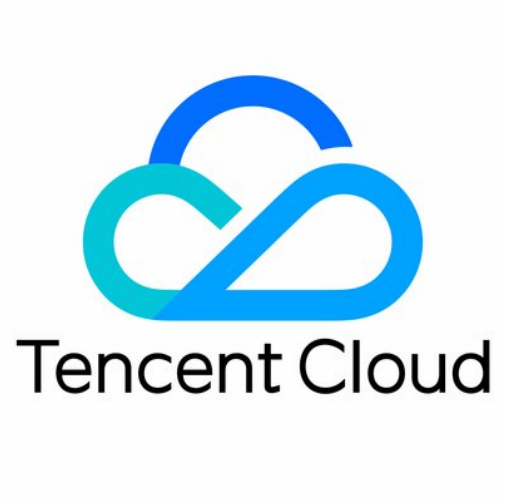
Content Delivery Network

設定ガイド

製品ドキュメント



©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

カタログ：

©2013-2022 Tencent Cloud. All rights reserved.

©2013-2022 Tencent Cloud. All rights reserved.

©2013-2022 Tencent Cloud. All rights reserved.

設定ガイド
ドメイン名管理
ドメイン名の操作

最終更新日：：2021-05-25 15:57:45

操作シナリオ

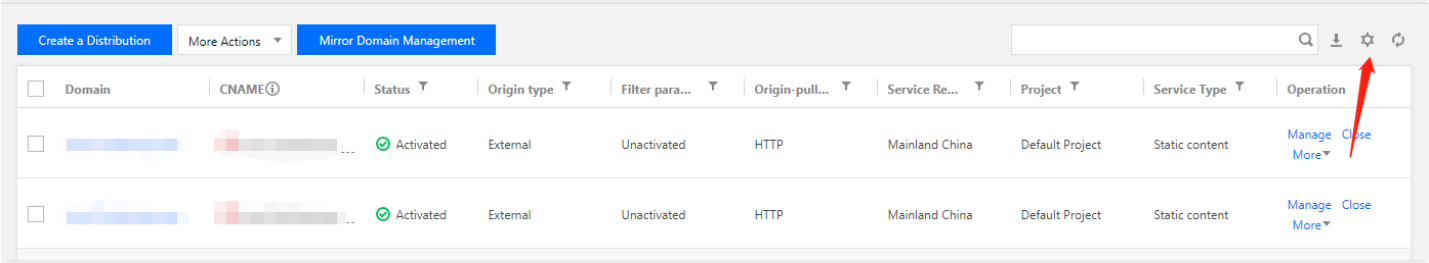
ドメイン名でTencent Cloud CDNのアクセラレーションサービスにアクセスします。アクセス済みのアクセラレーションドメイン名を管理する必要がある場合は、CDNコンソールにログインして、左側のメニューから【ドメイン名管理】を選択してドメイン名管理ページを開き、関連操作を実行します。

Tencent Cloud CDNはドメイン名リストのカスタマイズ調整、ドメイン名のアクセラレーションサービスのバッチ起動/終了、およびドメイン名の項目/タグ/設定のバッチ変更などの操作をサポートし、効率的なドメイン名の管理を支援します。

操作ガイド

リストのカスタマイズ調整

検索ボックスの右側の　をクリックして、リスト設定ポップアップを開くと、特定のドメイン名設定項目の表示を指定または表示をキャンセルすることができ、さらにリスト表示の順番を調整することができます。



ドメイン名設定のエクスポート

©2013-2022 Tencent Cloud. All rights reserved.

検索ポップアップの右側の  をクリックすると、直ちにドメイン名リスト中のドメイン名基本設定リストがエクスポートされます。フォーマットはExcelで、一度にエクスポートされるドメイン名の上限は1000です。

プロジェクトの編集

正常に機能するドメイン名の所属プロジェクトの変更をサポートしています。

- 単一ドメイン名の操作：ドメイン名の右側の【その他】をクリックして、ドメイン名の所属プロジェクトを修正します。

- バッチ操作：複数のドメイン名を選択して、上部の【更なる操作】中で「プロジェクトの編集」をクリックします。（注：一度に最大50のドメイン名を選択できます）

タグ編集

- 単一ドメイン名の操作：クリックしてドメイン名へ進み、ドメイン名の【基本情報】中の「タグ」で修正します。
- バッチ操作：複数のドメイン名を選択して、上部の【更なる操作】中で「タグ編集」をクリックします。（注：一度に最大50のドメイン名を選択することができます。変更してすぐには有効になりません。リフレッシュして最新のタグ内容を確認する必要があります）

- アクセラレーションサービスの停止

正常に機能するドメイン名に対し、アクセラレーションサービスをオフにすることができます。オフにすると、ネットワーク全体のCDNアクセラレーションノード上のドメイン名関連設定はオフラインになります。この時そのドメイン名のアクセスがCDNノードに到達しても、直接404が返され、正常に機能しません。そのためドメイン名をオフにする前に、ドメイン名に対応する名前解決が、Tencent Cloud CDN以外で割り当てられたCNAMEアドレスとして設定済みであることを確認する必要があります。

> 注意：
> ドメイン名アクセラレーションサービスを完全にオフにすると、消費は発生しなくなります。

- 単一ドメイン名の操作：右側の【その他】をクリックしてドメイン名を閉じます。
- バッチ操作：【起動済み】状態のドメイン名にチェックを入れ、上部の【その他の操作】中でバッチ操作により閉じます。

アクセラレーションサービスの有効化

©2013-2022 Tencent Cloud. All rights reserved.

すでにオフにされているドメイン名に対して再びアクセラレーションサービスを有効化するには、アクセラレーションサービスを有効にして、そのドメイン名設定をネットワーク全体のアクセラレーションノードに再び配信します。

- 単一ドメイン名の操作：ドメイン名の状態が【すでにオフ】である場合は、右側の【その他】をクリックしてドメイン名を有効化することができます。
- バッチ操作：【すでにオフ】状態のドメイン名にチェックを入れ、上部の【更なる操作】中でバッチ操作により起動します。

> 注意：
> すでに有効な状態のドメイン名で、3か月内に操作または消費が発生していない場合、非アクティブなドメイン名であると判断されます。Tencent Cloud CDNシステムはそのアクセラレーションサービスを自動的にオフにします。

アクセラレーションドメイン名の削除

ドメイン名の状態が【すでにオフ】である時にのみ削除操作を実行することができます。削除すると、ドメイン名に対応している設定は直接削除されて元に戻すことができず、その統計データの表示もできなくなりますので、慎重に操作してください。

- 単一ドメイン名の操作：右側の【その他】をクリックしてドメイン名を削除します。
- バッチ操作：【すでにオフ】状態のドメイン名にチェックを入れ、上部の【更なる操作】中でバッチ操作により削除します。

一括変更設定

一括変更設定機能では、複数のアクセラレーションドメイン名に対して、ドメイン名設定を同時に変更することができます。複数のドメイン名に対し、特定のドメイン名設定項目の変更を行いたい場合に、この機能を使えば、1つ1つのドメイン名に対して操作する必要なく一括で操作でき、設定効率をアップさせることができます。詳細については一括変更設定をご参照ください。

設定のコピー

設定のコピー機能では、既存のアクセラレーションドメイン名の設定を1つ以上の新しく追加されたアクセラレーションドメイン名にコピーすることができます。必要に応じて1つの既存ドメイン名を選択し、そのドメイン名の設定を新しく追加するドメイン名にコピーできます。詳細については設定のコピーをご参照ください。

©2013-2022 Tencent Cloud. All rights reserved.

ドメイン名の検索

最終更新日：：2020-02-29 13:26:33

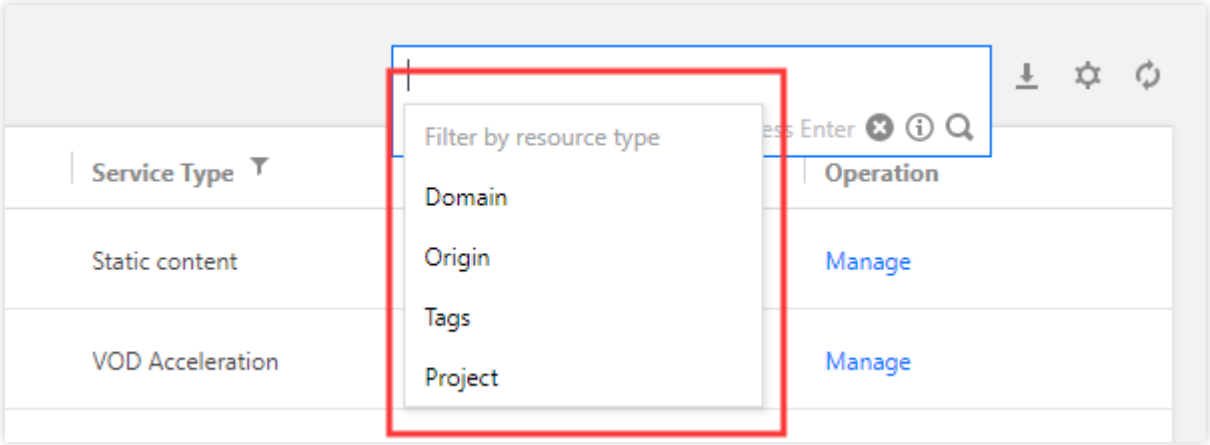
操作シナリオ

ドメイン名検索の総合検索機能で指定したドメイン名を迅速に見つけることができます。ドメイン名、オリジンサーバー、タグやプロジェクトなど複数の条件とキーワードによるフィルタリングをサポートしています。

> タブはTencent Cloud提供のクラウドリソースを表示するマークです。タグドキュメンテーションでタグのことを把握して管理することができます。

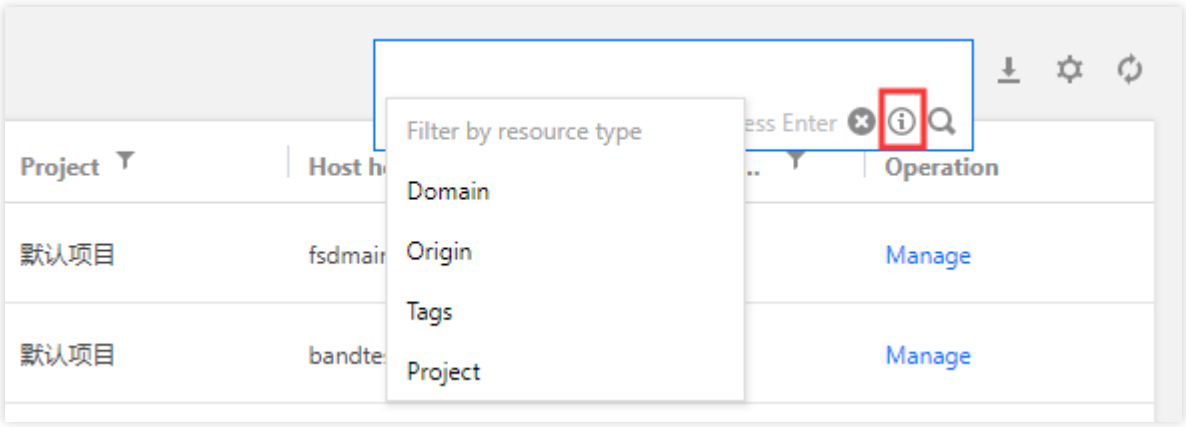
操作手順

1. CDNコンソールにログインして、左側のメニューで【Domain Management 】をクリックすると、管理ページに入ります。
2. クリックしてドメイン名検索の入力枠を有効化して、ドメイン名、オリジンサーバー、タグや所属するプロジェクトの中の一つか複数のリソース属性を選択して、対応する数値を入力してドメイン名の検索フィルタリングを行います。



3. 入力されるリソース属性又は入力のフォーマットについて疑問がある場合は、【i】アイコンをクリックすることで、検索ヘルプを取得することができます。

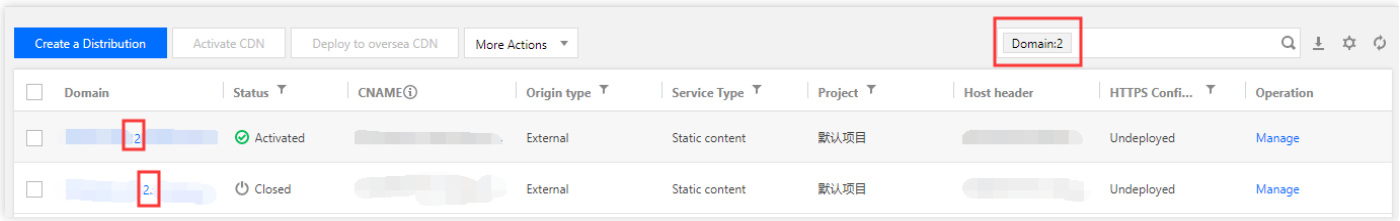
©2013-2022 Tencent Cloud. All rights reserved.



- マスターオリジンサーバーのみ検索をサポートしています。バックアップオリジンサーバーは検索をサポートしていません。
- 複数IPオリジンサーバーの検索は、オリジンサーバーの間には「;」で区切ります。
- ドメイン名、オリジンサーバーは単一キーワードによる検索しかサポートしていません。

検索に関する説明

- ドメイン名による検索：ドメイン名または一部を入力してマッチングします。曖昧検索をサポートしています。

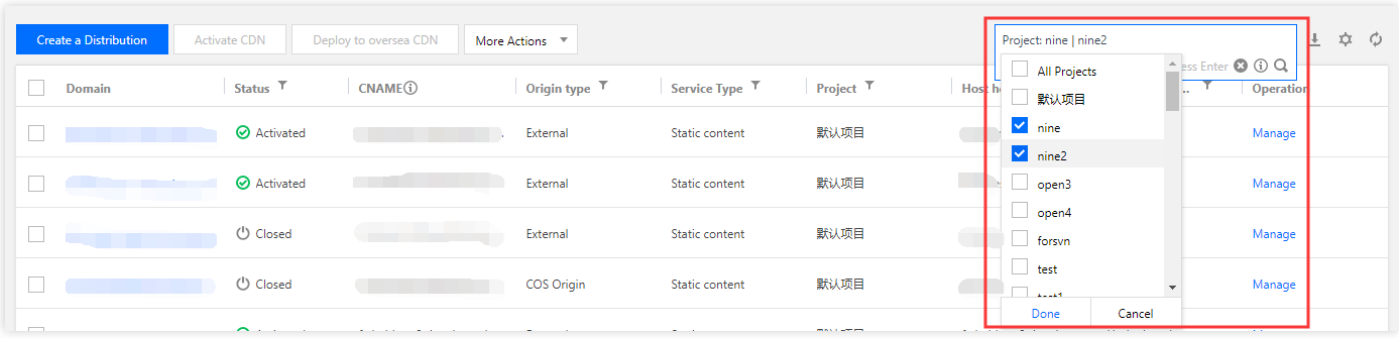


- オリジンサーバーによる検索：オリジンサーバー名または一部を入力してマッチングします。曖昧検索をサポートしています。

- タグによる検索：タブ名称名または一部を入力すると、タグ名称を含むドメイン名リストを戻します。タグ名称による検索は曖昧検索をサポートしていません。

©2013-2022 Tencent Cloud. All rights reserved.

- 所属するプロジェクトの検索：複数プロジェクトを選んでフィルタリングすることができます。



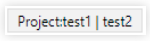
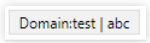
- 複数条件によるフィルタリングをサポートしています。即ち、ドメイン名やオリジンサーバー、タグ、所属するプロジェクトの中の一つか複数の条件を選んでフィルタリングすることができます。複数条件でフィルタリングする場合は、エンターで区切ります。

- 複数キーワードによるフィルタリングをサポートしています。即ち、各フィルタリング条件は複数のキーワードを入力することができます。キーワードの間は | で区切ります。

検索に対するヘルプ

種類	入力形式	例	検索枠の例	説明
単一キーワード	【キーワード】	www.test.com	www.test.com	「www.test.com」を含むドメイン名をフィルタリングします。
単一ドメイン名の属性	【属性】:【キーワード】	オリジンサーバー：1.1.1.1	Origin:1.1.1.1	「1.1.1.1」を含むドメイン名をフィルタリングします。
複数ドメイン名の属性	【属性】:【キーワード】【エンター】 【属性】:【キーワード】	ドメイン名：test オリジンサーバー：1.1.1.1	Domain:test Origin:1.1.1.1	ドメイン名に「test」という文字を含んで、オリジンサーバーに「1.1.1.1」を含むドメイン名をフィルタリングします。

©2013-2022 Tencent Cloud. All rights reserved.

種類	入力形式	例	検索枠の例	説明
複数ドメイン名の属性及び複数キーワード	【属性】:【キーワード】|【キーワード】	所属するプロジェクト：test1|test2		所属するプロジェクトに「test1」又は「test2」を含むドメイン名をフィルタリングします。ドメイン域名とオリジンサーバーの属性は複数キーワードによる検索をサポートしていません。
文字をコピーします	（貼り付けられた文字）	test abc		「test」又は「abc」という文字を含むドメイン名をフィルタリングします。

属性を入れなければ、CDNはグロバール検索を行えないため、デフォルトで【ドメイン名】の属性を入れて検索してください。即ち単一キーワードを入力する場合は、検索枠における内容が「ドメイン名:www.test.com」です。文字を貼り付ける場合は、検索枠の内容は「ドメイン名:test|abc」です。

©2013-2022 Tencent Cloud. All rights reserved.

設定のコピー

最終更新日：：2021-01-20 17:44:09

設定シナリオ

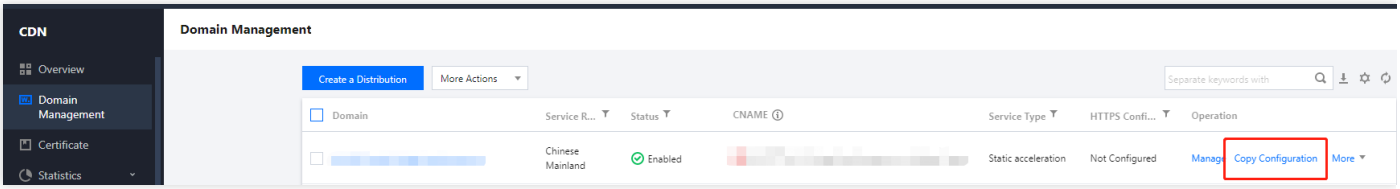
設定のコピー機能では、既存のアクセラレーションドメイン名の設定を1つ以上の新しく追加されたアクセラレーションドメイン名にコピーすることができます。 必要に応じて1つの既存ドメイン名を選択し、そのドメイン名の設定を新しく追加するドメイン名にコピーできます。これにより、新しく追加するドメイン名にコンソールのドメイン名設定を1つずつ設定する必要がなくなり、ドメイン名に簡単かつ迅速にアクセスできます。

⚠ 注意：

-無効化済み/禁止済み/ICP申告期限切れ/独自の証明書を保有/サポートされていないリージョンの差別化履歴設定を持つドメイン名がある場合、設定のコピー機能はサポートされません。
-コピーされるドメイン名に特別なバックエンド設定（コンソール以外の設定）がある場合、その特別な設定はコピーできません。

設定ガイド

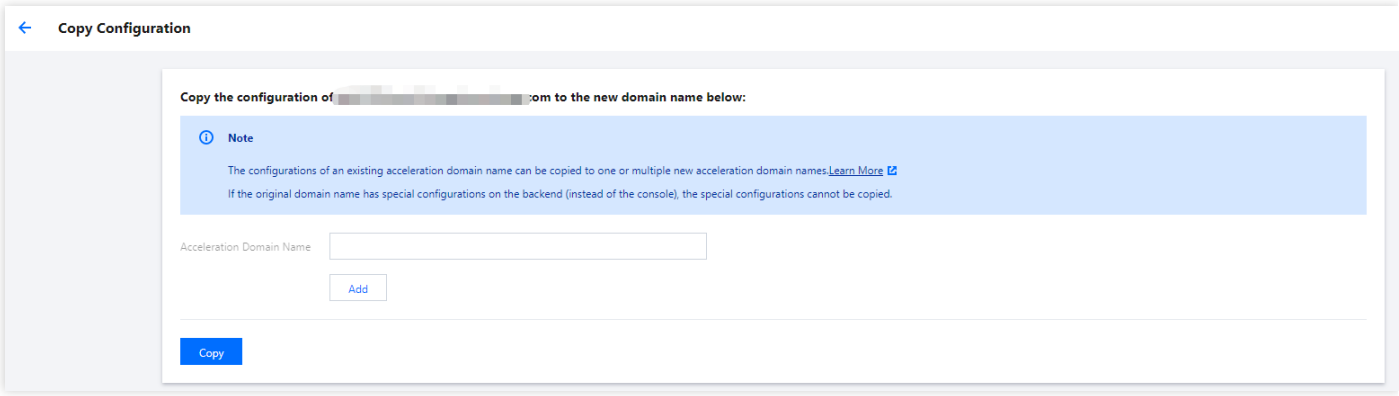
1. CDNコンソールにログインし、左側のメニューバーで【Domain Management】を選択し、ドメイン名操作列にある【設定のコピー】をクリックすると、設定のコピー画面が表示されます。



新しいアクセラレーションドメイン名を追加できます。提出後、現在のアクセラレーションドメイン名の設定

©2013-2022 Tencent Cloud. All rights reserved.

が新しく追加されたドメイン名にコピーされます。



説明：

-提出後に操作を中断することはできません。新しいドメイン名が正常に追加された後、そのドメイン名の設定を正常に管理できます。

- ドメイン名が追加されると、関連するドメイン名の設定がネットワーク全体のCDNアクセラレーションノードに配信されますが、ライブネットワークサービスに直接影響を与えることはありません。 アクセラレーションを有効にする必要がある場合は、CNAME設定を行う必要があります。手順の詳細については、CNAMEの設定をご参照ください。

©2013-2022 Tencent Cloud. All rights reserved.

一括変更設定

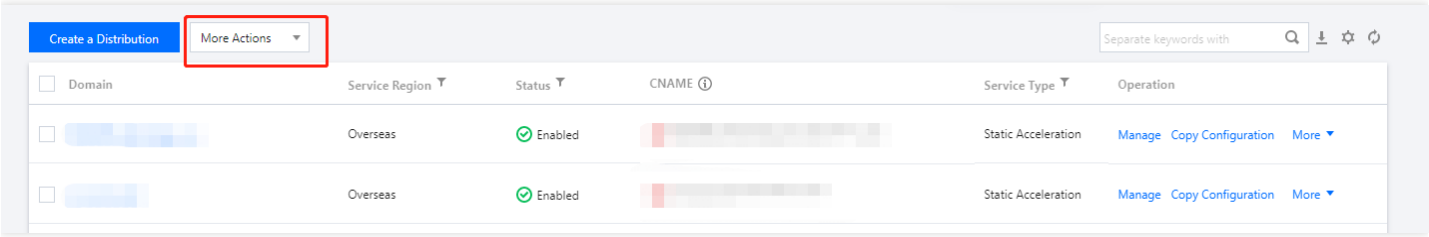
最終更新日：：2021-06-15 15:54:46

機能シナリオ

一括変更設定では、複数のアクセラレーションドメイン名に対して、ドメイン名設定を同時に変更する機能をサポートしています。複数のドメイン名に対し、特定のドメイン名設定項目の変更を行いたい場合に、この機能を使えば、1つ1つのドメイン名に対して操作する必要なく一括で操作でき、設定効率をアップさせることができます。

操作ガイド

CDN コンソールにログインし、左側のメニューバーから【Domain Management】を選択して、ドメイン名管理のページに入ります。アクティブになっているドメイン名を2つもしくは2つ以上選択した時に、上側の【更なる操作】の中で【一括変更設定】をクリックすると、一括変更設定のページに入れます。



注意：

- すでに無効化/封鎖/ロックされているドメイン名については、一括変更設定機能はサポートされません。
- 選択したドメイン名に特別なバックエンド設定（コンソール以外の設定）がある場合、その特別な設定は変更できません。

その他の説明

- 設定変更の操作後は元に戻せません。変更後は通常のドメイン名設定で管理することが可能です。
- 一部の設定項目はアクセラレーションリージョン/サービスタイプ/HTTPS証明書と関連付けられているため、アクセラレーションリージョン/サービスタイプ/HTTPS設定の状態が同じドメイン名を選択して、一括変更を

©2013-2022 Tencent Cloud. All rights reserved.

行うことを推奨します。

- HTTPS証明書の設定の一括変更については、証明書管理のページで行ってください。ここではサポートしていません。
- 1回につき、最大50ドメイン名の同時変更をサポートしています。ドメイン名が多いほど、変更を配布する時間が長くなります。一括変更1回あたりに選択するドメイン名を多くしすぎないでください。
- この機能はドメイン名のすべての設定項目をカバーしているわけではなく、まだサポートされていない設定項目がいくつかあります。今後少しずつアップデートし、リリースしていく予定です。

©2013-2022 Tencent Cloud. All rights reserved.

ドメイン名の設定
設定の概要

最終更新日：：2021-10-26 15:53:17

設定概要

Tencent Cloud CDNはリクエストの各段階でさまざまなカスタマイズ設定をサポートしているため、ご自身のビジネスニーズに応じて調整が可能です。

基本設定

基本設定にはアクセラレーションリージョンや業務タイプ等、ドメイン名のアクセラレーションサービスの基本情報、およびオリジンサーバーの関連設定、CDNアクセラレーションに必須の設定内容を含みます。

設定名	機能説明
基本情報	ドメイン名の所属項目、アクセラレーションリージョン、業務タイプ等の基本情報を修正します。
オリジンサーバー設定	複数のIPポーリングback-to-origin設定、ドメイン名back-to-origin、加重back-to-origin、back-to-origin Host設定、back-to-originプロトコル設定をサポートします。ホットバックアップオリジンサーバー設定をサポートします。**グローバルアクセラレーションドメイン名は国内外の異なる設定をサポートします。**

アクセス制御

アクセス制御の設定では、ユーザーの実際のリクエスト内容に応じて各種ルールを設定し、アクセスの遮断または承諾を行います。

設定名	機能説明
リンク不正アクセス防止の設定	refererブラックリスト/ホワイトリストの設定では、HTTPリクエストのrefererヘッダーへのアクセスに応じて、リクエストを拒否/承諾するかを判定します。**グローバルアクセラレーションドメイン名は国内外で異なる設定をサポートします。**
IPブラックリスト/ホワイトリストの設定	IPブラックリスト/ホワイトリストの設定では、HTTPリクエストのclient ipへのアクセスに応じて、リクエストを拒否/承諾するかを判定します。**グローバルアクセラレーションドメイン名は国内外で異なる設定をサポートします。**

©2013-2022 Tencent Cloud. All rights reserved.

設定名	機能説明
IP アクセス制限の設定	単一IP、単一ノードのアクセス制限を設定します。アクセス回数を超えたclient ipからのリクエストは直接拒否されます。
認証設定	タイムスタンプによるホットリンク防止の設定は、複数のタイムスタンプ署名アルゴリズムとルールをサポートします。 **グローバルアクセラレーションドメイン名は国内外で異なる設定をサポートします。**
ビデオドラッグ	ストリーミングメディアVODアクセラレーションシナリオに使用します。 ビデオドラッグの機能をオンにした後、startパラメータによってビデオの再生開始位置の指定をサポートします。
UAブラックリスト/ホワイトリストの設定	UAブラックリスト/ホワイトリストの設定は、HTTPリクエストのUser-Agentヘッダーのアクセスに基づいて、リクエストを拒否/承諾するかを判定します。
ダウンストリーム速度制限設定	シングルリンクのダウンストリーム速度制限を設定し、CDNのアクセス帯域幅をある程度制御できます。

キャッシュ設定

キャッシュ設定はCDNノードのキャッシュ動作を制御します。

設定名	機能説明
フィルタパラメータ構成	ノードがリソースをキャッシュする際に、URL？後のパラメータへのアクセスを無視するかどうかを設定します。 **URL後のパラメータが異なるコンテンツを意味する場合は、フィルタパラメータ構成をオンにしないことをお勧めします。**
キャッシュの有効期限の設定	パスやファイルタイプに応じて、CDNノード上のファイルキャッシュの有効期限の設定をサポートします。
ステータスコードキャッシュの設定	オリジンサーバーが異常なステータスコード（404や405）で応答した際、応答コンテンツに対するCDNノード上のキャッシュ有効期限を設定します。
HTTPヘッダーキャッシュの設定	デフォルトでは、CDNノードはすべてのオリジンサーバーのレスポンスヘッダーをキャッシュしますが、必要に応じてオフにすることができます。
大文字と小文字を区別しないキャッシュ設定	デフォルトでは、CDNノードは大文字と小文字を区別してキャッシュしますが、必要に応じて大文字と小文字を無視することができます。
URL書き換え設定	URLの書き換え設定をカスタマイズし、URL302を目標URLにリダイレクトすることをサポートします。

©2013-2022 Tencent Cloud. All rights reserved.

back-to-origin設定

back-to-origin設定はCDNノードがオリジンサーバーへのリクエストの送信を制御します。

設定名	機能説明
Range back-to-originの設定	デフォルトの状態では、CDNノードがそれぞれ分割してback-to-originを行います。オリジンサーバーがサポートしていない場合は、この設定をオフにすることができます。
back-to-origin Request Headerの設定	back-to-originリクエスト時に、正しいclient ipを伴う等、必要に応じて指定されたヘッダー情報を追加します。
back-to-originの301/302追従設定	back-to-originの301/302追従設定をオンにすることをサポートします。
back-to-originタイムアウト時間の設定	back-to-originのTCP接続タイムアウト時間（デフォルトでは5秒）とback-to-originのロード時間（デフォルトでは10秒）を設定します。

HTTPSアクセラレーションの設定

HTTPSアクセラレーション設定モジュールはHTTPSに関するさまざまな設定をサポートします。

設定名	機能説明
HTTPS設定	所有する証明書をアップロードするか、委託された証明書を使用し、HTTPSアクセラレーションを起動します。
HTTP2.0の設定	オンにすると、CDNエッジノードはHTTP2.0プロトコルをサポートします。 **HTTP2.0プロトコルをオンにする前に、証明書の設定が必要になります。**
強制的ジャンプ設定	証明書の設定の有無にかかわらず、HTTPSがHTTPリクエストに強制的にジャンプするよう設定することができます。 証明書が設定済みの場合は、HTTPがHTTPSリクエストに強制的にジャンプするよう設定することができます。
OCSPステープリングの設定	オンにすると、OCSPステープリングをサポートします。 **OCSPステープリングをオンにする前に、証明書の設定が必要になります。**
HSTS設定	オンにすると、strict-transport-securityヘッダーを追加します。 **HSTSの設定を行う前に、証明書の設定が必要になります。**

高度な設定

設定名	機能説明

©2013-2022 Tencent Cloud. All rights reserved.

設定名	機能説明
ネットワーク帯域幅の制限の設定	国内外のアクセラレーションの上限帯域幅の設定をサポートし、それを超えた場合に必要に応じてアクセラレーションサービスを停止することができます。 **グローバルドメイン名は国内外で異なる設定をサポートします。**
SEO最適化の設定	オンにすると、アクセスIPが検索エンジン向きかどうかを自動的に認識します。確認後、自動的にback-to-originし、検索エンジンの重み付けの安定性確保に努めます。
Response Headerの設定	必要に応じてHTTP Response Headerの設定を行い、リクエスト応答中にクライアントに戻します。
インテリジェント圧縮の設定	ファイルタイプと範囲を指定し、GzipまたはBrotli圧縮を行います。

©2013-2022 Tencent Cloud. All rights reserved.

基本設定
基本的な情報

最終更新日：：2020-12-28 10:48:35

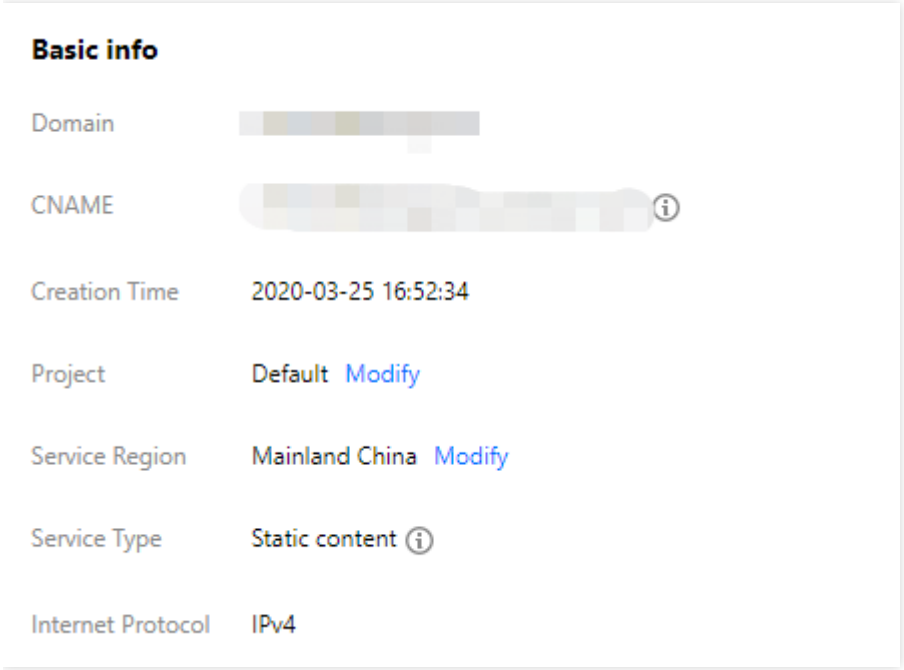
設定の概要

Tencent Cloud CDNに接続されているサービスの場合、ドメイン名基本情報モジュールで、ドメイン名の作成日時とそれに対応するCNAMEドメイン名、サービス地域、プロジェクト、サービスタイプ、サポートされているプロトコルなどの情報を確認できます。また、必要に応じてサービス地域、サービスタイプ、所属するプロジェクトなどの情報を変更することもできます。

設定ガイド

基本情報の表示

CDNコンソールにログインし、メニューバーで【ドメイン管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。一番上の欄に、ドメイン名の基本情報が表示されます。



説明：

©2013-2022 Tencent Cloud. All rights reserved.

