3 solicitar o URL **https://www.example01.com/file.html** e o valor do campo de referência na solicitação for **www.bcd.com**, a CDN retornará o conteúdo.

2.6.3 Configuração de uma ACL

Este tópico descreve como configurar uma ACL. Você pode definir uma política de filtragem para filtrar solicitações de endereços IP específicos para restringir o acesso e impedir roubo de conteúdo e ataques.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Access Control**.
5. Na área **ACL**, clique em **Edit**. A caixa de diálogo **Configure ACL** é exibida.

Configure ACL

i 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

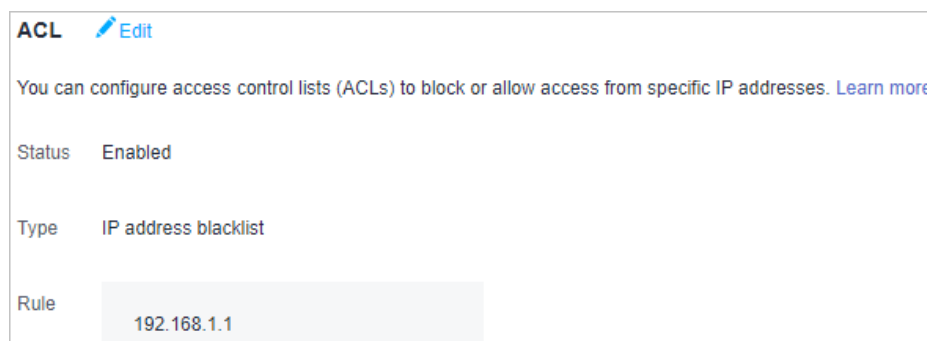
6. Ative o **Status** para habilitar este item de configuração.
7. Selecione um tipo e insira regras.

Parâmetro	Descrição
Tipo	<ul style="list-style-type: none"> ● Lista negra de endereços IP: se o endereço IP de um usuário estiver incluído na lista negra de endereços IP, o código de status 403 será retornado quando o usuário acessar um nó CDN. ● Lista branca de endereços IP: se o endereço IP de um usuário não estiver incluído na lista branca de endereços IP, o código de status 403 será retornado quando o usuário acessar um nó CDN. <p>NOTA</p> <ul style="list-style-type: none"> ● Uma lista negra de endereços IP ou uma lista branca de endereços IP podem ser configuradas.
Regra	<ul style="list-style-type: none"> ● Até 150 endereços IP ou sub-redes são suportados. Digite um endereço IP ou sub-rede em cada linha. ● Apenas as máscaras de sub-rede de 8, 16, 24 e 32 bit são suportadas. ● A parte do endereço IP da sub-rede deve ser o primeiro endereço IP nesse bloco. ● Endereços IP duplicados e segmentos de endereços IP serão removidos. ● Não há suporte para curingas, por exemplo, 192.168.0.*. ● Endereços IPv6 são permitidos.

8. Clique em **OK**.

Exemplos

Suponha que você configurou a seguinte ACL para o nome de domínio **www.example.com**:



- Um usuário solicita **http://www.example.com/abc.jpg**. O endereço IP do cliente do usuário 192.168.1.1 é incluído na lista negra, então o código de erro 403 é retornado.
- Um usuário solicita **http://www.example.com/abc.jpg**. O endereço IP do cliente do usuário 192.168.1.3 não está incluído na lista negra, portanto, o conteúdo solicitado é retornado.

2.6.4 Configuração de uma lista negra ou lista branca do agente de usuário

Você pode configurar uma lista negra ou uma lista branca do agente de usuário para seu nome de domínio para identificar e filtrar visitantes e melhorar a segurança do nome de domínio.

Conhecimento de fundo

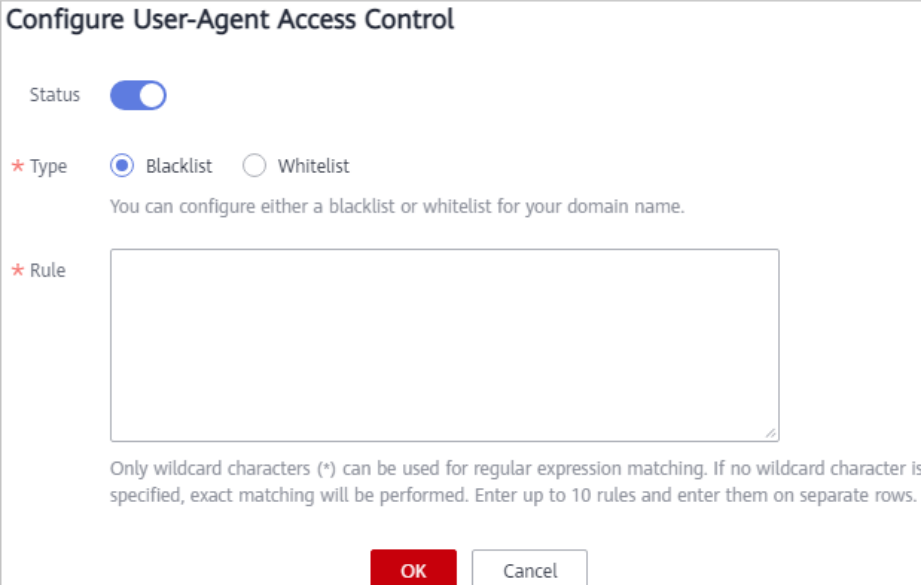
Você pode configurar uma lista negra ou uma lista branca do agente de usuário para filtrar solicitações para seu nome de domínio com base no campo de agente de usuário.

Lista negra: solicitações que incluam campos na lista negra não podem acessar o conteúdo e 403 serão retornadas.

Lista branca: somente solicitações que incluam campos na lista branca podem acessar o conteúdo. Outras solicitações falharão e 403 serão devolvidas.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Access Control**.
5. Na área **User-Agent Access Control**, clique em **Edit**. A caixa de diálogo **Configure User-Agent Access Control** é exibida.



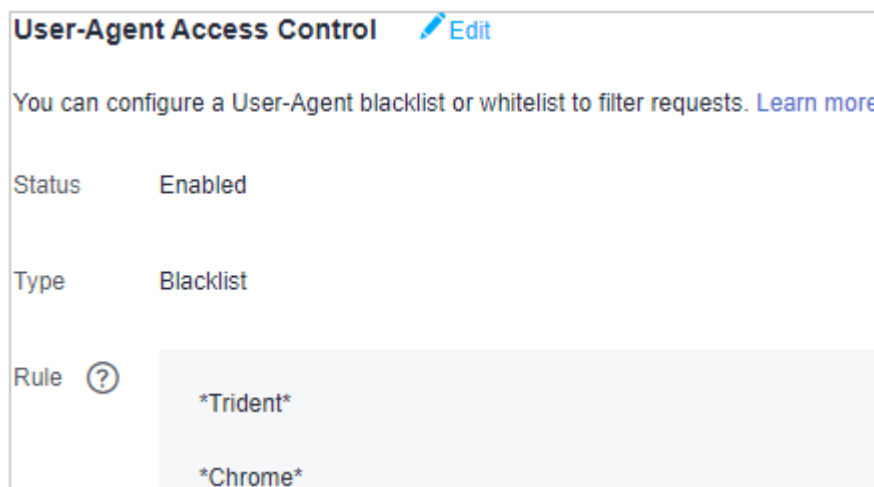
6. Ative o **Status** para habilitar este item de configuração.
7. Selecione um tipo e insira regras.

Parâmetro	Descrição
Tipo	<ul style="list-style-type: none"> ● Lista negra: solicitações que incluem campos na lista negra não podem acessar o conteúdo. ● Lista branca: somente solicitações que incluam campos na lista branca podem acessar o conteúdo.
Regra	<ul style="list-style-type: none"> ● Somente letras, números, espaços e os seguintes caracteres especiais são permitidos: *.-_(),/. ● Somente caracteres curinga (*) podem ser usados para correspondência de expressões regulares. Se nenhum caractere curinga for incluído, a correspondência exata será usada. ● Insira até 100 caracteres para uma regra. ● Insira até 10 regras e insira-as em linhas separadas.

8. Clique em **OK**.

Exemplos

Suponha que você configurou a seguinte lista negra do agente de usuário para o nome de domínio **www.example.com**:



Se o **User-Agent** no cabeçalho de uma solicitação HTTP for um dos seguintes:

```
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 ou **Chrome** está incluído na lista negra, então 403 é retornado.

2.6.5 Configuração de assinatura de URL

2.6.5.1 Método de assinatura A

Por padrão, os recursos públicos são distribuídos por CDN. A assinatura de URL protege esses recursos de serem baixados e roubados por usuários mal-intencionados. A CDN da

Huawei Cloud fornece quatro métodos de assinatura de URL. Este tópico descreve o método de assinatura A.

 **NOTA**

- Se o nome de domínio tiver configurações especiais, a assinatura de URL não poderá ser configurada para esse nome de domínio no console da CDN.
- Quando a assinatura de URL é configurada, as solicitações do usuário incluem parâmetros de autenticação. Se **Ignore specific parameters** não estiver configurado:
 - A recuperação de conteúdo se tornará frequente.
 - Se o servidor de origem for um bucket do OBS, serão cobradas taxas para o tráfego de saída do bucket.

Como funciona

Um exemplo de URL assinado se parece com:

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

A tabela a seguir descreve os parâmetros em um URL assinado.

Tabela 2-6 Descrição do parâmetro

Parâmetro	Descrição
DomainName	Nome de domínio de aceleração.
timestamp	Hora em que o servidor de autenticação gera uma URL assinada, ou seja, a hora de início da autenticação. O valor é um inteiro decimal, indicando o número total de segundos decorridos desde 00:00:00 de 01 de janeiro de 1970.
Período de validade	Quanto tempo um URL assinado permanece eficaz. O valor varia de 0s a 31.536.000s. Exemplo: se o período de validade for definido como 1800s, os usuários poderão acessar a CDN dentro de 1800s desde o horário indicado pelo timestamp . A autenticação falha e o URL fica inacessível se os usuários acessarem o CDN 1800s posteriormente.
rand	Número aleatório. O valor recomendado é um UUID, que não pode conter hífen (-), por exemplo, 202cb962ac59075b964b07152d234b70 .
uid	ID do usuário. Este parâmetro não é usado agora. Você pode configurá-lo para 0 .
md5hash	Uma seqüência de 32 caracteres calculada usando o algoritmo MD5. A cadeia consiste em dígitos (0 a 9) e letras minúsculas.
sha256	Uma seqüência de 32 caracteres calculada usando o algoritmo SHA256. A cadeia consiste em dígitos e letras minúsculas.
Filename	URL de volta à origem. Seu valor deve começar com uma barra (/) e não inclui os parâmetros após o ponto de interrogação (?).

Parâmetro	Descrição
PrivateKey	Chave de assinatura, que é usada para gerar um URL assinado, por exemplo, huaweicloud123. A chave contém de 6 a 32 caracteres e pode conter apenas letras e dígitos.
Parâmetro de autenticação	Parâmetro de autenticação transportado em um URL. O valor padrão é auth_key .

Método de verificação

Depois de receber uma solicitação, um nó CDN verifica a solicitação da seguinte maneira:

1. Verifica se os parâmetros de autenticação estão incluídos na solicitação. Caso contrário, a solicitação é considerada inválida e um código de erro HTTP 403 é retornado.
2. Verifica se a hora do sistema atual está dentro do intervalo [timestamp, timestamp +período válido]. Se a hora atual do sistema exceder o intervalo, o nó de CDN considerará que a solicitação expira e retornará um código de erro HTTP 403. Se a hora atual do sistema estiver dentro do intervalo, o próximo passo prossegue.
3. Constrói uma cadeia de caracteres, calcula **HashValue** com a cadeia usando o algoritmo MD5 e SHA256 e compara **HashValue** com o valor **md5hash** ou **sha256** na solicitação. Se o valor **md5hash** ou **sha256** for o mesmo que **HashValue**, a autenticação será bem-sucedida e um arquivo será retornado. Caso contrário, a autenticação falhará e um código de erro de HTTP 403 será retornado. **HashValue** é calculado da seguinte forma:

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

Ou

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

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Access Control** e clique em **Sign URL**.

Figura 2-6 Os URLs de assinatura

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

- Defina os parâmetros de acordo com a tabela a seguir e clique em **OK**.

Tabela 2-7 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos.
Algoritmo de criptografia	MD5 ou SHA256 .
Período (s) de validade	Por quanto tempo o URL assinado permanece efetivo. O valor varia de 0s a 31.536.000s.

Calculadora de assinatura de URL

Usando a calculadora de assinatura de URL, você pode gerar um URL assinado para os usuários. Defina parâmetros de acordo com [Tabela 2-8](#) e clique em **Generate** para gerar um URL assinado que expirará em um momento específico.

Figura 2-7 Calculadora de assinatura de URL

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[redacted].com/test?auth_key=1638762163-2ee4991dcf95460fb94800283ec548a3-0-225443abb6d0c7e0389a967d8c8d021a`

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

NOTA

Escape caracteres especiais no URL assinado, se houver.

Tabela 2-8 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos. O valor deve ser o mesmo que a chave de assinatura especificada na configuração de assinatura de URL.
Caminho de acesso	Caminho do conteúdo, que começa com uma barra (/) e não carrega uma string de consulta.
Algoritmo de criptografia	MD5 ou SHA256 .
Hora de início	Hora em que o URL assinado entrará em vigor.

Parâmetro	Descrição
Período (s) de validade	<p>Por quanto tempo o URL assinado permanece efetivo. O valor varia de 0s a 31.536.000s. Se esse valor for maior que o período de validade definido na configuração de assinatura de URL, o último será usado.</p> <p>Exemplo: se você definir esse parâmetro para 2000s, mas o período de validade definido na configuração de assinatura de URL for 1800s, o período de validade dos URLs assinados será 1800s.</p>

Exemplo

O seguinte utiliza o algoritmo MD5 como exemplo:

1. Suponha que o URL de retorno à origem seja o seguinte:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Defina **PrivateKey** para **huaweicloud123**.
3. A autenticação entra em vigor a partir das 00:00:00 de 30 de junho de 2017. **Timestamp** é **1498752000**. Defina o período de validade para 1800s.
4. O nó CDN constrói uma cadeia de caracteres para o cálculo de **HashValue**.
`/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3-1498752000-0-0-huaweicloud123`
5. O nó CDN calcula **HashValue** de acordo com a cadeia de caracteres assinada.
`HashValue = md5sum("/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3-1498752000-0-0-huaweicloud123") = 40e64d69aac7d15edfc6ec8a080042cb`
6. O URL da solicitação é o seguinte:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3?auth_key=1498752000-0-0-40e64d69aac7d15edfc6ec8a080042cb`

Se o pedido estiver dentro do prazo de validade (das 00:00:00 em 30 de junho de 2017 para 00:30:00 em 30 de junho de 2017) e o **HashValue** calculado é o mesmo que o valor **md5hash** (40e64d69aac7d15edfc6ec8a080042cb) transportado em pedido, a autenticação for bem-sucedida.

2.6.5.2 Método de assinatura B

Por padrão, os recursos públicos são distribuídos por CDN. A assinatura de URL protege esses recursos de serem baixados e roubados por usuários mal-intencionados. A CDN da Huawei Cloud fornece quatro métodos de assinatura de URL. Este tópico descreve o método de assinatura B.

NOTA

- Se o nome de domínio tiver configurações especiais, a assinatura de URL não poderá ser configurada para esse nome de domínio no console da CDN.
- Quando a assinatura de URL é configurada, as solicitações do usuário incluem parâmetros de autenticação. Se **Ignore specific parameters** não estiver configurado:
 - A recuperação de conteúdo se tornará frequente.
 - Se o servidor de origem for um bucket do OBS, serão cobradas taxas para o tráfego de saída do bucket.

Como funciona

Um exemplo de URL assinado se parece com:

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

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

Se a autenticação é bem sucedida, o URL da volta-à-origem é:

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

A tabela a seguir descreve os parâmetros em um URL assinado.

Tabela 2-9 Descrição do parâmetro

Parâmetro	Descrição
DomainName	Nome de domínio de aceleração.
timestamp	Hora em que o servidor de autenticação gera uma URL assinada, ou seja, a hora de início da autenticação. O formato é YYYYMMDDHHMM, por exemplo, 201706301000 .
Período de validade	Quanto tempo um URL assinado permanece eficaz. O valor varia de 0s a 31.536.000s. Exemplo: se o período de validade estiver definido como 1800s e timestamp for 201706301000 , o URL expirará às 10:30:00 da manhã em 30 de junho de 2017.
md5hash	Uma cadeia de 32 caracteres calculada usando o algoritmo MD5. A cadeia consiste em dígitos (0 a 9) e letras minúsculas.
sha256	Uma seqüência de 32 caracteres calculada usando o algoritmo SHA256. A cadeia consiste em dígitos e letras minúsculas.
Filename	URL de volta à origem. Seu valor deve começar com uma barra (/) e não inclui os parâmetros após o ponto de interrogação (?).
PrivateKey	Chave de assinatura, que é usada para gerar um URL assinado, por exemplo, huaweicloud123. A chave contém de 6 a 32 caracteres e pode conter apenas letras e dígitos.

Método de verificação

Depois de receber uma solicitação, um nó CDN verifica a solicitação da seguinte maneira:

1. Verifica se os parâmetros de autenticação estão incluídos na solicitação. Caso contrário, a solicitação é considerada inválida e um código de erro de HTTP 403 é retornado.
2. Verifica se a hora do sistema atual está dentro do intervalo [timestamp, timestamp +período válido]. Se a hora atual do sistema exceder o intervalo, o nó de CDN considerará que a solicitação expira e retornará um código de erro HTTP 403. Se a hora atual do sistema estiver dentro do intervalo, o próximo passo prossegue.
3. Constrói uma cadeia de caracteres, calcula **HashValue** com a cadeia usando o algoritmo MD5 e SHA256 e compara **HashValue** com o valor **md5hash** ou **sha256** na solicitação. Se o valor **md5hash** ou **sha256** for o mesmo que **HashValue**, a autenticação será bem-

sucedida e um arquivo será retornado. Caso contrário, a autenticação falhará e um código de erro HTTP 403 será retornado. **Hash Value** é calculado da seguinte forma:

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

Ou

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

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Access Control** e clique em **Sign URL**.

Figura 2-8 Os URLs de assinatura

Sign URL

Status

Signing Method Method A Method B Method C1 Method C2

Signed URL example:
<http://hwcdn.example.com/201706301000/51415b2256b64a9772a30edf69c00b08/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 Decimal

Validity Period (s)

OK Cancel

5. Defina os parâmetros de acordo com a tabela a seguir e clique em **OK**.

Tabela 2-10 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos.
Algoritmo de criptografia	MD5 ou SHA256 .

Parâmetro	Descrição
Período (s) de validade	Quanto tempo um URL assinado permanece eficaz. O valor varia de 0s a 31.536.000s.

Calculadora de assinatura de URL

Usando a calculadora de assinatura de URL, você pode gerar um URL assinado para os usuários. Defina parâmetros de acordo com [Tabela 2-11](#) e clique em **Generate** para gerar um URL assinado que expirará em um momento específico.

Figura 2-9 Calculadora de assinatura de URL

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.\[redacted\].com/202112061142/7c21604fbacd9f99f830674e83c5743e/test](http://www.[redacted].com/202112061142/7c21604fbacd9f99f830674e83c5743e/test)

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

Tabela 2-11 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos. O valor deve ser o mesmo que a chave de assinatura especificada na configuração de assinatura de URL.
Caminho de acesso	Caminho do conteúdo, que começa com uma barra (/) e não carrega uma string de consulta.

Parâmetro	Descrição
Algoritmo de criptografia	MD5 ou SHA256 .
Hora de início	Hora em que o URL assinado entrará em vigor.
Período (s) de validade	Por quanto tempo o URL assinado permanece efetivo. O valor varia de 0s a 31.536.000s. Se esse valor for maior que o período de validade definido na configuração de assinatura de URL, o último será usado. Exemplo: se você definir esse parâmetro para 2000s, mas o período de validade definido na configuração de assinatura de URL for 1800s, o período de validade dos URL assinados será 1800s.

 **NOTA**

Escape caracteres especiais no URL assinado, se houver.

Exemplo

O seguinte utiliza o algoritmo MD5 como exemplo:

1. Suponha que o URL de retorno à origem seja o seguinte:

```
http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
```

2. Defina **PrivateKey** para **huaweicloud123**.

3. **timestamp** é **201706301000**.

4. O nó CDN constrói uma string para calcular **md5hash**.

```
huaweicloud123201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
```

5. O nó CDN calcula **md5hash** de acordo com a string de caracteres assinada.

```
md5hash = md5sum("huaweicloud123201706301000/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3") = 51415b2256b64a9772a30edf69c00b08
```

6. A URL da solicitação é:

```
http://hwcdn.example.com/201706301000/51415b2256b64a9772a30edf69c00b08/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3
```

Se o pedido estiver dentro do prazo de validade (das 10:00:00 do dia 30 de junho de 2017 para as 10:30:00 do dia 30 de junho de 2017) e o **md5hash** calculado é o mesmo que o valor **md5hash** (51415b2256b64a9772a30edf69c00b08) realizada na solicitação, a autenticação é bem sucedida.

2.6.5.3 Método de assinatura C1

Por padrão, os recursos públicos são distribuídos por CDN. A assinatura de URL protege esses recursos de serem baixados e roubados por usuários mal-intencionados. A CDN da Huawei Cloud fornece quatro métodos de assinatura de URL. Este tópico descreve o método de assinatura C1.

 **NOTA**

- Se o nome de domínio tiver configurações especiais, a assinatura de URL não poderá ser configurada para esse nome de domínio no console da CDN.
- Quando a assinatura de URL é configurada, as solicitações do usuário incluem parâmetros de autenticação. Se **Ignore specific parameters** não estiver configurado:
 - A recuperação de conteúdo se tornará frequente.
 - Se o servidor de origem for um bucket do OBS, serão cobradas taxas para o tráfego de saída do bucket.

Como funciona

Um exemplo de URL assinado se parece com:

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

A tabela a seguir descreve os parâmetros em um URL assinado.

Tabela 2-12 Descrição do parâmetro

Parâmetro	Descrição
DomainName	Nome de domínio de aceleração.
timestamp	Hora em que o servidor de autenticação gera uma URL assinada, ou seja, a hora de início da autenticação. O valor é um número inteiro hexadecimal, indicando o número total de segundos decorridos desde 00:00:00 01 de janeiro de 1970.
Período de validade	Quanto tempo um URL assinado permanece eficaz. O valor varia de 0s a 31.536.000s. Exemplo: se o período de validade for definido como 1800s, os usuários poderão acessar a CDN dentro de 1800s desde o horário indicado pelo timestamp . A autenticação falha e o URL fica inacessível se os usuários acessarem a CDN 1800s posteriormente.
md5hash	Uma cadeia de 32 caracteres calculada usando o algoritmo MD5. A cadeia consiste em dígitos (0 a 9) e letras minúsculas.
sha256	Uma seqüência de 32 caracteres calculada usando o algoritmo SHA256. A cadeia consiste em dígitos e letras minúsculas.
Filename	URL de volta à origem. Seu valor deve começar com uma barra (/) e não inclui os parâmetros após o ponto de interrogação (?).
PrivateKey	Chave de assinatura, que é usada para gerar um URL assinado, por exemplo, huaweicloud123. A chave contém de 6 a 32 caracteres e pode conter apenas letras e dígitos.

Método de verificação

Depois de receber uma solicitação, um nó de CDN verifica a solicitação da seguinte maneira:

1. Verifica se os parâmetros de autenticação estão incluídos na solicitação. Caso contrário, a solicitação é considerada inválida e um código de erro de HTTP 403 é retornado.

2. Verifica se a hora do sistema atual está dentro do intervalo [timestamp, timestamp +período válido]. Se a hora atual do sistema exceder o intervalo, o nó de CDN considerará que a solicitação expira e retornará um código de erro HTTP 403. Se a hora atual do sistema estiver dentro do intervalo, o próximo passo prossegue.
3. Constrói uma cadeia de caracteres, calcula **HashValue** com a cadeia usando o algoritmo MD5 e SHA256 e compara **HashValue** com o valor **md5hash** ou **sha256** na solicitação. Se o valor **md5hash** ou **sha256** for o mesmo que **HashValue**, a autenticação será bem-sucedida e um arquivo será retornado. Caso contrário, a autenticação falhará e um código de erro HTTP 403 será retornado. **HashValue** é calculado da seguinte forma:

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

Ou

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

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Access Control** e clique em **Sign URL**.

Figura 2-10 Os URLs de assinatura

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)

OK Cancel

5. Defina os parâmetros de acordo com a tabela a seguir e clique em **OK**.

Tabela 2-13 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos.
Algoritmo de criptografia	MD5 ou SHA256 .
Período (s) de validade	Por quanto tempo o URL assinado permanece efetivo. O valor varia de 0s a 31.536.000s.

Calculadora de assinatura de URL

Usando a calculadora de assinatura de URL, você pode gerar um URL assinado para os usuários. Defina parâmetros de acordo com [Tabela 2-14](#) e clique em **Generate** para gerar um URL assinado que expirará em um momento específico.

Figura 2-11 Calculadora de assinatura de URL

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://www.com/e2d6fa501a9544a9f00bb5334e4a25eb/61ad86b3/test>

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

NOTA

Escape caracteres especiais no URL assinado, se houver.

Tabela 2-14 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos. O valor deve ser o mesmo que a chave de assinatura especificada na configuração de assinatura de URL.
Caminho de acesso	Caminho do conteúdo, que começa com uma barra (/) e não carrega uma cadeia de consulta.
Algoritmo de criptografia	MD5 ou SHA256 .
Hora de início	Hora em que o URL assinado entrará em vigor.
Período (s) de validade	Por quanto tempo o URL assinado permanece efetivo. O valor varia de 0s a 31.536.000s. Se esse valor for maior que o período de validade definido na configuração de assinatura de URL, o último será usado. Exemplo: Se você definir esse parâmetro para 2000s, mas o período de validade definido na configuração de assinatura de URL for 1800s, o período de validade dos URLs assinados será 1800s.

Exemplo

O seguinte utiliza o algoritmo MD5 como exemplo:

1. Suponha que o URL de retorno à origem seja o seguinte:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Defina **PrivateKey** para **huaweicloud123**.
3. A autenticação entra em vigor a partir das 10:00:00 do dia 30 de junho de 2017. **Timestamp** é **5955b0a0**. Defina o período de validade para 1800s.
4. O nó CDN constrói uma string para calcular **md5hash**.
`huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0`
5. O nó CDN calcula **md5hash** de acordo com a string de caracteres assinada.
`md5hash = md5sum(huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0) = aecf1b07f481bbb8122eef5cd52a4bc1`
6. A URL da solicitação é:
`http://hwcdn.example.com/aecf1b07f481bbb8122eef5cd52a4bc1/5955b0a0/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`

Se o pedido estiver dentro do prazo de validade (das 10:00:00 do dia 30 de junho de 2017 para as 10:30:00 do dia 30 de junho de 2017) e o **md5hash** calculado é o mesmo que o valor **md5hash** (aecf1b07f481bbb8122eef5cd52a4bc1) realizado no pedido, a autenticação é bem sucedida.

2.6.5.4 Método de assinatura C2

Por padrão, os recursos públicos são distribuídos por CDN. A assinatura de URL protege esses recursos de serem baixados e roubados por usuários mal-intencionados. A CDN da Huawei Cloud fornece quatro métodos de assinatura de URL. Este tópico descreve o método de assinatura C2.

 **NOTA**

- Se o nome de domínio tiver configurações especiais, a assinatura de URL não poderá ser configurada para esse nome de domínio no console da CDN.
- Quando a assinatura de URL é configurada, as solicitações do usuário incluem parâmetros de autenticação. Se **Ignore specific parameters** não estiver configurado:
 - A recuperação de conteúdo se tornará frequente.
 - Se o servidor de origem for um bucket do OBS, serão cobradas taxas para o tráfego de saída do bucket.

Como funciona

Um exemplo de URL assinado se parece com:

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

A tabela a seguir descreve os parâmetros em um URL assinado.

Tabela 2-15 Descrição do parâmetro

Parâmetro	Descrição
DomainName	Nome de domínio de aceleração.
timestamp	Hora em que o servidor de autenticação gera uma URL assinada, ou seja, a hora de início da autenticação. O valor é o número total de segundos decorridos desde 00:00:00 de 01 de janeiro de 1970. É um número inteiro decimal ou hexadecimal.
Período de validade	Quanto tempo um URL assinado permanece eficaz. O valor varia de 0s a 31.536.000s. Exemplo: se o período de validade for definido como 1800s, os usuários poderão acessar a CDN dentro de 1800s desde o horário indicado pelo timestamp . A autenticação falha e a URL fica inacessível se os usuários acessarem o CDN 1800s mais tarde.
md5hash	Uma seqüência de 32 caracteres calculada usando o algoritmo MD5. A cadeia consiste em dígitos (0 a 9) e letras minúsculas.
sha256	Uma seqüência de 32 caracteres calculada usando o algoritmo SHA256. A string consiste em dígitos e letras minúsculas.
Filename	URL de volta à origem. Seu valor deve começar com uma barra (/) e não inclui os parâmetros após o ponto de interrogação (?).
PrivateKey	Chave de assinatura, que é usada para gerar um URL assinado, por exemplo, huaweicloud123. A chave contém de 6 a 32 caracteres e pode conter apenas letras e dígitos.
Parâmetro de autenticação	Parâmetro de autenticação transportado em um URL. O valor padrão é auth_key .
Timestamp	Nome do parâmetro Timestamp transportado no URL da solicitação.

Método de verificação

Depois de receber uma solicitação, um nó CDN verifica a solicitação da seguinte maneira:

1. Verifica se os parâmetros de autenticação estão incluídos na solicitação. Caso contrário, a solicitação é considerada inválida e um código de erro HTTP 403 é retornado.
2. Verifica se a hora do sistema atual está dentro do intervalo [timestamp, timestamp+valid period]. Se a hora atual do sistema exceder o intervalo, o nó CDN considerará que a solicitação expira e retornará um código de erro HTTP 403. Se a hora atual do sistema estiver dentro do intervalo, o próximo passo prossegue.
3. Constrói uma cadeia de caracteres, calcula **HashValue** com a cadeia usando o algoritmo MD5 e SHA256 e compara **HashValue** com o valor **md5hash** ou **sha256** na solicitação. Se o valor **md5hash** ou **sha256** for o mesmo que **HashValue**, a autenticação será bem-sucedida e um arquivo será retornado. Caso contrário, a autenticação falhará e um código de erro HTTP 403 será retornado. **HashValue** é calculado da seguinte forma:

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

Ou

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

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Access Control** e clique em **Sign URL**.

Figura 2-12 Os URLs de assinatura

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=aecf1b07f481bbb8122eef5cd52a4bc1×tamp=5955b0a0` [Learn more](#)

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

Encryption Algorithm MD5 SHA256

Time Format Decimal Hexadecimal

Validity Period (s)

OK Cancel

- Defina os parâmetros de acordo com a tabela a seguir e clique em **OK**.

Tabela 2-16 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos.
Formato da hora	Formato da hora no URL assinado.
Algoritmo de criptografia	MD5 ou SHA256 .
Período (s) de validade	Por quanto tempo o URL assinado permanece efetivo. O valor varia de 0s a 31.536.000s.

Calculadora de assinatura de URL

Usando a calculadora de assinatura de URL, você pode gerar um URL assinado para os usuários. Defina parâmetros de acordo com **Método de assinatura C2** e clique em **Generate** para gerar um URL assinado que expirará em um momento específico.

Figura 2-13 Calculadora de assinatura de URL

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...:t?auth_key=4c80143fc4da3076c56d77f8427b3883×tamp=1638762163`

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

 **NOTA**

Escape caracteres especiais no URL assinado, se houver.

Tabela 2-17 Descrição do parâmetro

Parâmetro	Descrição
Chave de assinatura	Senha de autenticação. Digite de 6 a 32 caracteres. Apenas letras e dígitos são permitidos. O valor deve ser o mesmo que a chave de assinatura especificada na configuração de assinatura de URL.
Caminho de acesso	Caminho do conteúdo, que começa com uma barra (/) e não carrega uma string de consulta.
Algoritmo de criptografia	MD5 ou SHA256 .
Hora de início	Hora em que o URL assinado entrará em vigor.
Formato da hora	Formato da hora no URL assinado. Formato de hora do URL assinado, que deve ser o mesmo especificado na configuração de assinatura de URL.
Período (s) de validade	Por quanto tempo o URL assinado permanece efetivo. O valor varia de 0s a 31.536.000s. Se esse valor for maior que o período de validade definido na configuração de assinatura de URL, o último será usado. Exemplo: se você definir esse parâmetro para 2000s, mas o período de validade definido na configuração de assinatura de URL for 1800s, o período de validade dos URLs assinados será 1800s.

Exemplo

O seguinte utiliza o algoritmo MD5 como exemplo:

1. suponha que o URL de retorno à origem seja o seguinte:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3`