元の【リクエストプロトコル】は【IPv6アクセス】に置き換えられました。既存のドメイン名のインターネットプロトコルが「IPv4 + IPv6」を選択した場合、IPv6アクセスは自動的に有効になります。

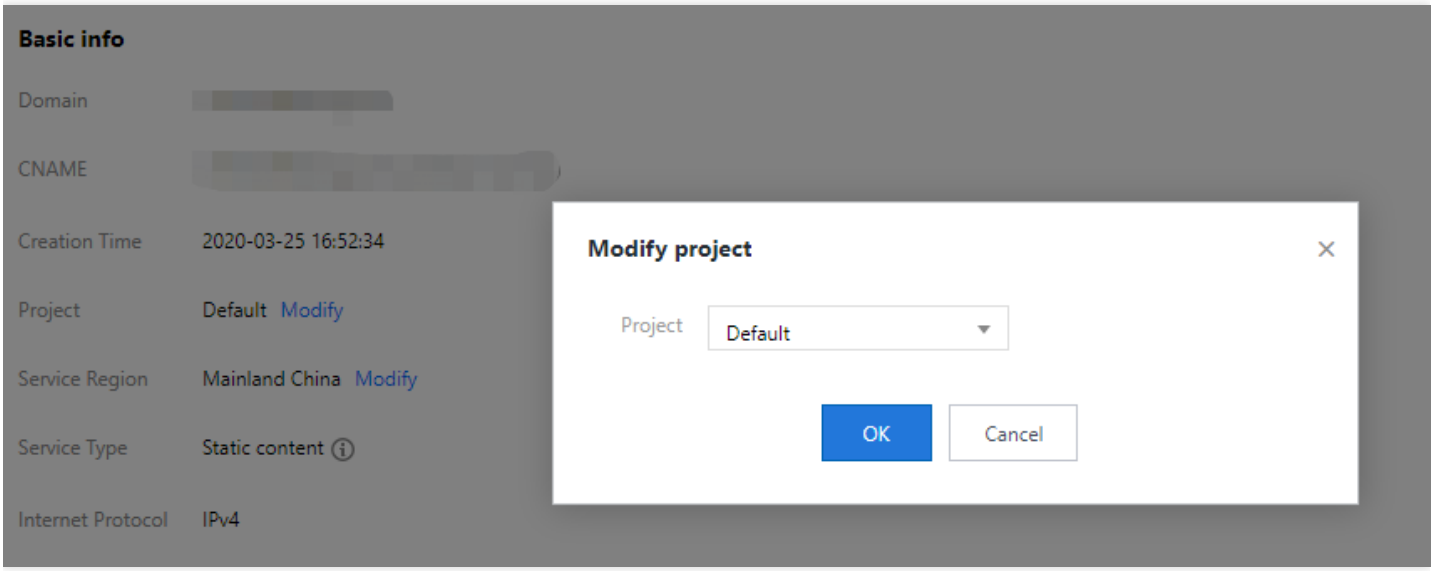
基本情報の変更

1. 所属するプロジェクトを変更する

所属するプロジェクトの右側にある【変更】をクリックして、ドメイン名が所属するプロジェクトを変更できます。ドメイン名が所属するプロジェクトを変更すると、プロジェクト次元データの統計とサブユーザーの権限が変更されるため、慎重に操作してください。

説明：

プロジェクトを作成するか、既存のプロジェクトを管理するには、プロジェクト管理ページに移動してください。



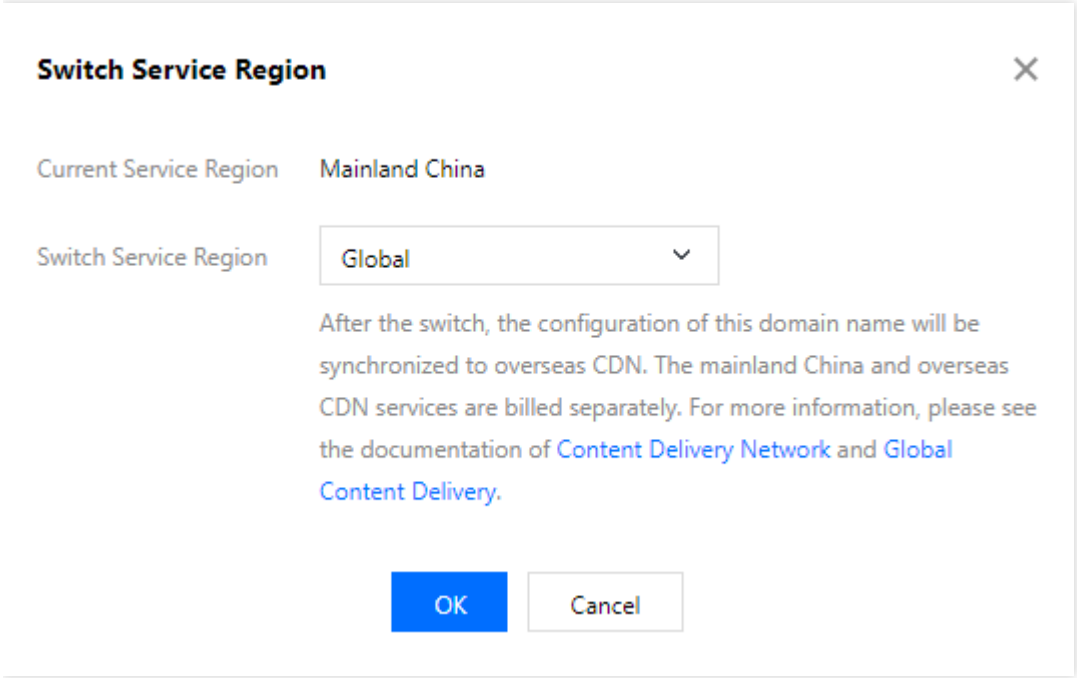
2. ドメイン名サービス地域を変更する

ドメイン名サービス地域の意味：

- ドメイン名がグローバルアクセラレーション用に設定されている場合、リクエストは最も近いグローバルCDNキャッシュノードにスケジュールされます。通常、中国本土のノードは中国本土のユーザーにサービスを提供し、中国本土以外のノードは中国本土以外のユーザーにサービスを提供します。
- ドメイン名が中国本土でアクセラレーション用に設定されている場合、グローバルユーザーからのアクセス要求は中国本土のアクセラレーションノードによって処理されます。
- ドメイン名が中国本土以外でアクセラレーション用に設定されている場合、グローバルユーザーからのアクセス要求は中国本土以外のアクセラレーションノードによって処理されます。

©2013-2022 Tencent Cloud. All rights reserved.

サービス地域の右側にある【変更】をクリックして、ドメイン名のサービス地域を変更できます。



⚠ **注意：**

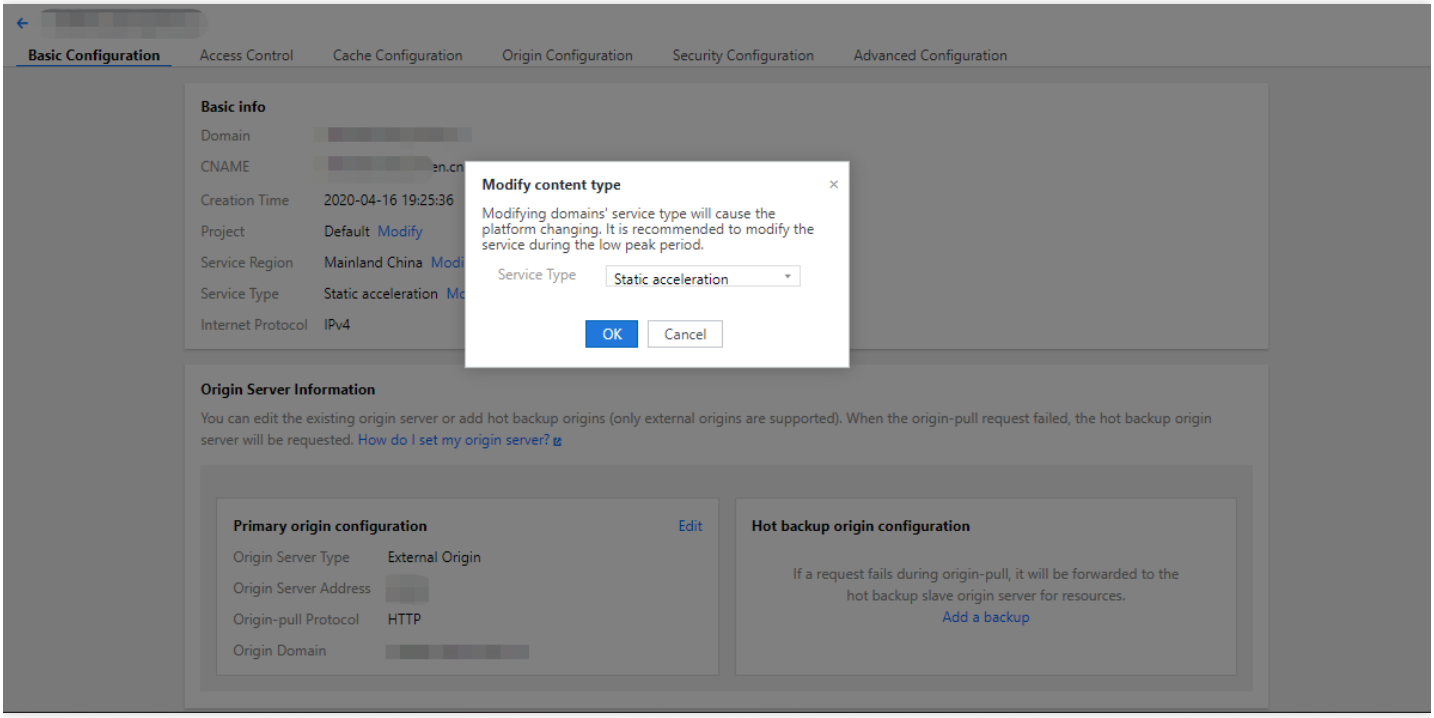
中国本土内外のアクセラレーションサービスは別々で課金され、料金は異なります。課金ポリシーの詳細については、こちらをご覧ください。

3. サービスタイプを変更する

Tencent Cloud CDNサービスは、さまざまなサービスタイプに基づいてアクセラレーション・パフォーマンスを最適化します。より良い結果を得るために、実際のサービスと同様のサービスタイプを選択することをお勧めしま

©2013-2022 Tencent Cloud. All rights reserved.

す。調整する必要がある場合は、サービスタイプの右側にある【変更】をクリックして変更してください。



⚠ 注意：

- サービスタイプを変更すると、CDNの基盤となるアクセラレーションプラットフォームが変更されます。この期間に、一部のリクエストが失敗することにより、back-to-origin帯域幅が増加する可能性があるため、オフピーク時に切り替えることをお勧めします。
- ご利用のドメイン名の【変更】ボタンが表示されない場合は、ドメイン名に特別な設定があることを意味します。さらにサポートが必要な場合、お問い合わせください。

4. IPv6アクセスを変更する

この機能を有効または無効にするには、IPv6アクセススイッチを切り替えます。有効にすると、IPv6プロトコルを介してCDNノードにアクセスできます。

⚠ 注意：

- IPv6アクセスは、中国本土でのみサポートされています。ドメイン名のアクセラレーションリージョンがグローバルである場合、 IPv6アクセスを有効にすると、中国本土でのみ有効になります。ドメイン名のアクセラレーションリージョンが中国本土以外である場合、この機能を有効にすることはできません。
- ドメイン名のアクセラレーションリージョンが「グローバル」で、IPv6アクセススイッチがオンになっている場合、アクセラレーションリージョンが「中国本土以外」のリージョンに切り替えられると、

©2013-2022 Tencent Cloud. All rights reserved.

IPv6アクセス機能は自動的に無効になり、有効にできなくなります。

- 「ストリーミングメディアVODアクセラレーション」は、IPv6アクセスは一時的にサポートされません。
- 一部のプラットフォームがアップグレードされているか、ドメイン名に特別な設定がある場合、IPv6アクセスは一時的にサポートされません。

©2013-2022 Tencent Cloud. All rights reserved.

オリジンサーバー設定

最終更新日：：2023-03-14 15:13:28

設定シーン

ドメイン名のオリジンサーバーの基本情報、Back-to-Originリクエストプロトコル、ホストヘッダーなどの情報を変更する場合、オリジンサーバー設定コンポーネントで関連操作を実施できます。

> 注意：
> アクセラレーションリージョンと同じリージョンのオリジンサーバーを設定することをお勧めします。例えば、アクセラレーションリージョンが中国本土の場合、中国本土のオリジンサーバーを設定してください。オリジンサーバーが中国香港または中国本土以外にある場合、Back-to-Originが国境を越えてアクセスするため、Back-to-Originの効果を保証できません。
> アクセラレーションリージョンがグローバルアクセラレーションの場合、ドメイン名の設定-オリジンサーバーの設定で、エリアにある独立したオリジンサーバーを設定できます。中国本土か中国本土以外によって、異なるオリジンサーバーへのBack-to-Originを実行することで、Back-to-Originの効果を保証します。

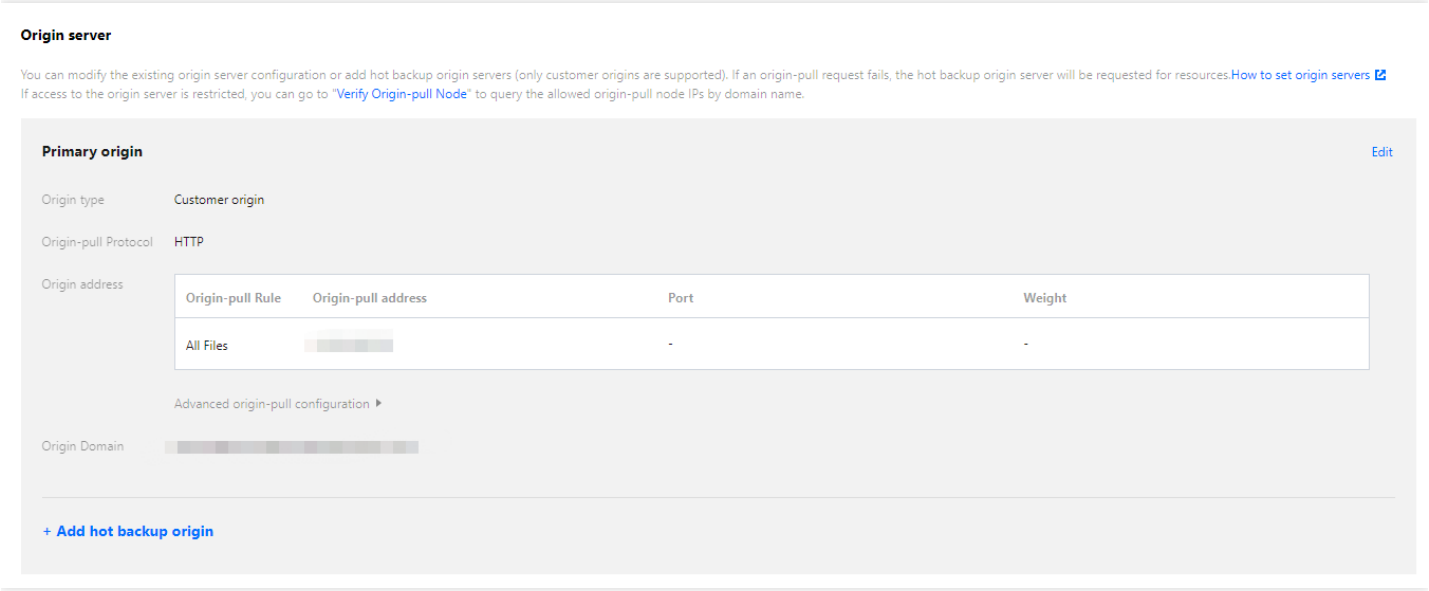
設定ガイド

プライマリーオリジンサーバーの設定

CDNコンソールにログインし、メニューバーで【ドメイン管理】を選択し、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。一番上の欄の基本情報の下にオリジンサーバー設定コンポーネ

©2013-2022 Tencent Cloud. All rights reserved.

ントがあります。



オリジンサーバータイプ

外部オリジンサーバー	安定して動作している業務サーバー（すなわち、オリジンサーバー）を持っている場合、業務サーバーのIPアドレスリストまたはドメイン名をオリジンサーバーのアドレスとして入力します。
COSソース	クラウドストレージからオリジンサーバーとして1つのバケットを選択します。プライベートバケットへのアクセスを有効にすることができます。
サードパーティCOS	Tencent Cloud以外のサードパーティCOSについては、AWS S3、Alibaba Cloud OSS、Huawei OBS、QiNiu kodoをサポートします。 **注：**ECDNでは、サードパーティCOSがサポートされていません。

オリジンプルプロトコル

CDN加速ノードがユーザーオリジンサーバーにback to originしたときに使用するプロトコル（HTTPまたはHTTPS）です。

HTTP Back-to-Origin	HTTP/HTTPSアクセスはHTTP Back-to-Originを使用します。
HTTPS Back-to-Origin	HTTP/HTTPSアクセスはHTTPS Back-to-Originを使用します。これにより、Back-to-Originデータの盗聴や改ざんを防ぐことができます。HTTPS Back-to-Originは、オリジンサーバーのCPUリソースを少し占有します（オリジンサーバーでHTTPSアクセスをサポートする必要がある）。

©2013-2022 Tencent Cloud. All rights reserved.

HTTP Back-to-Origin	HTTP/HTTPSアクセスはHTTP Back-to-Originを使用します。
プロトコル追従	HTTPアクセスはHTTP Back-to-Originを使用し、HTTPSアクセスはHTTPS Back-to-Originを使用します。一部の重要なセンシティブデータのみをHTTPSプロトコルで転送し、その他の業務ではHTTPプロトコルで転送する場合、「プロトコル追従」を選択することをお勧めします（オリジンサーバーはHTTPSアクセスをサポートする必要があります）

注意：
HTTPS Back-to-Originを使用する場合、オリジンサーバーでHTTPSアクセスをサポートすることを確認してください。サポートしない場合、Back-to-Originに失敗します。

オリジンサーバーアドレス

外部オリジンサーバー	• オリジンサーバーとして、複数のIPまたはドメイン名（1行に1個）を入力できます。 **マルチIPポーリングBack-to-Origin：**オリジンサーバーとして、複数のIPまたはドメイン名（1行に1個）を入力できます。Back-to-Origin中にポーリングされます。CDNではデフォルトでオリジンサーバー検出機能が有効になっています。IPのBack-to-Originに失敗し、または1分間で実行したBack-to-Originが5回を超えると、600s以内にこのIPアドレスでのBack-to-Originを実行しなくなります。600s経つと、このIPアドレスでのBack-to-Originを実行できるようになります。 **ドメイン名Back-to-Origin：**オリジンサーバーとして独立したドメイン名を設定できます。このドメイン名は、CDNアクセラレーションドメイン名を使用できません。IPv6ドメイン名Back-to-Originがサポートされません。 **注：**オリジンサーバーアドレスに、CDNアクセラレーションに導入し、オリジンサーバーが現在のアクセラレーションドメイン名を指しているサイトを入力することはできません。そうすると、解析が無限ループになり、Back-to-Originに失敗します。 • ポート(0～65535)とウェイト(1～100)が設定可能：オリジンサーバー：ポート：ウェイト（ポートを省略した場合、オリジンサーバー：：ウェイト） **注：**ウェイトは数字の大きさでソートされます。数字が大きいほど、ウェイトが大きく、Back-to-Originの優先度が高いです。 • オリジンサーバーアドレスは最大511文字を入力できます。
COSオリジンサーバー	• Tencent Cloud COSからオリジンサーバーとして1つのバケットを選択します。 • パケットの設定と実際の運用シーンに合わせて、デフォルトドメイン名、静的サイトまたはグローバルアクセラレーションドメイン名を選択します。例えば、バケットで静的サイトの設定が有効になっている場合、静的サイトを選択してください。 • ご利用のCOSバケットへの読書き権限にプライベート読取りが設定されている場合、CDNを許可しBack-to-Origin認証を有効にする必要があります。つまり、プライベートバケットへのアクセスを許可してください。

©2013-2022 Tencent Cloud. All rights reserved.

サードパーティCOS	• リソースがすでにサードパーティCOSに保存されている場合、オリジンサーバーとして有効なバケットアクセスアドレスを入力してください。現在サポートしているサードパーティCOSには、AWS S3、Alibaba Cloud OSS、Huawei OBS、QiNiu kodoがあります。**例：** `my-bucket.s3.ap-east-1.amazonaws.com` **または** `my-bucket.oss-cn-beijing.aliyuncs.com` **。** `http://` または `http://` プロトコルヘッダーを含むことができません。 • サードパーティプライベートバケットへBack-to-Originする場合、有効なキーを入力しBack-to-Origin認証を有効にする必要があります。つまり、プライベートバケットへのアクセスを許可してください。

Origin domain

Origin domainとは、back-to-origin中にCDNノードがオリジンサーバーのIPアドレスでアクセスするWebサイトのドメイン名を指します。具体的な設定例の説明については、Origin domainの設定をご参照ください。

> 説明：
> オリジンサーバーアドレスとOrigin domainの違いは以下の通りです：
> • オリジンサーバーアドレス：back-to-originリクエストの送信先のIPアドレスを指定します。
> • Origin domain：back-to-originリクエストの送信先のIPアドレスに対応するWebサイトを指定します。

外部オリジンサーバー	デフォルトでは、現在のアクセラレーションドメイン名とします。ワイルドカードドメイン名が接続されている場合、ワイルドカードドメイン名になり、実際のOrigin domainはアクセスドメイン名になります。実際の業務状況に応じて変更できます。
COSオリジンサーバー	デフォルトでは、バケットのアクセスアドレスとし、オリジンサーバーのアドレスと同じで、変更できません。
サードパーティCOS	デフォルトでは、バケットのアクセスアドレスとし、オリジンサーバーのアドレスと同じで、変更できません。

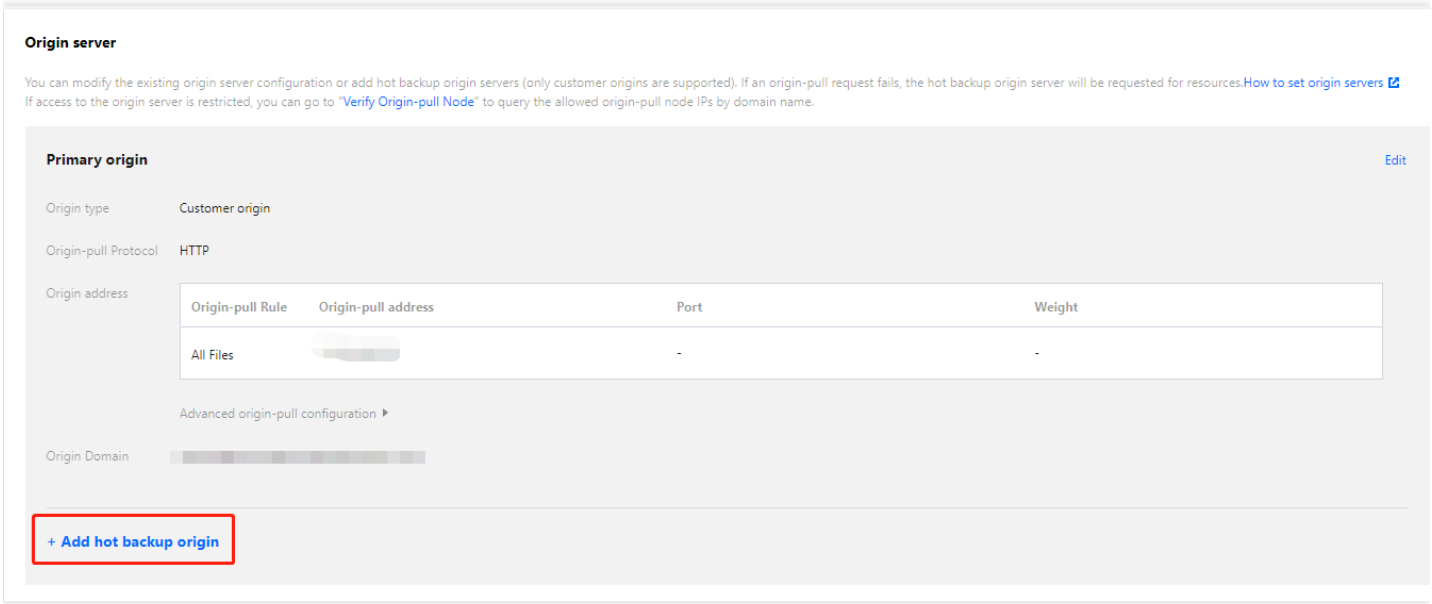
ホットバックアップオリジンサーバーの設定

プライマリオリジンサーバーにホットバックアップオリジンサーバーを追加できます。すべてのBack-to-Originリクエストは、最初にプライマリオリジンサーバーに転送されます。4XXまたは5XXエラーコードが返された場合、

©2013-2022 Tencent Cloud. All rights reserved.

または接続タイムアウト、プロトコル非互換などが発生した場合、リクエストがホットバックアップオリジンサーバーに転送され、リソースを取得し、Back-to-Originの高可用性を確保します。

ホットバックアップオリジンサーバーは独自のオリジンサーバーアドレスとOrigin domainを設定できます。



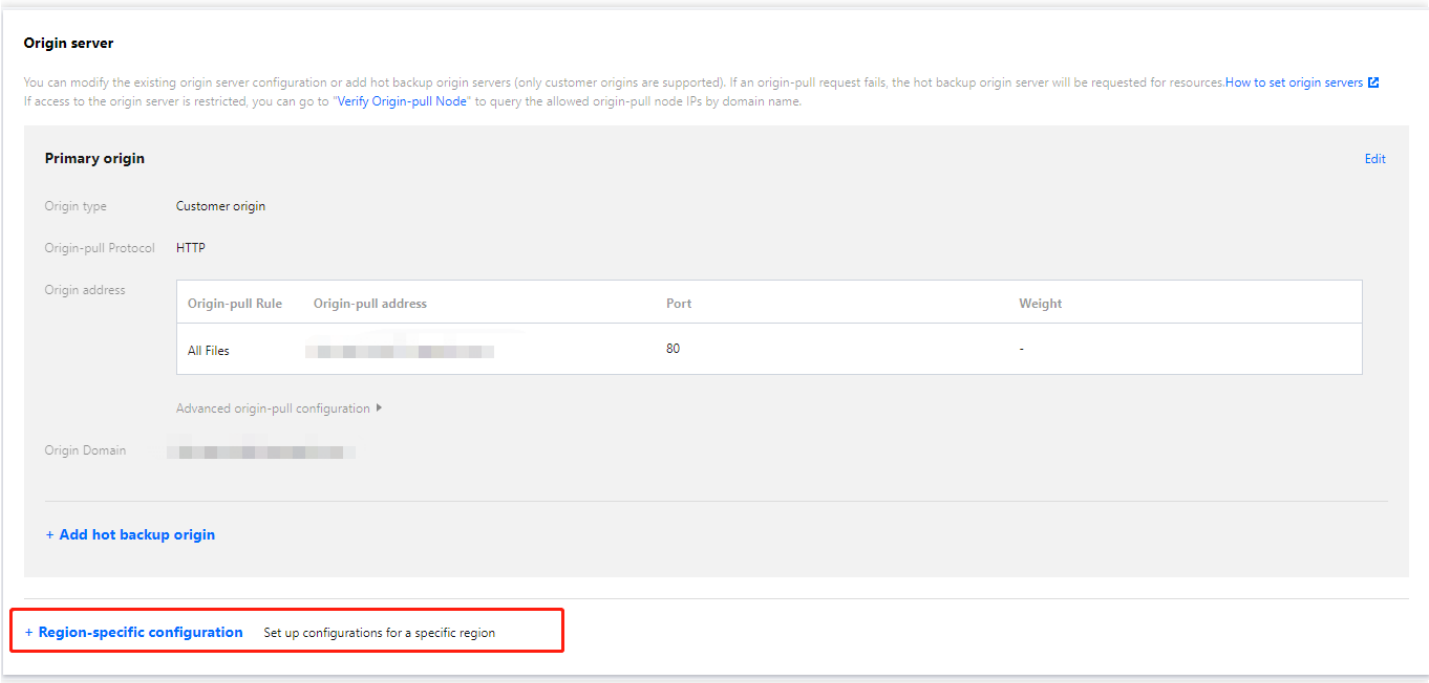
注意：

- ホットバックアップオリジンサーバーのオリジンサーバータイプは、COSオリジンサーバーとサードパーティCOSをサポートしません。
- プライマリオリジンサーバーでIPv6オリジンサーバーが有効になっている場合、ホットバックアップオリジンサーバーの追加がサポートされません。
- ホットバックアップオリジンサーバーで、ウェイトの設定がサポートされません。

リージョンの特別な設定

ご利用のアクセラレーションドメイン名のサービス提供リージョンがグローバルの場合、国際トラフィックの発生を防ぐために、ドメイン名のサービス提供リージョンごとにオリジンサーバーを設定したければ、下部にある**リージョンごとの設定**をクリックしてください。

©2013-2022 Tencent Cloud. All rights reserved.



異なるBack-to-Originポリシーを設定するリージョンを選択し、対応するオリジンサーバーの情報を入力します。具体的な設定例の説明については、リージョンの特別な設定をご参照ください。

注意：

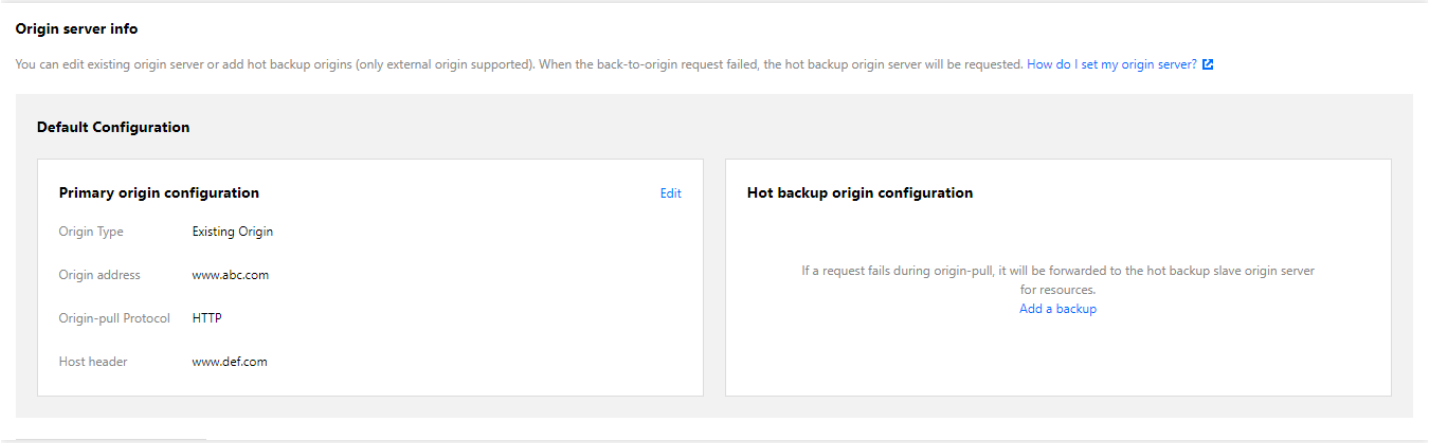
- オリジンサーバーのタイプがサードパーティCOSの場合、リージョンの特別な設定がサポートされません。

設定例

Origin domainの設定

CDNオリジンサーバーの設定が以下の場合、アクセラレーションドメイン名「www.test.com」の設定を以下だとすれば、

©2013-2022 Tencent Cloud. All rights reserved.

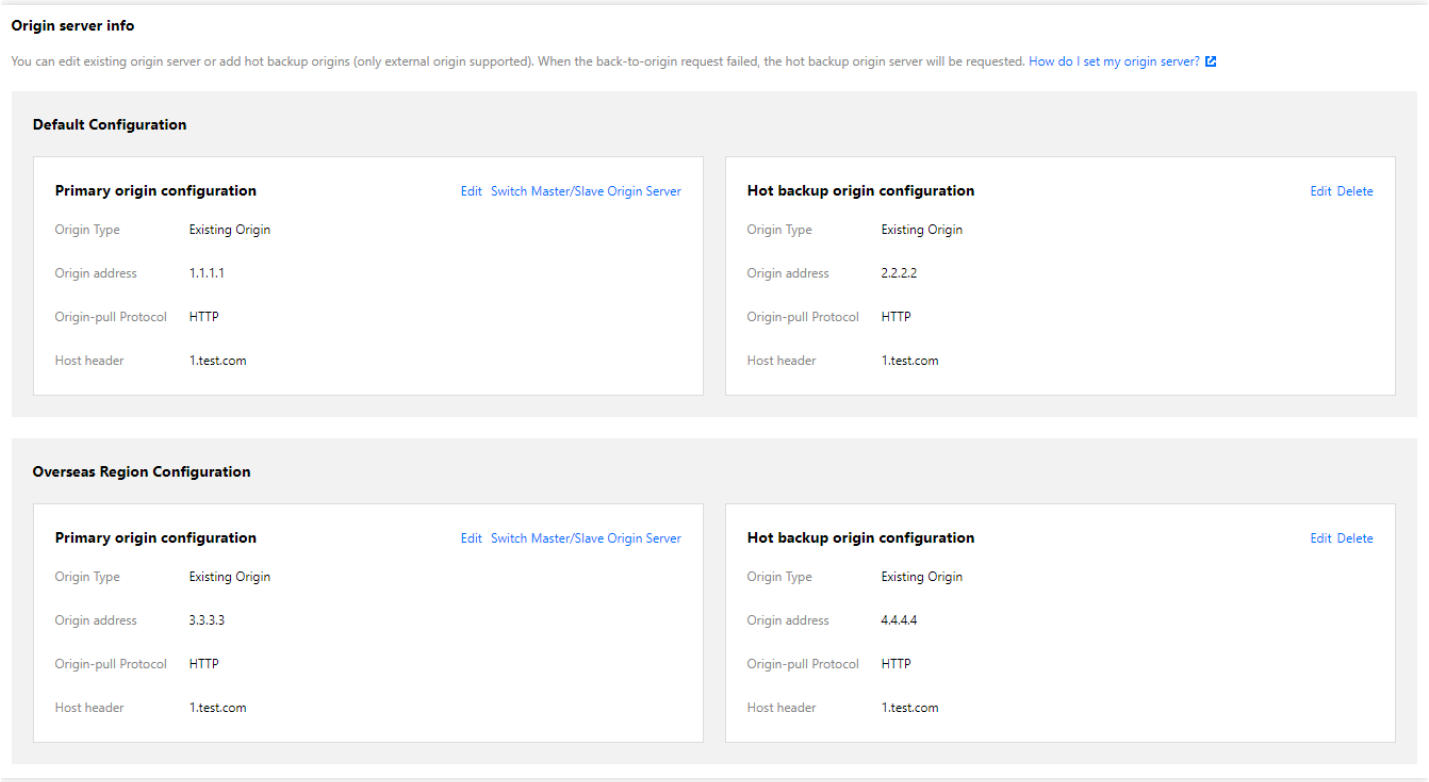


ユーザーアクセスパスは次のとおりです：
ユーザーはリソース `http://www.test.com/test.txt` にアクセスします。この時点では、CDNノードにこのリソースがキャッシングされていない場合、CDNノードのBack-to-Originは `www.abc.com` ドメイン名を解決してオリジンサーバーのアドレスを取得します。オリジンサーバーのアドレスを `1.1.1.1` とすれば、 `1.1.1.1` サーバーにアクセスし、その上のWebサイトwww.def.comのパス配下にあるtest.txtファイルを見つけて、ユーザーに返します。

リージョンの特別な設定

Tencent Cloud CDNオリジンサーバーの設定が以下の場合、アクセラレーションドメイン名「www.test.com」の設定を以下のとおりであるとすると：

©2013-2022 Tencent Cloud. All rights reserved.



実際のBack-to-Originは次のとおりです：

1. 中国本土のユーザーが `http://www.test.com/test.txt` ファイルにアクセスします。中国本土のノードにこのリソースがキャッシングされていない場合、Back-to-Originリクエストがサーバー `1.1.1.1` に転送されます。Webサイト `1.test.com` にあるtest.txtファイルを見つけて、このリソースがあれば直接ユーザーに返します。このリソースがなければ、ステップ2に進みます。
2. CDN中国本土のノードがプライマリオリジンサーバーへのBack-to-Originに失敗し、リソースが見つからなかった場合、Back-to-Originリクエストはサーバー `2.2.2.2` に転送されます。Webサイト `2.test.com` にあるtest.txtファイルを見つけて、ユーザーに返してキャッシングします。
3. この時点で、中国本土以外のユーザーも `http://www.test.com/test.txt` ファイルにアクセスするとすれば、中国本土以外のノードにこのリソースがキャッシングされていない場合、Back-to-Originリクエストがサーバー `3.3.3.3` に転送されます。Webサイト `3.test.com` にあるtest.txtファイルを見つけて、このリソースがあれば直接ユーザーに返します。このリソースがなければ、ステップ4に進みます。
4. CDN中国本土以外のノードが中国本土以外のプライマリオリジンサーバーへのBack-to-Originに失敗し、リソースが見つからなかった場合、Back-to-Originリクエストがサーバー `4.4.4.4` に転送されます。Webサイト `4.test.com` にあるtest.txtファイルを見つけて、中国本土以外のユーザーに返してキャッシングします。

©2013-2022 Tencent Cloud. All rights reserved.

高度なback-to-origin設定

最終更新日：：2021-11-24 15:30:30

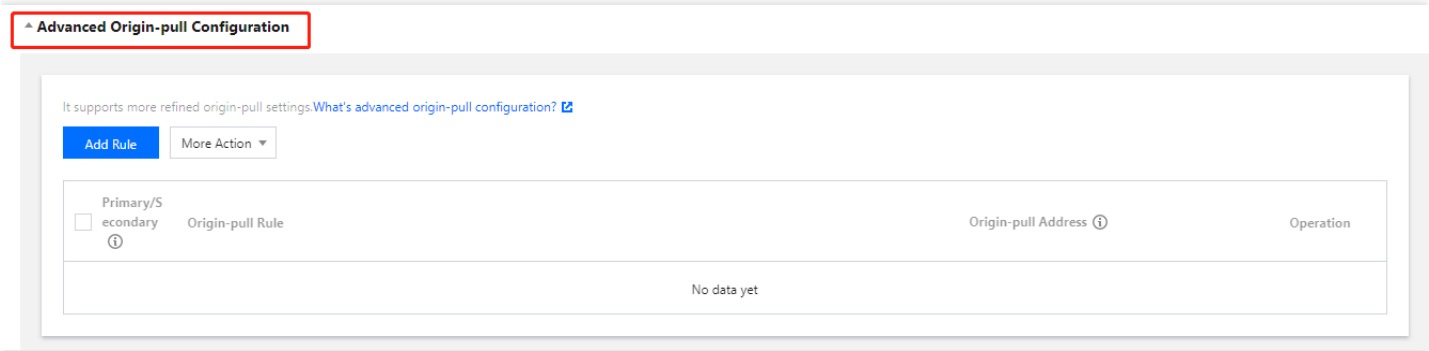
Tencent Cloud CDNは、より細かい粒度のback-to-origin設定をサポートし、それぞれのルールに基づき、それぞれのオリジンサーバーアドレスにback-to-originします。例えば、サブパスでのback-to-origin（ファイルタイプ、フォルダ、フルパスファイル（例：/test/1.jpg）、トップページを指定してback-to-origin）、Client IPの所在リージョンに基づくback-to-originなどです。

注意：

- Client IPの所在リージョンに基づくback-to-originは、現在、内部テスト中であり、全面的にリリースされていません。全面的なリリースまで、しばらくお待ちください。
- 現在はメインラインのみをサポートし、プライマリオリジンサーバーに基づきより細かい粒度のback-to-origin設定を行います（オリジンサーバーのタイプ、back-to-origin HOSTは、デフォルトでプライマリオリジンサーバーの設定を継承します。ルールごとの変更はサポートしていません）。

設定ガイド

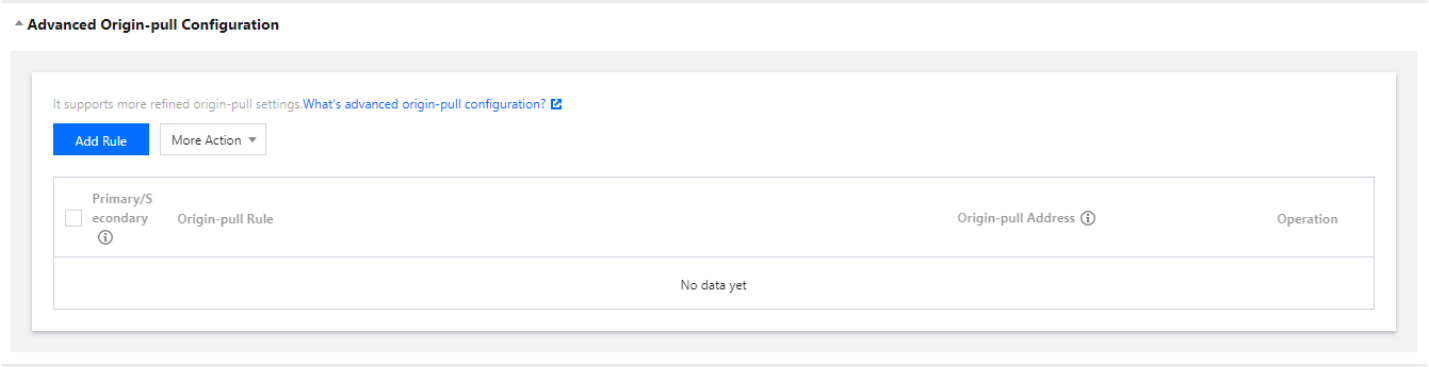
CDNコンソールにログインし、左側のメニューバーで【ドメイン名管理】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定ページに移動します。Tab【基本設定】ページの【オリジンサーバー情報】モジュール最下部に【高度なback-to-origin設定】が表示されていますので、クリックして開きます。



ルールの追加

必要に応じて高度なback-to-origin設定のルールを追加することができます。プライマリオリジンサーバーの【編集】をクリックし、【高度なback-to-origin設定】をクリックすれば編集が可能となります。

©2013-2022 Tencent Cloud. All rights reserved.



設定ルール

- 1つのドメイン名につき、最大50件のルールを追加できます。
- 1つのルール中のback-to-originアドレスは1つの IP/ドメイン名オリジンサーバーとポート（0 - 65535）の入力をサポートし、ポートはデフォルトにすることができます。back-to-originプロトコルで「HTTPS」または「プロトコルに従う」が選択されている場合は、ポートを443にしか設定できず、またはポートを設定することができません。
- 更なる操作：複数のルールを調整する際の優先度をサポートします。一括編集/削除の複数のルールをサポートします。

説明：

- 最下部の優先度が最上部より高い-この相対位置の優先度の調整は、複数のサブパスのback-to-originルール（ファイルタイプ/フォルダ/フルパスファイル/トップページback-to-originルールの指定）、またはClient IPの存在するリージョンに基づく複数のback-to-originルールなど、同一タイプのback-to-originルールのみに限定されます。
- 同一リクエストが異なるタイプのback-to-originルールに適合する場合は、タイプの優先度に従って実行され、順序はサブパス＞Client IPとなります。
  例：'江蘇に帰属するClient IPは1.1.1.1 にback-to-originする'および'/test は 2.2.2.2 にback-to-originする'が設定されている場合、江蘇に帰属するClient IPが /test にアクセスすると、 2.2.2.2 にback-to-originします。

©2013-2022 Tencent Cloud. All rights reserved.

HTTPS back to originアルゴリズムの説明

最終更新日：：2021-11-15 14:25:27

現在、HTTPS back to originがサポートしているアルゴリズムは次のとおりです（順不同）。

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA	ECDHE-ECDSA-AES256-SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
SRP-AES-256-CBC-SHA	SRP-RSA-AES-256-CBC-SHA	SRP-DSS-AES-256-CBC-SHA
DH-RSA-AES256-SHA	DH-RSA-AES256-SHA256	DH-RSA-AES256-GCM-SHA384
DH-DSS-AES256-SHA	DH-DSS-AES256-SHA256	DH-DSS-AES256-GCM-SHA384
DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA256	DHE-RSA-AES256-GCM-SHA384
DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA256	DHE-DSS-AES256-GCM-SHA384
CAMELLIA256-SHA	DH-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA
PSK-3DES-EDE-CBC-SHA	DH-DSS-CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA
ECDH-RSA-AES256-SHA	ECDH-RSA-AES256-SHA384	ECDH-RSA-AES256-GCM-SHA384
ECDH-ECDSA-AES256-SHA	ECDH-ECDSA-AES256-SHA384	ECDH-ECDSA-AES256-GCM-SHA384
AES256-SHA	AES256-SHA256	AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA256	ECDHE-RSA-AES128-GCM-SHA256

©2013-2022 Tencent Cloud. All rights reserved.

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-SHA	ECDHE-ECDSA-AES128-SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
SRP-AES-128-CBC-SHA	SRP-RSA-AES-128-CBC-SHA	SRP-DSS-AES-128-CBC-SHA
DH-RSA-AES128-SHA	DH-RSA-AES128-SHA256	DH-RSA-AES128-GCM-SHA256
DH-DSS-AES128-SHA	DH-DSS-AES128-SHA256	DH-DSS-AES128-GCM-SHA256
DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA256	DHE-RSA-AES128-GCM-SHA256
DHE-DSS-AES128-SHA	DHE-DSS-AES128-SHA256	DHE-DSS-AES128-GCM-SHA256
ECDH-RSA-AES128-SHA	ECDH-RSA-AES128-SHA256	ECDH-RSA-AES128-GCM-SHA256
ECDH-ECDSA-AES128-SHA	ECDH-ECDSA-AES128-SHA256	ECDH-ECDSA-AES128-GCM-SHA256
CAMELLIA128-SHA	DH-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA
PSK-RC4-SHA	DH-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA
AES128-SHA	AES128-SHA256	AES128-GCM-SHA256
SEED-SHA	DH-RSA-SEED-SHA	DH-DSS-SEED-SHA
DES-CBC3-SHA	DHE-RSA-SEED-SHA	DHE-DSS-SEED-SHA
IDEA-CBC-SHA	PSK-AES256-CBC-SHA	PSK-AES128-CBC-SHA
EDH-RSA-DES-CBC3-SHA	ECDH-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA

©2013-2022 Tencent Cloud. All rights reserved.

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
EDH-DSS-DES-CBC3-SHA	ECDH-ECDSA-DES-CBC3-SHA	ECDHE-ECDSA-DES-CBC3-SHA
RC4-SHA	ECDH-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA
RC4-MD5	ECDH-ECDSA-RC4-SHA	ECDHE-ECDSA-RC4-SHA
SRP-3DES-EDE-CBC-SHA	SRP-RSA-3DES-EDE-CBC-SHA	SRP-DSS-3DES-EDE-CBC-SHA
DH-DSS-DES-CBC3-SHA	DH-RSA-DES-CBC3-SHA	-

©2013-2022 Tencent Cloud. All rights reserved.

アクセス制御
リンク不正アクセス防止の設定

最終更新日：：2021-04-14 19:34:35

設定シナリオ

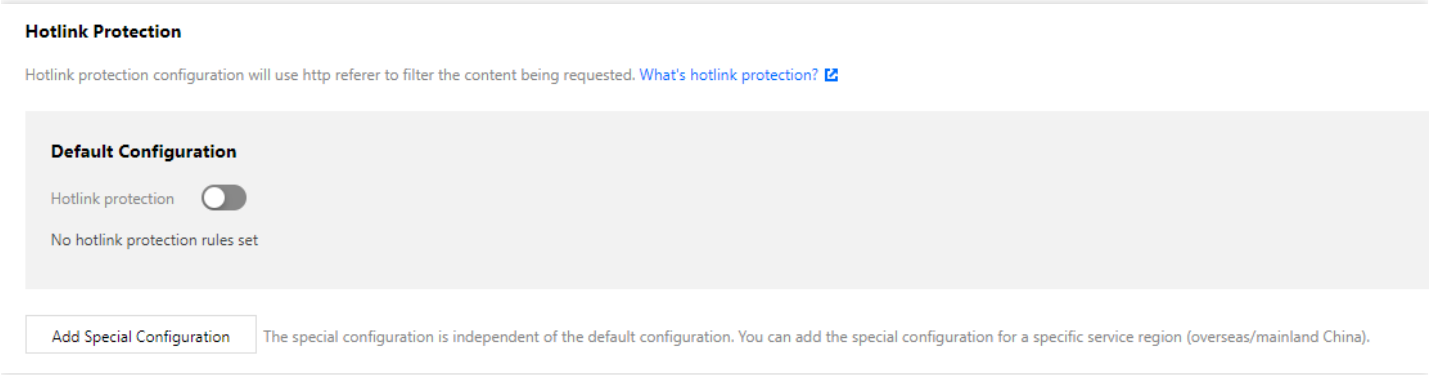
ビジネスリソースへのアクセスのソースを制御する場合、Tencent Cloud CDNはreferer リンク不正アクセス防止設定機能を提供しています。

HTTP Request Header中のrefererフィールドの値にアクセス制御ポリシーを設定することにより、アクセスソースを制御して、悪意のあるユーザーによる盗用を防ぐことができます。

設定ガイド

設定の確認

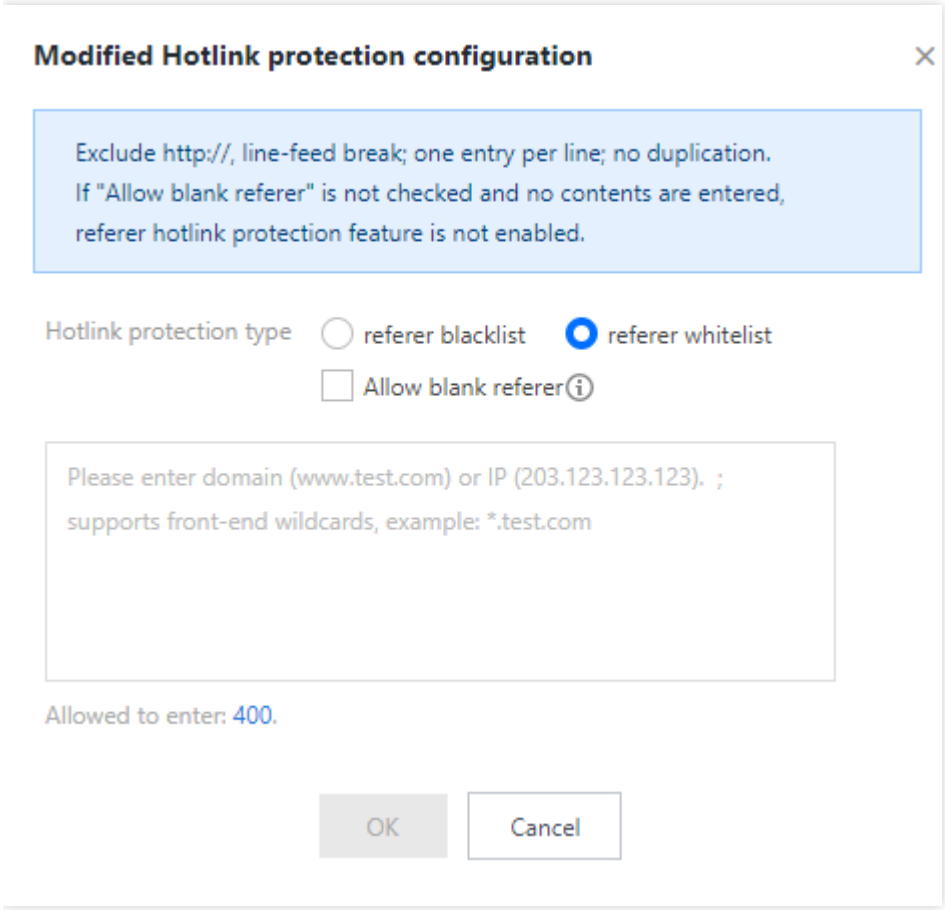
CDNコンソールにログインし、メニューバーで【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定ページに入ります。第2欄の【アクセス制御】からリンク不正アクセス防止設定を確認できます。デフォルトでは、リンク不正アクセス防止設定がオフになっています。



設定を有効にする

スイッチをクリックし、リンク不正アクセス防止のタイプを選択してリストに入力します。空の referを許可するかにチェックを入れて、【確認】をクリックすれば、リンク不正アクセス防止設定を有効にすることができます。

©2013-2022 Tencent Cloud. All rights reserved.



refererブラックリスト：

- リクエストされたrefererフィールドがブラックリストに設定されている内容にマッチしている場合、CDNノードはリクエストされた情報を返さず、403ステータスコードが返されます。
- リクエストされたrefererフィールドがブラックリストに設定されている内容にマッチしていない場合、CDNノードはリクエストされた情報を正常に返します。
- **空のrefererを含む**というオプションが選択された場合、refererフィールドが空であるか、refererフィールド（たとえば、ブラウザリクエスト）がない場合、CDNノードはリクエストされた情報を返さず、403ステータスコードが返されます。

refererホワイトリスト：

- リクエストされたrefererフィールドがホワイトリストに設定されている内容にマッチしている場合、CDNノードはリクエストされた情報を正常に返します。
- リクエストされたrefererフィールドがホワイトリストに設定されている内容にマッチしていない場合、CDNノードはリクエストされた情報を返さず、403ステータスコードが返されます。
- ホワイトリストを設定する場合、CDNノードはホワイトリストで設定された文字列に一致するリクエストのみを返すことができます。

©2013-2022 Tencent Cloud. All rights reserved.

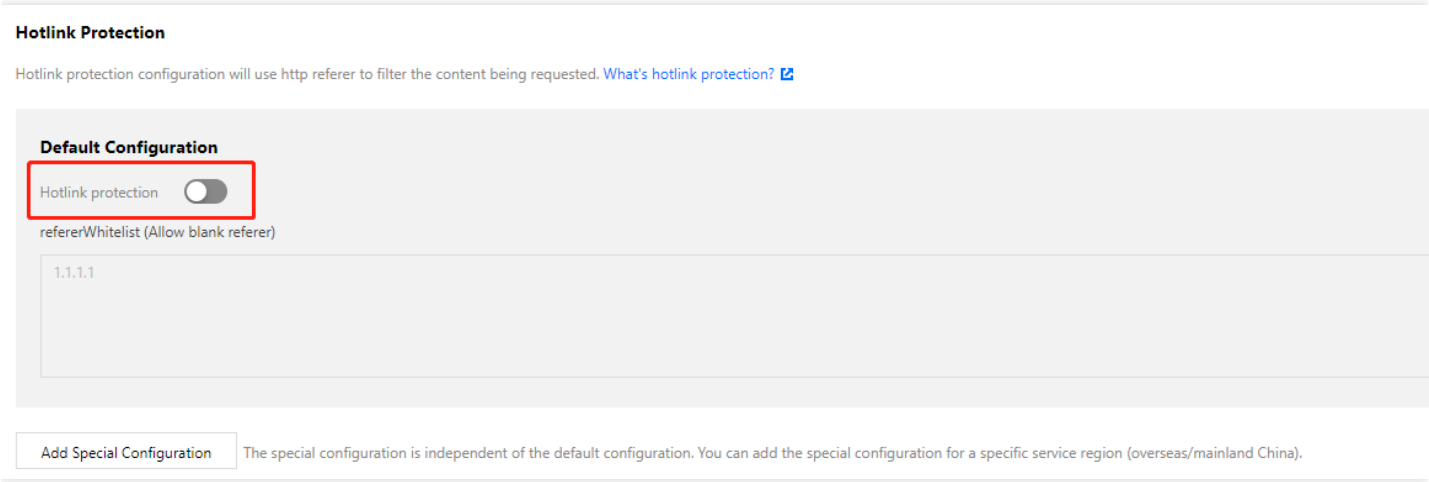
- **空のrefererを含む** というオプションが選択された場合、refererフィールドが空であるか、refererフィールド（たとえば、ブラウザリクエスト）がない場合、CDNは正常にリクエストされた情報を返します。

設定の制約：

- リンク不正アクセス防止は、ドメイン名/IPルールをサポートしています。IPルールが使用されている場合、プレフィックスマッチングが利用可能です。ドメイン名ルールが使用されている場合、プレフィックスマッチングはサポートされていません。即ち、 `www.abc.com` が設定されている場合、 `www.abc.com/123` がマッチしますが、 `www.abc.com.cn` がマッチしません。 `127.0.0.1` が設定されている場合、 `127.0.0.1/123` もマッチします。
- リンク不正アクセス防止は、ワイルドカードマッチングをサポートします。つまり、 `*.qq.com` 設定されている場合、 `www.qq.com` と `a.qq.com` の両方がマッチします。

設定を無効にする

リンク不正アクセス防止機能を無効に切り替えることができます。スイッチがオフの場合、以下の既存の設定があっても、この機能は実稼働環境では有効になりません。スイッチがオンの場合、設定がネットワーク全体で有効になる前に、先に設定の再確認を行っています。

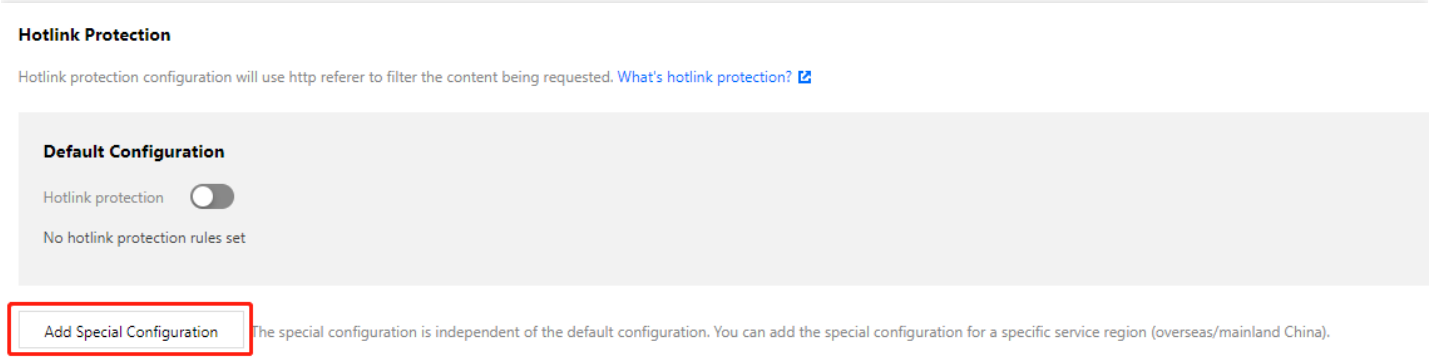


地域の特別な設定

アクセラレーションドメイン名がグローバルアクセラレーション用に設定されており、中国本土と中国本土以外のアクセラレーションリージョンに異なるrefererリンク不正アクセス防止を設定する場合は、設定の下にある【特

©2013-2022 Tencent Cloud. All rights reserved.

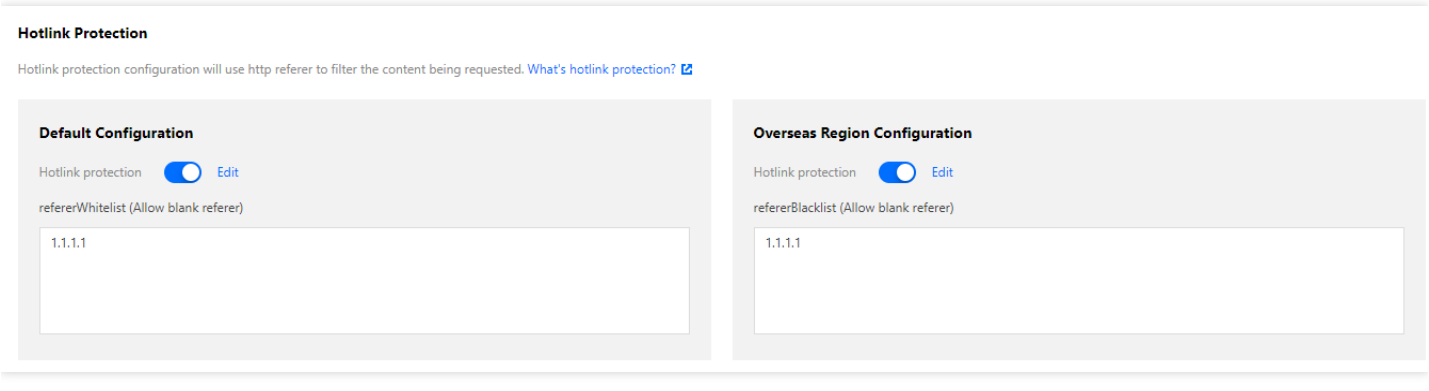
別な設定の追加】をクリックして設定できます。



> ⚠ **注意：**
>
> 地域の特別な設定が追加された後、現在では削除することはできません。設定をオフにして無効にできます。

設定例

アクセラレーションドメイン名 `www.test.com` のリンク不正アクセス防止が次のように設定されている場合、



実際のアクセス状況は次のとおりです。

1.refererが `1.1.1.1` である中国本土のユーザーがリクエストを開始すると、中国本土用に設定されたホワイトリストがヒットし、リクエストされたコンテンツが直接返されます。
2. refererが空である中国本土以外のユーザーがリクエストを開始すると、中国本土以外用に設定されたブラックリストがヒットし、403コードが返されます。

©2013-2022 Tencent Cloud. All rights reserved.

IPブラックリスト/ホワイトリスト設定

最終更新日：：2023-04-23 14:15:52

設定シーン

Tencent Cloud CDNは、業務リソースのアクセス元を制御するためのIPブラックリスト/ホワイトリスト設定機能を提供します。

クライアント側のIPに対してアクセス制御ポリシーを設定することにより、アクセス元を効果的に制御し、悪意のあるIP盗用や攻撃を防ぐことができます。

設定ガイド

設定の確認

CDNコンソールにログインし、メニューバーで**ドメイン名管理**を選択し、ドメイン名の右側の**管理**をクリックすると、ドメイン名設定画面に入ります。第2欄の**アクセス制御**でIPブラックリスト/ホワイトリストの設定を確認できます。デフォルトでは、無効になっています。

設定を有効にする

スイッチをクリックすれば設定を有効にできます。初めて設定を有効にする場合、ルールが存在しなければ、デフォルトではルールを新規作成する画面が表示されます。有効になっている場合、IPブラックリスト/ホワイトリストはルールに設定している優先度で反映されます。一番下にあるルールの優先度が最も高いです。

> 注意：
> ご利用のアクセラレーションドメイン名のサービスエリアがグローバルアクセラレーションの場合、設定されたIPブラックリスト/ホワイトリストはグローバル範囲で有効になります。中国本土と中国本土以外の設定が一致しない場合については、現状ではサポートしていません。

ルールの新規作成/変更

IPブラックリストで**ルールを新規作成**ボタンをクリックすると、新しいIPブラックリスト/ホワイトリスクルールが作成されます。

IP ブラックリスト

クライアントIPがブラックリスト中のIPまたはIPセグメントに該当する場合、CDNノードにアクセスすると、514ステータスコードが直接返されます。

©2013-2022 Tencent Cloud. All rights reserved.

IPホワイトリスト

クライアントIPがホワイトリスト中のIPまたはIPレンジに該当しない場合、CDNノードにアクセスすると、514ステータスコードが直接返されます。

設定ルール

- 同一ルールでは、IPブラックリストとIPホワイトリストのどちらかを選択します。両方とも設定することはできません。
- IPブラックリスト/ホワイトリストはそれぞれ500個まで入力可能です。
- IP:ポートという形のブラックリスト/ホワイトリストがサポートされません。
- IPV4とIPV6予約済みアドレスおよびIPレンジをIPブラックリスト/ホワイトリストとして設定できません。
- ルールの優先度は下にある優先度の方が高いです。
  ルールを変更する場合、ルールの右側の操作欄で、**変更**ボタンをクリックして、ルールの内容を変更できます。

ルール優先度の変更

ルールの優先度を変更する場合、ルールリストの上側で**優先度を変更**をクリックしルールの優先度を変更するモードに切り替えます。以下に示す画面で操作欄でルールの優先度を変更できます。上向き矢印はルールを上へ移動し、下向き矢印はルールを下へ移動します。変更後に、**保存**をクリックすると、変更後のルールの優先度が保存されます。

> 注意：
> リスト下位の方は優先度が上部より高いです。

ルールの削除

ルールを削除する場合、ルールの操作欄で、**削除**ボタンをクリックすると、このルールを削除するか旨の確認ウィンドウが表示されます。OKをクリックすると、ルールが完全に削除されます。

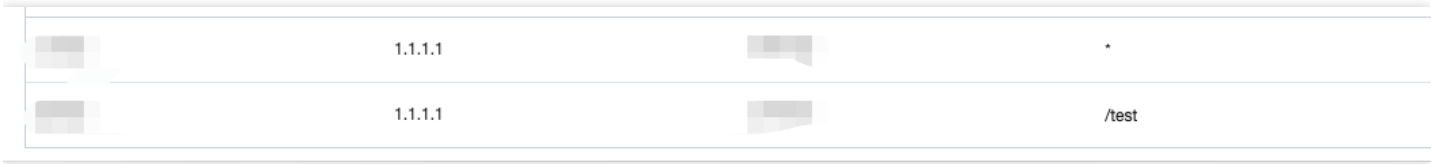
設定を無効にする

設定状態の右側のスイッチをクリックすると、設定が無効になります。設定が無効になっている場合、IPブラックリスト/ホワイトリストルールを変更できるが、現在のネットワークでは直ちに反映されません。設定を有効にすれば、ルールが反映されます。

設定例

アクセラレーションドメイン名 `www.test.com` のIPブラックリスト/ホワイトリストの設定が以下のとおりである場合：

©2013-2022 Tencent Cloud. All rights reserved.



実際のアクセス状況は次のとおりです：

1. クライアント側のIPが1.1.1.1の場合、リソース `https://www.test.com/test/vod.mp4` にアクセスしようとすると、一番下にあるブラックリストルールに該当し、このユーザからのアクセスを許可せず、514を返します。
2. クライアント側のIPが1.1.1.2の場合、リソース `https://www.test.com/test/vod.mp4` にアクセスしようとすると、このIPがブラックリストルールに存在しないため、ブラックリストルールに該当しません。ただし、このユーザがアクセスしようとする内容がホワイトリストルールに該当します。このルールでは、IPが1.1.1.1のユーザからのアクセスのみを許可し、このユーザからのアクセスを許可せず、514を返します。
3. クライアント側のIPが1.1.1.1の場合、リソース `https://www.test.com/vod.mp4` にアクセスしようとすると、ブラックリストルールに該当せず、ホワイトリストルールに該当し、このIPからのアクセスを許可し、アクセス内容を返します。

©2013-2022 Tencent Cloud. All rights reserved.