2. Defina **PrivateKey** para **huaweicloud123**.
3. A autenticação entra em vigor a partir das 10:00:00 do dia 30 de junho de 2017. **Timestamp** é **5955b0a0**. Defina o período de validade para 1800s.
4. O nó CDN constrói uma string para calcular **md5hash**.
`huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0`
5. O nó CDN calcula **md5hash** de acordo com a string de caracteres assinada.
`md5hash = md5sum(huaweicloud123/T128_2_1_0_sdk/0210/M00/82/3E/test.mp35955b0a0) = aecf1b07f481bbb8122eef5cd52a4bc1`
6. A URL da solicitação é:
`http://hwcdn.example.com/T128_2_1_0_sdk/0210/M00/82/3E/test.mp3?auth_key=aecf1b07f481bbb8122eef5cd52a4bc1×tamp=5955b0a0`

Se o pedido estiver dentro do prazo de validade (das 10:00:00 do dia 30 de junho de 2017 para as 10:30:00 do dia 30 de junho de 2017) e o **md5hash** calculado é o mesmo que o valor **md5hash** (aecf1b07f481bbb8122eef5cd52a4bc1) realizado no pedido, a autenticação é bem sucedida.

2.6.6 Configuração de autenticação remota

A CDN da Huawei Cloud suporta autenticação remota. Quando um usuário solicita um recurso de um nó CDN, a CDN encaminha a solicitação do usuário para um servidor de autenticação específico e determina se o recurso deve ser devolvido ao usuário com base no resultado retornado pelo servidor de autenticação.

Conhecimento de fundo

A autenticação remota é semelhante à assinatura de URL. As diferenças são as seguintes:

- Assinatura de URL: a autenticação é realizada por nós CDN.
- Autenticação remota: os nós CDN encaminham solicitações de usuários para um servidor de autenticação específico para autenticação.

O processo de autenticação remota é o seguinte.

Figura 2-14 Processo de autenticação remota

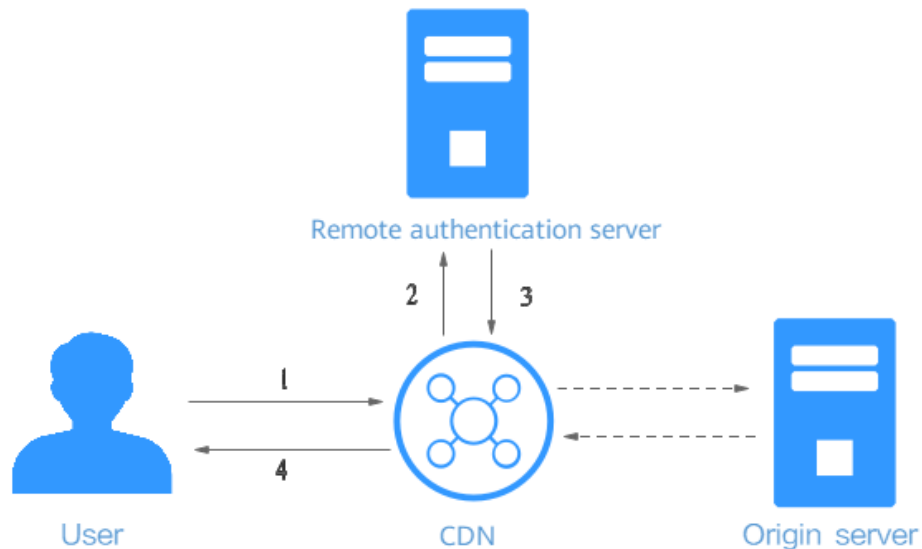


Tabela 2-18 Descrição do processo

Etapa	Descrição
1	Um usuário carrega parâmetros de autenticação para acessar um nó CDN.
2	O CDN encaminha a solicitação para um servidor de autenticação remoto.
3	O servidor de autenticação remoto verifica a solicitação e retorna um código de status para o nó CDN.
4	O nó CDN determina se o recurso solicitado deve ser devolvido ao utilizador com base no código de estado recebido.

Restrições

Nomes de domínio com configurações especiais não suportam autenticação remota.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na aba do **Access Control** e clique em **Remote Authentication**.

Figura 2-15 Configurando a autenticação 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

Tabela 2-19 Parâmetros

Parâmetro	Descrição	Exemplo
Endereço do servidor de autenticação	Endereço IP de um servidor alcançável. <ul style="list-style-type: none"> ● O endereço deve incluir http:// ou https://. ● O endereço não pode ser um endereço local, como localhost ou 127.0.0.1. ● O endereço não pode ser um nome de domínio de aceleração adicionado na CDN. 	https://example.com/auth
Método de solicitação	Método de solicitação suportado pelo servidor de autenticação. GET, POST e HEAD são suportados.	GET
Tipo de arquivo	<ul style="list-style-type: none"> ● Todos: as solicitações para todos os arquivos são autenticadas. ● Específico: solicitações de arquivos de tipos específicos são autenticadas. Exemplo: jpg MP4 ● Os tipos de arquivo não diferenciam maiúsculas de minúsculas. Por exemplo, jpg e JPG indicam o mesmo tipo de arquivo. Separe os tipos de arquivo por barras verticais (). 	Tudo
Parâmetros a reter	Parâmetros que precisam ser autenticados nas solicitações do usuário. Você pode reter ou ignorar todos os parâmetros de URL ou reter parâmetros de URL específicos. <ul style="list-style-type: none"> ● Os parâmetros são insensíveis a maiúsculas e minúsculas. Use barras verticais () para separá-los. 	Tudo
Parâmetros de assinatura de URL personalizados	Parâmetros a serem adicionados quando os nós CDN encaminham solicitações de usuário para o servidor de autenticação remoto. Você pode selecionar parâmetros predefinidos ou personalizar parâmetros (parâmetros e valores não diferenciam maiúsculas de minúsculas).	Selecionar http_host . Valor: \$http_host .

Parâmetro	Descrição	Exemplo
Solicitar cabeçalhos para reter	Cabeçalhos a serem autenticados nas solicitações do usuário. Você pode reter ou ignorar todos os cabeçalhos de solicitação ou reter cabeçalhos de solicitação específicos. Os cabeçalhos são insensíveis a maiúsculas e minúsculas. Use barras verticais () para separá-los.	Tudo
Parâmetros de autenticação de cabeçalho de solicitação personalizada	Solicitar cabeçalhos a serem adicionados quando os nós CDN encaminham solicitações de usuário para o servidor de autenticação remoto. Você pode selecionar cabeçalhos de solicitação predefinidos ou personalizar cabeçalhos de solicitação (cabeçalhos e valores não diferenciam maiúsculas de minúsculas).	Selecionar http_referer . Valor: \$http_referer .
Código do estado de sucesso	Código de status retornado pelo servidor de autenticação remoto aos nós CDN quando a autenticação é bem-sucedida. ● Intervalo de valores: 2xx e 3xx.	200
Código de status de falha	Código de status retornado pelo servidor de autenticação remoto aos nós CDN quando a autenticação falha. ● Intervalo de valores: 4xx e 5xx.	403
Código de status de resposta personalizada	Código de status retornado pelos nós CDN aos usuários quando a autenticação falha. ● Faixa de valor: 2xx, 3xx, 4xx, e 5xx.	403
Intervalo de tempo limite	Duração desde o momento em que um nó CDN encaminha uma solicitação de autenticação até o momento em que o nó CDN recebe o resultado retornado pelo servidor de autenticação remoto. Insira 0 ou um valor entre 50 e 3000. A unidade é milissegundo.	60

Parâmetro	Descrição	Exemplo
Ação após o tempo limite	<p>Como os nós CDN processam uma solicitação de usuário após o tempo limite de autenticação.</p> <ul style="list-style-type: none"> ● Aceitar: a solicitação do usuário será aceita e o recurso solicitado será devolvido. ● Rejeitar: a solicitação do usuário será rejeitada e o código de status de resposta personalizado configurado será retornado. 	Rejeitar

5. Configure os parâmetros conforme solicitado e clique em **OK**.

2.7 Configurações avançadas

2.7.1 Configurações de cabeçalho HTTP (solicitações de origem cruzada)

Cabeçalhos HTTP são parte de uma solicitação HTTP ou mensagem de resposta que definem os parâmetros operacionais de uma transação HTTP.

O compartilhamento de recursos de origem cruzada (CORS) é um mecanismo que permite o acesso de origem cruzada. Quando o site A acessa recursos no site B, uma solicitação de origem cruzada é enviada. Se o site B não permitir que o site A acesse os recursos, ocorrerá um problema entre domínios. Nesse caso, você pode configurar as configurações do cabeçalho HTTP e adicionar cabeçalhos personalizados nas mensagens de resposta retornadas ao solicitante para implementar funções como CORS.

Precauções

A configuração do cabeçalho HTTP é específica do nome de domínio. Quando uma nova configuração entra em vigor, as mensagens de resposta serão adicionadas aos cabeçalhos usados para quaisquer recursos dentro de todo o domínio. No entanto, a configuração de cabeçalho HTTP afeta apenas o comportamento de resposta dos clientes (navegadores). Eles não afetam o comportamento do cache de nós CDN.

Cabeçalhos de resposta suportados

A CDN da Huawei Cloud permite que você personalize os seguintes cabeçalhos de resposta HTTP diferentes:

- **Content-Disposition**

O cabeçalho Content-Disposition pode iniciar um download no lado do cliente e especificar o nome do arquivo a ser baixado.

Quando um servidor envia um arquivo para um navegador, desde que o formato do arquivo seja suportado (por exemplo, TXT ou JPG), o arquivo é aberto usando o navegador por padrão. Se o arquivo precisar ser tratado como um anexo e salvo com um

nome de arquivo específico, você poderá usar o campo de cabeçalho Content-Disposition para especificar esse requisito.

 **NOTA**

Se você usar um bucket do OBS criado após 1o de janeiro de 2022 como o servidor de origem e quiser ativar a visualização on-line, defina Content-Disposition como inline. Para obter detalhes, consulte [Como faço para visualizar objetos no OBS através de um navegador?](#)

- **Content-Language**

O cabeçalho Content-Language especifica o idioma preferido ou a combinação de idiomas do navegador. O conteúdo pode ser personalizado para diferentes usuários.

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

O cabeçalho Access-Control-Allow-Origin carrega os nomes de domínio permitidos para o CORS após a autenticação do servidor. Para uma simples solicitação CORS, o navegador determina se o conteúdo do recurso solicitado deve ser retornado ao cliente com base nesse cabeçalho de mensagem. Para uma solicitação de pré-verificação, o navegador determina se deve iniciar uma solicitação CORS real para o servidor com base nesse cabeçalho da mensagem.

 **NOTA**

Para evitar erros entre domínios causados pelo cache do navegador, limpe o cache do navegador depois de configurar o Access-Control-Allow-Origin.

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

O cabeçalho Access-Control-Allow-Methods carrega os métodos que são permitidos para o acesso CORS após a autenticação do servidor. Para uma simples solicitação CORS, o navegador determina se o conteúdo do recurso solicitado deve ser retornado ao cliente com base nesse cabeçalho de mensagem. Para uma solicitação de pré-verificação, o navegador determina se deve iniciar uma solicitação CORS real para o servidor com base nesse cabeçalho da mensagem.

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

O cabeçalho Access-Control-Max-Age determina por quanto tempo os resultados de pré-verificação para solicitações CORS permitidas pelo servidor podem ser armazenados em cache. O navegador determina a idade máxima do cache para os resultados da solicitação de pré-verificação com base nesse cabeçalho da mensagem. Desde que o período definido por esse cabeçalho não tenha expirado, o navegador pode determinar se deve iniciar uma solicitação CORS ao servidor com base nos resultados. Uma vez que esse período expira, o navegador precisa enviar outra solicitação de pré-verificação para o servidor.

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

Access-Control-Expose-Headers especifica os cabeçalhos de resposta que o navegador pode expor ao cliente. Você pode usar esse campo para definir os cabeçalhos de resposta visíveis para o cliente. Os seguintes cabeçalhos de resposta são visíveis para o cliente por padrão: Cache-Control, Content-Language, Content-Type, Expires, Last-Modified e Pragma.

- **Personalizado**

Se os cabeçalhos de resposta anteriores não puderem atender às suas necessidades, você poderá criar cabeçalhos de resposta. Um cabeçalho de resposta personalizado pode conter de 1 a 100 caracteres, começando com uma letra e consistindo em letras, dígitos e hífen (-).

Procedimento

1. Efetue login no [console de CDN](#).
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Advanced Settings**.
5. Na área **HTTP Header**, clique em **Edit**. A caixa de diálogo **Configure HTTP Header** é exibida.

6. Clique em **Add** e selecione uma operação de cabeçalho de resposta na lista suspensa.

Operação de cabeçalho de resposta	Descrição
Definir	<ul style="list-style-type: none"> ● Se o cabeçalho já existir na resposta, o valor do cabeçalho configurado substituirá o original. ● Se o cabeçalho não existir na resposta, o cabeçalho será adicionado à resposta.
Excluir	O cabeçalho será excluído da resposta.

NOTA

- Alguns cabeçalhos não podem ser definidos ou excluídos. Para mais detalhes, consulte [Restrições](#).
 - Você pode adicionar até 10 configurações de cabeçalho de resposta HTTP.
7. Defina o parâmetro e o valor do cabeçalho.

Parâmetro	Descrição	Valor de exemplo
Content-disposition	<p>Inicia um download no lado do cliente e especifica o nome do arquivo a ser baixado.</p> <p>Requisitos de valor: para uma configuração típica, veja o exemplo à direita.</p>	attachment;filename=FileName.xls

Parâmetro	Descrição	Valor de exemplo
Content-Language	<p>Especifica o idioma da página de resposta do cliente.</p> <p>Requisitos de valor: para uma configuração típica, veja o exemplo à direita.</p>	<p>zh-CN en-US</p>
Access-Control-Allow-Origin	<p>Especifica os URLs de domínio estrangeiro (origens de solicitação) que têm permissão para acessar o recurso no compartilhamento de recursos de origem cruzada (CORS).</p> <p>Requisitos de valor:</p> <ul style="list-style-type: none"> ● digite até 256 caracteres para um URL. ● Um URL deve começar com http:// ou https://. ● Se isso for definido como *, não serão os permitidos URLs após o curinga (*). 	<p>Exemplo 1: https:// www.example.com</p> <p>Exemplo 2: *</p> <p>NOTA Nomes de domínio curinga não são suportados.</p>
Access-Control-Allow-Methods	<p>Especifica os métodos de solicitação HTTP que podem ser usados em uma solicitação CORS.</p> <p>Requisitos de valor: vários métodos podem ser configurados ao mesmo tempo. Separe-os com vírgulas (,).</p>	<p>GET, POST, HEAD</p>
Access-Control-Max-Age	<p>Especifica por quanto tempo armazenar em cache os resultados de pré-verificação de solicitações CORS em recursos específicos.</p> <p>Requisitos de valor: este valor é expresso em segundos. O intervalo de valores é 1-1000000000.</p>	<p>86400</p>