IPアクセス頻度制限設定

最終更新日：：2021-10-26 16:05:28

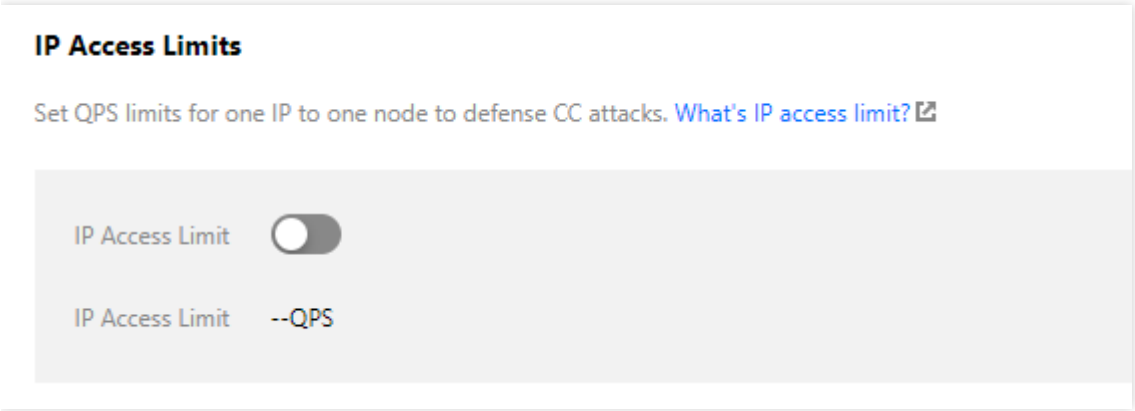
設定シナリオ

Tencent Cloud CDNサービスは、ビジネスソースへのアクセスのソース元を制御するためのIPアクセス頻度制限機能を提供します。クライアントIPからノードへの1秒あたりのアクセス数を制限することにより、高頻度のCC攻撃から防御し、悪意のあるユーザーによる盗用を防止することができます

設定ガイド

設定の確認

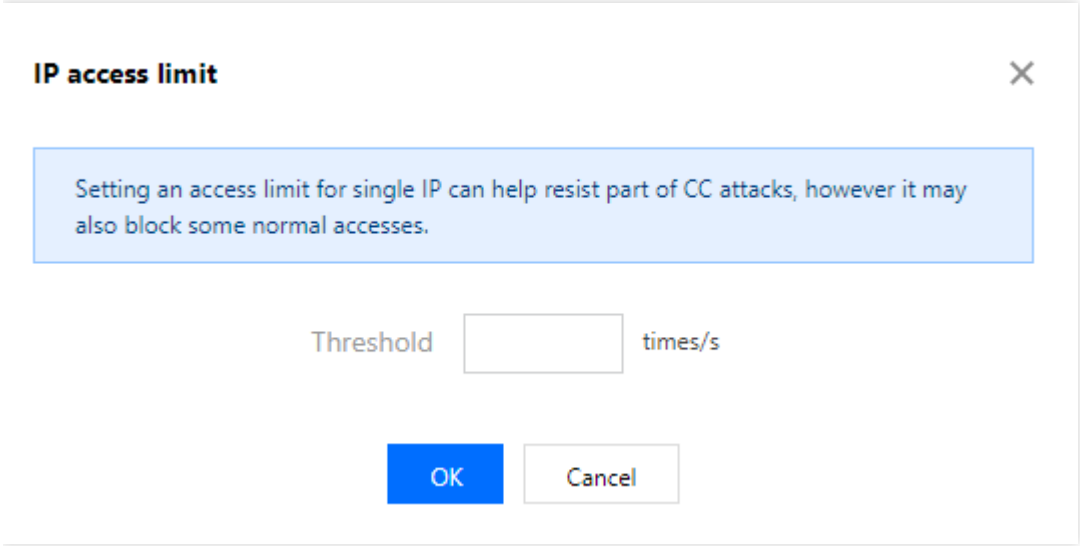
CDNコンソールにログインし、メニューバーで【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。第2欄の【アクセス制御】でIPアクセス頻度制限の設定を確認できます。デフォルトでは設定は無効で、しきい値は空です。



設定を有効にする

スイッチをクリックし、頻度のしきい値を入力して【OK】をクリックすると、IPアクセス頻度制限機能が有効になります。

©2013-2022 Tencent Cloud. All rights reserved.

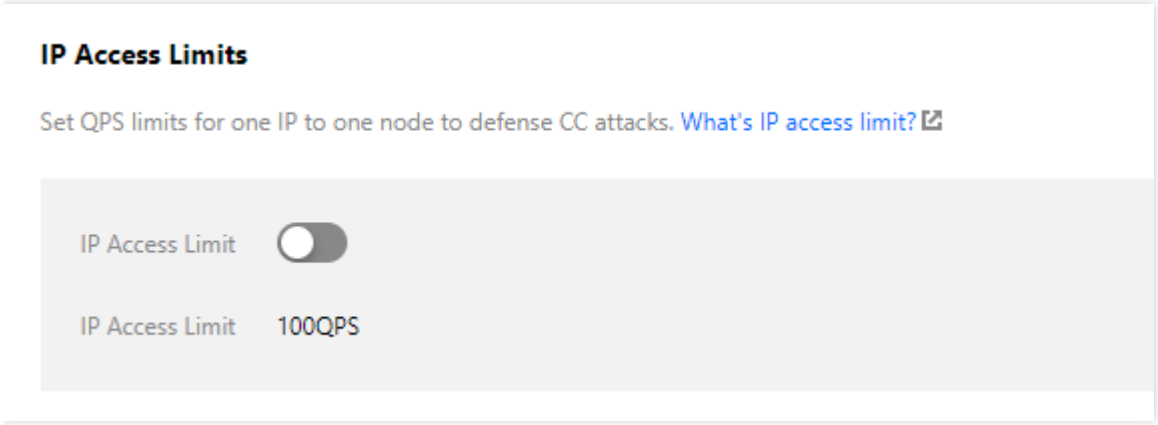


設定についての説明

- 設定を有効にすると、QPS制限を超えるリクエストに対して直接514エラーが返されます。アクセス頻度の制限を低く設定する場合、利用頻度の高いユーザーのアクセスに影響する可能性があります。実際のビジネスニーズや使用シナリオに従って、適切なしきい値を設定してください。
- IPアクセス制限は、単一IPの単一ノードのアクセス回数のみを制限します、悪意のあるユーザーが大量のIPを使用してネットワーク全体のノードを攻撃する場合、この機能は効果的に制御できません。

設定を無効にする

設定スイッチを使用すると、ワンクリックでオフにすることができます。スイッチがオフの場合、既存の設定があっても、この機能は実稼働環境では有効になりません。スイッチがオンの場合、この設定はネットワーク全体で有効になります。



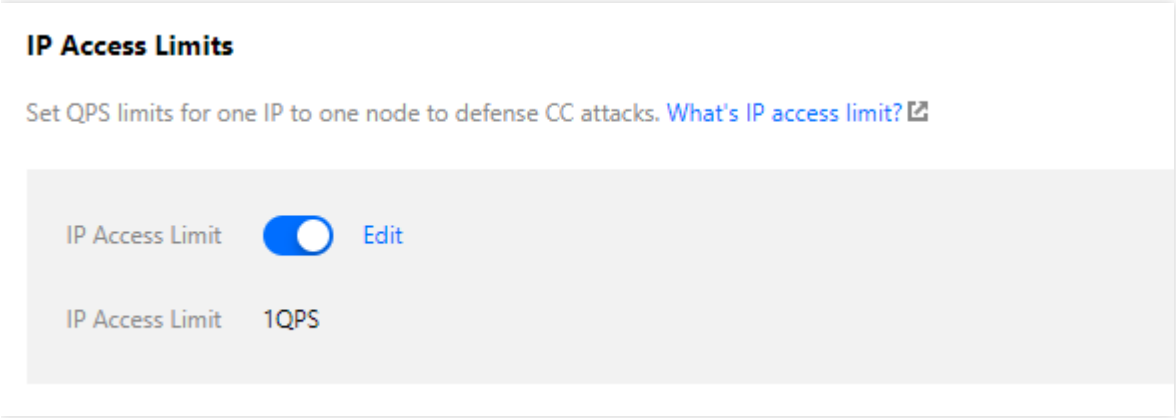
注意：

©2013-2022 Tencent Cloud. All rights reserved.

ご利用のアクセラレーションドメイン名のサービスエリアがグローバルアクセラレーションの場合、設定されたIPアクセス頻度制限はグローバルに有効になります。中国本土と中国本土以外の設定が一致しない場合については、現状ではサポートしていません。

設定例

アクセラレーションドメイン名 `www.test.com` のIPアクセス制限の設定は以下のとおりです。



実際のアクセス状況は次のとおりです。

1. クライアントIPが `1.1.1.1` であるユーザーは、1秒間にリソース `http://www.test.com/1.jpg` を10回リクエストし、いずれもCDNアクセラレーションノードAの同じサーバーにアクセスしました。この場合、このサーバーで10個のアクセスログが生成されましたが、その中の9つはQPS制限を超えたため、ステータスコード「514」が返却されます。
2. クライアントIPが `2.2.2.2` であるユーザーは、1秒間にリソース `http://www.test.com/1.jpg` を2回リクエストします。アクセス要求は、ネットワークの状態により、処理のために2つのCDNアクセラレーションノードに分散される場合があります。 この場合、各ノードはコンテンツを正常に返します。

©2013-2022 Tencent Cloud. All rights reserved.

ビデオのドラッグ構成

最終更新日：：2022-04-14 18:39:38

設定シナリオ

- ビデオドラッグは主にVODシナリオで発生します。ユーザーが再生の進捗状況をドラッグすると、サーバーへ以下のようなリクエストが送信されます。
  `http://www.test.com/test.flv?start=10`
  この場合、10バイト目以降のデータが返されます。VODシナリオのビデオファイルはいずれも各CDNノードにキャッシュされているため、この設定を有効にすることで、各ノードがこのようなリクエストに直接応答することができます。
- ビデオドラッグをオンにするにはパラメータ無視設定を同時にアクティブ化する必要があります。つまりキャッシュキールールの中の全てのルールのパラメータ無視設定を「すべて無視」にし、オリジンサーバーがrangeリクエストをサポートしている必要があります。サポートされるファイル形式はmp4、flv、tsです。

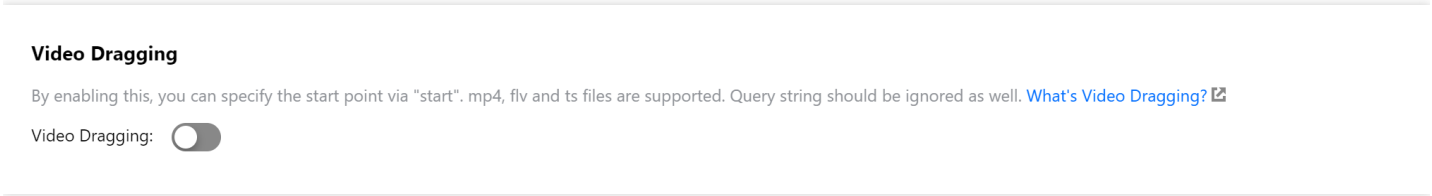
ファイルタイプ	meta情報	start パラメータの説明	リクエストの例
MP4	オリジンサーバーのビデオのmeta情報がファイルのヘッダーに含まれなければなりません。meta情報が最後にあるビデオを対応していません	startパラメータは時刻を示し、単位が秒です、小数点によるミリ秒までの表示を対応しています（例えばstart = 1.01は開始時間が1.01sであることを示している）。CDN はstart表される時刻の前のキーフレーム（現在のstartがキーフレームでない場合）を位置づけます	`http://www.test.com/demo.mp4?start=10` は第10秒から再生を開始することを示しています

©2013-2022 Tencent Cloud. All rights reserved.

ファイルタイプ	meta情報	start パラメータの説明	リクエストの例
FLV	オリジンサーバーのビデオはmeta情報を備えなければなりません	start パラメータはバイトを示しています、CDN はstart表される時刻の前のキーフレーム（現在のstartがキーフレームでない場合）を自動的に位置づけます	`http://www.test.com/demo.flv?start=10` は第10秒から再生を開始することを示しています
TS	特別な要件はありません	startパラメータはバイトを示し、CDNはstartパラメータが示すバイトに自動的に配置されます	`http://www.test.com/demo.ts?start=10` は10番目のバイトから再生を開始することを意味します

設定の確認

CDNコンソールにログインし、左側のメニューバーから【ドメイン名管理】を選択し、業務タイプがストリーミングメディアVODアクセラレーションであるドメイン名を選択して、ドメイン名の設定画面に入ると、Tabの【アクセス制御】画面に【ビデオドラッグ】が表示されます。デフォルトではオフ状態になっています。



©2013-2022 Tencent Cloud. All rights reserved.

認証設定
設定の説明

最終更新日：：2021-01-25 11:38:13

設定シナリオ

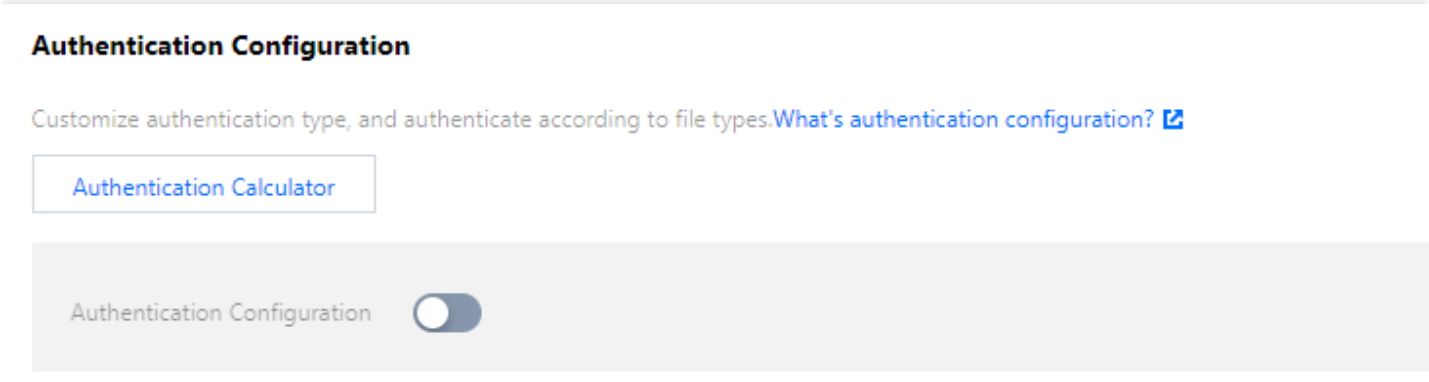
通常、CDNを介して配信されるコンテンツはデフォルトでパブリックリソースであり、ユーザーはURLでコンテンツにアクセスできます。悪意のあるユーザーがコンテンツを盗用して利益を得ることを防ぐために、refererブラックリスト/ホワイトリスト、IPブラックリスト/ホワイトリスト、およびIPアクセス回数制限などのアクセス制御ポリシーに加えて、高度なタイムスタンプ認証を設定することで、盗用から防御することもできます。

> ⚠ **注意：**
>
> タイムスタンプのリンク不正アクセス防止を設定した後、クライアントはリクエストを開始するときに設定に従って署名演算を実行して、サーバーに送信する必要があります。CDNノードはサーバーで署名を検証し、検証が正常に完了した場合にパスさせます。

設定ガイド

設定の確認

CDNコンソールにログインし、左側のナビゲーションメニューバーで【ドメイン管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。【アクセス制御】タブで、認証設定を確認できます。認証設定はデフォルトで無効になっています。

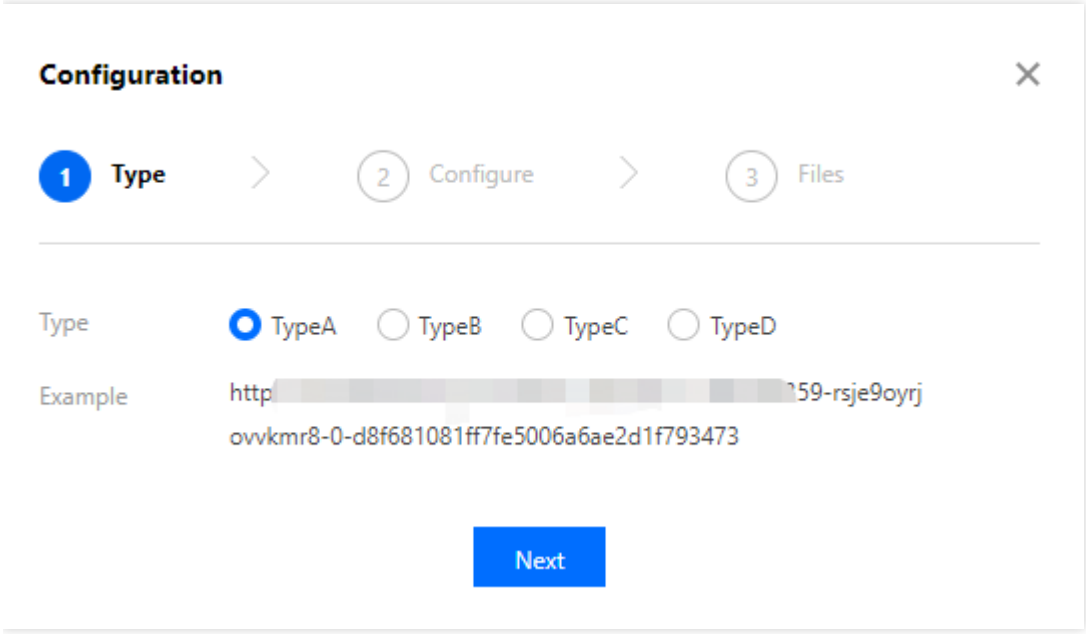


設定の変更

©2013-2022 Tencent Cloud. All rights reserved.

1. 設定を変更する

CDNサービスでは、4種類の認証署名計算モデルをご提供します。上記の【認証計算機】を使用して、各種認証方式と設定後の最終的な成果を確認することもできます。アルゴリズムの詳細説明については、 TypeA、TypeB、TypeC、TypeD をご参照ください。

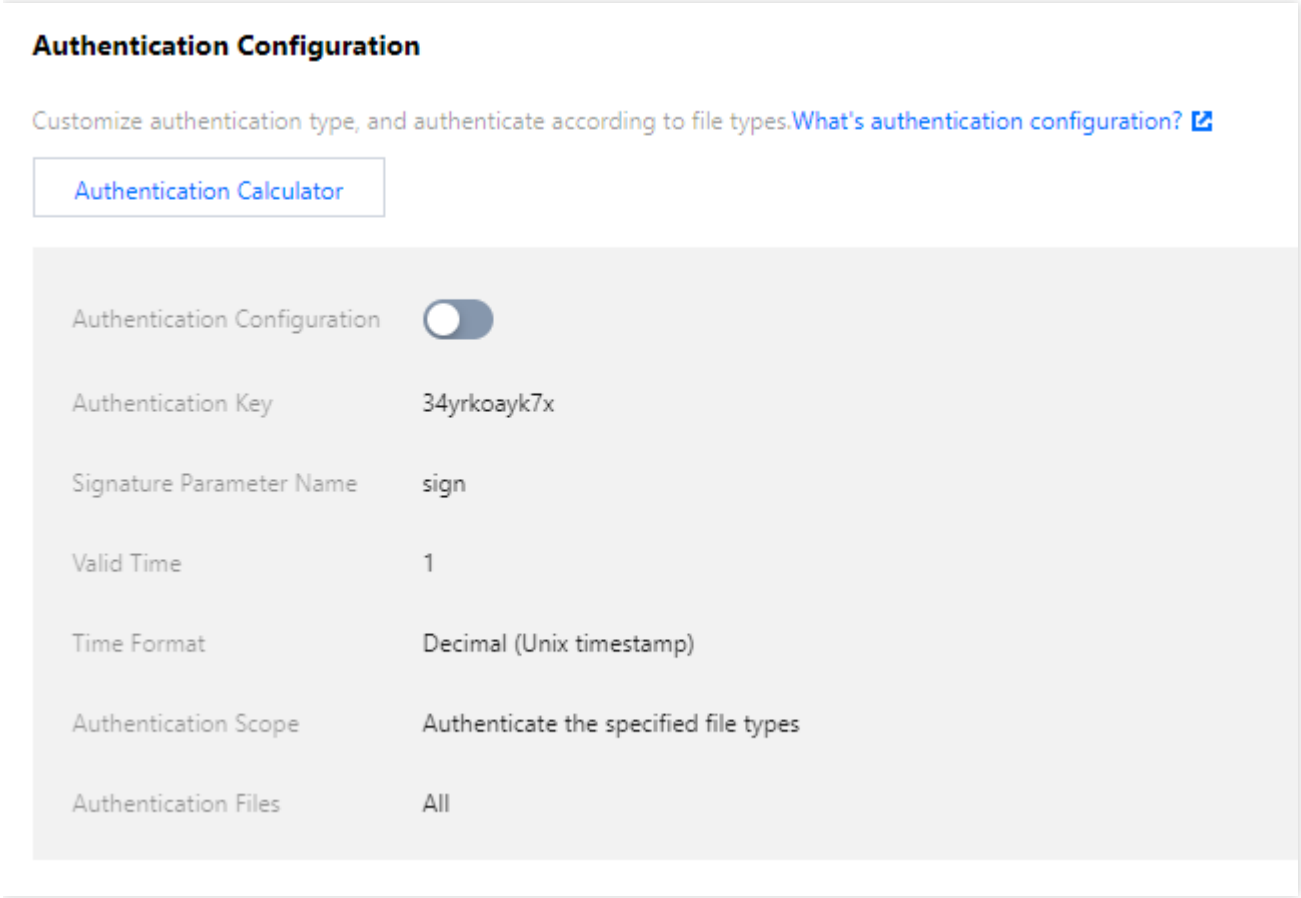


2. 設定を無効にする

認証設定スイッチを切り替えて、この機能を無効にすることができます。スイッチがOFFの場合、既存の設定は実稼働環境では有効になりません。次回ONをクリックすると、ネットワーク全体で設定が有効になる前に、先に設

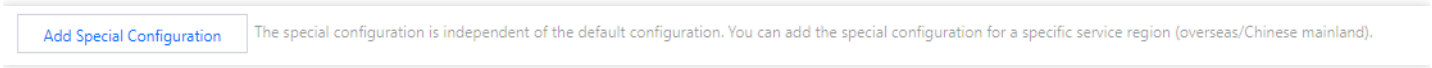
©2013-2022 Tencent Cloud. All rights reserved.

定の2回目の確認が行われます。



3. リージョンの特別な設定

アクセラレーションドメイン名がグローバルアクセラレーション用に設定されており、中国本土内外のアクセラレーションリージョンに異なる認証を設定する場合は、設定の下にある【特別な設定の追加】をクリックして設定できます。

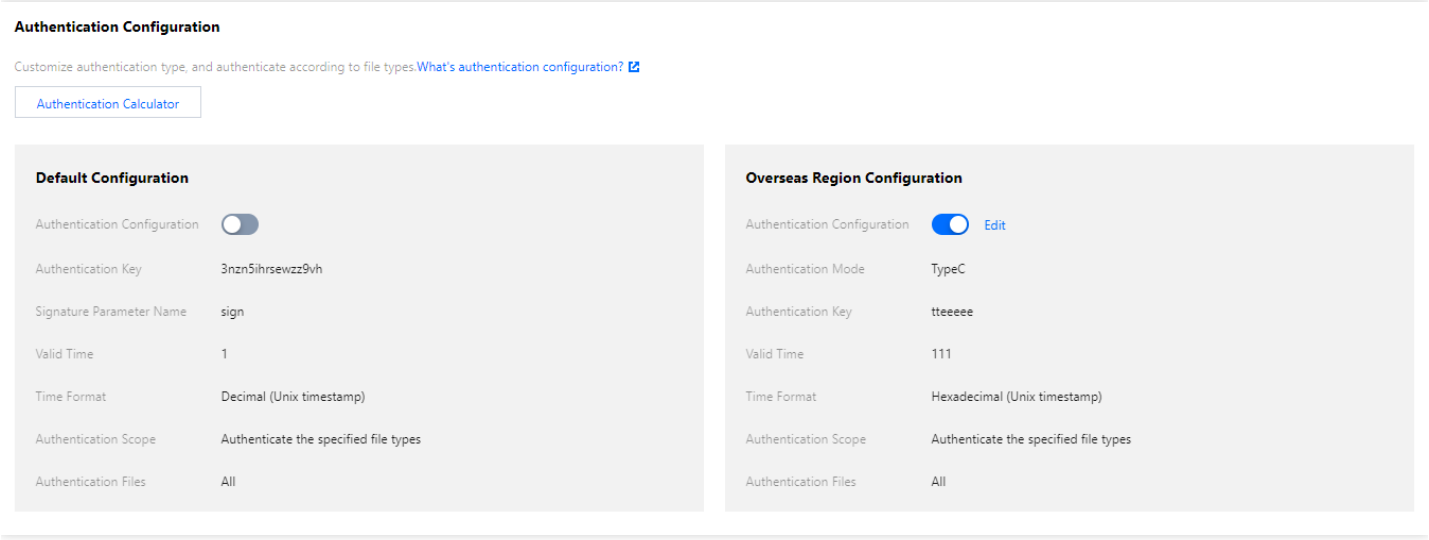


> ⚠ **注意：**
>
> リージョンの特別な設定が追加された後、現在では削除することはできません。設定をオフにして無効にできます。

設定例

©2013-2022 Tencent Cloud. All rights reserved.

ドメイン名 `cloud.tencent.com` がグローバルアクセラレーションドメイン名の場合、認証設定は下記のようになります。



実際の効果は次のようになります。

1. 中国本土のユーザーが、実際にリソース `http://cloud.tencent.com/1.jpg` にアクセスする場合、直接リクエストを開始できます。
2. 中国本土以外のユーザーが、実際にリソース `http://cloud.tencent.com/1.jpg` にアクセスする場合、リクエストURL形式は `http://cloud.tencent.com/509301d10da7b862052927ed7a947f43/5e561139/1.jpg` となります。

サンプルコード

各認証の計算方法は、Python Demoを例に、以下に示します。

```
import requests
import json
import sys
import time
import hashlib

def generate_url(category, ts=None):
url = 'http://www.test.com' # テストドメイン名
path = '/1.txt' # アクセスパス
suffix = '?a=1&b=2' # URLパラメータ
key = 'abc123456789' # 認証キー
now = int(time.mktime(time.strptime(ts, "%Y%m%d%H%M%S")) if ts else time.time())
```

©2013-2022 Tencent Cloud. All rights reserved.

```
# 時間が入力された場合、入力されたtsを使用します。入力されていない場合、現在のtsを使用します。
sign_key = 'key' # url署名フィールド
time_key = 't' # url時間フィールド
ttl_format = 10 # 時間の進数、10または16。typeDのみ対応
if category == 'A': #Type A
ts = now
rand_str = '123abc'
sign = hashlib.md5('%s-%s-%s-%s-%s' % (path, ts, rand_str, 0, key)).hexdigest()
request_url = '%s%s?%s=%s' % (url, path, sign_key, '%s-%s-%s-%s' % (ts, rand_str,
0, sign))
print(request_url)
elif category == 'B': #Type B
ts = time.strftime('%Y%m%d%H%M', time.localtime(now))
sign = hashlib.md5('%s%s%s' % (key, ts, path)).hexdigest()
request_url = '%s/%s/%s%s%s' % (url, ts, sign, path, suffix)
print(request_url)
elif category == 'C': #Type C
ts = hex(now)[2:]
sign = hashlib.md5('%s%s%s' % (key, path, ts)).hexdigest()
request_url = '%s/%s/%s%s%s' % (url, sign, ts, path, suffix)
print(request_url)
elif category == 'D': #Type D
ts = now if ttl_format == 10 else hex(now)[2:]
sign = hashlib.md5('%s%s%s' % (key, path, ts)).hexdigest()
request_url = '%s%s?%s=%s&%s=%s' % (url, path, sign_key, sign, time_key, ts)
print(request_url)


if __name__ == '__main__':
if len(sys.argv) == 1:
print('usage: python generate_url.py A 20200501000000')
args = sys.argv[1:]
generate_url(*args)
```

©2013-2022 Tencent Cloud. All rights reserved.

TypeA

最終更新日：：2021-08-27 11:24:17

アルゴリズムの説明

URL形式へのアクセス

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

> 注意：
> アクセスURLに中国語を含むことはできません。

アルゴリズムの説明

- timestamp：10進数（UNIXタイムスタンプ）です。
- rand：ランダム文字列です。大文字と小文字、数字で構成される0～100桁のランダム文字列です。
- uid:0
- md5hash：MD5（ファイルパス-timestamp-rand-uid-カスタマイズキー）。

リクエスト例

`http://cloud.tencent.com/test.jpg?sign=1582791032-im1acp76sx9sdqe601v-0-dd63f95e739ed4b47427a129d21ef4e3`

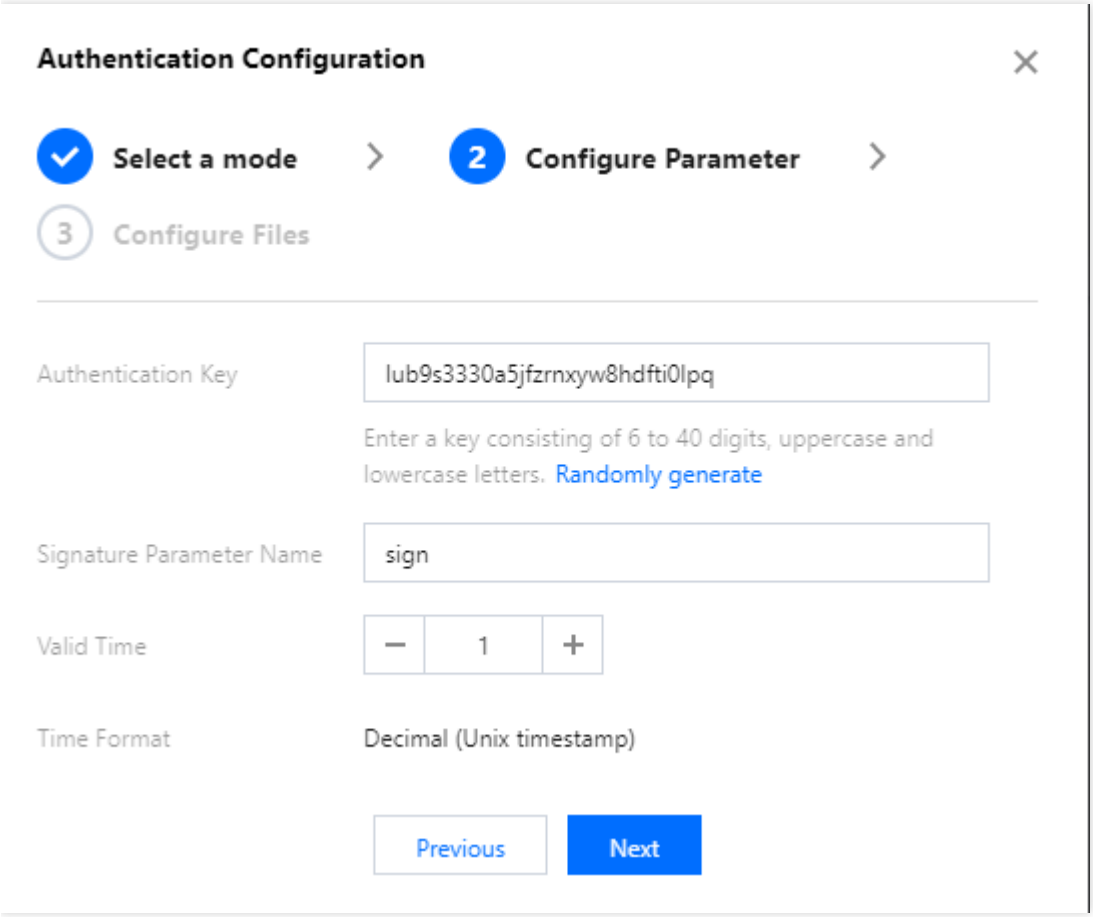
> 注意：
> MD5を計算する際に、リクエストパスが `http://cloud.tencent.com/test.jpg` の場合、MD5を計算する際のパスは `/test.jpg` となります。

設定ガイド

パラメータの説明

©2013-2022 Tencent Cloud. All rights reserved.

TypeAに必要な設定は以下のとおりです：



))

認証キーをカスタマイズする：キーは6～40桁のアルファベットの大文字、小文字と数字で構成されています。キーを大切に保管してください。ユーザー側とサーバー側のみ知っている必要があります。

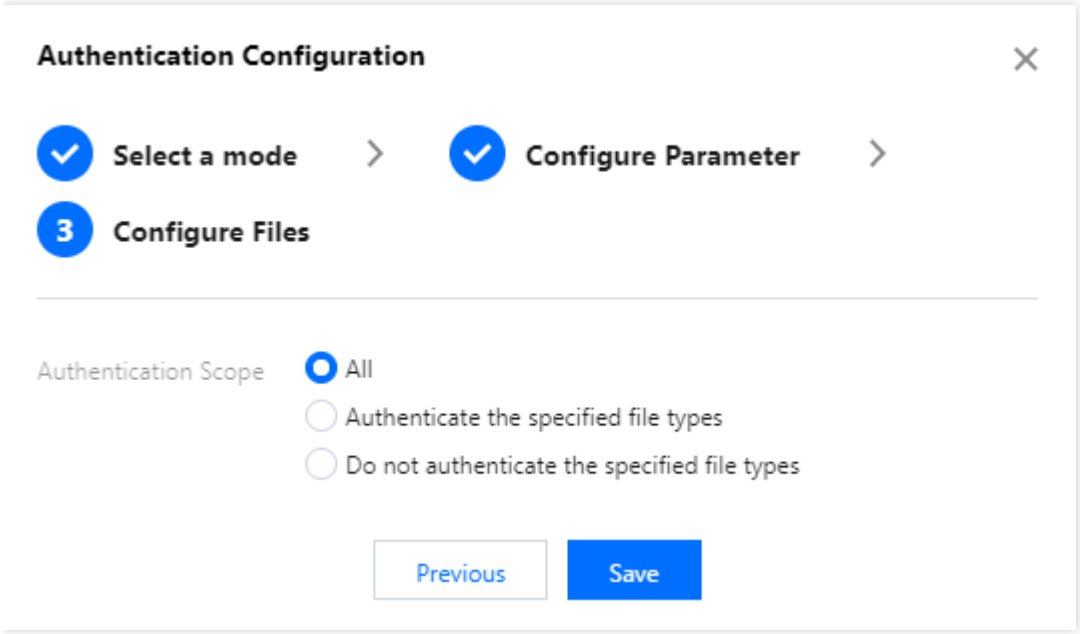
認証パラメータ名をカスタマイズする：例の中のsignを任意の1～100桁のアルファベットの大文字、小文字、数字、またはアンダーバーを組み合わせたパラメータ名に置き換え、CDNがリクエストを受信した後 、指定された認証パラメータに基づいて対応する値を取得し、MD5の計算を行い、それが伝達されたmd5hash値と一致すれば、認証は検証にパスし、検証にパスしない場合は403コードを直接返します。

有効時間をカスタマイズする：リクエストに含まれるtimestampと、設定された有効時間を介して、現在の時刻と比較し、リクエストが期限切れかどうかを判定します。期限切れの場合、403コードを直接返します。有効時間の単位は秒で、最大630720000秒まで設定可能です。

有効化対象

キー、パラメータ名、および期限切れ時間を設定した後、必要に応じて認証対象を指定でき、以下の3つのモードをサポートします。

©2013-2022 Tencent Cloud. All rights reserved.



- 指定されたドメイン名下のすべてのファイルを認証が必要なように設定できます。
- 指定されたタイプのファイルを認証不要に、他のすべてのファイルは認証される必要があります。
- 指定されたタイプのファイルは認証される必要があります。

注意事項

キャッシュのヒット率

TypeA認証方式が有効になっているドメイン名は、アクセスURLに認証パラメータが保持されます。CDNノードでリソースをキャッシュする時、対応するパラメータが自動的に無視され、ドメイン名キャッシュのヒット率には影響しません。

> 注意：
> 設定後は対応するパラメータを自動的に無視することで、設定された認証パラメータを無視することになり、認証範囲内のファイルのキャッシュキーに影響を与え、ここでの優先レベルは【キャッシュ設定 - キャッシュキールール設定】のキャッシュキールールを上回ることになります。
> たとえば、ここでのTypeA設定が：認証パラメータ：sign - 認証範囲：jpgの場合、たとえ【キャッシュ設定 - キャッシュキールール設定】が「すべてのファイル - パラメータを無視しない」となっていても、jpgタイプのファイルについては「sign」パラメータを自動的に無視します。

back-to-originのポリシー

TypeA認証方式が有効になっているドメイン名は、アクセスする際の形式が次のとおりです。

©2013-2022 Tencent Cloud. All rights reserved.

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

認証が完了した後、命中されたCDNノードがない場合、ノードはback to originリクエストを送信します。形式はアクセスリクエストと一致しており、signパラメータは保持されます。オリジンサーバーは必要に応じて無視されるか、２次検証が行われます。

©2013-2022 Tencent Cloud. All rights reserved.

TypeB

最終更新日：：2021-01-25 14:36:36

アルゴリズムの説明

アクセスURLの形式

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

アルゴリズムの説明

- timestamp：YYYYMMDDHHMM形式のタイムスタンプ。
- md5hash：MD5（カスタムキー+タイムスタンプ+ファイルパス）。

リクエスト例

`http://cloud.tencent.com/202003032017/b91bad39a0f9c885ddebd6b6164de3c4/test.jpg`

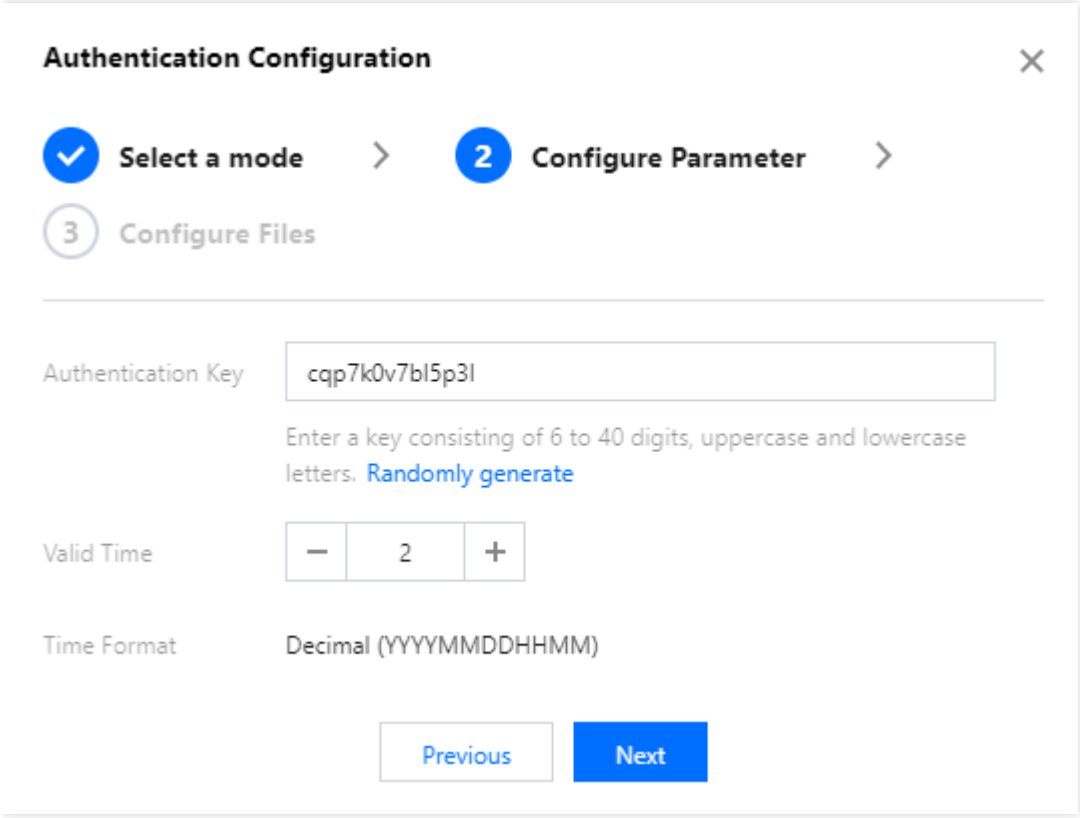
> ⚠ **注意：**
>
> MD5値を計算する際に、もしリクエストパスが `http://cloud.tencent.com/test.jpg` の場合、MD5を計算する際のパスは `/test.jpg` となります。

設定ガイド

パラメータの説明

©2013-2022 Tencent Cloud. All rights reserved.

TypeBに必要な設定は以下のとおりです。

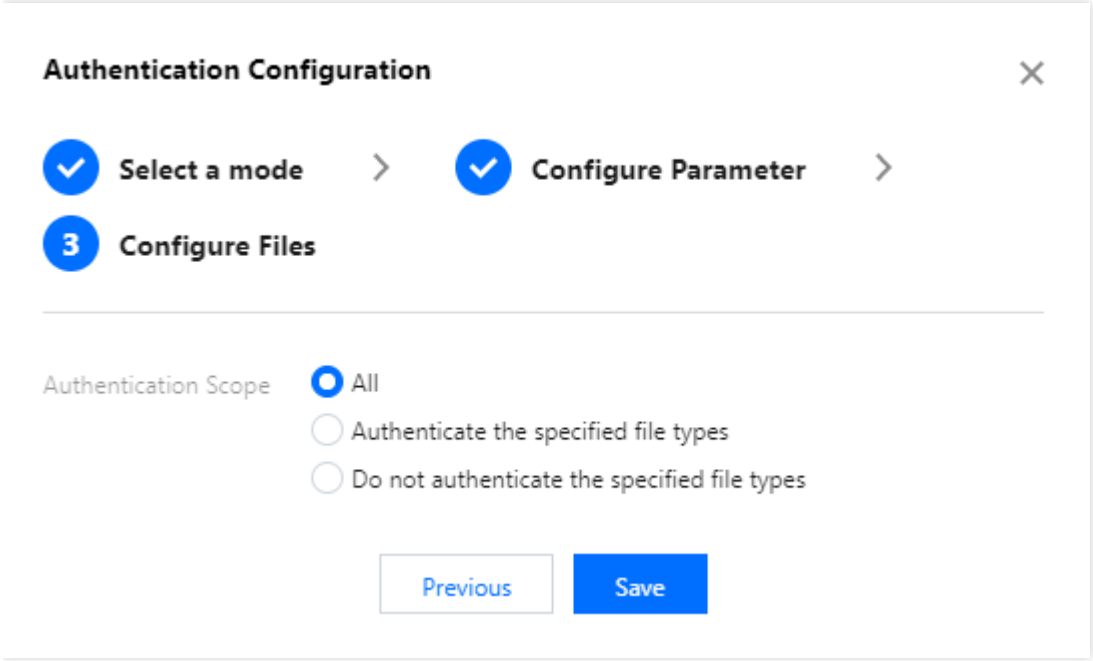


認証キーをカスタマイズ： キーは6～32文字の大文字と小文字および数字で構成されています。キーを大切に保管してください。ユーザー側とサーバー側のみ知っている必要があります。
有効時間をカスタマイズ：リクエストパス中のタイムスタンプ値と設定された有効時間を介して、現在の時刻と比較し、リクエストの有効期限が切れているかどうかが判断されます。有効期限が切れた場合は、403エラーが直接返されます。

オブジェクト

キー、パラメータ名、および有効期間を設定した後、必要に応じて認証オブジェクトを指定できます。次の3つの認証モードがサポートされています。

©2013-2022 Tencent Cloud. All rights reserved.



- 指定されたドメイン名配下のすべてのファイルは認証される必要があります。
- 指定されたタイプのファイルを認証不要に、他のすべてのファイルは認証される必要があります。
- 指定されたタイプのファイルは認証される必要があります。

注意事項

キャッシュヒット率

TypeB認証方式が有効になっているドメイン名は、アクセスURLパスに署名とタイムスタンプが保持されます。CDNノードでリソースをキャッシュする時、パス内のフィールドが自動的に無視され、キャッシュヒット率には影響しません。

back-to-originポリシー

TypeB認証方式が有効になっているドメイン名のアクセス形式は次のとおりです。

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

認証が成功した後、CDNノードでヒットが見つからない場合、ノードはback-to-originリクエストを送信します。**back-to-originリクエストは、md5hashとタイムスタンプがパスから削除されます**。オリジンサーバーは認証情報を処理する必要はありません。

©2013-2022 Tencent Cloud. All rights reserved.

TypeC

最終更新日：：2022-09-29 19:18:33

サイトのリソースが違法なサイトによってダウンロードされ、盗用されないよう保護するために、必要に応じてType ABCDの4つの認証方式の1つを選択できます。ここでは、Type Cの各パラメータフィールドと原理について詳しくご説明します。

アルゴリズムの説明

- **アクセスURLの形式**
  `http://DomainName/md5hash/timestamp/FileName`

  > 注意：
  > アクセスURLに中国語を含むことはできません。

- **認証フィールドの説明**

フィールド	説明
DomainName	CDNドメイン名。
Filename	リソースのアクセスパスは、認証時にFilenameがスラッシュ（ `/` ）で始まる必要があります。
timestamp	サーバーが認証URLを発行する時間は、16進数の整数型の正数のUnixタイムスタンプを使用し、UTC時間1970年01月01日00時00分00秒から現在の総秒数までで、その定義と所在するタイムゾーンは関係ありません。
md5hash	MD5アルゴリズムによって計算した固定長は32桁の文字列です。具体的な計算公式は次のとおりです： • md5hash = md5sum(pkeytimestampuri) パラメータの間にはいかなる符号もありません • pkey： カスタムキー：6 ～40桁のアルファベットの大文字、小文字と数字で構成されています。キーを大切に保管してください。クライアントとサーバーのみ知っている必要があります。 • uri リソースのアクセスパスはスラッシュ（/）で始まる必要があります。 • timestamp: 値は上記のtimestampです。

- **認証ロジックの説明**
  CDNサーバーはクライアントからのリクエストを受けると、url内のtimestampパラメータ+認証URLの有効期限

©2013-2022 Tencent Cloud. All rights reserved.

を解析して現在の時間と比較します。

i. timestamp + 認証URLの有効期限が現在の時間より小さい場合、サーバーは期限切れによる失効と判定し、HTTP 403エラーが返されます。
ii. timestamp+認証URLの有効期限が現在の時間より大きい場合、MD5アルゴリズムを使用してmd5hashの値を計算し、さらに計算したmd5hash値とurlで渡したmd5hash値を比較し、一致する場合はそのままにし、一致しない場合はHTTP 403エラーを返します。

設定ガイド

Type-Cで認証する設定を例として、パラメータおよびコンソールを以下のように設定します。

- **フィールド設定**
  - 認証キー：dimtm5evg50ijsx2hvuwyfoiu65
  - 認証URLの有効期間：1s
  - 署名アルゴリズムがサーバー認証URLを発行した時間：2020年02月27日16:10:32（UTC+8）は、10進数の整数値1582791032(timestamp)に変換されます
  - オリジンサーバーアドレスのリクエスト： `http://cloud.tencent.com/test.jpg`

- 発行プロセス
  - 認証パラメータの取得

パラメータ	値
uri	リソースのアクセスパスは /test.jpgです
timestamp	1582791032
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - 署名文字列の結合：dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg
  - 署名文字列のmd5値の計算：md5hash = md5sum(pkeytimestampuri) =md5sum(dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg) = ea68b93ac23ebbc6eebf7f163c6e9c4c

- **認証URLの発行：**

`http://cloud.tencent.com/ea68b93ac23ebbc6eebf7f163c6e9c4c/1582791032/test.jpg`
クライアントがURLの暗号化によってアクセスする場合、CDNサーバーが計算したmd5hash値とアクセスリクエスト内にあるmd5hash値が同じであれば、いずれもea68b93ac23ebbc6eebf7f163c6e9c4cとなり、認証に合格し、そうでなければ認証に失敗します。

©2013-2022 Tencent Cloud. All rights reserved.

注意事項

キャッシュのヒット率

TypeC認証方式が有効になっているドメイン名は、URLへのアクセスパスに署名とタイムスタンプが保持されます。CDNノードでリソースをキャッシュする時、認証パスが自動的に無視され、ドメイン名キャッシュのヒット率には影響しません。

back-to-originのポリシー

TypeC認証方式が有効になっているドメイン名について、アクセスする際の形式は次のとおりです。

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

認証にパスした後、ヒットしたCDNノードがない場合、ノードはback-to-originリクエストを送信します。**back-to-originリクエストは、パス中のmd5hashとtimestampパス**を削除します。オリジンサーバーは特別な処理を行う必要はありません。

©2013-2022 Tencent Cloud. All rights reserved.

TypeD

最終更新日：：2021-01-25 14:52:24

アルゴリズムの説明

URL形式へのアクセス

`http://DomainName/FileName?sign=md5hash&t=timestamp`

アルゴリズムの説明

- timestamp：10進数/16進数（UNIXタイムスタンプ）はオプションです。
- md5hash：MD5（カスタマイズキー+ファイルパス+timestamp）。

リクエスト例

`http://cloud.tenloud.tencent.com/test.jpg?sign=0f8201d814dfaf64cf54e74c5f7dbcb0&t=1582791032`

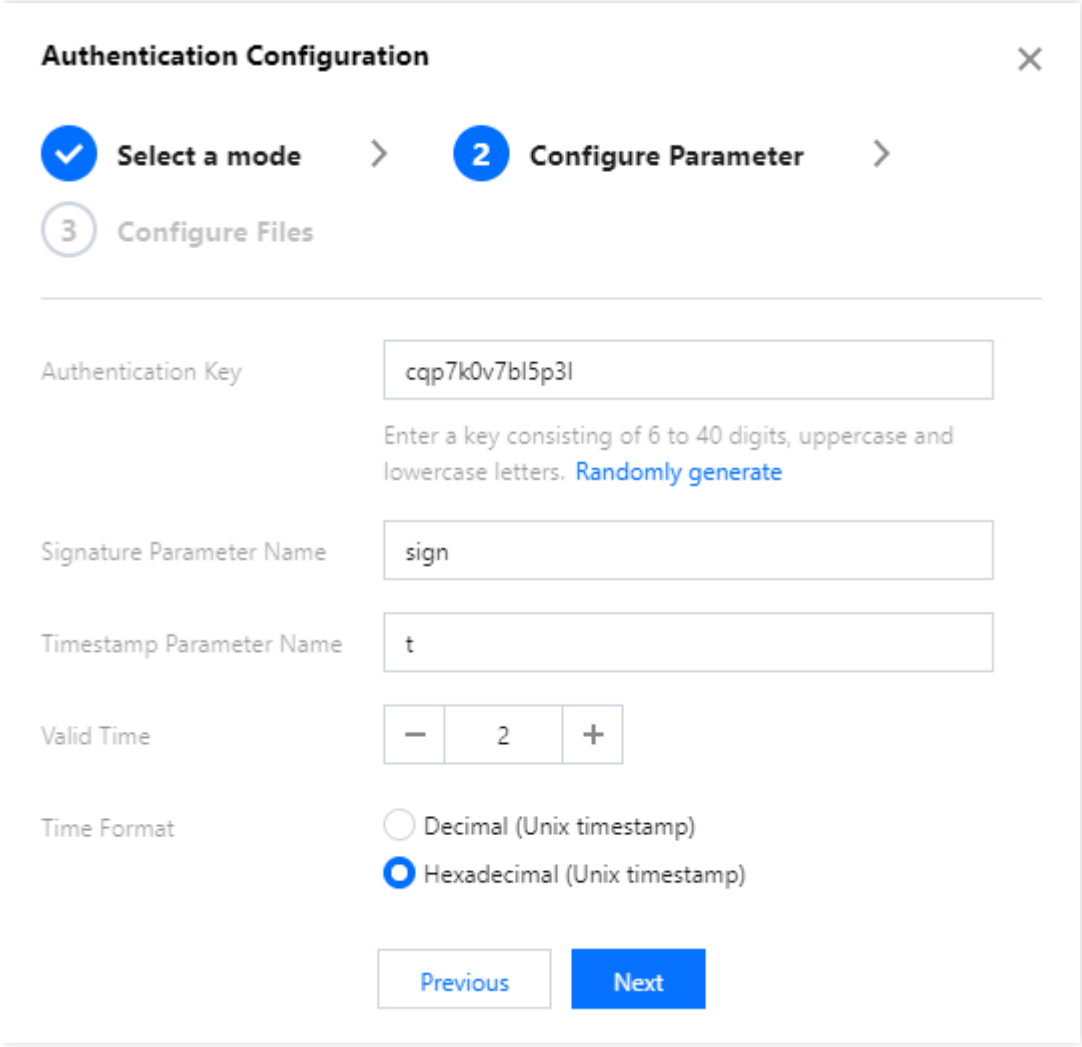
> ⚠ **注意：**
>
> MD5を計算する際に、もしリクエストパスが `http://cloud.tencent.com/test.jpg` の場合、MD5を計算する際のパスは `/test.jpg` となります。

設定ガイド

パラメータの説明

©2013-2022 Tencent Cloud. All rights reserved.

TypeDに必要な設定は以下のとおりです。

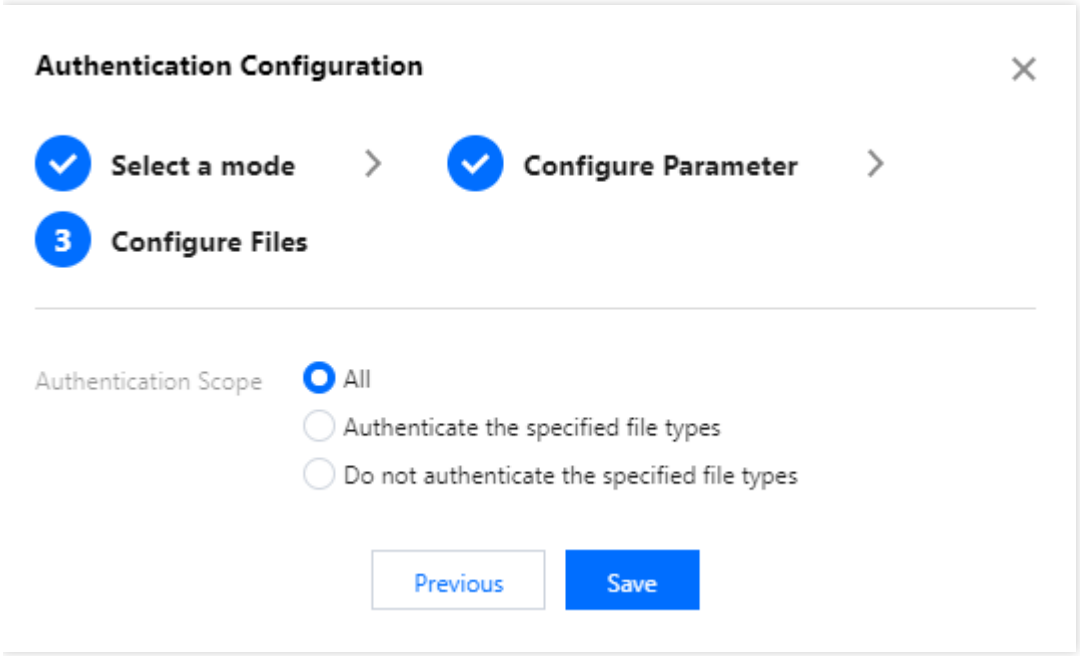


認証キーをカスタマイズする： キーは6～32桁の大文字と小文字と数字で構成されています。キーを大切に保管してください。ユーザー側とサーバー側のみ知っている必要があります。
カスタマイズ認証パラメータ名とタイムスタンプパラメータ名：上記例のsignを、1～100桁の大文字、小文字、数字、またはアンダースコアで構成されるパラメータ名に置き換えます。リクエストを受信すると、CDNは指定された署名パラメータにより対応する値を取り出し、MD5計算を実行します。渡されたmd5hash値にマッチする場合、署名の検証は成功し、検証が失敗した場合は、直接403を返します。
有効時間をカスタマイズ：タイムスタンプパラメータ名でtimestamp値と設定された有効時間を介して、現在の時刻と比較し、リクエストが期限切れかどうかを判定します。期限切れの場合、直接403を返します。有効時間の単位は秒です。

有効化対象

キー、パラメータ名、および期限切れ時間を設定した後、必要に応じて認証対象を指定でき、以下の3つのモードをサポートします。

©2013-2022 Tencent Cloud. All rights reserved.



- 指定されたドメイン名配下のすべてのファイルを認証が必要なように設定できます。
- 指定されたタイプのファイルを認証不要に、他のすべてのファイルを認証が必要なように設定できます。
- 指定されたタイプのファイルを認証させることができます。

注意事項

キャッシュ命中率

TypeD認証方式が有効になっているドメイン名は、URLへのアクセスに認証パラメータが保持されます。CDNノードでリソースをキャッシュする時、対応するパラメータが自動的に無視され、ドメイン名キャッシュの命中率には影響しません。

！対応するパラメータは設定後に自動的に無視されるため、すなわち、設定された認証パラメータとタイムスタンプパラメータがフィルタリングされるため、認証範囲内のファイルのキャッシュキーに影響し、また、ここでの優先順位は【キャッシュ設定 - キャッシュキールール設定】でのキャッシュキールールより高くなります。
たとえば、ここでのTypeDは、「認証パラメータ：sigh - タイムスタンプパラメータ：jpg」に設定されている場合、【キャッシュ設定 - キャッシュキールール設定】で「すべてのファイル - パラメータはフィルタリングされない」と設定されている場合でも、jpgファイルは自動的に「sign」と「t」パラメータをフィルタリングします。

©2013-2022 Tencent Cloud. All rights reserved.

back-to-originのポリシー

TypeD認証方式が有効になっているドメイン名は、アクセスする際の形式が次のとおりです。

```
http://DomainName/FileName?sign=md5hash&t=timestamp
```

認証が完了した後、命中されたCDNノードがない場合、ノードはback-to-originリクエストを送信します。**形式はアクセスリクエストと一致しており、sign/tパラメータは保持されます**。オリジンサーバーは必要に応じて無視されるか、２次検証が行われます。

©2013-2022 Tencent Cloud. All rights reserved.

UAブラックリスト/ホワイトリスト設定

最終更新日：：2021-01-07 15:05:04

設定シナリオ

Tencent Cloud CDNは、User-Agentのブラックリスト・ホワイトリストのルールを設定することにより、アクセス制御を実装できます。
ユーザーのHTTPリクエストヘッダーでUser-Agentのルールを判断することにより、必要に応じてユーザーからのアクセスを許可するか、拒否できます。

設定ガイド

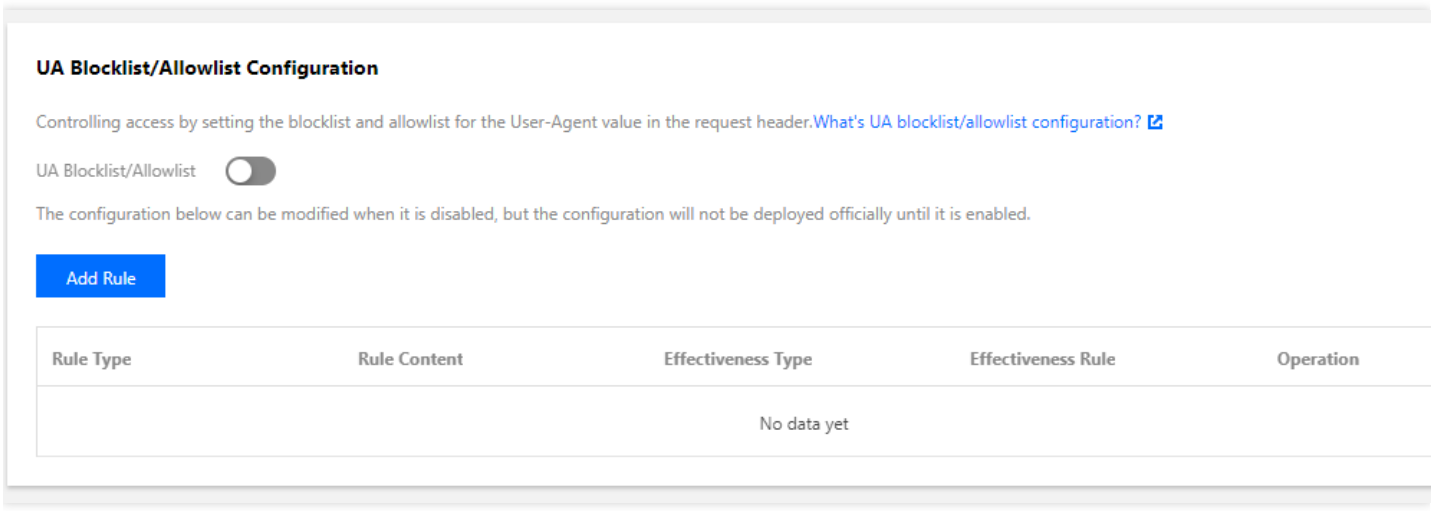
設定の制約

- すべてをブラックリストに、または、すべてをホワイトリストにのみ設定できます。ブラックリストとホワイトリストのルールを同時に設定することはできません。
- 最大10件までのブラックリストルールまたはホワイトリストルールを設定できます。
- ルールの内容はワイルドカード文字 `*` をサポートし、複数の値の場合は `|` て区切ります。
- 有効化タイプは、すべてのファイル、ファイルタイプ、ファイルディレクトリ、および指定されたファイルパスの4つのモードをサポートします。現在、正規表現のマッチングはサポートされていません。

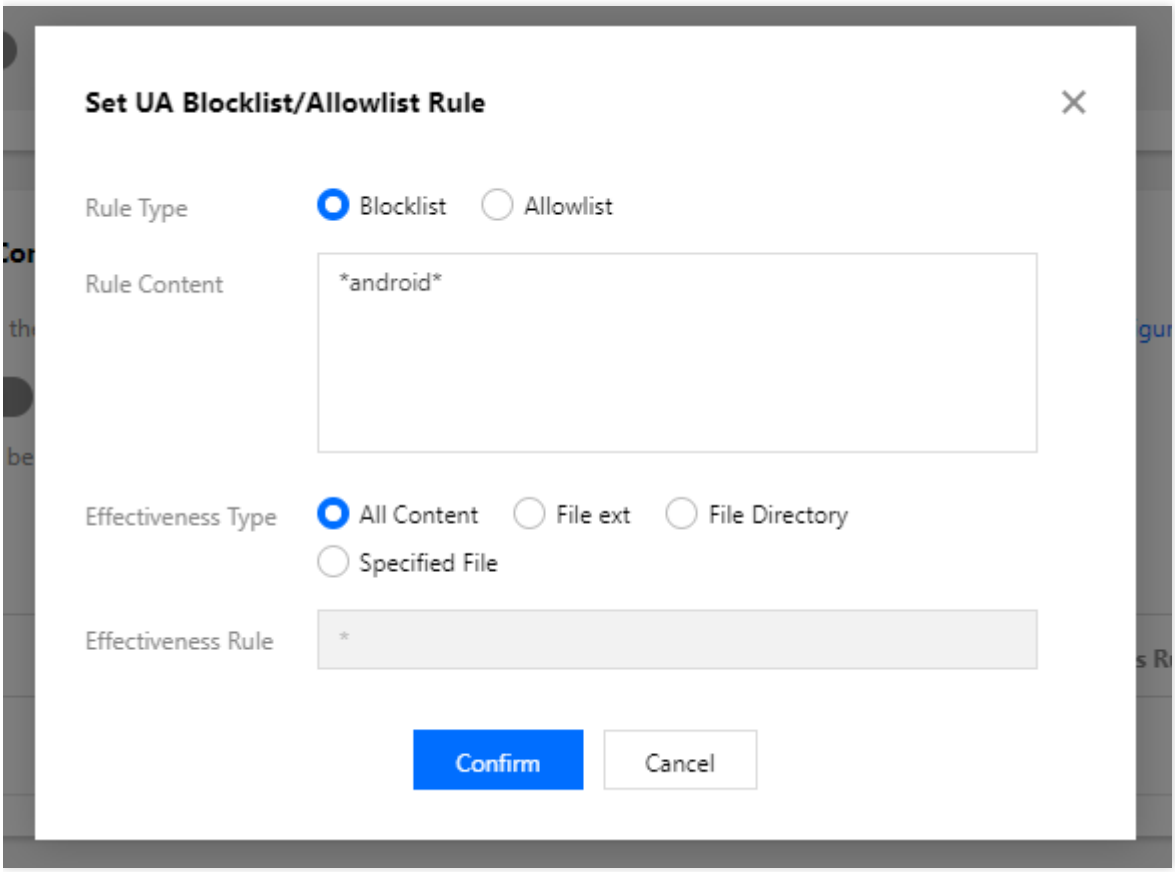
設定についての説明

CDNコンソールにログインし、メニューバーで【ドメイン管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。第2欄の【アクセス制御】でUAブラックリスト・ホワイトリスト設定を確認できます。デフォルト設定は無効です。

©2013-2022 Tencent Cloud. All rights reserved.