Access-Control-Expose-Headers	<p>Especifica as informações do cabeçalho de resposta visíveis para o cliente de uma solicitação CORS.</p> <p>Requisitos de valor: vários cabeçalhos podem ser configurados ao mesmo tempo. Separe-os com vírgulas (,).</p>	<p>Content-Length, Content-Encoding</p>

Parâmetro	Descrição	Valor de exemplo
Personalizado	Especifica o cabeçalho de resposta personalizado para uma solicitação CORS. Requisitos de valor: digite até 256 caracteres, que podem conter letras, dígitos, espaços e caracteres especiais (. - * # ! % & + ^ - ' / ; ; = @ ?).	x-testcdn

8. Clique em **OK**.

Restrições

- Se o seu nome de domínio tiver configurações especiais, Content-Type, Cache-Control e Expires não poderão ser configurados.
- Os seguintes cabeçalhos de resposta podem ser modificados, mas não podem ser excluídos.

Content-Base	Content-Disposition
Server	Content-Language

- CDN não suporta os seguintes cabeçalhos de resposta:

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 erro personalizadas

Quando um erro é relatado durante o acesso do usuário, uma página de erro é exibida no cliente do usuário. Você pode personalizar a página de erro no console da CDN para otimizar a experiência do usuário.

Precauções

- Você pode personalizar páginas de erro para códigos de status 4xx e 5xx.
- Se a aceleração da CDN estiver ativada para as páginas de erro personalizadas, você será cobrado pela CDN.
- Páginas de erro não podem ser personalizadas para nomes de domínio com configurações especiais.

Procedimento

1. Efetue login no [console da CDN](#).
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.
4. Clique na guia **Advanced Settings**.
5. Na área **Custom Error Pages**, clique em **Add**.

Customize Error Page

★ Error Code

★ Redirect Mode 301 302


★ Destination URL

Parâmetro	Descrição	Exemplo
Código de erro	Código de erro cuja página de erro precisa ser personalizada.	404
Modo de redirecionamento	Modo de redirecionar a página de código de erro para uma nova página. As opções são 301 e 302 .	301
URL de destino	Nova página para a qual a página de código de erro é redirecionada. O valor deve começar com <code>http://</code> ou <code>https://</code> .	<code>https://example.com/error404.html</code>

6. Configure os parâmetros e clique em **OK**.

Exemplos

A imagem **abc.jpg** foi excluída do servidor de origem e o cache nos nós CDN expirou. Quando um usuário acessa <https://example.com/abc.jpg>, um código de estado 404 é retornado. Suponha que você defina as seguintes configurações no console da CDN:



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

Resultado: quando outro usuário acessa o <https://example.com/abc.jpg>, o usuário será redirecionado para <https://example.com/error404.html>.

2.7.3 Compressão inteligente

Conhecimento de fundo

Se a compactação inteligente estiver ativada, o CDN compactará automaticamente os arquivos estáticos. Isso pode economizar muita largura de banda reduzindo o tamanho do arquivo e acelerando a transferência de arquivos. A compressão inteligente inclui a compressão gzip e a compressão Brotli. O desempenho da compressão Brotli é de 15% a 25% maior do que o da compressão gzip.

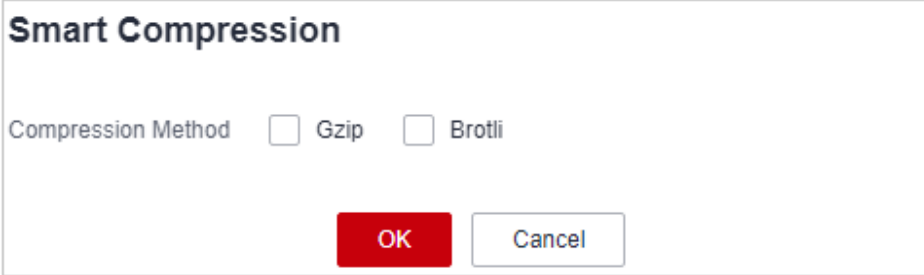
Restrições

- A compactação inteligente se aplica a arquivos JS, HTML, CSS, XML, JSON, SHTML e HTM. Ele só comprime arquivos estáticos de 256 bytes para 2 MB.
- Não habilite esta função se a verificação MD5 tiver sido configurada para o servidor de origem. Quando o CDN comprime arquivos estáticos, o valor MD5 é alterado. Como resultado, o valor MD5 do arquivo compactado é diferente do valor do arquivo no servidor de origem.
- Alguns navegadores não suportam a compressão Brotli. Verifique os navegadores suportados [neste site](#).
- Não é possível ativar a compactação inteligente para nomes de domínio com configurações especiais.
- Se a compactação gzip e Brotli estiverem ativadas, a compactação Brotli será executada preferencialmente.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Domains**.
3. Na lista de domínios, clique no nome de domínio de destino ou clique em **Configure** na coluna **Operation**.

4. Clique na guia **Advanced Settings**.
5. Clique em **Edit** ao lado de **Smart Compression**.



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

6. Selecione um método de compactação e clique em **OK**.

3 Atualização e pré-aquecimento de cache

3.1 Visão geral

O CDN pode atualizar e pré-aquecer o conteúdo.

- **Atualização de cache**

Depois de enviar uma solicitação de atualização de cache, o conteúdo em cache nos nós de CDN será forçado a expirar. Se um usuário solicitar esse conteúdo, a CDN precisará recuperar conteúdo novo do servidor de origem e, em seguida, armazenar em cache esse novo conteúdo.

- **Pré-aquecimento de cache**

Depois de enviar uma solicitação de pré-aquecimento de cache, o servidor de origem envia proativamente o conteúdo mais atual para um nó CDN para ser armazenado em cache. Se um usuário solicitar o conteúdo, o nó CDN retornará imediatamente o conteúdo em cache. Ele não precisa recuperar nenhum conteúdo novo.

Pré-requisitos

A atualização e o pré-aquecimento do cache só podem ser configurados para nomes de domínio no estado **Enabled** ou **Configuring**. Para obter mais informações sobre o status do domínio, consulte [Exibição de informações básicas do domínio](#).

3.2 Atualização de cache

Cenários típicos

Lançamento de novos conteúdos: depois que o novo conteúdo substitui o conteúdo antigo com o mesmo nome nos servidores de origem, para permitir que todos os usuários acessem o conteúdo mais recente, você pode enviar solicitações para atualizar os URLs ou diretórios correspondentes do conteúdo, forçando o conteúdo em cache nos nós a expirar.

Limpeza de conteúdo não compatível: quando o conteúdo não compatível é detectado e excluído dos servidores de origem, o conteúdo em cache nos nós ainda pode ser acessado. Você pode atualizar os URLs para excluir o conteúdo em cache.

Precauções

- Se um URL for reescrito, você deve usar o caminho de recurso real do novo URL para atualização de cache.
- Alguns recursos podem ser armazenados em cache em navegadores. Atualize o cache do navegador depois que o cache do nó for atualizado.
- Você também pode criar uma tarefa de atualização de cache para um nome de domínio chamando uma API. Para obter detalhes, consulte [Visão geral da API](#).
- Demora cerca de 5 minutos para que uma tarefa de atualização de cache entre em vigor.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console da CDN é exibido.

2. No painel de navegação, escolha **Preheating & Refresh**.
3. Clique na guia **Cache Refreshing**, selecione o tipo de atualização e insira os URLs ou diretórios a serem atualizados.

Figura 3-1 Atualização de cache

The screenshot shows the 'Cache Refreshing' interface in the Huawei Cloud console. At the top, there are tabs for 'Cache Preheating', 'Cache Refreshing' (which is selected and highlighted with a red box), 'Task Progress', and 'URL Query'. A 'Feedback' icon is in the top right corner. Below the tabs is a blue information box with a warning icon and the following text: 'Cached content on CDN nodes is not updated in real time. If content on origin servers is updated, you can submit cache refreshing requests (or call an API) to force the cached content on CDN nodes to expire. • If you select URL refreshing, submit complete URLs of the files you want to refresh. File caches will not be refreshed if you submit file directories. • If you select directory refreshing and refresh the root directory, all caches on CDN nodes will expire. CDN will need to retrieve content from the origin server for all requests and the origin server may break down due to too many requests. Exercise caution when you refresh the root directory. • If you refresh a directory, all caches of files in the directory and its subdirectories will be refreshed, and the subdirectories do not consume quotas.' Below this is a 'Type' selector with 'URL' and 'Directory' options. A note states: '* URLs You can refresh 2,000 more URLs today.' There is a large text input area with a 'Format:' label and two example URLs: 'http://www.example.com/file01.html' and 'http://www.example.com/file02.html'. A 'Submit' button is at the bottom left. At the bottom center, it says 'It will take about 5 minutes for the task to complete.'

Tabela 3-1 Descrição do parâmetro

Tipo	Descrição
<p>Atualização de URL</p> <ul style="list-style-type: none"> ● CDN atualiza um arquivo específico. 	<ul style="list-style-type: none"> ● Cada conta pode atualizar um máximo dos 2000 URLs por dia e um máximo dos 1000 URLs por tarefa. ● A parte http:// ou https:// da URL deve ser incluída. ● Insira um URL por linha. <p>Exemplos:</p> <p>http://www.example.com/file01.html</p> <p>http://www.example.com/file02.html</p> <p>https://example.huawei.com/download/app/abc.apk</p>
<p>Atualização de diretório</p>	<p>Modos de atualização:</p> <ul style="list-style-type: none"> ● Atualizar recursos atualizados: atualizar recursos que foram atualizados em um diretório (incluindo subdiretórios). ● Atualizar todos os recursos: atualizar todos os recursos em um diretório, incluindo recursos em subdiretórios. <p>Regras de configuração:</p> <ul style="list-style-type: none"> ● cada conta pode atualizar um máximo de 100 diretórios por dia de cada vez. ● Um URL deve conter http ou https e terminar com uma barra (/). ● Insira um URL por linha. <p>Exemplos:</p> <p>http://www.example01.com/folder01/</p> <p>http://www.example01.com/folder02/</p>

4. Clique em **Submit**.

Depois que uma tarefa de atualização for enviada, você poderá exibir o status da tarefa na guia **Task Progress**.

3.3 Pré-aquecimento de cache

Cenários típicos

Acesso inicial: quando você conecta um nome de domínio ao CDN pela primeira vez, pode pré-aquecer arquivos grandes, incluindo vídeos, para melhorar a experiência do usuário.

Versão do pacote de instalação: antes de lançar um pacote de instalação de software ou pacote de atualização, você pode pré-aquecer o conteúdo para os nós de CDN distribuídos globalmente. Depois que o software ou atualização é iniciado, os nós de CDN respondem diretamente às solicitações de download de um grande número de usuários, o que melhora a velocidade de download e reduz significativamente a pressão sobre o servidor de origem.

Atividade promocional: antes de lançar uma campanha promocional, você pode pré-aquecer o conteúdo estático envolvido na página de atividade para os nós da CDN. Após o início da atividade, os nós da CDN respondem às solicitações do usuário para acessar todo o conteúdo estático, o que garante a disponibilidade do serviço e melhora a experiência do usuário.

Precauções

- O tempo necessário para concluir uma tarefa de pré-aquecimento depende do número e do tamanho dos arquivos a serem pré-aquecidos e das condições da rede.
- Se o status de pré-aquecimento do cache de um URL for **Completed**, o pré-aquecimento será concluído.
- O pré-aquecimento de um grande número de arquivos pode ocupar totalmente os recursos de largura de banda do servidor de origem. Portanto, é aconselhável pré-aquecer os arquivos em lotes.
- Arquivos dinâmicos, como arquivos ASP, JSP e PHP, não podem ser pré-aquecidos.
- Você também pode criar uma tarefa de pré-aquecimento de cache para um nome de domínio chamando uma API. Para obter detalhes, consulte [Visão geral da API](#).

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console de CDN é exibido.

2. No painel de navegação, escolha **Preheating & Refresh**.
3. Clique na guia **Cache Preheating** e insira os URL a serem pré-aquecidos.

Figura 3-2 Pré-aquecimento de cache

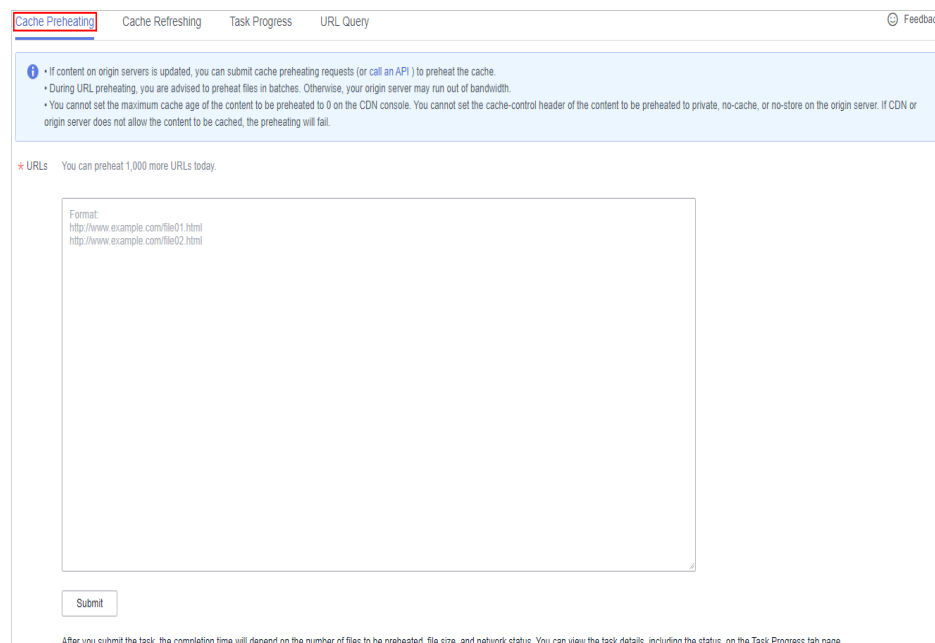


Tabela 3-2 Descrição do parâmetro

Tipo	Descrição
Pré-aquecimento do URL <ul style="list-style-type: none"> ● O CDN pré-aquece um arquivo específico. 	<ul style="list-style-type: none"> ● A parte http:// ou https:// da URL deve ser incluída. ● Insira um URL por linha. ● Cada conta pode pré-aquecer um máximo dos 1000 URLs por dia ou por tarefa. Exemplo: http://www.example.com/file01.html http://www.example.com/file02.html https://example.huawei.com/download/app/abc.apk

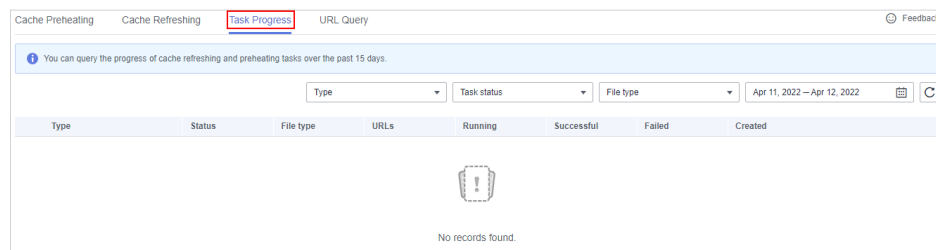
4. Clique em **Submit**.

Depois que uma tarefa de pré-aquecimento for enviada, você poderá exibir o status da tarefa na guia **Task Progress**.

3.4 Exibição de progressos de tarefa

Depois que uma tarefa de atualização ou pré-aquecimento do cache for enviada, você poderá exibir o status da tarefa na página de guia **Task Progress**.

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Preheating & Refresh**.
3. Selecione a guia **Task Progress** para verificar o status das tarefas de atualização e pré-aquecimento.



NOTA

- Na página de guia **Task Progress**, você pode exibir o status das tarefas de atualização e pré-aquecimento do cache nos últimos 15 dias.
- Você também pode consultar os registros de atualização de cache e pré-aquecimento dos últimos 15 dias na página de guia **URL Query**.

3.5 Perguntas frequentes

Quais são as diferenças entre atualização de cache e pré-aquecimento de cache?

As diferenças entre atualizar e pré-aquecer o cache são:

- **Atualização de cache**
Depois de enviar uma solicitação de atualização de cache, o conteúdo em cache nos nós CDN será forçado a expirar. Se um usuário solicitar esse conteúdo, a CDN precisará recuperar conteúdo novo do servidor de origem e, em seguida, armazenar em cache esse novo conteúdo.