無効の状態で、【Add Rule】をクリックして、必要に応じてブラック（ホワイト）リストを1件ずつ追加できます。

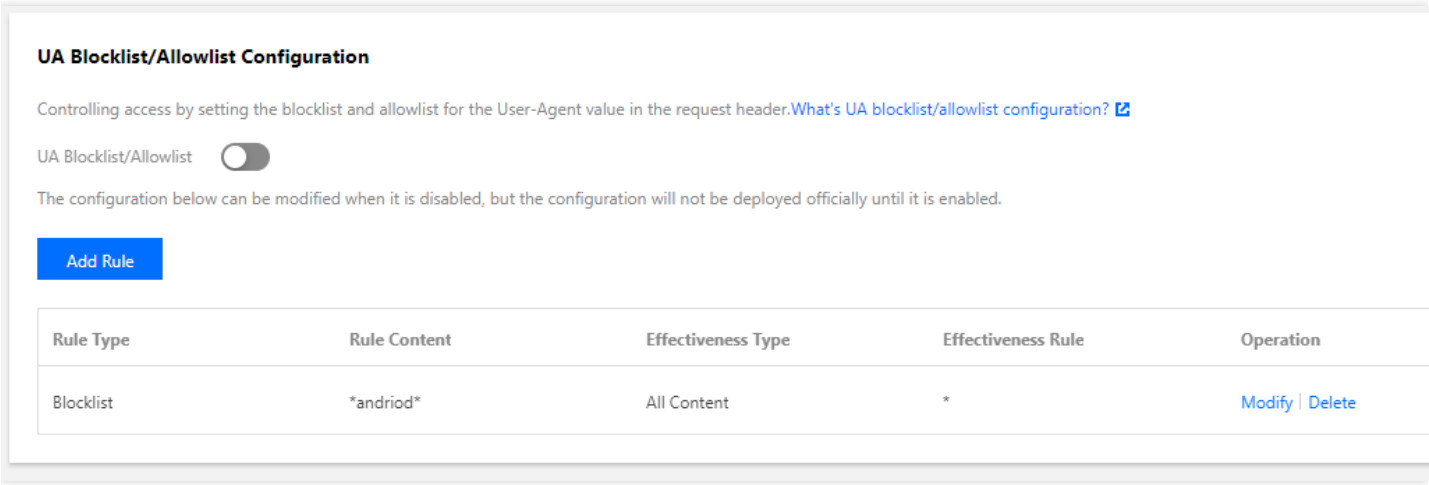


⚠ 注意：

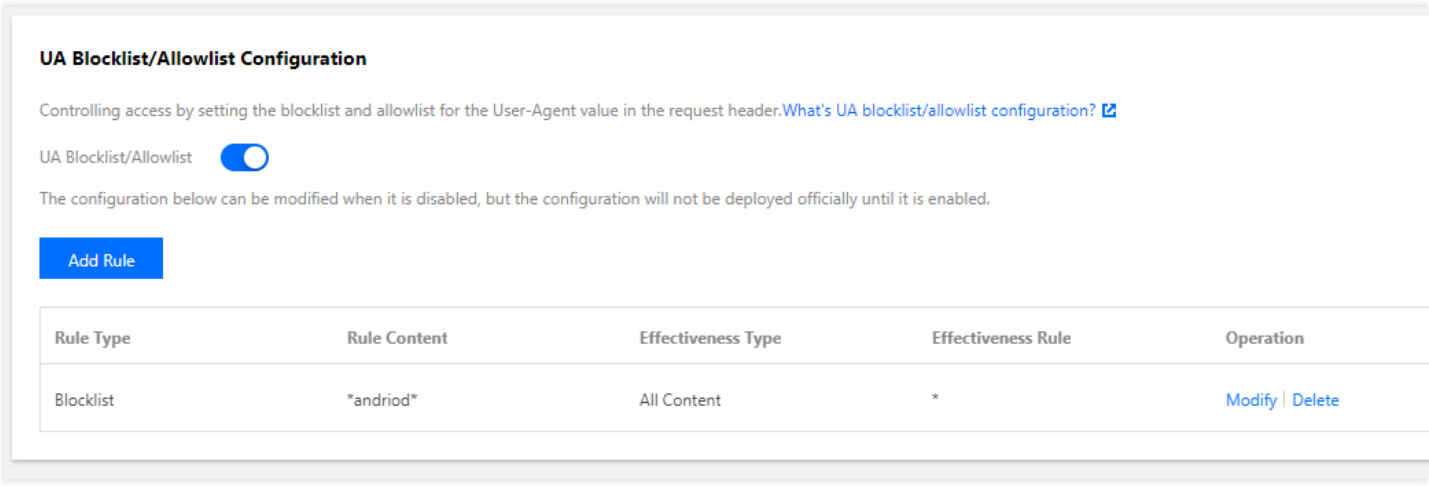
1. ワイルドカード `*` のみがサポートされており、現在、他の正規表現はサポートされていません。
2. `*` がない場合、他のすべての文字は完全一致となります。

©2013-2022 Tencent Cloud. All rights reserved.

ルールが追加された後も、全体の設定は無効の状態となるため、ライブ ネットワーク上のサービスには影響しません。

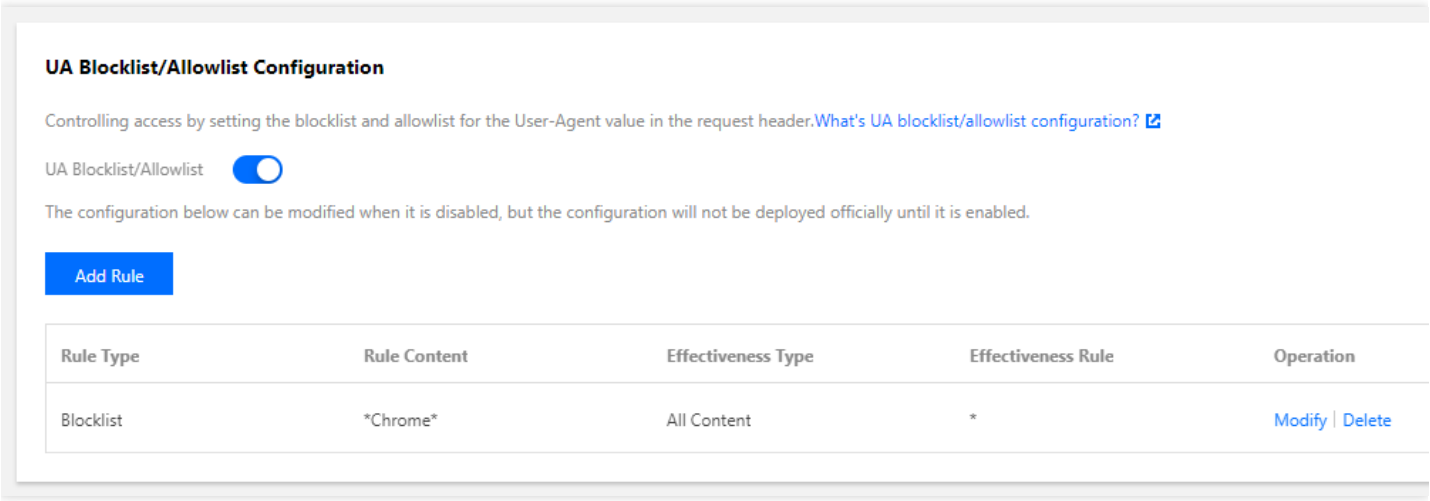


【UA Blocklist/Allowlist】ボタンをクリックすると、設定済みのブラック（ホワイト）リストはライブネットワークに配信されます。



設定例

アクセラレーションドメイン名 `cloud.tencent.com` のUAブラックリスト・ホワイトリストが以下のように設定されている場合、



HTTP Request HeaderのUser-Agentが以下のような場合、

```
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
```

ブラックリストに該当し、403が返されます。

©2013-2022 Tencent Cloud. All rights reserved.

下り速度制限の設定

最終更新日：：2023-03-14 15:13:28

設定シーン

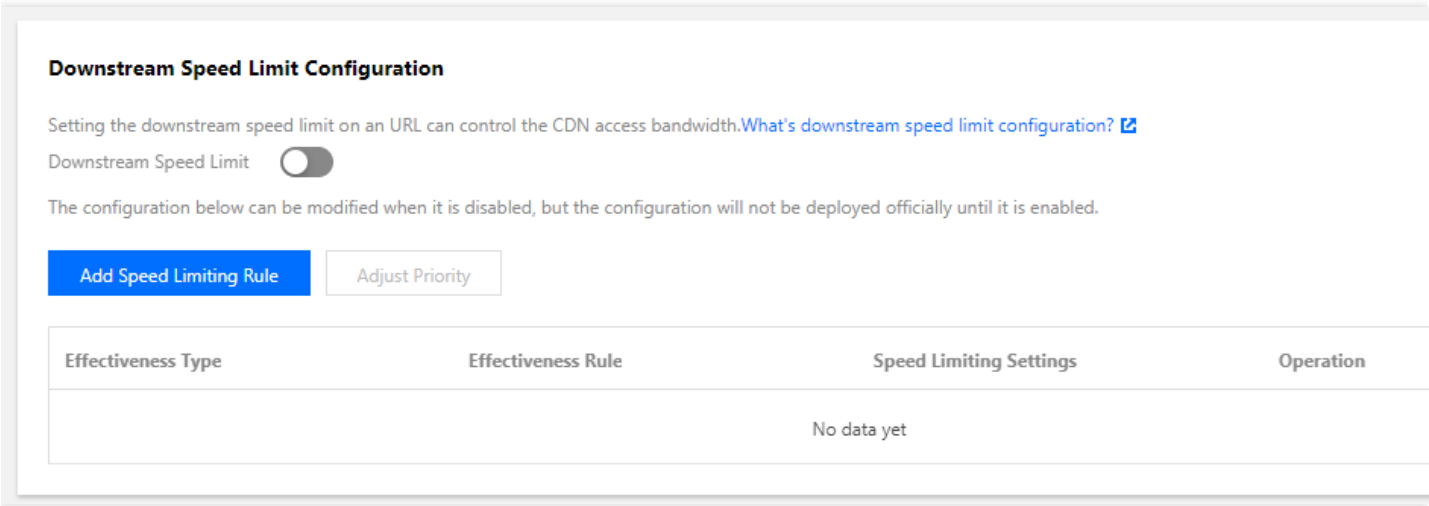
Tencent Cloud CDNは最大ダウンストリーム速度の設定を提供し、サーバー側のシングルリンクの最大ダウンストリーム速度を設定できます。
ダウンストリーム速度を制限することで、CDNピーク帯域幅をある程度制御できます。これは電子商取引の販促、ゲームの新しいバージョンのリリースまたは更新などの運用シーンによく使用されます。

> 注意：
> 正常に最大ダウンストリーム速度を設定した場合、このドメイン名にアクセスするすべてのユーザが制限され、ユーザビリティとCDNアクセラレーションの効果にある程度影響しますので、ご注意ください。

設定ガイド

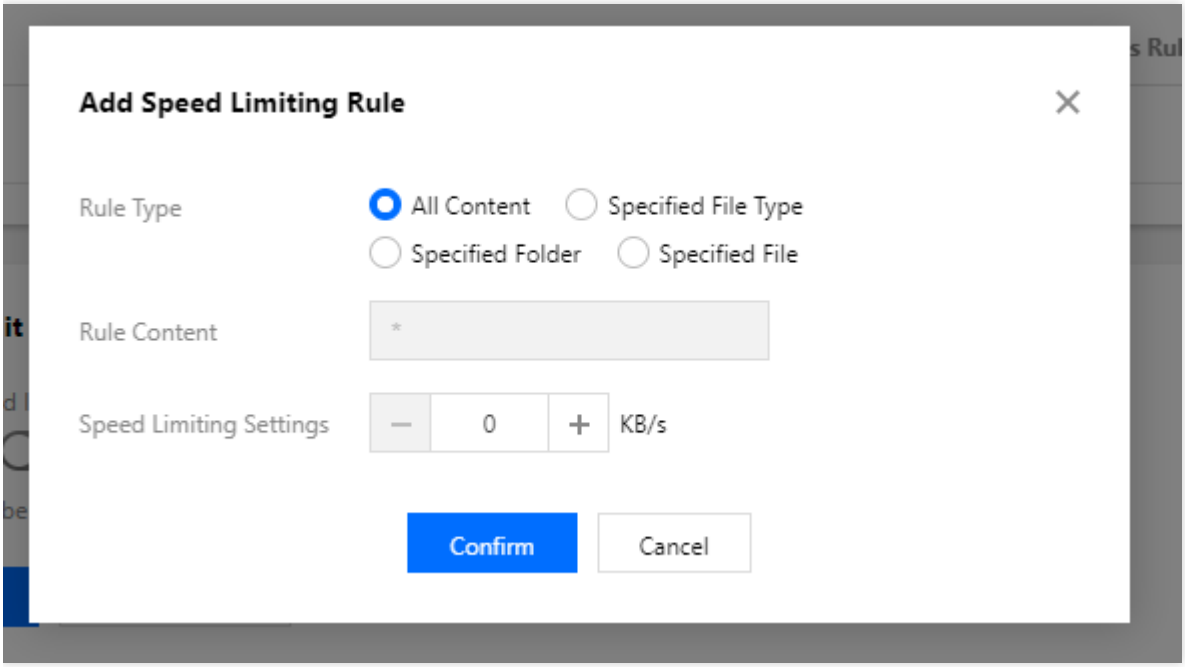
設定の確認

CDNコンソールにログインし、メニューバーで**ドメイン名管理**を選択し、ドメイン名の右側にある**管理**をクリックすると、ドメイン名設定画面に入ります。第2欄の**アクセス制御**でダウンストリーム速度制限の設定を確認できます。デフォルトでは無効になっています：



ルールの新規作成

最大速度ルールを新規作成をクリックして、ルールを設定できます：



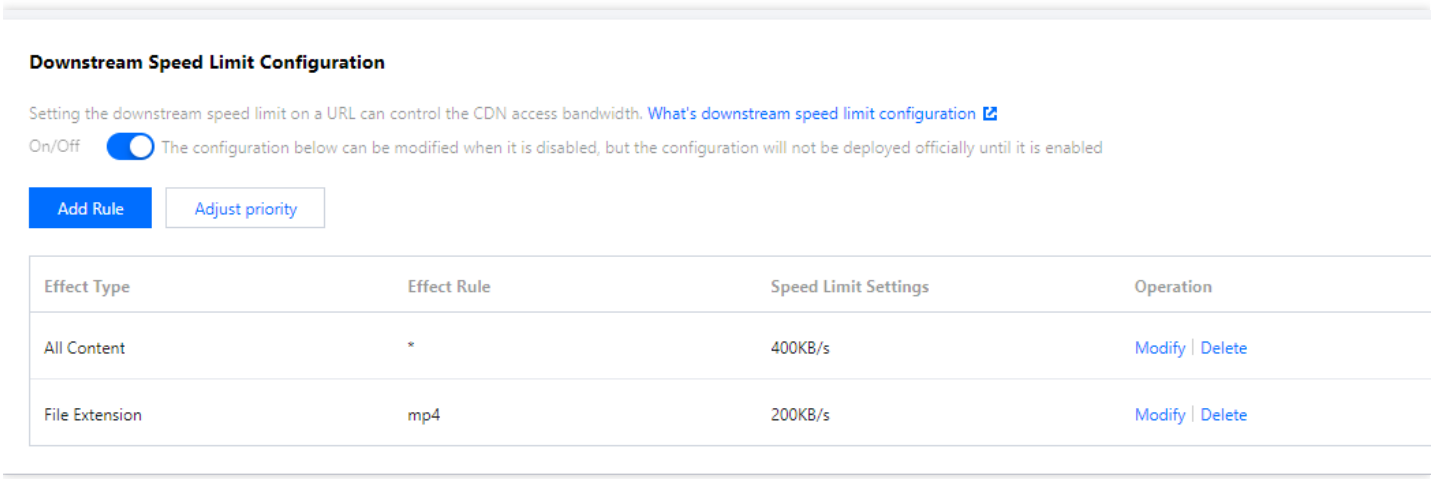
上限の設定

- 最大ダウンストリーム速度ルールは最大10個設定できます。
- 最大速度の単位はKB/sです。設定可能な値は1～1000000の正整数です。
- 有効化のタイプは、全ファイル、ファイルタイプ、ファイルディレクトリ、指定されたファイルパスの4つのモードをサポートしています。正規表現によるマッチングは現在サポートしていません。
- ルールが複数存在する場合、上にあるルールの優先度が低いです。言い換えると、下位にあるルールの優先度は上位にあるルールより高いです。

設定例

アクセラレーションドメイン名 `cloud.tencent.com` の最大ダウンストリーム速度の設定は以下のとおりです：

©2013-2022 Tencent Cloud. All rights reserved.



ユーザがアクセスするリソースが `http://cloud.tencent.com/test.mp4` の場合、サーバー側で200KB/sの最大ダウンストリーム速度で応答します。
ユーザがアクセスするリソースが `http://cloud.tencent.com/test.flv` の場合、サーバー側で400KB/sの最大ダウンストリーム速度で応答します。

©2013-2022 Tencent Cloud. All rights reserved.

リモート認証

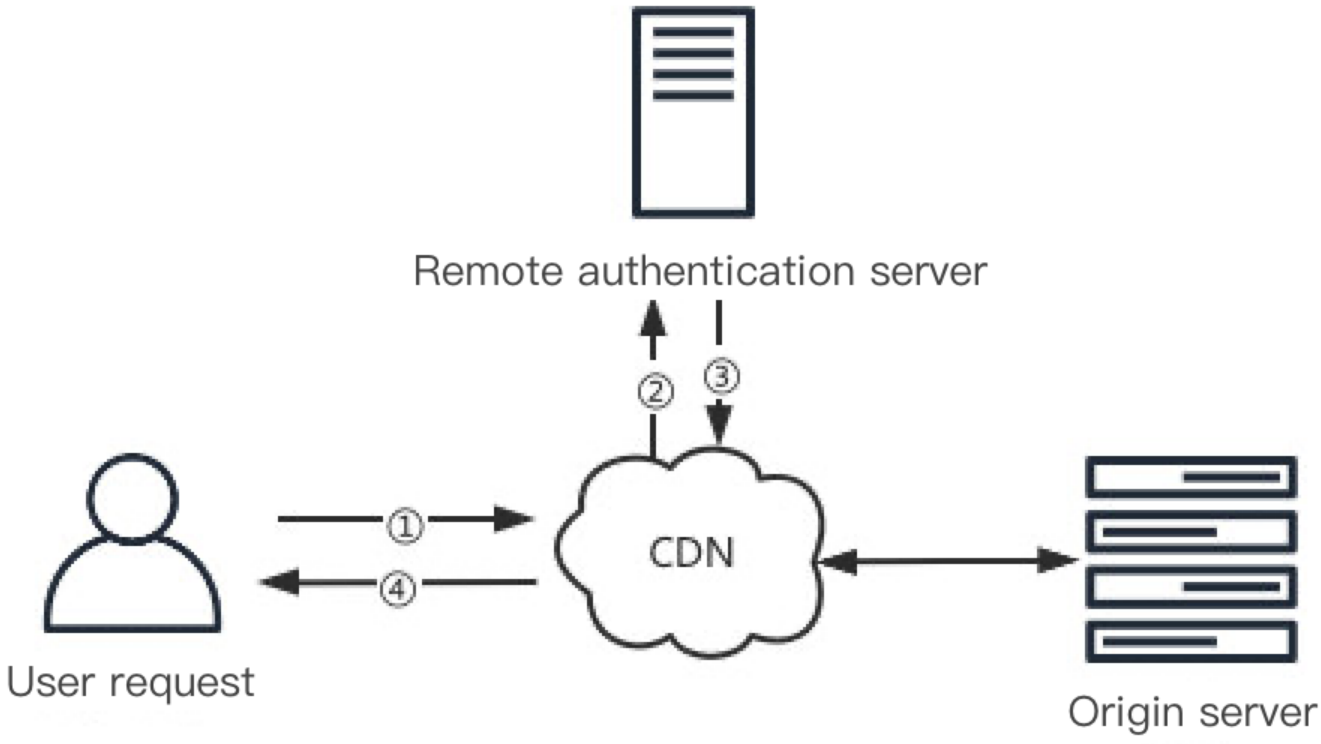
最終更新日：：2022-01-27 14:17:35

リモート認証

設定シナリオ

お客様のリソースへの不正なユーザーからのアクセスを防止するため、Tencent CloudはCDNエッジでの高度なタイムスタンプ認証をサポートするほか、リクエストをお客様の指定するリモート認証サーバーに転送し、この認証サーバーによってユーザーリクエストを検証し、CDNがリモート認証サーバーから返された検証結果に基づいてサービス提供を継続するかどうかを決定する方法もサポートしています。

リモート認証のリクエストフローは次のとおりです。



1. エンドユーザーがリソースに対するリクエストを送信します。
2. CDNがリクエストをリモート認証サーバーに同期転送します。
3. リモート認証サーバーが認証結果を返します。
4. CDNノードが認証結果に基づいて、そのユーザーのリクエストへの応答を継続するかどうかを決定します。

©2013-2022 Tencent Cloud. All rights reserved.

注意：

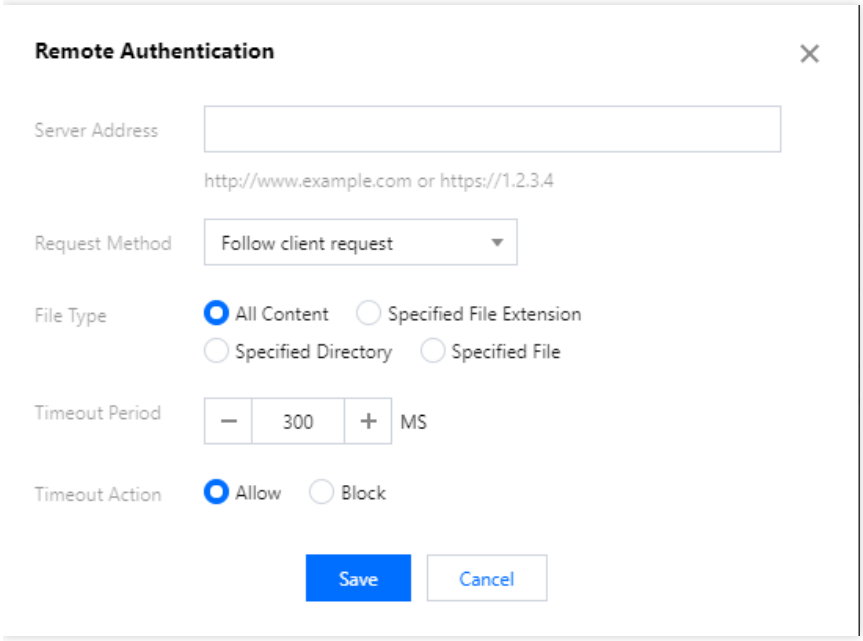
- CDNノードはリモートサーバーが返すステータスコードに基づいて認証が成功したかどうかを判断します。認証成功のステータスコードは `200` / `206` / `304` であり、それ以外のステータスコードの場合はすべて認証失敗です。認証成功の場合は承諾（200を返す）、失敗の場合はブロック（403を返す）となります。
- 現在は同期リモート認証のみサポートしており、CDNはリモート認証サーバーから返された認証結果を受け取ってからでなければ応答できません。
- 一部の海外プラットフォームではリモート認証設定をサポートしていません。ドメイン名のアクセラレーションリージョンを変更すると、リモート認証機能が無効となる場合があります。
- VODアクセラレーションは現時点ではリモート認証設定をサポートしていません。

設定ガイド

CDNコンソールにログインし、メニューバーで**ドメイン名管理**を選択して、ドメイン名の右側にある**管理**をクリックし、ドメイン名設定ページに進みます。**アクセス管理**でリモート認証に関連する設定を行うことができます。

- リモート認証アドレス：HTTP/HTTPSプロトコルをサポートしています。ドメイン名またはIPアドレスを入力することができます。
- リクエスト方法：リモートサーバーへのリクエスト送信方法は、エンドユーザーのリクエスト方法に準拠するか、またはGET/POST/HEADなどのリクエスト方法を指定することができます。
- 認証ファイルタイプ：認証ファイルの有効範囲を設定します。**すべてのコンテンツ/指定されたファイル拡張子/指定されたファイルディレクトリ/指定されたファイル**に対するリモート認証の有効化をサポートしています。
- 認証のタイムアウト時間：リモート認証サーバーの応答タイムアウト時間を設定します。最大30,000ミリ秒以内とします。
- タイムアウト時の実行動作：リモート認証のタイムアウト後の実行動作を設定します。デフォルトの動作は承諾です。

©2013-2022 Tencent Cloud. All rights reserved.



デモの説明

お客様のアクセラレーションドメイン名が `www.example.com` の場合の、リモート認証設定は次のようになります。

- リモート認証アドレス： `www.remoteauth.com` 。
- リクエスト方法：エンドユーザーのリクエスト方法に準拠。
- 認証ファイルタイプ：すべてのコンテンツ。
- 認証のタイムアウト時間：1500ミリ秒。
- タイムアウト時の実行動作：ブロック。

このときのユーザーリクエスト応答フローのサンプルは次のとおりです。

1. ユーザーがGETリクエストを送信： `http://www.example.com/v001/test.txt?token=Gf6Gq04ymjdSTXusvTmh8yalO82YsuKUQb63ToXOFc&e=1467565695283&sign=854124740723b575a7cfa4fc40f0be30` 。
2. CDNがリクエストを受信し、リモート認証サーバーにGETリクエストを送信： `http://www.remoteauth.com/v001/test.txt?token=Gf6Gq04ymjdSTXusvTmh8yalO82YsuKUQb63ToXOFc&e=1467565695283&sign=854124740723b575a7cfa4fc40f0be30` 。
3. リモート認証サーバーがステータスコード200を返します。
4. CDNが認証成功と判断し、ステータスコード200を返し、コンテンツの応答を正常に行います。

©2013-2022 Tencent Cloud. All rights reserved.

アクセスポート設定

最終更新日：：2023-06-13 11:11:22

設定シナリオ

CDNは、デフォルトで80/8080/443のアクセスポートが有効になっています。実際の業務のニーズに応じて、アクセスポートのいずれかをご自身で無効にすることができます。

注意：

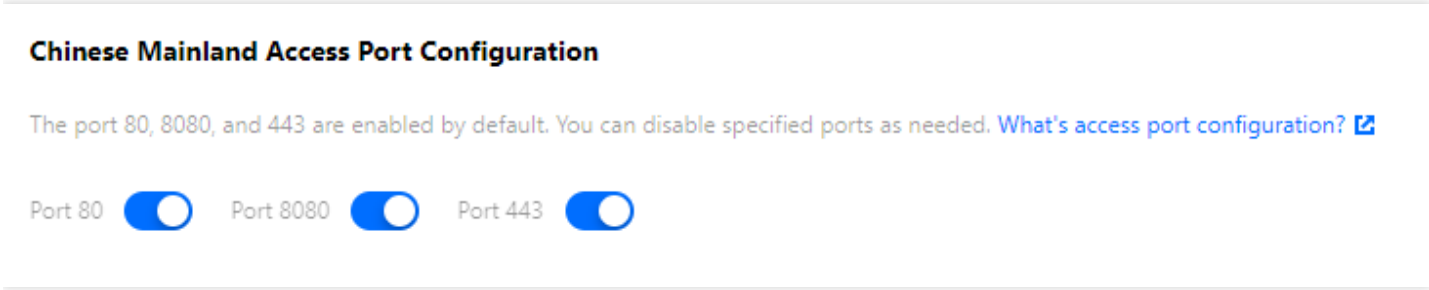
- アクセスポート設定は、現在中国国外ではサポートしていません。ドメイン名のアクセラレーションリージョンがグローバルである場合、設定変更後は中国国内でのみ有効となります。
- 一部のプラットフォームはアップグレード中のため、この設定機能を開放していません。

設定ガイド

設定の確認

CDNコンソールにログインし、左側のメニューバーで【Domain Management】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定画面に入ります。タブを【アクセス制御】に切り替えると、【中国国内アクセスポート設定】が表示されます。

デフォルトの状態では、80/8080/443のアクセスポートがいずれも有効になっています。



設定の変更

必要に応じて、有効になっているアクセスポートを無効にすることができます。無効にした後、再度有効にすることも可能です。

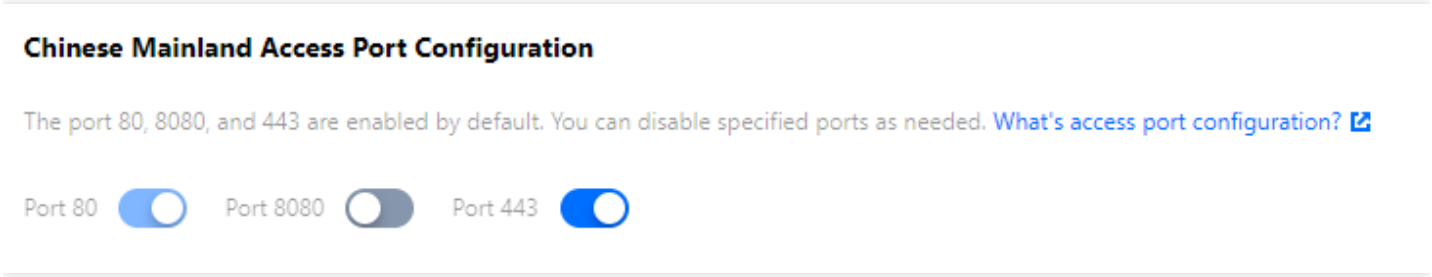
変更に関する制約

©2013-2022 Tencent Cloud. All rights reserved.

- ドメイン名でHTTPSを有効にしているか、またはHTTPSに強制的にリダイレクトさせる場合、443のアクセスポートを無効にすることはできません。
- 80と8080のアクセスポートを同時に無効にすることはできません。

設定例

アクセラレーションドメイン名 `www.test.com` の**中国国内アクセスポート設定**の例は次のとおりです。



実際のアクセス状況は次のとおりです。

CDNノードが8080ポートのアクセスを拒否

- ドメイン名のアクセラレーションリージョンがグローバルとなる場合は、中国国内でのみ有効となり、CDNの中国国内のノードで8080ポートのアクセスが拒否されます。

©2013-2022 Tencent Cloud. All rights reserved.

キャッシュ設定
キャッシュキールール設定

最終更新日：：2021-04-25 14:19:55

設定シナリオ

Tencent Cloud CDNは、キャッシュ時にKey-Value形式を使用してリソースをマッピングします。Keyはキャッシュキーで、キャッシュされたリソースの一意の識別子です。キャッシュキールールを設定することにより、異なるファイルタイプのコンテンツに[フィルタリングパラメータ]と、[大文字と小文字を区別しない]機能を設定して、キャッシュキーを最適化できます。

フィルタリングパラメータ

- ユーザーがURLを介してリソースにアクセスする場合、以下のリンクを使用して2つの異なる画像を表示するなど、いくつかの特別なパラメータを使用する場合があります。
  `http://cloud.tencent.com/1.jpg?version=1`
  `http://cloud.tencent.com/1.jpg?version=2`
  このシナリオでは[フィルタリングパラメータ]機能を無効にする必要があり、完全なURLをキャッシュキーとして画像の内容をそれぞれキャッシュし、リソースを区別します。

- オーディオ・ビデオのシナリオで、タイムスタンプ署名パラメータを使用し、アクセス認証を行う場合：
  `http://cloud.tencent.com/1.mp4?sign=XXXXXX`
  このシナリオでは[フィルタリングパラメータ]機能を有効にする必要があります。「?」の前のリンク `http://cloud.tencent.com/1.mp4` をキャッシュキーとします。ノードは1つのリソースのみをキャッシュし、タイムスタンプ署名が絶えず変化している場合でも、署名認証を介してキャッシュに直接ヒットすることができます。

大文字小文字を区別しない

業務シナリオにおいて、リソースのURLパスの大文字と小文字の違いがリソースの内容に影響する場合は、[大文字小文字を区別しない]設定を無効にすることができます。
業務シナリオにおいて、リソースのURLパスの大文字と小文字の違いがリソースの内容に影響しない場合は、[大文字小文字を区別しない]設定を有効にし、ヒット率を上げることができます。

⚠ 注意：

©2013-2022 Tencent Cloud. All rights reserved.

プラットフォームはアップグレード中であり、現在のところ大文字と小文字を区別しない設定を有効化することはできません。

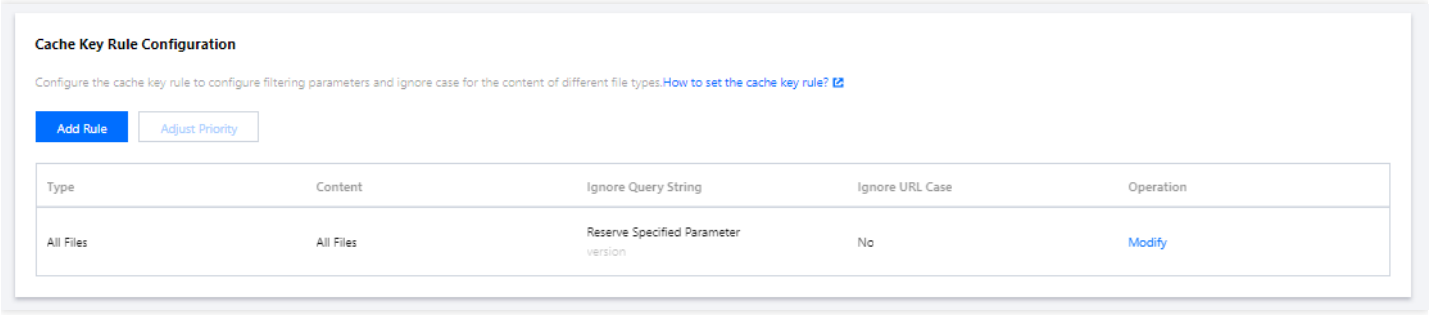
設定ガイド

設定の確認

CDNコンソールにログインし、左側のメニューバーで【ドメイン名管理】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定ページに移動します。Tabを【キャッシュ設定】に切り替えると、【キャッシュキールールの設定】が表示されます。

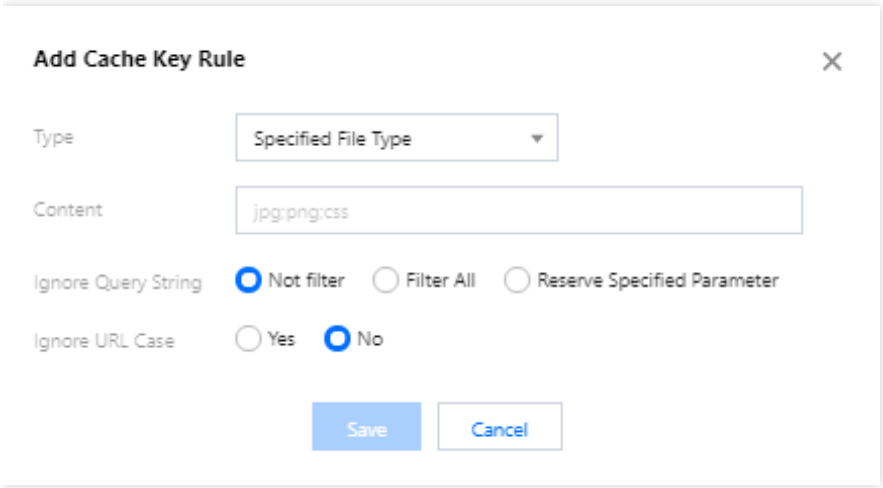
アクセラレーションドメイン名を追加する際には、業務タイプに応じて、[フィルタリングパラメータ]機能がデフォルトで無効または有効となります。

- アクセラレーションドメイン名で静的アクセラレーション業務タイプを選択した場合、フィルタリングパラメータはデフォルトでは無効です。キャッシュキールールの設定では、すべてのファイルルールの【フィルタリングパラメータ】が「フィルタリングしない」に同期されます。
- アクセラレーションドメイン名でダウンロードやストリーミングメディアのVOD業務タイプを選択した場合、[フィルタリングパラメータ]機能はデフォルトで有効になります。キャッシュキールールの設定では、すべてのファイルルールの【フィルタリングパラメータ】が「すべてフィルタリングする」に同期されます。



ルールの追加

必要に応じてキャッシュキーのルールを追加できます。



設定の制約

- 1つのドメイン名で最大20件までキャッシュキールール（デフォルトルールを含む）を追加できます。
- 複数あるルールは優先順位を変更できます。下部の優先順位が上部のものよりも高くなります（デフォルトルールの優先順位を変更できません）。
- 1つのファイルタイプ/フォルダ/フルパスファイルルールでは、最大100グループのコンテンツを入力でき、異なるコンテンツ間は「;」で区切ります。例：ファイルタイプ - jpg;png。
- フィルタリングパラメータ - 指定されたパラメータを保持
  - すべてのファイル：最大6つのパラメータ名を入力でき、1つのパラメータ名の上限は20文字となります。
  - ファイルタイプ/フォルダ/フルパスファイル：最大5つのパラメータ名を入力でき、1つのパラメータ名の上限は20文字となります。
    複数のパラメータ名の間は「;」で区切ります。例：key1;key2;key3。

ルールの変更

追加されたキャッシュキーのルールを変更することができます。キャッシュキーのルール操作欄の【変更】をクリックして変更します。

> **⚠ 注意：**
>
> デフォルトルールはフィルタリングパラメータと、大文字と小文字を区別しない設定のみ変更可能であり、タイプとコンテンツの変更はサポートしていません。

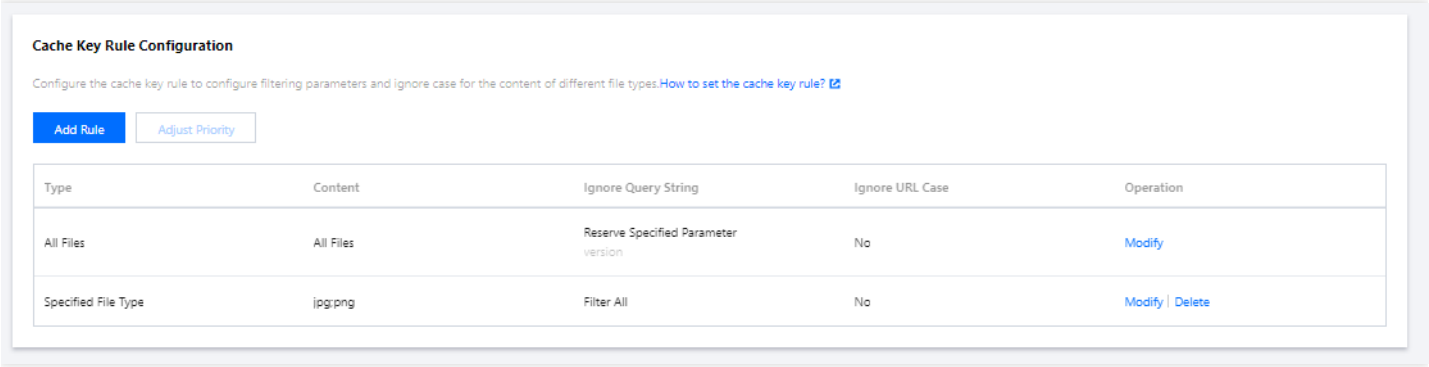
ルールの削除

追加されたキャッシュキーのルールを削除できます。キャッシュキーのルール操作欄の【削除】をクリックして削除します(デフォルトではルールを削除できません)。

©2013-2022 Tencent Cloud. All rights reserved.

設定例

アクセラレーションドメイン名 `www.test.com` の【キャッシュキールールの設定】が次の場合、



実際のアクセス状況は次のとおりです。

クライアントがリソース `www.test.com/abc.jpg?version=1&colour=red` と `www.test.com/abc.JPG?version=1&colour=red` をリクエストし、リクエストがいずれもCDNノードXにアクセスして、ノードXに上記の2つのリソースのキャッシュがない場合：

- オリジンサーバーへ戻って `abc.jpg` 画像リソースを取得し、CDNノードX上にキャッシュするようにリクエストします。フィルタリングパラメータが「すべてフィルタリングする」になっているため、「?」以前のリンク `www.test.com/abc.jpg` がキャッシュキーになります。
- クライアントが `www.test.com/abc.JPG?version=1&colour=red` をリクエストする場合、大文字と小文字を区別しない設定が有効になっていないため、以前にキャッシュした `www.test.com/abc.jpg` リソースにヒットしません。オリジンサーバーへ戻って `abc.JPG` 画像リソースを取得し、CDNノードX上にキャッシュするようにリクエストします。対応するキャッシュキーは `www.test.com/abc.JPG` になります。

©2013-2022 Tencent Cloud. All rights reserved.

ノードのキャッシュの有効期限の設定

最終更新日：：2022-09-15 16:16:19

ノードのキャッシュの有効期限の設定を利用すれば、CDNノードにキャッシュされたオリジンサーバーのリソースの有効期限を設定し、CDNノードにキャッシュされたオリジンサーバーのリソースを更新する頻度を調整することができます。業務ニーズに応じて、ディレクトリ、ファイルの拡張子、ファイルのフルパスでキャッシュするリソースの有効期限を設定することができます。

機能説明

CDNはノードのキャッシュの有効期限の設定で指定された有効期限に従って、CDNノードにキャッシュされたリソースが期限切れになったかを判断します。

- CDNノードにおける、ユーザーがアクセスするリソースのキャッシュが期限切れになっていない場合、CDNノードはそのままキャッシュをユーザーに返します。
- ユーザーのアクセスするリソースがCDNノードにキャッシュされていない場合、または、CDNノードにおける、ユーザーがアクセスするリソースのキャッシュが期限切れになった場合、CDNノードはオリジンサーバーから最新のリソースを取得しキャッシュすると同時に、ユーザーに返します。

オリジンサーバーのリソースを更新した直後に、CDNノードでのキャッシュを更新する必要がある場合、キャッシュを更新 機能を使用し、CDNノードで期限切れになっていないキャッシュを自発的に更新することで、CDNノードでのキャッシュとオリジンサーバーのリソースとの一致性を確保します。

注意事項

- キャッシュの有効期限はBack-to-Originの実行頻度に影響を与えます。業務ニーズに応じてリソースのキャッシュの有効期限を設定することをお勧めします。キャッシュの有効期限が短いと、CDNが頻繁にBack-to-Originを実行し、オリジンサーバーの帯域幅が増えます。キャッシュの有効期限が長いと、CDNのキャッシュの更新が遅れ、ユーザーが最新のリソースを取得することに影響します。
- CDNノードでは、Tencent Cloud CDNキャッシュルールと優先度に従ってリソースがキャッシュされます。ただし、CDNノードにキャッシュされたリソースは、リクエスト頻度が低い原因で、期限切れになっていなくても、ノードから削除されることがあります。
- オリジンサーバーにおけるリソースの更新前後に、異なるリソース名を使用することをお勧めします。例えば、バージョン(img-v1.jpg、img-v2.jpg)で中身が異なるリソースに名前を付けます。これは、オリジンサーバーでリソースが変わった後、CDNノードでキャッシュが期限切れになっていないため、古いリソースをユーザーに返すことを防ぐためです。

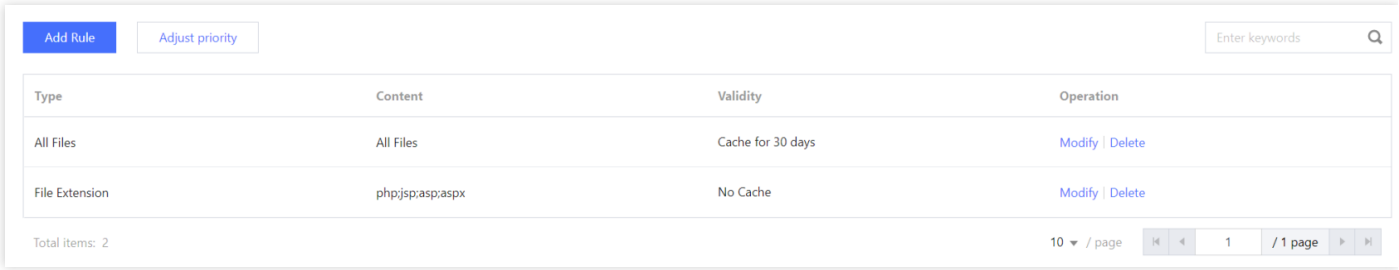
©2013-2022 Tencent Cloud. All rights reserved.

- 古いバージョン（標準モード）のノードのキャッシュの有効期限の設定機能を利用中の場合、高度モードでの設定をサブミットし、最新版のノードのキャッシュの有効期限の設定にアップグレードすることで、より多くの機能を利用することをお勧めします。高度モードにアップグレードした場合、元の標準モードに戻ることができないので、ご注意ください。古いバージョンのノードのキャッシュの有効期限の設定については、ノードのキャッシュの有効期限の設定（旧）をご参照ください
- オリジンサーバーでレスポンスヘッダーCache-Controlを設定することで、CDNノードにおけるキャッシュの有効期限（キャッシュオプション:オリジナルサーバーと同様）を制御することができます。なお、CDNノードでレスポンスヘッダーCache-Controlがユーザーに渡されるため、ブラウザのキャッシュの有効期限に対する制御が実現できます。CDNノードでブラウザのキャッシュの有効期限を設定する場合、ブラウザのキャッシュの有効期限の設定 で、CDNノードからユーザーに渡すレスポンスヘッダーCache-Controlを指定してください。

設定説明

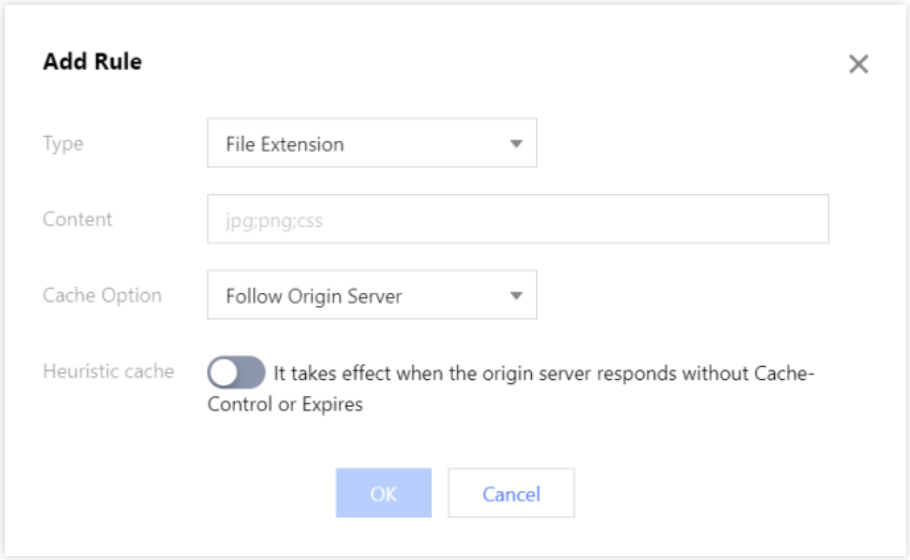
操作プロセス

1. CDNコンソールにログインします。
2. 左側のメニューで**ドメイン名管理**をクリックし、ドメイン名管理リストへ進みます。
3. 設定するドメイン名を選択し、**管理**をクリックして、ドメイン名の設定ページへ進みます。
4. **キャッシュ設定**をクリックし、キャッシュ設定タグに切り替えます。タグで**ノードキャッシュ期限の設定**を確認できます。



5. **ルールを新規作成**をクリックし、新規ルールページへ進み、ノードのキャッシュの有効期限の設定を追加します。

©2013-2022 Tencent Cloud. All rights reserved.



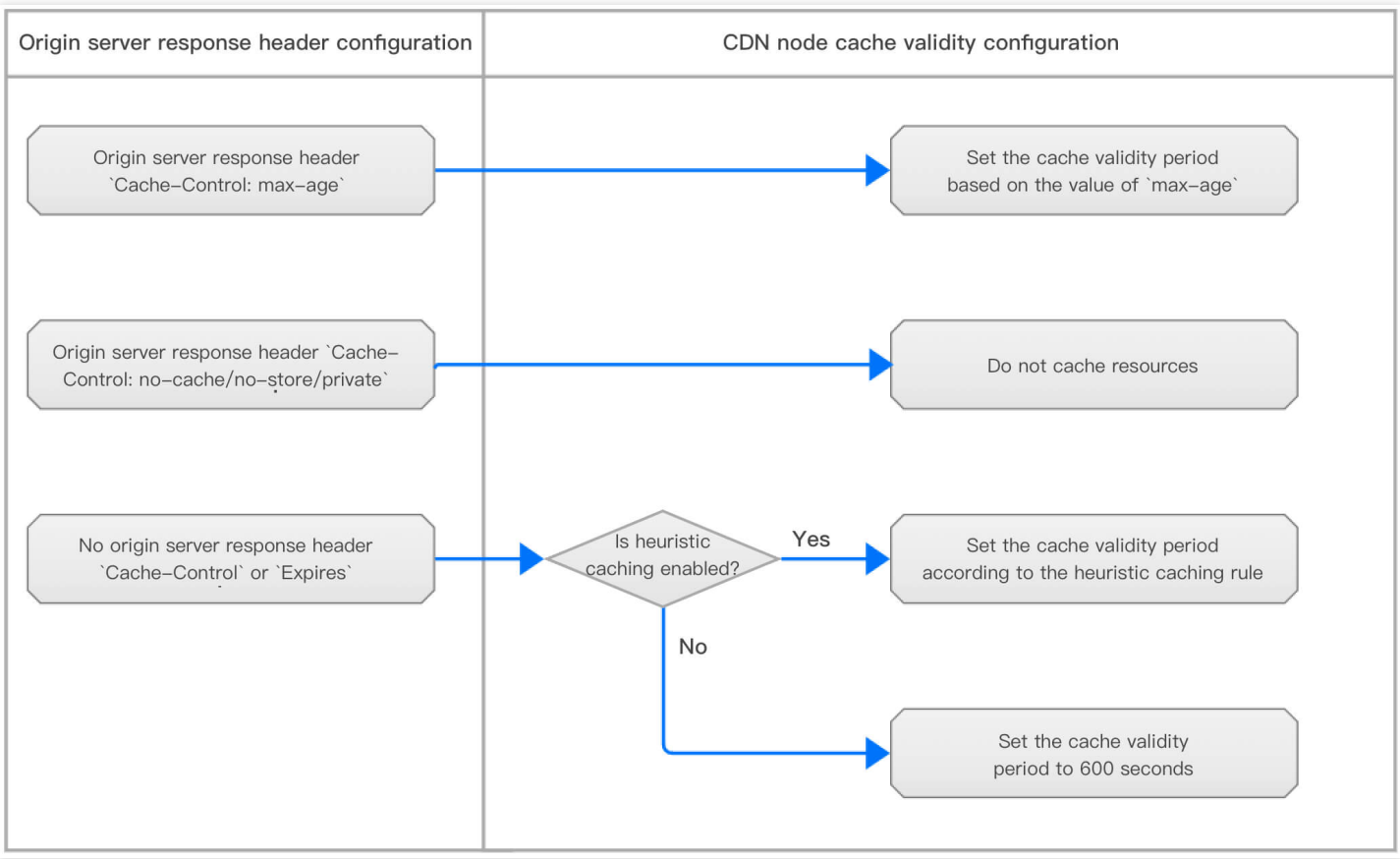
設定項目	説明
タイプ	すべてのファイル、ファイルの拡張子、ファイルのディレクトリ、フルパスのファイル、ホームページを設定することが可能です。 すべてのファイル：すべてのファイルを指定してルールを設定します。デフォルトルールとします。 ファイルの拡張子：ファイルの拡張子を指定してルールを設定します。 ファイルのディレクトリ：ファイルのディレクトリを指定してルールを設定します。 フルパスのファイル：ファイルのフルパスを指定してルールを設定します。 ホームページ：ドメイン名のルートディレクトリを指定してルールを設定します。
詳細	選択したファイルタイプによって、入力する内容には制約があります。 タイプがすべてのファイルの場合、すべてのファイルとします。 タイプがファイルの拡張子の場合、ファイルの拡張子を入力できます。拡張子が複数ある場合、「；」で区切ります。例：jpg;png;css。 タイプがファイルのディレクトリの場合、ファイルのディレクトリを入力できます。「/」で終わらないでください。ディレクトリが複数ある場合、「；」で区切ります。例：/test;/a/b/c。 タイプがフルパスのファイルの場合、ファイルのフルパスを入力できます。フルパスが複数ある場合、「；」で区切ります。例：/index.html;/test/.jpg。

©2013-2022 Tencent Cloud. All rights reserved.

設定項目	説明
キャッシュオプション	オリジンサーバーと同様、キャッシュを格納する、キャッシュを格納しないルールで設定することが可能です。 オリジンサーバーと同様：オリジンサーバーのレスポンスヘッダーCache-Controlに応じて、CDNノードのキャッシュの有効期限を設定します。ヒューリスティックキャッシュへの設定をサポートします。 キャッシュを格納する：CDNノードのキャッシュの有効期限を設定します。強制キャッシュへの設定をサポートします。 キャッシュを格納しない：CDNノードでリソースをキャッシュしないことを設定します。

Tencent Cloud CDNキャッシュルールと優先度

キャッシュオプション：オリジンサーバーと同様



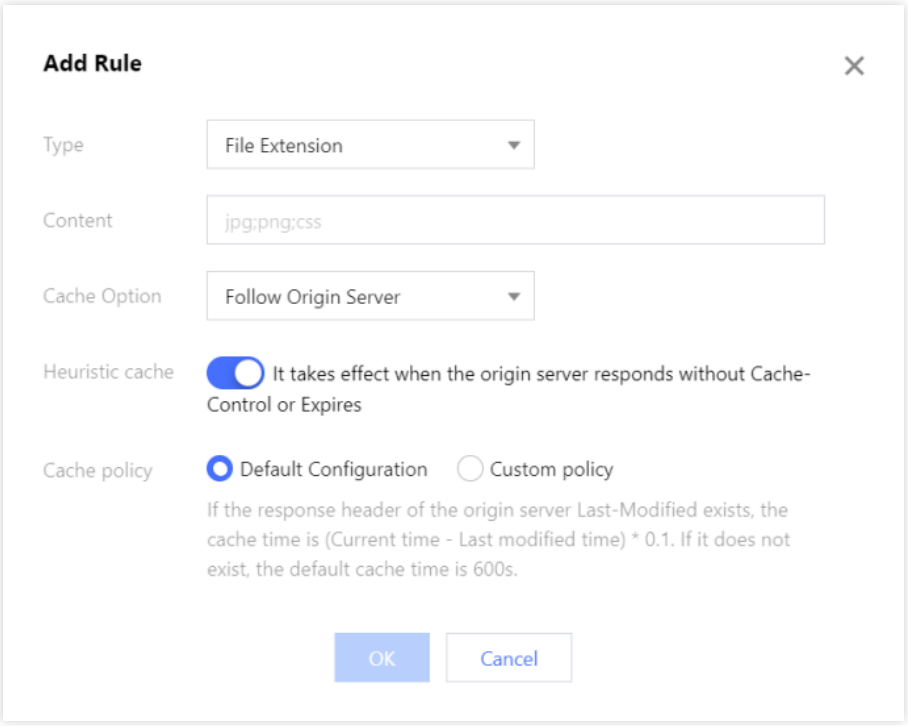
CDNノードで、オリジンサーバーのレスポンスヘッダーCache-Controlに応じてキャッシュの有効期限を設定します。

- オリジンサーバーのレスポンスヘッダーCache-Controlのフィールドがmax-ageである場合、max-ageの値に応じてCDNノードのキャッシュの有効期限を設定します。例えば、Cache-Control：max-age=300の場合、キャッシュの有効期限が300秒になります。

©2013-2022 Tencent Cloud. All rights reserved.

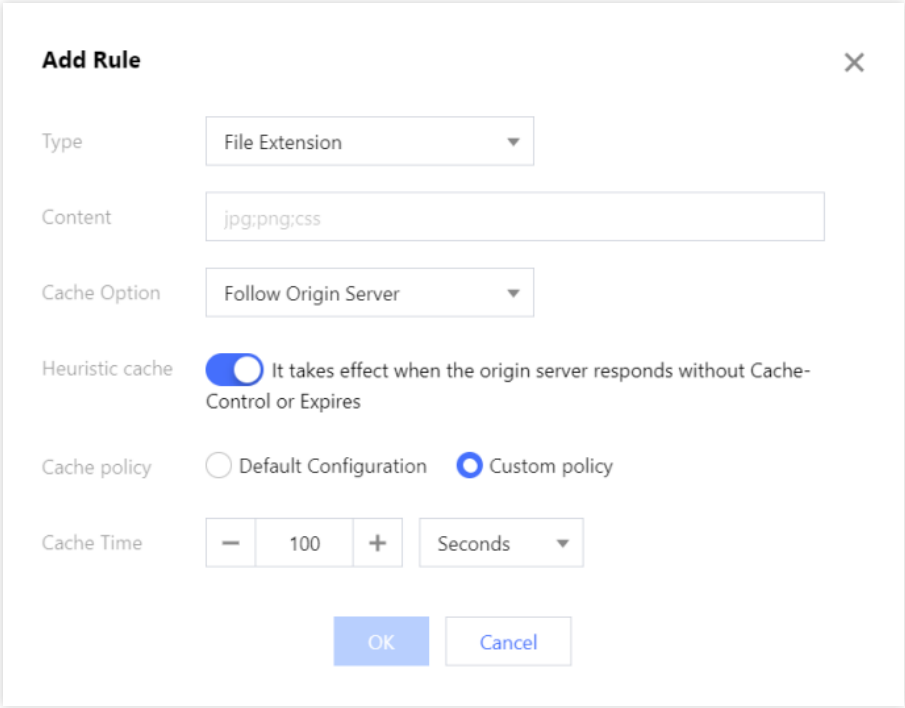
- オリジンサーバーのレスポンスヘッダーCache-Controlのフィールドがno-cache 、no-storeまたはprivateである場合、CDNノードでリソースをキャッシュしません。
- オリジンサーバーのレスポンスヘッダーにCache-ControlまたはExpiresがない場合、ヒューリスティックキャッシュの状態に応じてキャッシュルールを設定します。詳しくは以下のとおりです：
  - ヒューリスティックキャッシュが無効になり、オリジンサーバーのレスポンスヘッダーにCache-ControlまたはExpiresがない場合、キャッシュの有効期限は600秒とします。
  - ヒューリスティックキャッシュが有効になり、オリジンサーバーのレスポンスヘッダーにCache-ControlまたはExpiresがない場合、以下のルールに従ってヒューリスティックキャッシュの有効期限を設定します。

    i. デフォルト設定：オリジンサーバーのレスポンスヘッダーにLast-Modifiedがある場合、キャッシュの有効期限は（現在の時間-Last-Modified）* 0.1とします。オリジンサーバーのレスポンスヘッダーにLast-Modifiedがない場合、キャッシュの有効期限はデフォルトで600秒とします。

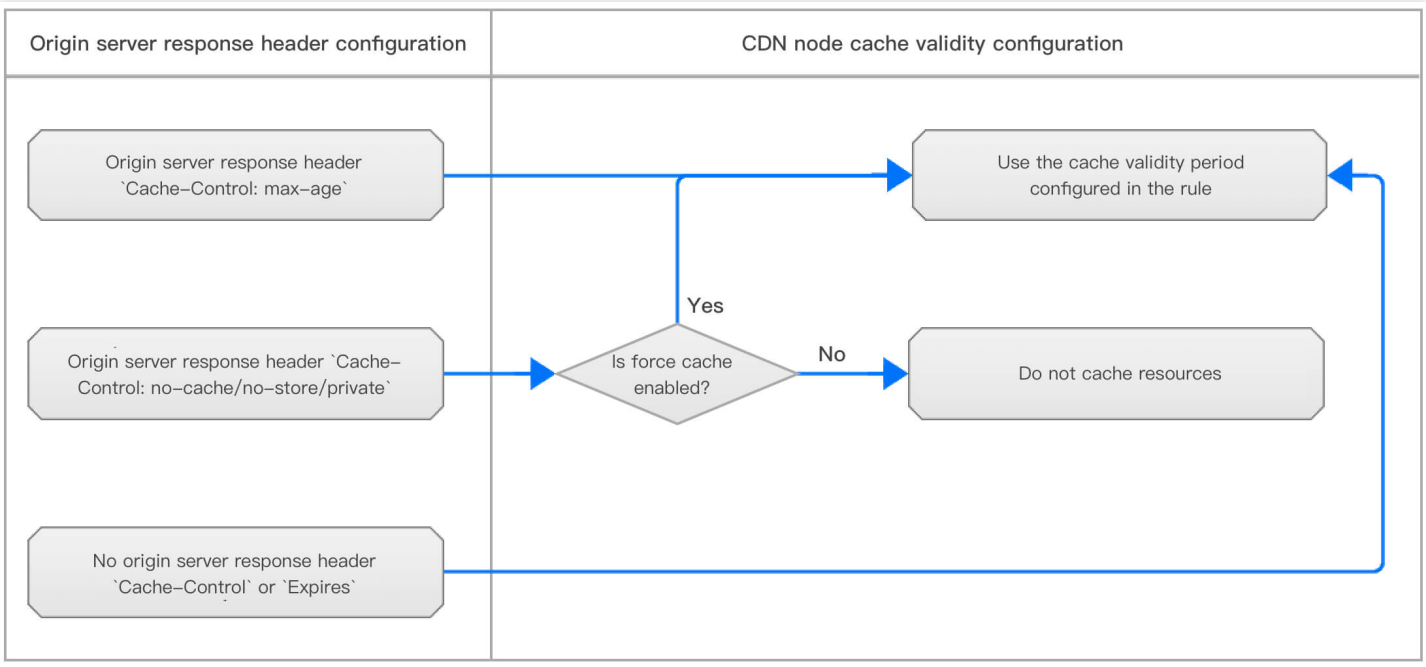


©2013-2022 Tencent Cloud. All rights reserved.

ii. **カスタムポリシー**：ヒューリスティックキャッシュの有効期限を設定できます。



キャッシュオプション：キャッシュを格納する

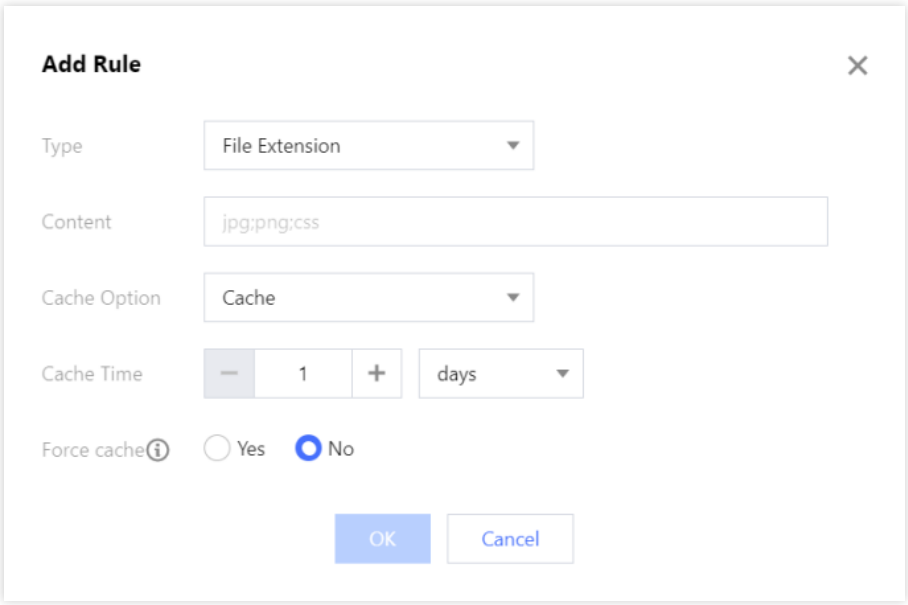


CDNノードのキャッシュの有効期限を設定します。

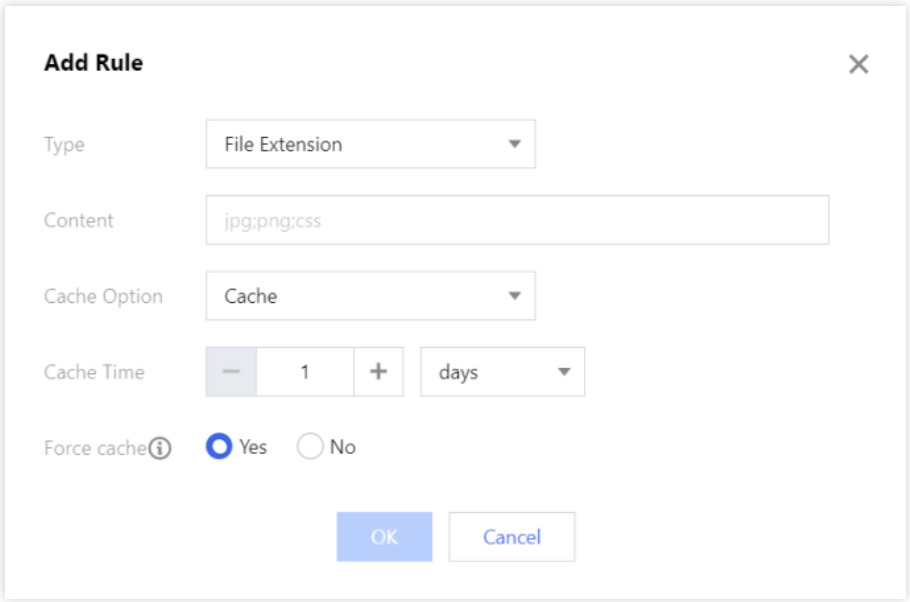
- 強制キャッシュの無効化：

©2013-2022 Tencent Cloud. All rights reserved.

- オリジンサーバーのレスポンスヘッダーCache-Controlのフィールドがmax-ageである場合、または、オリジンサーバーのレスポンスヘッダーにCache-Controlがない場合、設定したCDNノードのキャッシュルールに従ってキャッシュを実行します。
- オリジンサーバーのレスポンスヘッダーCache-Controlのフィールドがno-cache 、no-storeまたはprivateである場合、CDNノードでリソースをキャッシュしません。



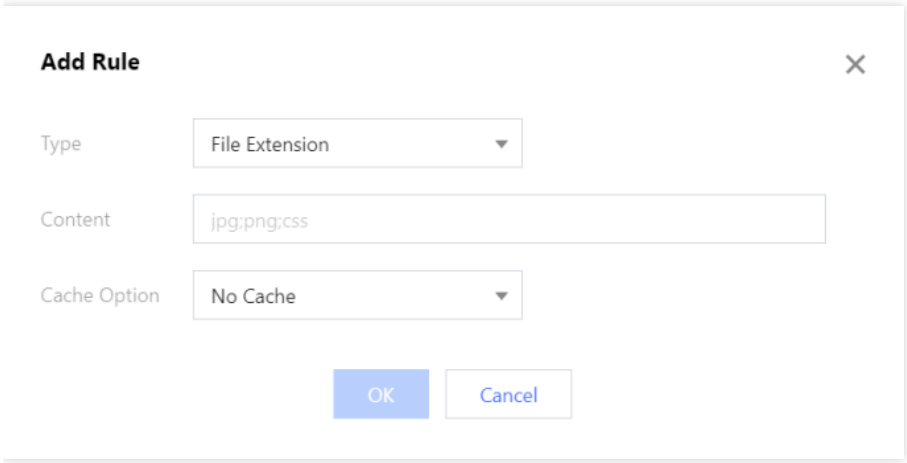
- 強制キャッシュの有効化：オリジンサーバーのレスポンスヘッダーCache-Controlを無視し、設定したCDNノードのキャッシュルールに従ってキャッシュを実行します。



キャッシュオプション：キャッシュを格納しない

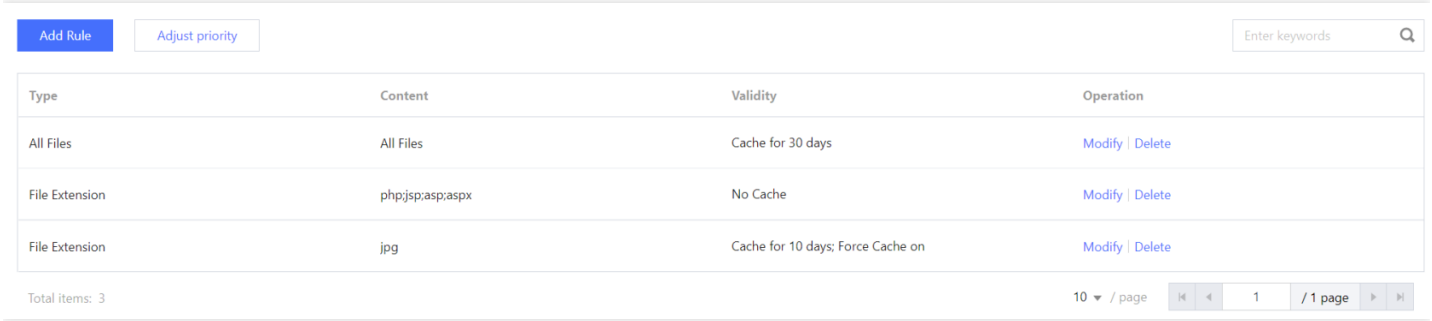
©2013-2022 Tencent Cloud. All rights reserved.