- **Pré-aquecimento de cache**
Depois de enviar uma solicitação de pré-aquecimento de cache, o servidor de origem envia proativamente o conteúdo mais atual para um nó CDN para ser armazenado em cache. Se um usuário solicitar o conteúdo, o nó CDN retornará imediatamente o conteúdo em cache. Ele não precisa recuperar nenhum conteúdo novo.

Para obter detalhes, consulte [Atualização de cache e pré-aquecimento](#).

Existe uma sequência entre a atualização e o pré-aquecimento do cache do CDN?

Se você quiser atualizar o conteúdo em cache nos nós da CDN após a atualização do conteúdo de origem, preste atenção ao seguinte:

- Você deve atualizar o cache primeiro. Demora cerca de 5 minutos para que uma tarefa de atualização de cache entre em vigor. Em seguida, execute a tarefa de pré-aquecimento do cache.
- Se você ignorar a atualização do cache e executar diretamente o pré-aquecimento do cache, o conteúdo armazenado em cache nos nós CDN não será atualizado.
- Se você acessar a CDN pela primeira vez e nenhum conteúdo for armazenado em cache nos nós da CDN, poderá executar diretamente o pré-aquecimento do cache para armazenar em cache o conteúdo nos nós da CDN.

A atualização do cache atualiza o conteúdo armazenado em cache em todos os nós?

Sim.

Por que uma determinada tarefa de pré-aquecimento está sendo processada por tanto tempo?

As possíveis causas incluem:

- A tarefa de pré-aquecimento foi enviada durante um horário de pico, portanto, ainda está na fila.
- Você está pré-aquecendo um grande número de arquivos. O pré-aquecimento recuperará o conteúdo do servidor de origem, portanto, o pré-aquecimento de um grande número de arquivos pode consumir toda a largura de banda disponível para o servidor de origem. Você é aconselhado a:
 - Divida as tarefas de pré-aquecimento em lotes.
 - Pré-aqueça os arquivos durante as horas de pico, por exemplo, à noite.
 - Aumente a largura de banda do servidor de origem.
- A tarefa de pré-aquecimento foi concluída, mas o status não é atualizado no console. Atualize a página do console e verifique novamente.

Como fazer para atualizar o cache da CDN onde o nome de domínio inclui um curinga?

Ao atualizar o cache de um nome de domínio que inclua um curinga, insira as URLs ou diretórios dos nomes de domínio de nível 2 a serem atualizados. Não insira uma URL que contenha um curinga, como **https://*.example.com/file01.html** ou **https://*.example.com/file02/**.

Exemplo:

- Um nome de domínio de aceleração é ***.example.com**.
- O nome de domínio de nível 2 que abriga o conteúdo a ser atualizado é **abc.example.com**.
 - Insira o URL a ser atualizado: **https://abc.example.com/file01.html**.
 - Informe o diretório a ser atualizado: **https://abc.example.com/file02/**.

Por que é que mesmo depois que eu pré-aqueci ou atualizei o cache, o conteúdo não foi atualizado?

É possível que o intervalo entre a atualização do cache e o pré-aquecimento seja muito curto. Como resultado, a atualização falha. Se um cache acaba de ser atualizado ou pré-aquecido, é recomendável que você aguarde pelo menos 5 minutos antes de repetir essa ação.

O que posso fazer se uma operação de pré-aquecimento de cache falhar?

É possível que:

- Um grande número de arquivos está sendo pré-aquecido ao mesmo tempo, e essa operação ocupou toda a largura de banda do servidor de origem. Neste caso, é aconselhável realizar operações de pré-aquecimento em lotes. Você também pode aumentar a largura de banda do servidor de origem para melhorar a eficiência do pré-aquecimento.
- A idade máxima do cache do conteúdo solicitado é 0. Nesse caso, altere a configuração de idade máxima do cache.
- **Cache-Control** é **private**, **no-cache** ou **no-store**. Se **Cache-Control** não estiver configurado, o valor padrão **private** será usado.
- Você solicitou o pré-aquecimento de diretórios, conteúdo dinâmico ou as URLs cuja idade máxima do cache é definida como 0.

O CDN suporta o pré-aquecimento do diretório?

Não. Apenas as URLs completas podem ser pré-aquecidas. O pré-aquecimento de diretórios não é suportado. Para obter detalhes, consulte [Atualização de cache e pré-aquecimento](#).

Preciso pré-aquecer/atualizar os URL de HTTP e de HTTPS separadamente?

Não. Você só precisa pré-aquecer/atualizar as URLs de HTTP ou de HTTPS.

Se o CDN estiver habilitado dentro e fora do continente chinês, ele precisa ser diferenciado ao atualizar e pré-aquecer?

Não. Você pode atualizar ou pré-aquecer diretamente as URLs correspondentes.

Posso pré-aquecer arquivos M3U8?

Sim.

Por que o sistema relata um erro indicando que não tenho permissão para atualizar o cache?

É possível que seu nome de domínio de aceleração tenha sido desativado. Ative o CDN para o nome de domínio novamente. Se a sua conta estiver em atraso, a CDN pode ter sido desativada para o seu nome de domínio de aceleração. Certifique-se de que o saldo da sua conta é suficiente.

O cache pode ser atualizado automaticamente depois que um arquivo estático no servidor de origem é atualizado?

Não. No entanto, você pode chamar as API para forçar o conteúdo atual a expirar e, em seguida, pré-aquecer o novo conteúdo. Para obter detalhes, consulte [Visão geral da API](#).

Por que o pré-aquecimento do diretório não é suportado e como a CDN solicita conteúdo do servidor de origem?

Você pode considerar a CDN como um usuário, que baixa o conteúdo do servidor de origem. Se a CDN oferecer suporte ao pré-aquecimento do diretório, o servidor de origem não saberá quais arquivos no diretório serão baixados quando o CDN enviar uma solicitação de acesso ao diretório ao servidor de origem. Se você solicitar um arquivo, o servidor de origem saberá exatamente o que é.

A atualização e o pré-aquecimento da CDN são obrigatórios?

Isso depende.

- Se um arquivo for atualizado em um servidor de origem, o arquivo também precisará ser atualizado em nós CDN.
- Recomenda-se que arquivos grandes, especialmente arquivos de vídeo, sejam pré-aquecidos para melhorar a experiência do usuário.
- O pré-aquecimento não é recomendado para arquivos pequenos.

Atualmente, a CDN não suporta atualização e pré-aquecimento automáticos. Você precisa executar manualmente essas operações.

4 Análise de estatísticas

4.1 Descrição de estatística

Tabela 4-1 exibe relatórios de análise estatística fornecidos pela CDN. Você pode aprender:

Tabela 4-1 Descrição das estatísticas

Indicador	Descrição
Estatísticas de utilização	Você pode consultar as estatísticas de utilização de tráfego/largura de banda e a taxa de acertos de tráfego para todos os seus nomes de domínio e exportar as estatísticas.
Estatísticas de acesso	Você pode consultar o total de solicitações, a taxa de acertos do cache e as consultas por segundo para todos os seus nomes de domínio, e exportar as estatísticas.
Estatísticas do servidor de origem	Você pode consultar o tráfego de recuperação, a largura de banda de recuperação e a taxa de falha de recuperação para todos os seus nomes de domínio, e exportar as estatísticas.
Hotspots	Você pode consultar os 100 principais URLs com base no uso de tráfego ou no total de solicitações para todos os nomes de domínio e exportar os detalhes desses 100 principais URLs.
Estatísticas de região & de operadora	Você pode consultar o uso de tráfego/largura de banda e o total de solicitações para todos os nomes de domínio por região ou operadora, e exportar estatísticas por região ou operadora.
Códigos de estado	Você pode consultar os códigos de status das solicitações para todos os nomes de domínio, e exportar os detalhes desses códigos de status.
Estatísticas de utilização para aceleração de todo o site	Você pode consultar o tráfego ou a largura de banda consumida por nomes de domínio cujo tipo de serviço é a aceleração de todo o site.

NOTA

- O CDN permite que você consulte estatísticas sobre nomes de domínio excluídos.
- Se tiver ativado a função de projecto empresarial, as estatísticas dos nomes de domínio eliminados não poderão ser consultadas.
- No console da CDN, há um atraso de cerca de 1 hora para dados nas páginas **Statistics Analysis** e **Dashboard**.

Você também pode consultar as seguintes informações na página **Dashboard**:

- Tráfego, largura de banda de pico, número de solicitações e taxa de acertos por mês
- Tráfego, largura de banda máxima, número de solicitações e taxa de acertos por dia
- Tendência de tráfego dos 5 principais nomes de domínio no dia atual
- Tendência de pico de largura de banda dos 5 principais nomes de domínio no dia atual
- Tendência de solicitação de nomes de domínio top 5
- Número total de nomes de domínio adicionados
- Quota restante em seus pacotes de tráfego

4.2 Estatísticas de utilização

Você pode consultar as estatísticas de utilização de tráfego/largura de banda e a taxa de acerto de tráfego de todos os seus nomes de domínio (excluindo aqueles excluídos se você tiver ativado a função de projeto da empresa).


- Os últimos 90 dias de dados podem ser consultados e cada consulta pode incluir até 31 dias de dados.
- Se nenhum dado estiver disponível dentro do intervalo de tempo consultado, nenhum dado será exibido nos gráficos de tendência de tráfego/largura de banda e taxa de acertos de tráfego ou na lista de utilização de tráfego/largura de banda de nome de domínio.
- A granularidade estatística mínima padrão é de 5 minutos. Se o período de consulta for de 8 dias ou mais, a granularidade estatística mínima será de 4 horas.
- Há um atraso de cerca de uma hora para os dados exibidos na página **Utilization Statistics**.
- Você pode exportar os resultados da consulta.
- A comparação de dados é suportada.

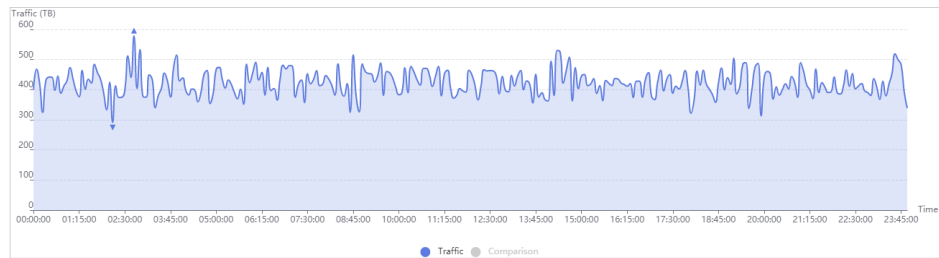
Restrições


Se a área de serviço do seu nome de domínio é global, você deve consultar as estatísticas deste nome de domínio escolhendo **Chinese mainland** e **International** respectivamente. A consulta pela área de serviço global não está disponível.

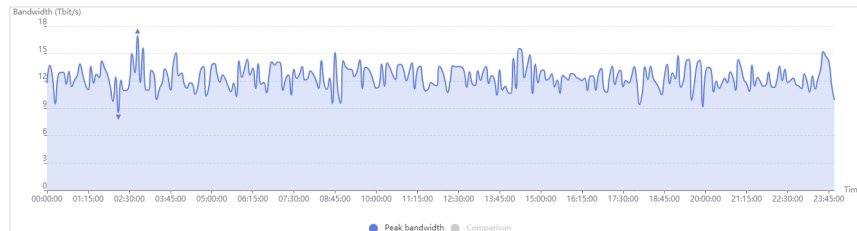
Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Statistical Analysis > Utilization Statistics**.
3. Defina critérios de pesquisa para consultar os seguintes dados:

- **Traffic:** exibe o tráfego de nomes de domínio específicos ao longo do tempo. Você pode clicar em entradas de legenda, por exemplo,  Traffic, para ocultar ou exibir as estatísticas correspondentes.



- **Peak Bandwidth:** exibe o pico de largura de banda de nomes de domínio específicos ao longo do tempo. Você pode clicar em entradas de legenda, por exemplo,  Peak bandwidth, para ocultar ou exibir as estatísticas correspondentes.



 **NOTA**

A largura de banda do percentil 95 e a largura de banda de pico média diária são mostradas para o mesmo período de tempo. Se nenhuma estatística de largura de banda for monitorada dentro do período de tempo consultado, a linha de largura de banda ou a linha de largura de banda de pico média diária não será exibida.






- **Traffic Hit Ratio:** exibe a taxa de acertos de tráfego de nomes de domínio específicos ao longo do tempo.

Traffic hit ratio = Tráfego gerado quando o cache é atingido/Tráfego total de solicitações

O tráfego total de solicitações é a soma do tráfego gerado quando o cache de nó da CDN é atingido e o tráfego gerado durante a recuperação de conteúdo.



- **Tráfego de nome de domínio/Utilização de largura de banda:** exibe o tráfego e a largura de banda de nomes de domínio específicos.

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

Você pode clicar em **Traffic**, **Traffic Hit Ratio**, ou **Peak Bandwidth** no cabeçalho da tabela para exibir as estatísticas de utilização em ordem decrescente ou crescente.

4.3 Estatísticas de acesso

Você pode consultar o número total de solicitações, a taxa de acertos de cache e as consultas por segundo de todos os seus nomes de domínio (excluindo aqueles excluídos se você tiver ativado a função de projeto empresarial).

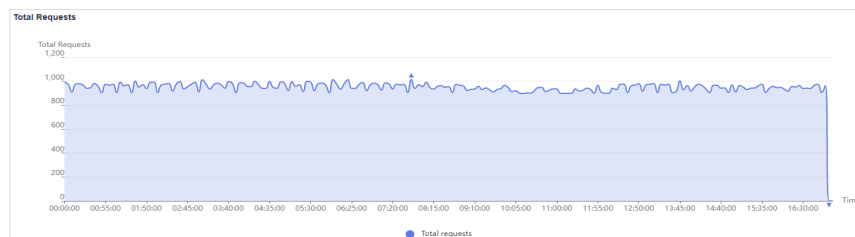
- Os últimos 90 dias de dados podem ser consultados e cada consulta pode incluir até 31 dias de dados.
- As informações de acesso são exibidas com base nas estatísticas do log. Os dados são sincronizados uma vez por hora.
- Se nenhum dado estiver disponível dentro do intervalo de tempo consultado, nenhum dado será exibido nos gráficos de tendência de solicitações totais, taxa de acertos de cache e consultas por segundo ou na lista de detalhes de acesso de nome de domínio.
- Você pode exportar os resultados da consulta.
- A granularidade estatística mínima padrão é de 5 minutos. Se o período de consulta for de 8 dias ou mais, a granularidade estatística mínima será de 4 horas.

Restrições

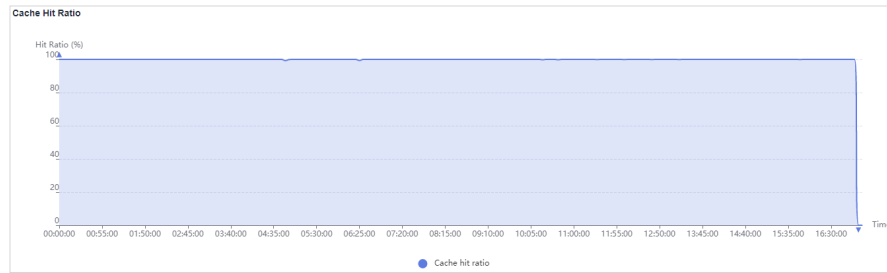
Se a área de serviço do seu nome de domínio é global, você deve consultar as estatísticas deste nome de domínio, escolhendo **Chinese mainland** e **Global (Chinese mainland not included)** respectivamente. A consulta por **Global** não está disponível.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Statistical Analysis > Access Statistics**.
3. Defina critérios de pesquisa para consultar os seguintes dados:
 - **Total Requests**: exibe o número de solicitações para nomes de domínio específicos ao longo do tempo.

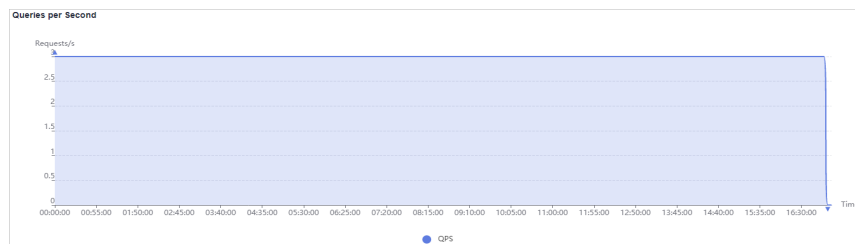


- **Cache Hit Ratio**: exibe a taxa de acertos de cache de nomes de domínio específicos ao longo do tempo.
$$\text{Cache hit ratio} = \frac{\text{Número de solicitações que atingiram o cache}}{\text{número de solicitações totais}}$$



- **Queries per Second:** exibe as consultas por segundo de nomes de domínio específicos ao longo do tempo.

Consultas por segundo é uma medida comum do número de consultas que os nomes de domínio recebem durante um segundo.



- **Acesso a nomes de domínio:** exibe o número de solicitações para nomes de domínio específicos, taxa de acerto de cache e consultas por segundo.

Você pode clicar em **Total Requests**, **Cache Hit Ratio**, ou **Queries per Second** no cabeçalho da tabela para exibir as estatísticas de acesso em ordem decrescente ou crescente.

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

4.4 Estatísticas do servidor de origem

Você pode consultar o tráfego de recuperação, a largura de banda de recuperação e a taxa de falha de recuperação de todos os seus nomes de domínio (excluindo aqueles excluídos se você tiver ativado a função de projeto da empresa).

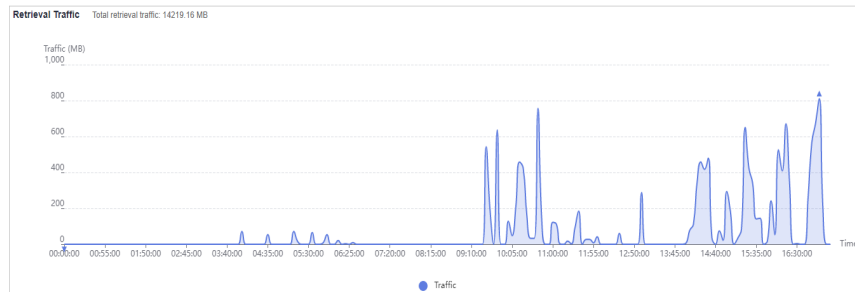
- Os últimos 90 dias de dados podem ser consultados e cada consulta pode incluir até 31 dias de dados.
- Se nenhum dado estiver disponível dentro do intervalo de tempo consultado, nenhum dado será exibido nos gráficos de tendência de taxa de falha de recuperação de tráfego/largura de banda e recuperação ou na lista de detalhes de recuperação de nome de domínio.
- A granularidade estatística mínima padrão é de 5 minutos. Se o período de consulta for de 8 dias ou mais, a granularidade estatística mínima será de 4 horas.
- Você pode exportar os resultados da consulta.

Procedimento

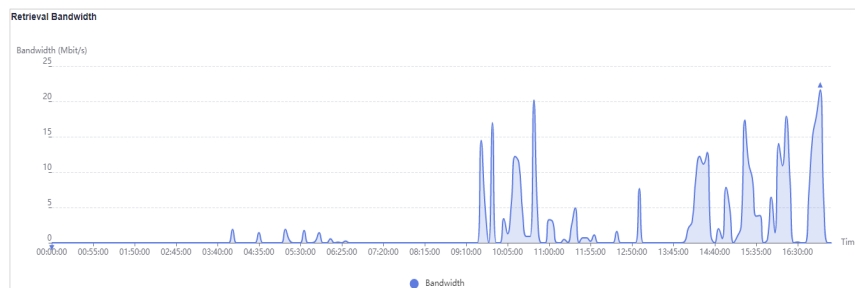
1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console da CDN é exibido.

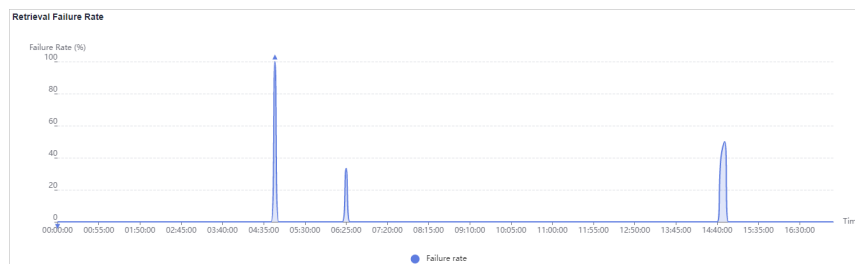
2. No painel de navegação, escolha **Statistical Analysis > Origin Server Statistics**.
3. Defina critérios de pesquisa para consultar os seguintes dados:
 - **Retrieval Traffic**: exibe o tráfego de recuperação de conteúdo de nomes de domínio específicos ao longo do tempo.



- **Retrieval Bandwidth**: exibe a largura de banda de recuperação de conteúdo de nomes de domínio específicos ao longo do tempo.



- **Retrieval Failure Rate**: exibe a taxa de falha de recuperação ao longo do tempo.
Taxa de falha de recuperação = Número de solicitações de recuperação com falha / Número de solicitações de recuperação totais



NOTA

Falhas de recuperação podem ser causadas por erros de configuração de host de recuperação, desconexão entre a CDN e o host de recuperação, incompatibilidade de HTTP e erros de host de recuperação.

- **Detalhes da recuperação de nome de domínio**: exibe o tráfego de recuperação, a largura de banda de recuperação e as taxas de falha de recuperação de nomes de domínio específicos.

Você pode clicar em **Retrieval Traffic**, **Retrieval Bandwidth**, ou **Retrieval Failure Rate** no cabeçalho da tabela para exibir as estatísticas de recuperação em ordem decrescente ou crescente.

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

4.5 Hotspots

Você pode consultar os 100 URLs que consomem mais tráfego e os 100 URLs mais solicitados.

- Os últimos 90 dias de dados podem ser consultados e cada consulta pode incluir até 31 dias de dados.
- Os 100 principais URLs são atualizadas todos os dias.
- Se nenhum dado estiver disponível dentro do intervalo de tempo consultado, nenhum dado será exibido na lista dos 100 principais URLs.
- Você pode exportar os resultados da consulta.
- Os 100 principais URLs são exibidos com base nas estatísticas de registro. O atraso de dados é de 4 a 6 horas.

Restrições

Se a área de serviço do seu nome de domínio é **Global**, você deve consultar as estatísticas deste nome de domínio, escolhendo **Chinese mainland** e **Global (Chinese mainland not included)** respectivamente. A consulta por **Global** não está disponível.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Statistical Analysis > Hotspots**.
3. Definir critérios de pesquisa.



Parameter	
Traffic	Total requests
Top 100 URLs (Traffic Usage)	
URL	Traffic
www. .site/	1.08 KB

Você pode consultar os 100 URLs que consomem mais tráfego e os 100 URLs mais solicitados. Você pode clicar em **Traffic** ou **Total Requests** nos cabeçalhos da tabela para classificar os 100 principais URLs em ordem crescente ou decrescente.

NOTA

O tráfego exibido na tabela é apenas para referência. Obtenha os dados reais de outras páginas de análise estatística.

4.6 Estatísticas de região & de operadora

Você pode consultar o uso de tráfego/largura de banda, o número de solicitações e a distribuição de visitantes de todos os nomes de domínio (excluindo aqueles excluídos se você ativou a função de projeto da empresa) por região ou transportadora.

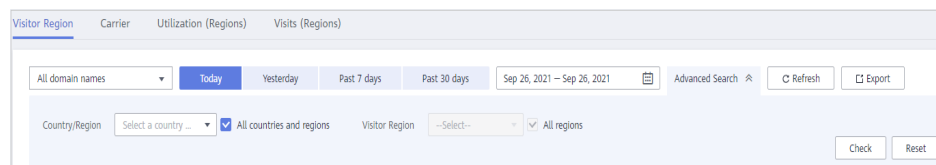
- Os últimos 90 dias de dados podem ser consultados e cada consulta pode incluir até 31 dias de dados.
- Se nenhum dado estiver disponível dentro do intervalo de tempo consultado, nenhum dado será exibido na lista de detalhes estatísticos do índice de operadoras.
- A granularidade estatística mínima é de 5 minutos.
- Você pode exportar os resultados da consulta.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console da CDN é exibido.

2. No painel de navegação, escolha **Statistical Analysis**.
3. Selecione **Region & Carrier Statistics** em **Statistical Analysis**.



4. Selecione uma guia e defina critérios de pesquisa para consultar os seguintes dados:

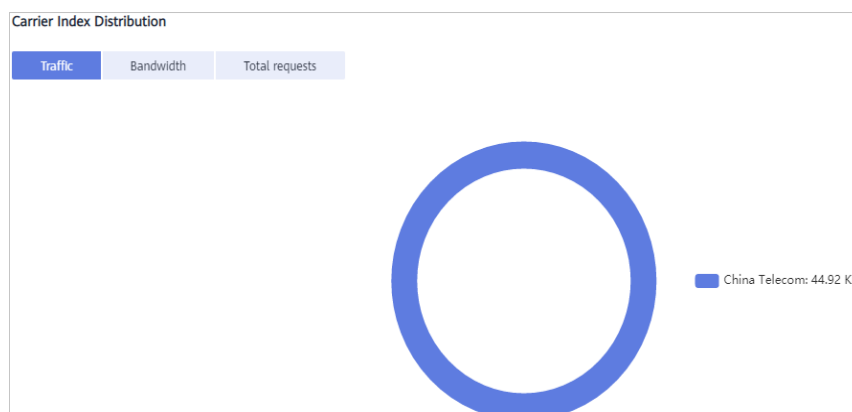
- **Região de visitantes:** exibe a região onde os visitantes estão localizados.

Se você selecionar **China** na lista suspensa **Country and Region**, poderá consultar os detalhes do visitante de 34 regiões administrativas provinciais na 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%)

- **Operadora:** inclui China Mobile, China Telecom, China Unicom China Education and Research Network (CERNET), Dr. Peng e China Mobile Tietong.

- i. **Carrier Index Distribution:** exibe a proporção que cada operadora ocupa em diferentes estatísticas de índice.

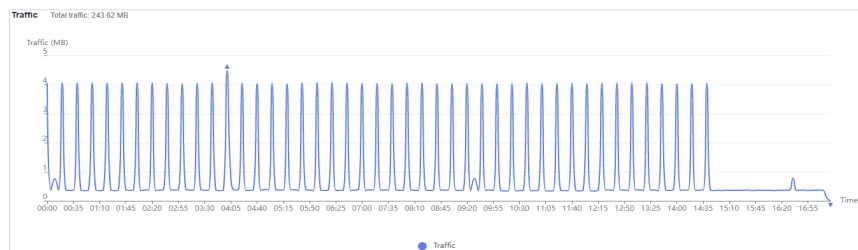


- ii. **Carrier Index Statistical Details:** exibe o tráfego, a largura de banda de pico e o número de solicitações por operadora. Você pode clicar em **Traffic**, **Peak Bandwidth** ou **Total Requests** no cabeçalho da tabela de **Carrier Index Statistical Details** para ver os dados em ordem crescente ou decrescente.

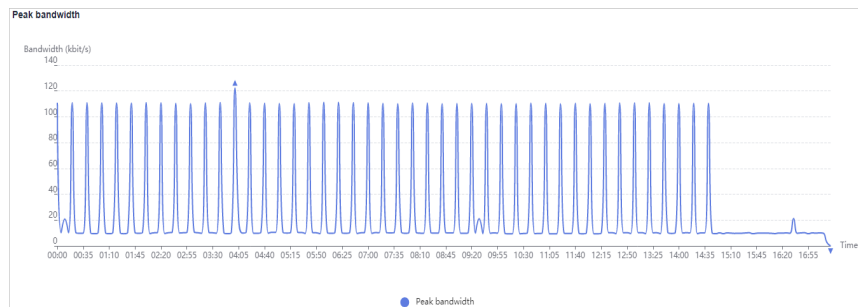
Carrier	Traffic (Percentage)	Peak Bandwidth (Percentage)	Total Requests (Percentage)
Other	110.64 MB (93.75%)	85.04 kbit/s (98.35%)	228 (1.19%)
China Mobile	7.03 MB (5.96%)	1.26 kbit/s (1.46%)	18,035 (94.12%)
China Mobile Tietong	349.32 KB (0.29%)	0.07 kbit/s (0.08%)	893 (4.66%)
China Telecom	5.07 KB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

– **Utilização (Regiões)**

- i. **Traffic:** exibe o tráfego de nomes de domínio específicos por país/região ou operadoras.



- ii. **Peak bandwidth:** exibe o pico de largura de banda de nomes de domínio específicos por país/região ou operadoras.

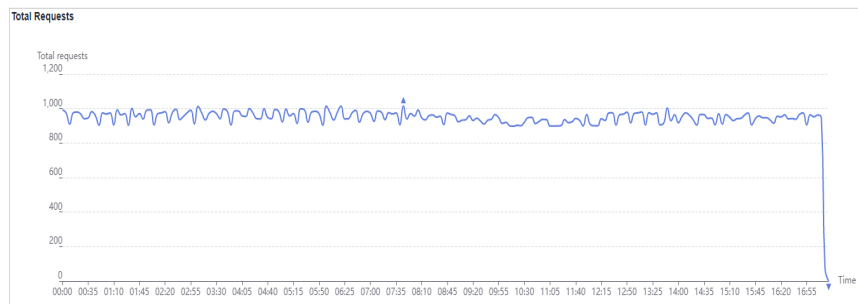


- iii. **Tráfego de nome de domínio/Utilização de largura de banda:** exibe o tráfego e a largura de banda de nomes de domínio específicos.

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

– **Visitas (Regiões)**

- i. **Total Requests:** exibe o número de solicitações para nomes de domínio específicos em um país/região específico.



- ii. **Acesso a nomes de domínio:** exibe detalhes de acesso de nomes de domínio específicos em um país/região específico.

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

4.7 Códigos de estado

Você pode consultar códigos de status retornados para solicitações para todos os nomes de domínio (excluindo aqueles excluídos se você tiver ativado a função de projeto da empresa).

- Os últimos 90 dias de dados podem ser consultados e cada consulta pode incluir até 31 dias de dados.
- Se nenhum dado estiver disponível dentro do intervalo de tempo consultado, nenhum dado será exibido na lista de códigos de status.
- A granularidade estatística mínima padrão é de 5 minutos. Se o período de consulta for de 8 dias ou mais, a granularidade estatística mínima será de 4 horas.
- Você pode exportar os resultados da consulta para um computador local.

Restrições

Se a área de serviço do seu nome de domínio é **Global**, você deve consultar as estatísticas deste nome de domínio, escolhendo **Chinese mainland** e **Global (Chinese mainland not included)** respectivamente. A consulta por **Global** não está disponível.

Procedimento

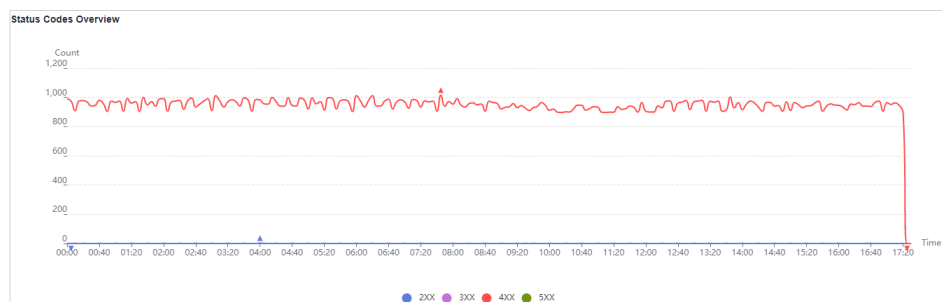
1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.

O console da CDN é exibido.

2. No painel de navegação, escolha **Statistical Analysis > Status Codes**.

3. Defina critérios de pesquisa para consultar os seguintes dados:

- **Status Codes Overview**: exibe o número de cada código de status ao longo do tempo.



Você pode clicar em entradas de legenda, por exemplo, **2XX**, para ocultar ou exibir as estatísticas de códigos específicos. As estatísticas são coletadas em códigos de status, incluindo **2XX**, **3XX**, **4XX**, e **5XX**.

Código de estado	Descrição
2XX	Códigos de resposta bem-sucedidos. Estes indicam que uma solicitação foi aceita e processada pelo servidor.

Código de estado	Descrição
3XX	Redirecionamento de mensagens. Estes indicam que o cliente precisa para executar mais operações para completar o pedido.
4XX	Códigos de resposta de erro do cliente. Estes indicam que houve um erro no lado do cliente, incluindo, mas não limitado a erros de sintaxe ou falha para completar o pedido.
5XX	Códigos de resposta de erro do servidor. Estes indicam que houve um erro quando o servidor estava processando a solicitação.

- **Status Code Statistics:** exibe o número e a proporção de diferentes códigos de status para nomes de domínio específicos.

Você pode clicar em **Count** ou **Percentage** no cabeçalho da tabela da lista de detalhes das estatísticas para exibir os dados correspondentes em ordem crescente ou decrescente.

Sum	Details	
Status Code	Count <input type="checkbox"/>	Percentage <input type="checkbox"/>
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 %

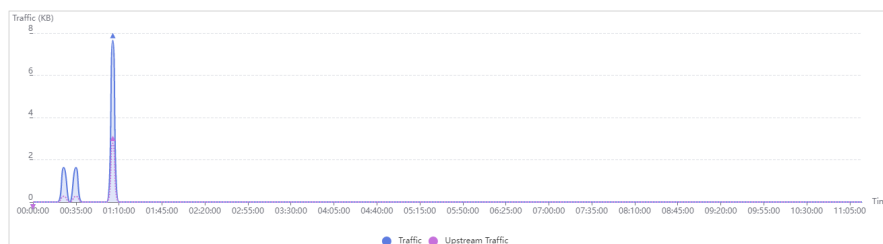
4.8 Estatísticas de utilização para aceleração de todo o site

Você pode consultar estatísticas de utilização de todos os nomes de domínio cujo tipo de serviço é aceleração de todo o site (excluindo aqueles excluídos se você tiver ativado a função de projeto da empresa).

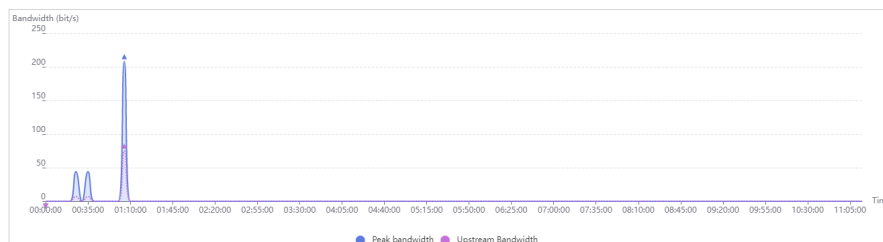
- Os últimos 90 dias de dados podem ser consultados e cada consulta pode incluir até 31 dias de dados.
- A granularidade estatística mínima padrão é de 5 minutos. Se o período de consulta for de 8 dias ou mais, a granularidade estatística mínima será de 4 horas.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Statistical Analysis > Utilization Statistics for Whole Site Acceleration**.
3. Defina critérios de pesquisa para consultar os seguintes dados:
 - **Traffic:** exibe o tráfego e o tráfego upstream usado para a aceleração do site inteiro.



- **Bandwidth:** exibe a largura de banda de pico e a largura de banda de upstream usada para a aceleração do site inteiro.



4.9 Perguntas frequentes

Por que não há dados na análise estatística?

- O registro CNAME configurado para seu nome de domínio está errado.
- As estatísticas CDN na página **Statistical Analysis** são uma hora mais tarde do que os dados em tempo real.

Se o problema não for causado por nenhum dos motivos anteriores, [enviar um tíquete de serviço](#).

O que poderia cair na categoria "Other" nas estatísticas da região de visitantes?

Other refere-se àqueles cuja região não pode ser identificada porque seus endereços IP não são registrados na biblioteca de endereços IP ou seus endereços IP não podem ser obtidos pela CDN.

Quanto tempo é o atraso da API dos 100 principais URLs nas estatísticas de hotspot CDN?

Chamar as APIs dos 100 principais URLs tem um atraso de cerca de 6 horas. A situação volta ao normal às 12h do dia seguinte.

Quais são os significados de HEAD, HIT e MISS em registros CDN?

- **HEAD**
O método HEAD é o mesmo que o método GET, exceto que o servidor não retorna o corpo da mensagem HEAD. Em uma resposta a uma solicitação HEAD, os metadados contidos no cabeçalho HTTP são os mesmos que em uma resposta a uma solicitação GET. HEAD pode ser usado para obter os metadados ocultos em uma solicitação, em vez de transmitir a própria entidade. Também é frequentemente usado para testar a validade, disponibilidade e alterações recentes de hiperlinks.
- **HIT**

Isso indica uma ocorrência no cache. Um nó de borda serve diretamente o conteúdo.

- **MISS**

Isso indica uma falta de cache. Um nó de borda precisa recuperar o conteúdo do servidor de origem.

Por quanto tempo os dados podem ser consultados?

Você pode consultar dados de CDN nos últimos 90 dias. O intervalo máximo de tempo de consulta é de 31 dias.

Por que a mensagem "Falha de autenticação abrangente" é retornada quando chamo uma API para baixar registros de CDN?

É possível que o projeto empresarial não seja encontrado. Você pode adicionar **enterprise_project_id=ALL** ao caminho da solicitação.

Exemplo:

```
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
```

O que significa OkHttp do agente de usuário em registros de CDN?

O OkHttp é um protocolo de solicitação usado pela estrutura de rede do Android para processar solicitações de rede.

5 Gerenciamento de pacotes

Se você é cobrado por tráfego, você pode economizar dinheiro comprando um pacote de tráfego na página **Traffic Packages**. Você também pode visualizar as informações básicas sobre pacotes de tráfego e gerenciá-los na página **Traffic Packages**.

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Traffic Packages**.

Figura 5-1 Pacotes de tráfego

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. Você pode executar as seguintes operações:
 - Exibição de informações básicas sobre um pacote de tráfego: aprenda sobre o consumo do seu pacote de tráfego a qualquer momento.
 - Configuração de alerta de cota restante: clique em **Remaining Quota Alert** para definir um alerta para cotas remanescentes de pacotes de tráfego válidos. Compre um novo pacote de tráfego ou recarregue sua conta em tempo hábil para evitar perdas de serviço causadas por atrasos.
 - Compra de pacotes de tráfego novamente: clique em **Buy Again** e compre pacotes com base em seus requisitos de serviço. Para obter detalhes, consulte [Compra de novo](#).
 - Compra de pacotes de tráfego: clique em **Buy Traffic Package** e compre pacotes com base em seus requisitos de serviço.

6 Gerenciamento de log

A CDN registra as solicitações para todos os nomes de domínio, incluindo aqueles excluídos. Se tiver ativado a função de projecto empresarial, a gestão de registos não está disponível para estes nomes de domínio eliminados. Você pode baixar logs de um período específico nos últimos 30 dias ou usar a [ferramenta de combinação de log](#) para combinar e baixar logs de dias diferentes nos últimos 30 dias. Em seguida, você pode analisar o acesso aos seus recursos de serviço em detalhes.

Descrição do log

Latência do arquivo de log: você pode consultar arquivos de log gerados nas últimas seis horas na página **Logs**.

As regras de nomeação de log são as seguintes: *Log time span-acceleration domain name-Service area.gz*. A área de serviço é representada por uma abreviação de duas letras. Logs que terminam em **cn** são para áreas na China continental, e aqueles que terminam em **ov** são para áreas fora da China continental. Portanto, um nome de log típico pode ser, **2018021123-www.example01.com-ov.gz**.

Por padrão, um arquivo de log é gerado para cada nome de domínio a cada hora, e 24 arquivos de log são gerados todos os dias.

Exemplo de conteúdo do arquivo de log

```
[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"
```

Tabela 6-1 descreve cada campo (da esquerda para a direita) no log.

Tabela 6-1 Descrição de um arquivo de log da CDN

No.	Descrição do campo	Exemplo
1	Tempo de geração do log	[05/Feb/2018:07:54:52 +0800]
2	Endereço de IP de acesso	x.x.x.x
3	Latência (ms)	1

No	Descrição do campo	Exemplo
4	Informações do referenciador	-
5	Identificador do protocolo HTTP	HTTP/1.1
6	Método de solicitação HTTP	GET
7	Nome de domínio de aceleração	www.test.com
8	Caminho solicitado	/test/1234.apk
9	Código de status HTTP	206
10	Tamanho da resposta (em bytes)	720
11	Status do hit do cache	HIT
12	Informações do agente de usuário, que ajudam os servidores a reconhecer o SO, a versão do SO, a CPU, o navegador e as informações de versão do 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>Informações de intervalo especificam as posições do primeiro e último bytes para os dados a serem retornados.</p> <p>bytes podem ser expressos pelos três métodos a seguir:</p> <ul style="list-style-type: none"> ● bytes=x-y: solicitação de conteúdo do x-ésimo ao y-ésimo byte. ● bytes=-y: solicitação de conteúdo dos últimos y bytes. ● bytes=x-: solicitação de conteúdo do x-ésimo para o último byte. 	bytes=-256

Download de logs

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Logs**.
3. Selecione o nome do domínio de aceleração e especifique o intervalo de tempo para a consulta.

Todos os logs do intervalo de tempo especificado são exibidos na lista de logs. Se nenhuma solicitação for recebida dentro do período consultado, nenhum registro será gerado e nenhum dado será exibido na página.

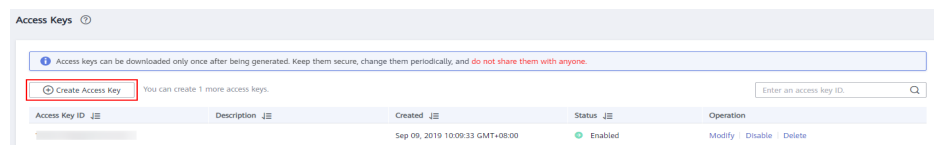
Figura 6-1 gerenciamento de logs

Name	Size	Start Time	End Time	Operation
2020	426.00 Byte	Nov 19, 2020 03:00:00 GMT+08:00	Nov 19, 2020 04:00:00 GMT+08:00	Download

4. Clique em **Download** na linha do log desejado para baixar o arquivo de log para um computador local.
5. Baixe a **ferramenta de combinação de log** e use a ferramenta para baixar os logs de um dia específico nos últimos 30 dias.

Antes de usar a ferramenta de combinação de log, **obter chaves de acesso**.

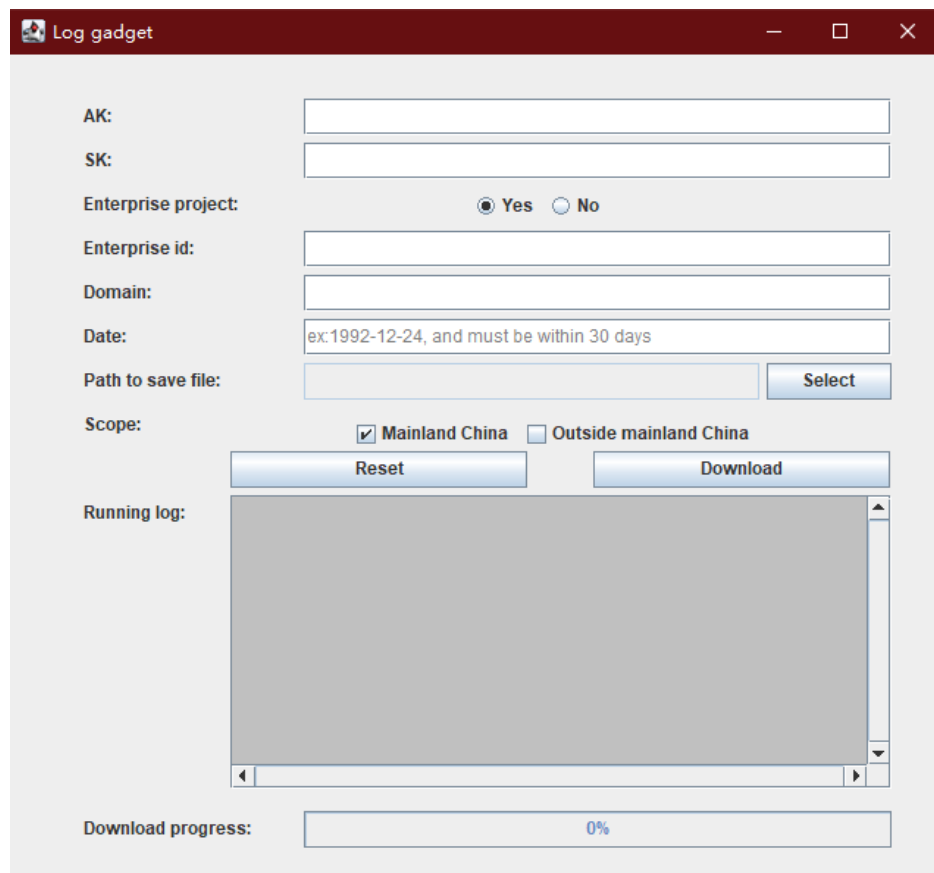
Figura 6-2 Obtenção de chaves de acesso



Clique em **Create Access Key** para obter as chaves de acesso. As teclas de acesso podem ser baixadas apenas uma vez. Para segurança da conta, é aconselhável alterar periodicamente suas chaves de acesso e mantê-las seguras.

Utilização da ferramenta de combinação de log

1. Baixe a ferramenta de combinação de log.
2. Clique duas vezes em logMerge.exe.



Parâmetro	Descrição
AK/SK	Para obter detalhes sobre como obter um par AK/SK, consulte Download de logs .
Projeto empresarial	Se você selecionar Yes , insira uma ID corporativa.
ID da empresa	Para obter detalhes sobre como obter uma ID de projeto empresarial, consulte Como obter uma ID de projeto empresarial?
Área	Nome de domínio de aceleração cujos logs devem ser visualizados.
Data	Selecione um dia nos últimos 30 dias, por exemplo, 2022-03-21.
Caminho para salvar o arquivo	Caminho para armazenar arquivos de log.
Escopo	China continental. Fora da China continental.
Registro em execução	O número de arquivos baixados e os nomes dos arquivos originais são exibidos. Se ocorrer um erro, uma mensagem de erro será exibida.

3. Clique em **Download** para baixar os logs do nome de domínio selecionado no dia especificado.

7 Gerenciamento de certificados

Conhecimento de fundo

Este tópico descreve como definir um certificado HTTPS de um nome de domínio e implantar a configuração de HTTPS em todos os nós de CDN para implementar a aceleração segura.

- **HTTP**

HTTP transfere conteúdo em texto simples sem qualquer criptografia de dados. Se um invasor interceptar pacotes transmitidos entre navegadores e servidores de sites, o conteúdo transmitido pode ser lido diretamente.

- **HTTPS**

Baseado em HTTP, o HTTPS usa Secure Sockets Layer (SSL) para criptografar a transmissão de dados. Com SSL, os servidores são autenticados usando certificados e as comunicações entre navegadores e servidores são criptografadas.

Cenários

- Se você tiver um certificado, poderá carregá-lo diretamente. Você também pode exibir e excluir certificados existentes.
- Você pode comprar certificados ou gerenciar certificados existentes no [SCM](#).

Configuração de um certificado

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console de CDN é exibido.
2. No painel de navegação, escolha **Certificates**.
3. Clique em **Configure Certificate** no canto superior esquerdo.

Figura 7-1 Configuração de um certificado próprio

Figura 7-2 Configuração de um certificado gerenciado pela Huawei

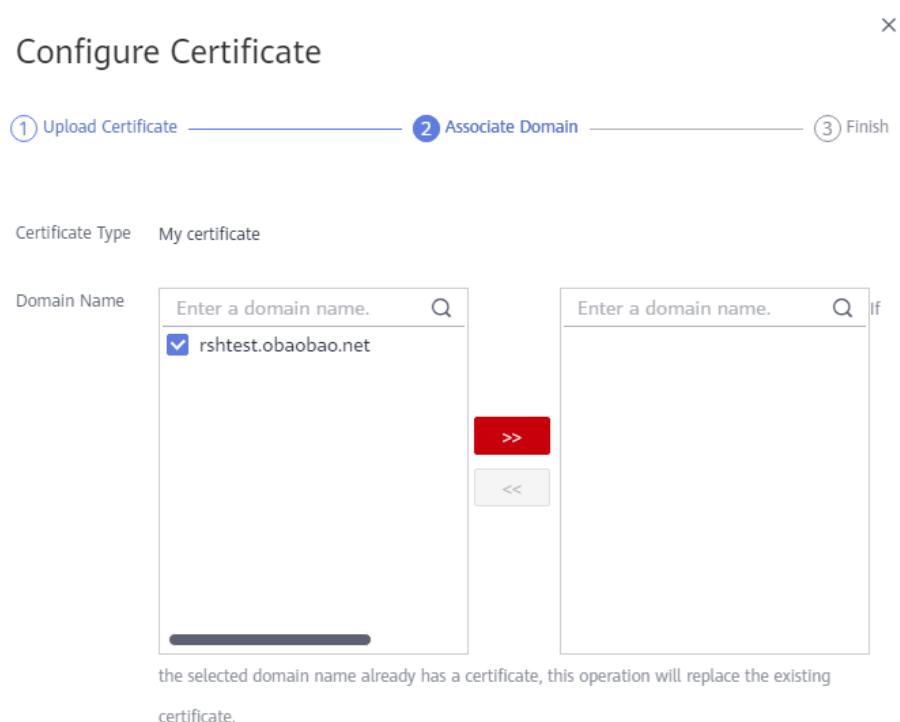
4. Definir parâmetros relacionados.

Parâmetro	Descrição
Tipo de certificado	My certificate ou Huawei-managed certificate
Nome do certificado	<ul style="list-style-type: none"> ● Se você selecionar My certificate, insira o nome do certificado. Um nome de certificado pode ter até 32 caracteres. ● Se você selecionar Huawei-managed certificate, vá para o console do CCM para enviar um certificado para a CDN e, em seguida, selecione o certificado na lista suspensa ao lado de Certificate Name no console da CDN. Para obter detalhes, consulte Como enviar um certificado SSL para outros serviços de nuvem.

Parâmetro	Descrição
Corpo de certificação	<ul style="list-style-type: none"> ● Se você selecionar My certificate, use um editor de texto local para abrir o certificado e copiar o conteúdo do certificado para a caixa de texto. Para obter detalhes sobre o formato do certificado, consulte Requisitos do certificado HTTPS. ● Se você selecionar Huawei-managed certificate, o conteúdo será preenchido automaticamente. <p>NOTA O corpo do certificado não pode conter espaços ou linhas em branco. Caso contrário, será exibida uma mensagem indicando que os parâmetros do certificado estão incorretos.</p>
Chave privada	<ul style="list-style-type: none"> ● Se você selecionar My certificate, use um editor de texto local para abrir a chave privada e copiar o conteúdo para a caixa de texto. Para obter detalhes sobre os requisitos de formato de chave privada, consulte Chave privada RSA. ● Se você selecionar Huawei-managed certificate, o conteúdo será preenchido automaticamente.
Protocolo de origem	<ul style="list-style-type: none"> ● Mantenha o valor original: se você configurou anteriormente um protocolo de origem, todas as solicitações de recuperação estarão em conformidade com essa configuração. Se nenhum protocolo de origem tiver sido configurado, o protocolo padrão, HTTP, será usado. ● HTTP: as solicitações de recuperação estarão em conformidade com o protocolo HTTP. ● HTTPS: as solicitações de recuperação estarão em conformidade com o protocolo HTTPS. ● O mesmo que o usuário: as solicitações de recuperação estarão em conformidade com o protocolo HTTP ou HTTPS, dependendo do usado pelas solicitações do usuário.
Redirecionamento forçado	<ul style="list-style-type: none"> ● Mantenha o valor original: se você configurou o redirecionamento anteriormente, todas as solicitações do usuário obedecerão a essa configuração. Se nenhum redirecionamento tiver sido configurado, Force Redirect será desabilitada por padrão. ● Padrão: as solicitações do usuário enviadas aos nós CDN suportam HTTP e HTTPS. ● HTTPS: todas as solicitações de usuários enviadas aos nós CDN serão forçadamente redirecionadas para HTTPS. ● HTTP: todas as solicitações do usuário enviadas aos nós CDN serão forçosamente redirecionadas para HTTP.

Parâmetro	Descrição
HTTP/2	<ul style="list-style-type: none">● Mantenha o valor original: se você configurou anteriormente o protocolo de acesso, todas as solicitações do usuário obedecerão a essa configuração. Se nenhum protocolo de acesso tiver sido configurado, HTTP/2 será desabilitado por padrão.● Ativar: HTTP/2 será ativado. Todas as solicitações do usuário enviadas aos nós de CDN estarão em conformidade com HTTP/2.● Desativar: HTTP/2 será desativado.

5. Clique em **Next** para associar o certificado ao seu nome de domínio.

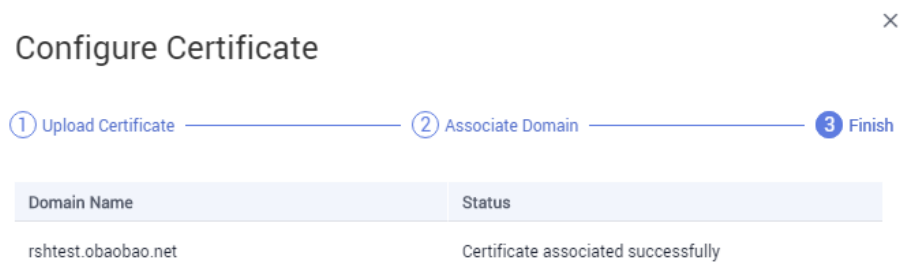


6. Selecione um nome de domínio a ser associado à esquerda, clique no ícone para associar o nome de domínio e clique em **Next**.

NOTA

Se o nome de domínio selecionado já usar um certificado, essa operação substituirá o certificado existente.

7. Clique em **Finish** para implementar a aceleração segura HTTPS para o nome de domínio associado.

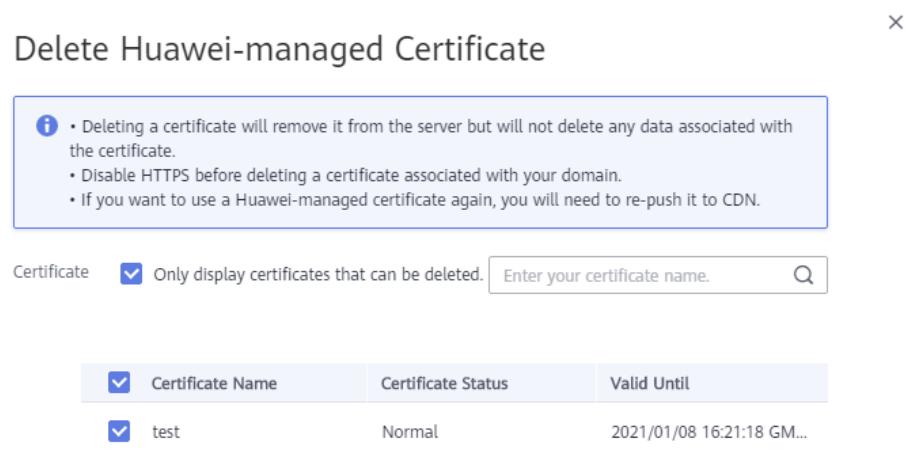


Exclusão de um certificado gerenciado

- A exclusão de um certificado o removerá do servidor, mas não excluirá nenhum dado associado ao certificado.
- Desative o HTTPS antes de excluir um certificado associado ao seu domínio.
- Para usar o certificado novamente, empurre-o novamente do SCM para a CDN.

Procedimento

1. Clique em **Delete Huawei-managed Certificate** no canto superior esquerdo.
2. Na página exibida, selecione o certificado a ser excluído e clique em **OK**.



3. Na caixa de diálogo exibida, clique em **OK**.

📖 NOTA

Para usar o certificado novamente, empurre-o novamente do SCM para a CDN.

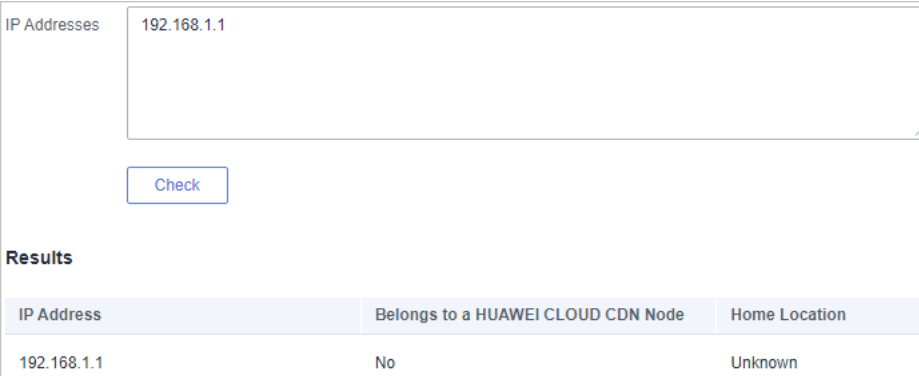
8 Verificação de endereços IP de nó

Se o conteúdo mostrado na página de acesso do nome de domínio de aceleração for anormal, você pode usar a ferramenta de verificação de endereço IP do nó para verificar se o endereço IP especificado é o endereço IP de um nó da CDN da HUAWEI CLOUD. Desta forma, você pode saber se a anormalidade é causada pela rede da operadora ou por outros motivos.

- Se o resultado da verificação mostrar que o endereço IP não é o de um nó da CDN da Huawei Cloud, o problema pode estar na rede da operadora. Nesse caso, entre em contato com sua operadora.
- Se o endereço IP pertencer a um nó da CDN da Huawei Cloud, retifique a falha consultando [Solução de problemas](#).

Procedimento

1. Faça login em [console da Huawei Cloud](#). Na página inicial do console de gerenciamento, escolha **Service List > Storage > CDN**.
O console da CDN é exibido.
2. No painel de navegação, escolha **Diagnosis > IP Address Check** para ir para a página de verificação de endereço IP do nó.



The screenshot displays 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 '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. Digite os endereços IP a serem verificados na caixa de texto **IP Addresses**.
Insira cada endereço IPv4 ou IPv6 em linhas separadas. Um máximo de 20 endereços IP podem ser verificados de cada vez.
4. Clique em **Check**.
Após a conclusão do diagnóstico, o sistema exibe os resultados na lista.

9 Gerenciamento de permissões

9.1 Criação de um usuário e concessão de permissões de CDN

Este capítulo descreve como usar [IAM](#) para implementar o controle de permissões refinado para seus recursos de CDN. Com o IAM, você pode:

- Crie usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM terá suas próprias credenciais de segurança para acessar os recursos da CDN.
- Conceda somente as permissões necessárias para que os usuários executem uma tarefa específica.
- Confie uma conta ou serviço de nuvem em Huawei Cloud para realizar O&M profissional e eficiente em seus recursos de CDN.

Se sua conta da Huawei Cloud não exigir usuários individuais do IAM, pule este capítulo.

Esta seção descreve o procedimento para conceder permissões.

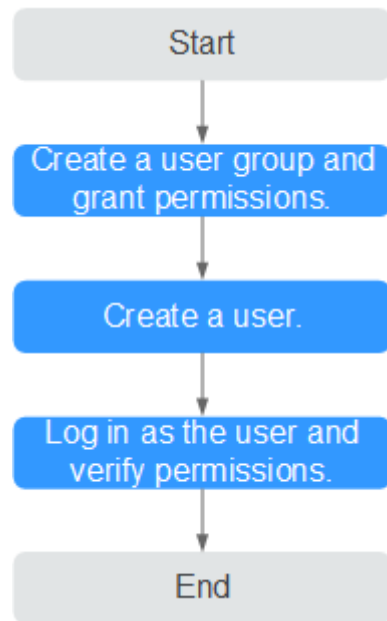
Pré-requisitos

Saiba mais sobre as permissões (consulte [Gerenciamento de permissões](#).) suportadas pela CDN e escolha políticas ou funções de acordo com suas necessidades. Para as políticas de sistema de outros serviços, consulte [Permissões do sistema](#).

Fluxo do processo

[Figura 9-1](#) mostra o processo de concessão de permissões de CDN.

Figura 9-1 Processo de concessão de permissões de CDN



1. **Criar um grupo de usuários e atribuir permissões.**

Crie um grupo de usuários no console do IAM e atribua a política de **CDN DomainReadOnlyAccess** ao grupo.

2. **Criar um usuário do IAM.**

Crie um usuário no console do IAM e adicione o usuário ao grupo criado em 1.

3. **Iniciar sessão** e verificar as permissões.

Efetue login no console de CDN como o usuário criado e verifique se ele só tem permissões de leitura para nomes de domínio de CDN.

- Ativar ou desativar um nome de domínio de aceleração. Se aparecer uma mensagem indicando que você não tem permissões suficientes para executar a operação, a política de **CDN DomainReadOnlyAccess** já entrou em 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

- Escolha qualquer outro serviço na **Service List**. Se aparecer uma mensagem indicando que você não tem permissões suficientes para acessar o serviço, a política de **CDN DomainReadOnlyAccess** já entrou em vigor.

9.2 Criação de uma política personalizada

Políticas personalizadas podem ser criadas para complementar as políticas definidas pelo sistema da CDN. Para as ações que podem ser adicionadas a políticas personalizadas, consulte **Políticas de permissões e ações suportadas**.

Você pode criar políticas personalizadas de uma das duas maneiras a seguir:

- Editor visual: selecione serviços de nuvem, ações, recursos e condições de solicitação sem a necessidade de conhecer a sintaxe da política.

- JSON: edite políticas JSON do zero ou com base em uma política existente.

Para obter detalhes, consulte [Criação de uma política personalizada](#). Esta seção fornece exemplos de políticas CCE personalizadas comuns.

Exemplo de políticas personalizadas

- Exemplo 1: permitir que os usuários criem nomes de domínio de aceleração

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

- Exemplo 2: permitir que os usuários definam uma lista negra de IP

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

- Exemplo 3: negar que os usuários excluam nomes de domínio de aceleração.

Uma política com apenas permissões "Negar" deve ser usada em conjunto com outras políticas para entrar em vigor. Se as permissões atribuídas a um usuário contiverem ações Permitir e Negar, as ações Negar terão precedência sobre as ações Permitir.

O método a seguir pode ser usado se você precisar atribuir permissões da política de **CDN Admin** a um usuário, mas também proibir o usuário de excluir nomes de domínio de aceleração. Crie uma política personalizada para negar a eliminação de nomes de domínio de aceleração e atribua ambas as políticas ao grupo ao qual o utilizador pertence. Em seguida, o usuário pode executar todas as operações no CDN, exceto excluir nomes de domínio de aceleração. O seguinte é um exemplo de política de negação:

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

- Exemplo 4: definir permissões para vários serviços em uma política

Uma política personalizada pode conter as ações de vários serviços que são do tipo global ou de nível de projeto. Veja a seguir um exemplo de política que contém ações de vários serviços:

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

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

10 Projetos empresariais

Enterprise Management da Huawei Cloud permite o gerenciamento unificado de recursos de nuvem por projeto empresarial. Você pode gerenciar recursos e pessoal em projetos corporativos e atribuir um ou mais grupos de usuários para gerenciar projetos empresariais. Você pode criar projetos empresariais de CDN no console do Enterprise Management para gerenciar seus recursos de domínio de maneira centralizada.

Criação de um projeto empresarial

Para criar um projeto empresarial de CDN:

1. No console do Enterprise Management, crie um projeto corporativo com base nos requisitos da sua empresa. Por exemplo, você pode criar projetos empresariais com base nos tipos de serviço dos nomes de domínio de aceleração de CDN. Para obter detalhes, consulte [Criação de um projeto corporativo](#).
2. Depois que um projeto da empresa é criado, você pode migrar seus recursos de nome de domínio para um projeto da empresa especificado. Para obter detalhes, consulte [Serviços de nuvem suportados pelo EPS](#).

NOTA

- Um projeto empresarial chamado **default** é criado por padrão. Este projeto é usado para gerenciar quaisquer recursos que não estão alocados a um projeto empresarial específico.
- A migração de um nome de domínio de aceleração entre projetos empresariais não afeta o serviço de aceleração.

Autorização do projeto empresarial

Depois que um projeto da empresa é criado e os recursos de CDN são migrados para o projeto da empresa, você pode adicionar grupos de usuários existentes e definir políticas de permissão de grupo de usuários para o projeto da empresa com base nos requisitos do site. Sem essas políticas, os membros do grupo de usuários não conseguirão acessar ou operar os recursos de domínio de CDN no projeto corporativo. Para obter detalhes sobre como definir políticas de permissão de grupo de usuários, consulte [Gerenciamento de permissões](#).

11 Auditoria

Cloud Trace Service (CTS) registra operações em recursos da nuvem na sua conta. Você pode usar os logs para realizar análises de segurança, rastrear alterações de recursos, auditar a conformidade e localizar falhas.

Ativação de CTS

Um rastreador será criado automaticamente depois que o CTS for habilitado. Todos os traços registrados pelo CTS estão associados a um rastreador. Atualmente, apenas um rastreador pode ser criado para cada conta.

Para obter detalhes sobre como habilitar o serviço de auditoria em nuvem, consulte [Ativação de CTS](#).

Operações de CDN gravadas pelo CTS

Tabela 11-1 Operações de CDN que podem ser gravadas pelo CTS

Operação	Descrição
createDomain	Criação de um nome de domínio
updateDomain	Atualização de um nome de domínio
deleteDomain	Remoção de um nome de domínio
enableDomain	Ativação de nomes de domínio
disableDomain	Desativação de nomes de domínio
updateOrigin	Configuração de um servidor de origem
updateOriginHost	Configuração de um host de recuperação
createRefer	Criação de uma regra de referência
createCertificate	Configuração de um certificado de domínio
createCacheRule	Criação de uma regra de cache

Operação	Descrição
createRefreshTask	Criação de uma tarefa de atualização de cache
createPreheatingTask	Criação de uma tarefa de pré-aquecimento de cache

Visualização de rastreamentos de CTS

Depois que você habilita o CTS, o sistema começa a gravar operações de CDN. Você pode ver as operações dos últimos sete dias no Console CTS. Para obter detalhes, consulte [Consulta de rastreamentos em tempo real](#).

Desativação de CTS

Você pode desabilitar rastreadores no console CTS. Depois que um rastreador for desativado, o sistema interromperá as operações de gravação, mas você ainda poderá visualizar registros históricos. Para obter detalhes sobre como desativar um rastreador, consulte [Desativação ou ativação de um rastreador](#).