CDNノードでリソースをキャッシュしないことを設定します。このリソースへの各ユーザーリクエストに対して、CDNはそのままBack-to-Originを実行しリソースを取得してユーザーに返します。



キャッシュルールが複数存在する場合の優先度

同時に複数のキャッシュルールを設定した場合、上位のルールに比べ、下位のルールの**優先度が高い**です。**優先度を調整**をクリックし、キャッシュルールをドラッグして優先順を調整することができます。



推奨設定

- よく更新しないスタティックファイル(ピクチャータイプ、アプリケーションダウンロードタイプなど）の場合、キャッシュの有効期限に30日を設定することをお勧めします。
- 頻繁に更新するスタティックファイル（js、cssなど）の場合、業務の更新頻度に応じてキャッシュの有効期限を設定することをお勧めします。
- ダイナミックファイル（php、jsp、asp、aspxなど）の場合、**キャッシュを格納しないことを設定しなければなりません**。

©2013-2022 Tencent Cloud. All rights reserved.

- **サイトへのログイン**（wordpressバックグランドから/wp-adminにアクセスするなど）や**インターフェース検索**などオリジンサーバーと直接通信する必要がある他のリクエストの場合、**キャッシュを格納しないことを設定しなければなりません**。そうしないと、アクセスエラーが発生する可能性があります。

設定の制約

- 1つのドメイン名に対して、キャッシュルールを最大100件まで追加できます。
- ルールが複数存在する場合、下位のルールの優先度は上位のルールより高いです。
- 1つのファイルの拡張子/ファイルのディレクトリ/フルパスのファイルルールでは、最大100グループのコンテンツを入力できます。異なるコンテンツを「;」で区切ります。例：ファイル拡張子の場合、jpg;pngになります。
- いかなるルールも設定していない場合、または、リクエストが設定されたルールをヒットしなかった場合、CDNノードでオリジンサーバーのレスポンスヘッダーCache-Controlに応じてキャッシュの有効期限を設定します。オリジンサーバーのレスポンスヘッダーにCache-Controlフィールドがない場合、CDNノードでこのリソースのキャッシュの有効期限はデフォルトで600sとします。
- CDNノードでは、GET、HEADタイプのリクエストだけをキャッシュし、 POSTやOPTIONSなど他のタイプのリクエストをキャッシュしません。

設定例

例1

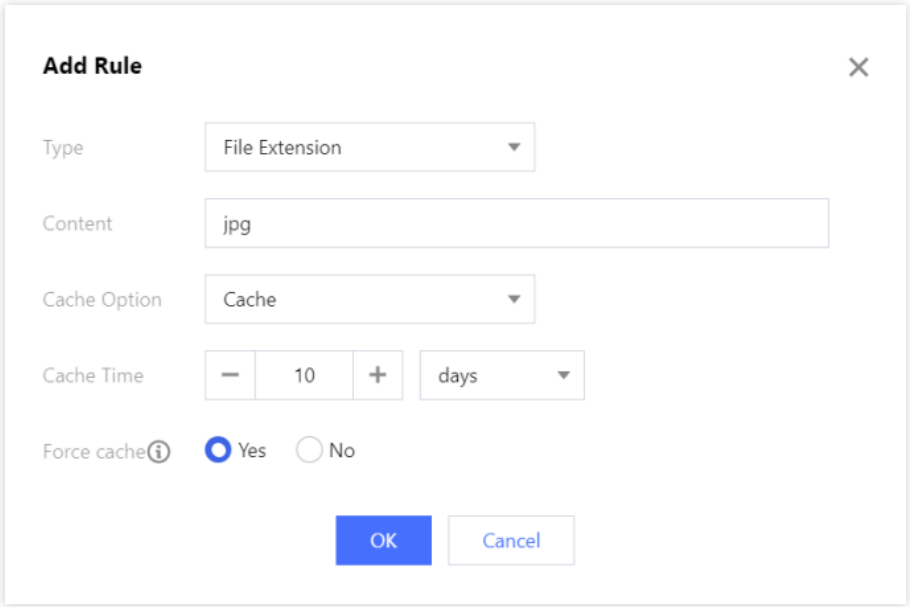
元のキャッシュルールは、「ファイルの拡張子がphp;jsp;asp;aspxのリソースをキャッシュせず、他のファイルは全部30日とする」です。

次のルール「ファイルの拡張子がjpg、pngのリソースは10日とし、かつ、オリジンサーバーのレスポンスヘッ

©2013-2022 Tencent Cloud. All rights reserved.

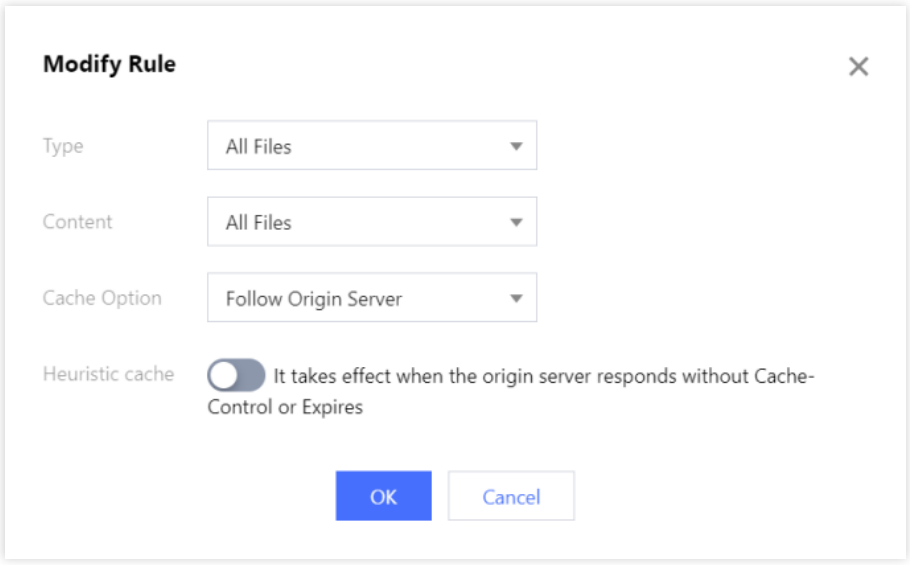
ダーCache-Controlを無視する」を追加します。つまり、強制キャッシュを有効にします。他のすべてのファイルのキャッシュルールは、「オリジンサーバーと同様」に変更します。

1. **ルールを新規作成**をクリックし、タイプはファイルの拡張子、内容はjpg;png、キャッシュオプションは「キャッシュを格納する」、キャッシュの有効期限は10日、強制キャッシュは有効として、**OK**をクリックします。



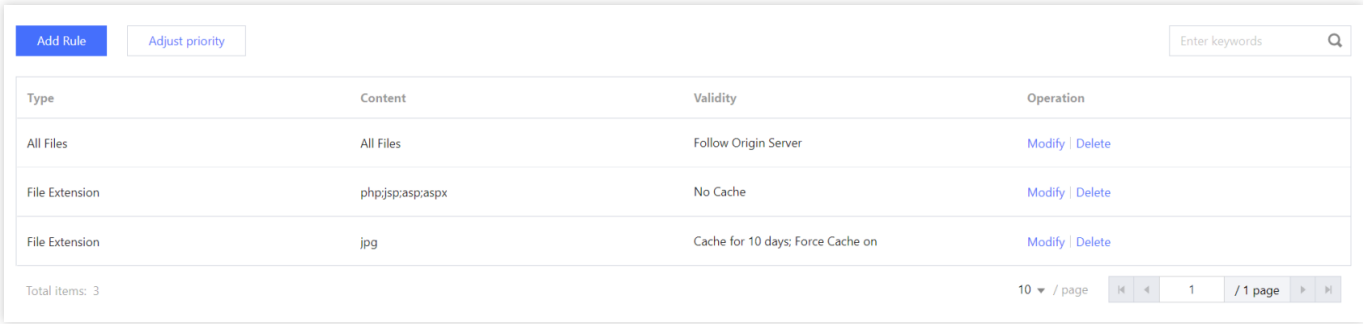
2. すべてのファイルのキャッシュルールを選択し、**変更**をクリックし、キャッシュオプションを「オリジンサーバーと同様」に変更して、**OK**をクリックします。

©2013-2022 Tencent Cloud. All rights reserved.



3. 変更後のキャッシュルールは以下のとおりです：

- ファイルの拡張子がjpg、pngのリソースのキャッシュの有効期限は10日とし、強制キャッシュを有効にします。
- ファイルの拡張子がphp;jsp;asp;aspxのリソースをキャッシュしません。
- 他のすべてのファイルのキャッシュの有効期限は30日とします。



実際のキャッシュ状況は以下のとおりです：

- オリジンサーバーのレスポンスヘッダーCache-Controlのフィールドがno-cache、no-storeまたはprivateにもかかわらず、ノードにおける、 `www.test.com/abc.jpg` リソースのキャッシュの有効期限は10日です。

©2013-2022 Tencent Cloud. All rights reserved.

- `www.test.com/def.php` リソースはノードにキャッシュされません。

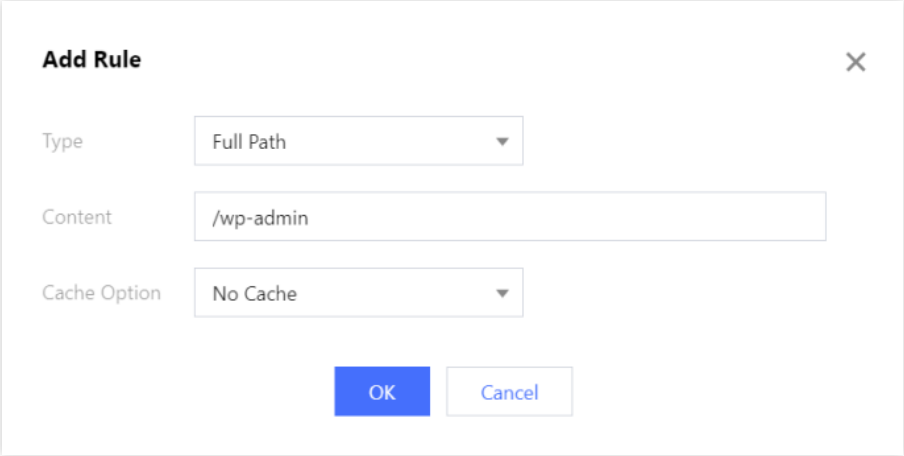
例2

WordPressを使用してサイトを構築したノードに対するキャッシュの有効期限の設定アドバイス

- バックグラウンドからログインする/wp-adminディレクトリ配下のリソースに対して、キャッシュしないことを設定しなければなりません。そうしないと、バックグラウンドからのログインに関するリソースがキャッシュされ、ログインエラーが発生します。他にインターフェース関連のリソースに対しても、キャッシュしないことを設定してください。
- 拡張子がphp;jsp;asp;aspxであるダイナミックリソースに対して、キャッシュしない（CDNのデフォルトキャッシュルール）ことを設定してください。
- 拡張子がhtml;js;cssのファイルは頻繁に更新されるため、更新頻度に応じてキャッシュの有効期限を設定してください。キャッシュの有効期限に7日を設定し、強制キャッシュを無効にすることをお勧めします。
- 他のすべてのファイルのキャッシュの有効期限は30日とします（CDNのデフォルトキャッシュルール）。

CDNのデフォルトキャッシュルールに加えて、以下の手順に従ってルールを追加します：

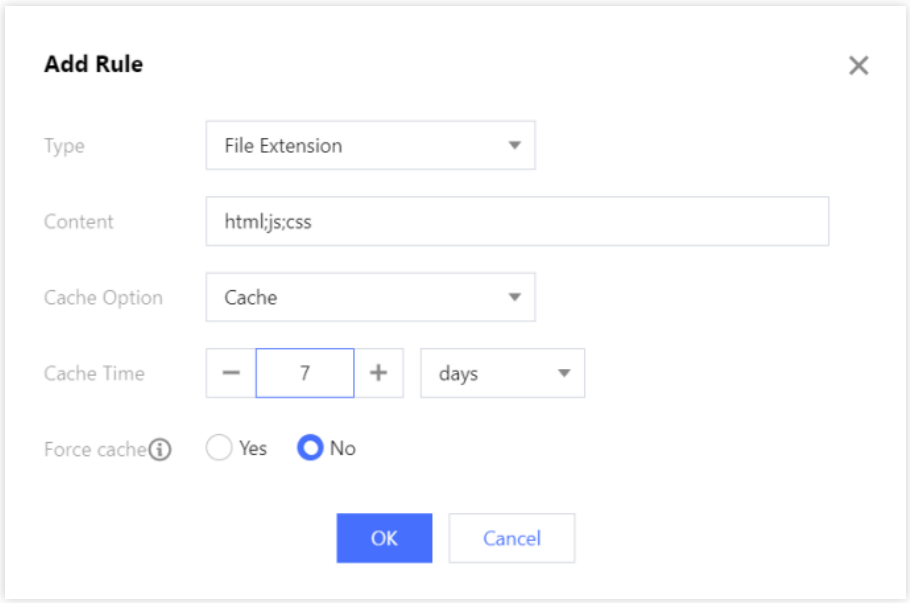
1. **ルールを新規作成**をクリックし、タイプはディレクトリ、内容は/wp-admin、キャッシュオプションは「キャッシュを格納しない」として、**OK**をクリックします。



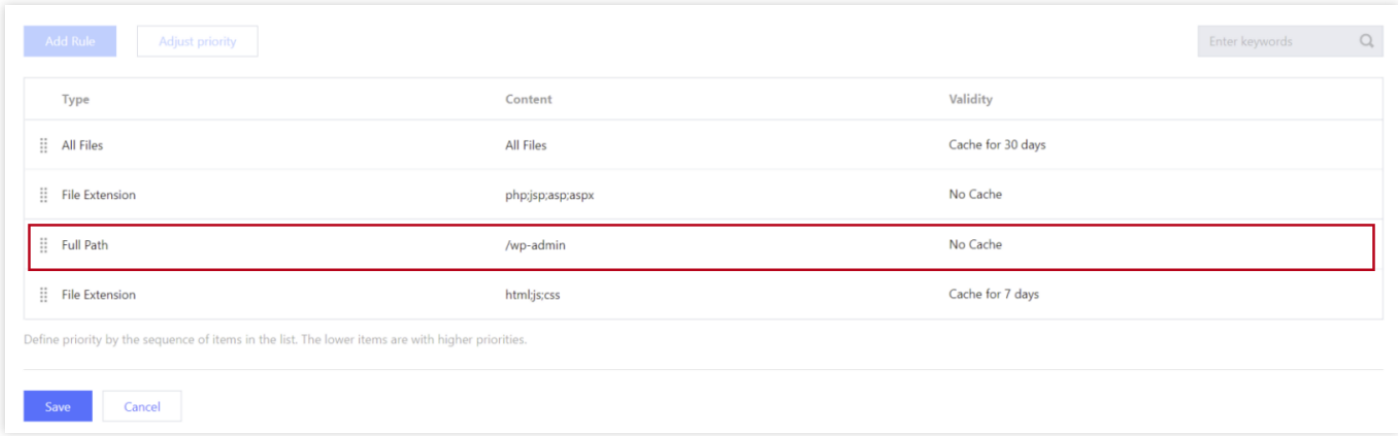
2. **ルールを新規作成**をクリックし、タイプはファイルの拡張子、内容はhtml;js;css、キャッシュオプションは「キャッシュを格納する」、キャッシュの有効期限は7日、強制キャッシュは無効として、**OK**をクリックしま

©2013-2022 Tencent Cloud. All rights reserved.

す。



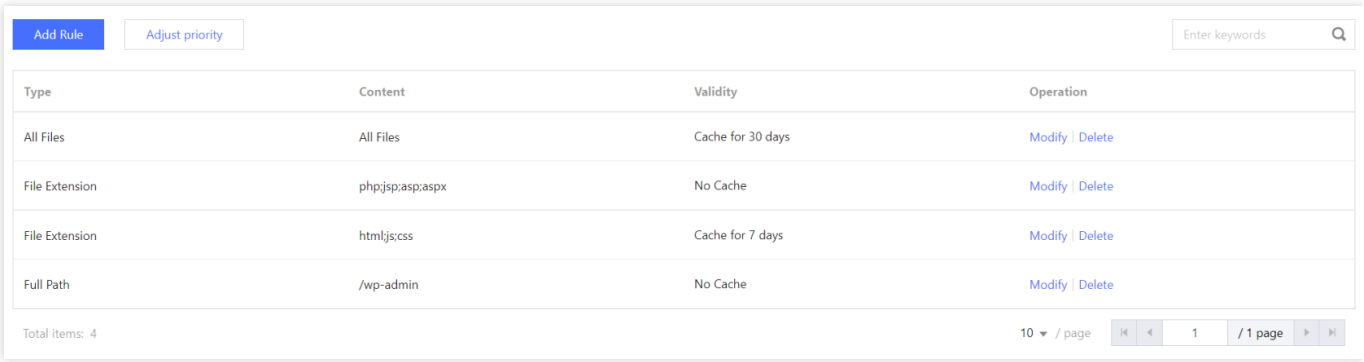
3. 下位のルールの優先度が上位のルールより高いため、**優先度を調整**をクリックし、「/wp-adminディレクトリをキャッシュしないルール」を最下位にドラッグし、優先度を最高にします。



4. 変更後のキャッシュルールは以下のとおりです：
   - /wp-adminディレクトリ配下のすべてのリソースをキャッシュしません。
   - ファイルの拡張子がhtml;js;cssのリソースのキャッシュの有効期限は7日とします。
   - ファイルの拡張子がphp;jsp;asp;aspxのリソースをキャッシュしません。

©2013-2022 Tencent Cloud. All rights reserved.

- 他のすべてのファイルのキャッシュの有効期限は30日とします。



よくあるご質問

- オリジンサーバーでファイルが変更された後、CDNアクセラレーションノード上のキャッシュはリアルタイムで自動的に更新されますか？
- どのようにユーザーからのアクセスがCDNノードのキャッシュをヒットしているかを判断しますか？

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコードキャッシュ設定

最終更新日：：2021-01-20 17:32:07

設定シナリオ

通常、CDNノードはオリジンサーバーからリクエストされたリソースを正常にプル（2XX状態コード）した場合、ノードはキャッシュ期限切れ設定のルールにしたがって処理します。
オリジンサーバーが2XX以外の状態コードに迅速に応答できず、かつ全てのリクエストをオリジンサーバーに渡すことを望まない場合は、状態コードのキャッシュ期限切れ時間を設定することで、CDNノードは2XX以外の状態コードに直接応答し、オリジンサーバーの負荷を引き下げることができます。
現在以下の状態コードをサポートしています。

- 4XX：400、401、403、404、405、407、414
- 5XX：500、501、502、503、504、509、514

> ⚠ **注意：**
>
> - 一部のプラットフォームはアップグレード中のため、現在404と403の状態コードのみをサポートしています。
> - 中国国外では現在404と403の状態コードのみをサポートしています。ドメイン名のアクセラレーションリージョンがグローバルの場合、404と403以外の状態コードのキャッシュルールは中国国内でのみ有効となります。

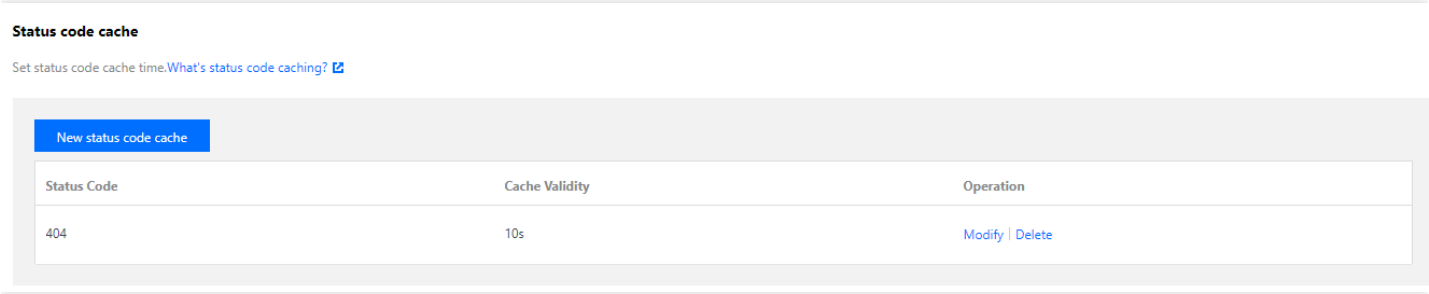
設定ガイド

設定の確認

CDN コンソールにログインし、メニューバーで【【Domain Management】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定画面に入ります。タブを【キャッシュ設定】に切り替えれば、【状態コードキャッシュ】が見つかります。

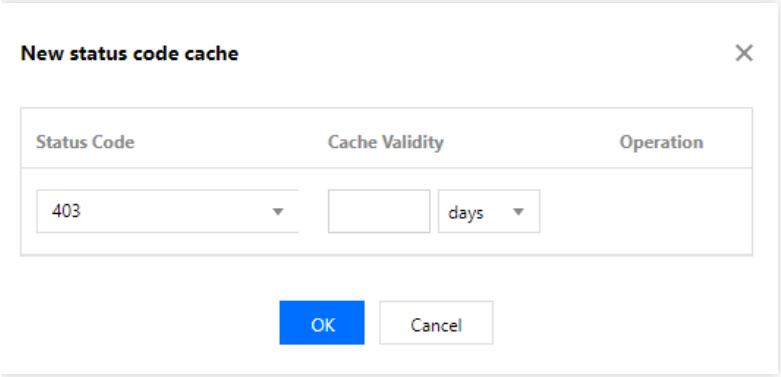
©2013-2022 Tencent Cloud. All rights reserved.

デフォルトで、「404 - キャッシュ時間10秒」のルール条項があります。



ルールの追加

必要に応じて状態コードのキャッシュルールを追加できます。【状態コードキャッシュの追加】をクリックします。



設定の制約：

- １つの状態コードには1条項のルールの追加のみサポートされています。追加を繰り返すことはできません。
- キャッシュ時間が0の場合は、キャッシュされません。

©2013-2022 Tencent Cloud. All rights reserved.

ヘッダーキャッシュ設定

最終更新日：：2021-04-20 14:05:51

設定シナリオ

リソースに加えて、Tencent Cloud CDNはデフォルトでオリジンサーバーからの次のヘッダーをキャッシュし、ユーザーに返します。

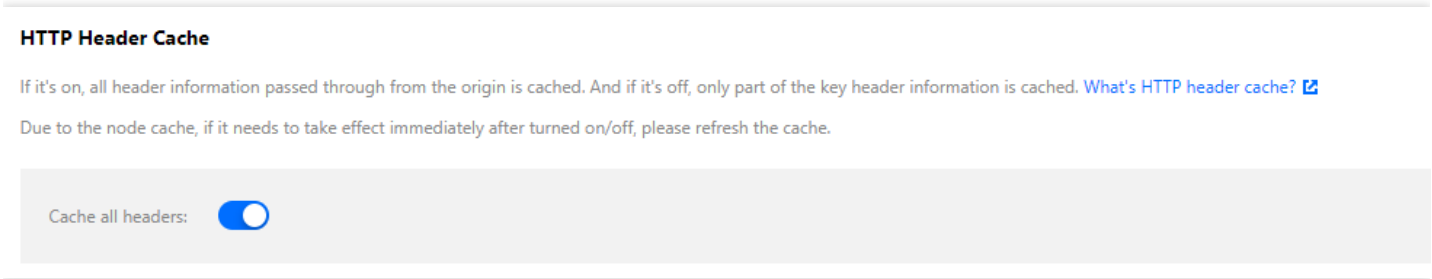
- Access-Control-Allow-Origin
- Timing-Allow-Origin
- Content-Disposition
- Accept-Ranges

オリジンサーバーに特別なヘッダーがある場合は、CDNによってキャッシュしてユーザーに返す必要がある場合は、ヘッダーキャッシュ設定を有効にすることで実現できます。

設定ガイド

設定の確認

CDNコンソールにログインし、左側のナビゲーションメニューバーで【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。【キャッシュ設定】タブで、HTTPヘッダーキャッシュ設定を確認できます。デフォルトでは無効になっています。



©2013-2022 Tencent Cloud. All rights reserved.

アクセスURL書き換え設定

最終更新日：：2021-08-06 11:22:51

設定シナリオ

実際のアクセスURLをオリジンサーバーと一致するURLに変更する必要がある場合、Tencent Cloud CDNはアクセスURL書き換え設定機能を提供しています。

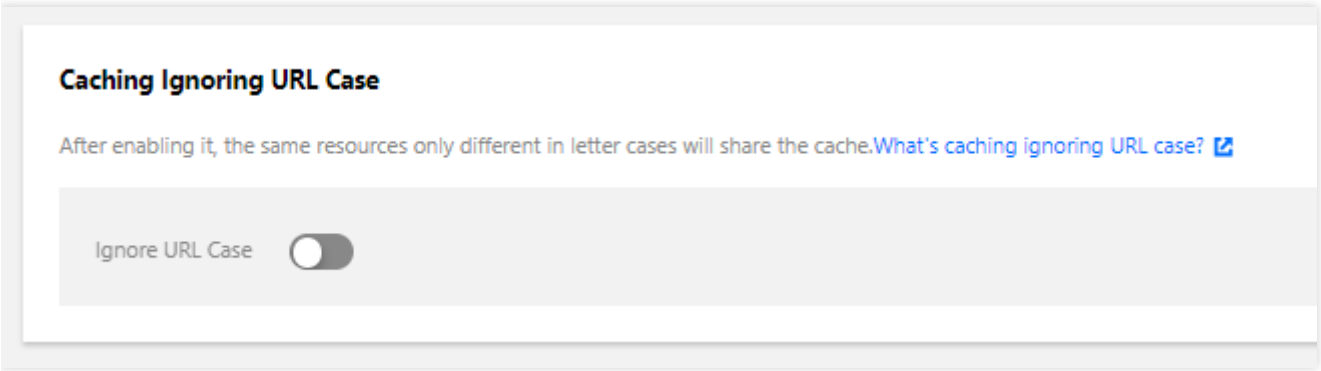
アクセスURLの書き換え設定をカスタマイズすることによって、302 URLを目標URLにリダイレクトすることができます。

設定ガイド

設定の確認

CDNコンソールにログインし、左側のメニューバーで【ドメイン名管理】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定画面に入ります。タブを【キャッシュ設定】に切り替えて、【アクセスURL書き換え設定】が表示されます。

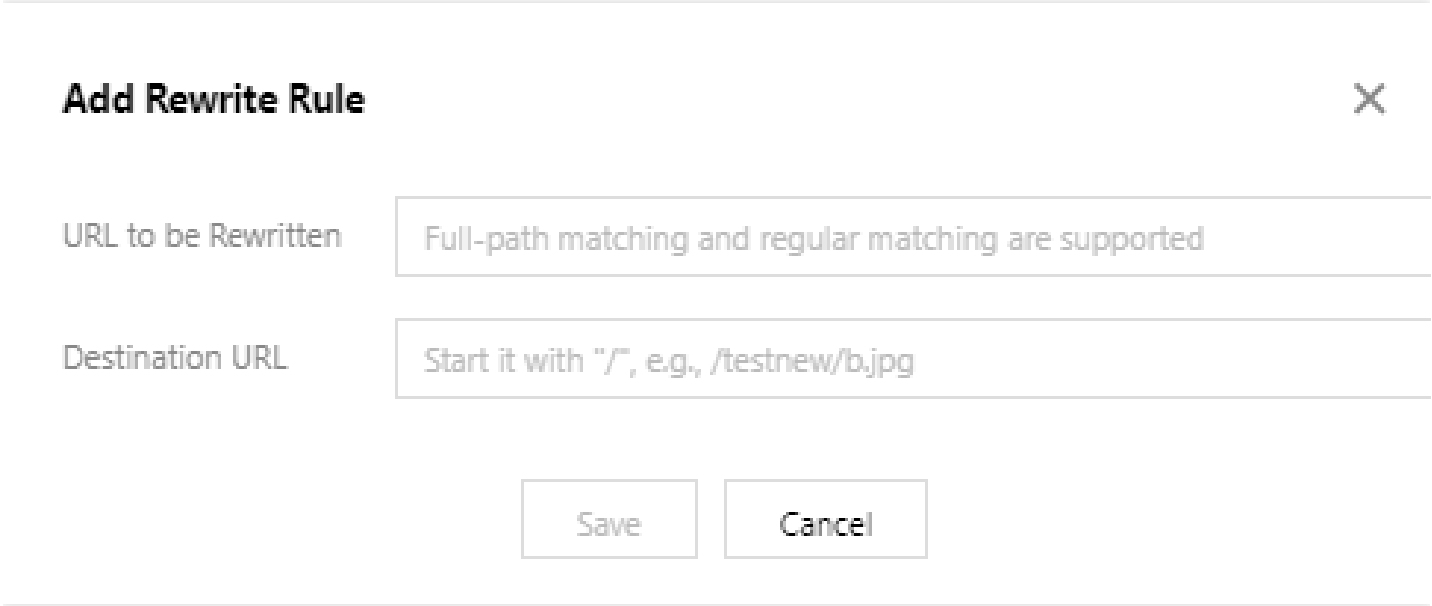
デフォルトの状態では、アクセスURL書き換え設定は無効状態になっています。



ルールの追加

©2013-2022 Tencent Cloud. All rights reserved.

必要に応じて書き換えルールを追加できます。【書き換えルールの追加】をクリックします。



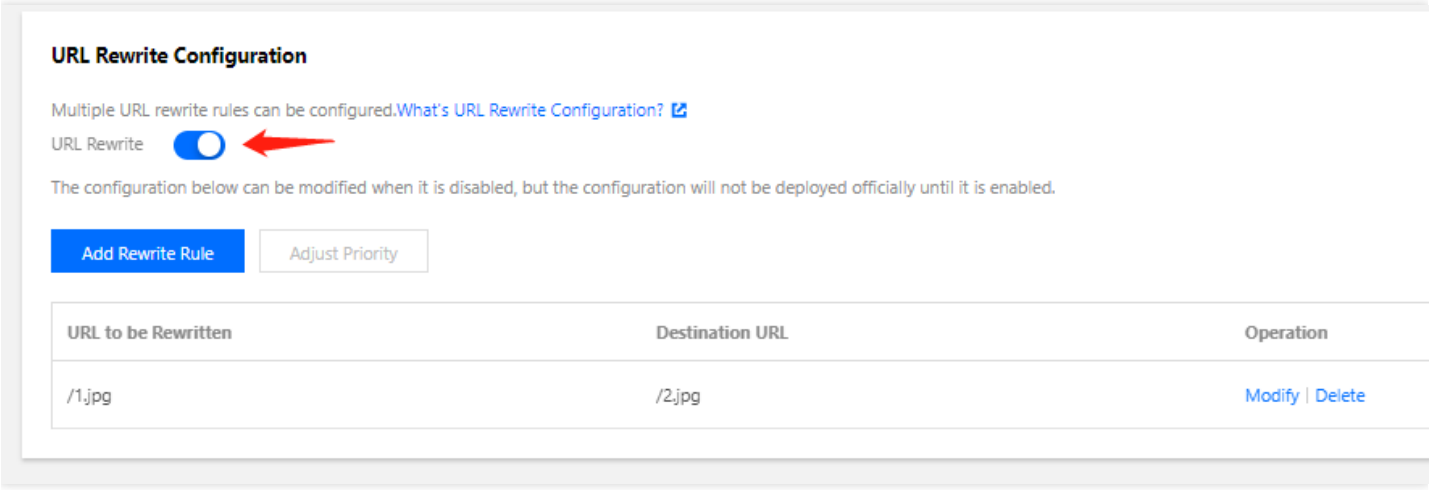
設定の制約

- 1つのドメイン名につき、最大100件の書き換えルールを追加できます。
- 複数あるルールは優先順位を変更できます。下部の優先順位が上部のものよりも高くなります
- 書き換え予定のURL：「/」で始まり、フルパス一致（例：/test/a.jpg）とワイルドカード `*` 一致（例：/test/*/*.jpg）をサポートします。ファイルディレクトリを指定する場合は、「/」で終わることはできません（例：/test）。
- 目標 Host：デフォルトは現在のドメイン名です（デフォルトではhttpヘッダーがつきます）。その他のドメイン名に変更できますが、 `http://` または `https://` のヘッダーを含める必要があります。
- 目標 Path：「/」で始まり（例：/newtest/b.jpg）、ワイルドカード `*` は `$n` （n=1,2,3...,例：/newtest/$1/$2.jpg）でキャプチャできます。ファイルディレクトリを指定する場合は、「/」で終わることはできません（例：/test）。
- ワイルドカード `*` は最大5件入力できます。キャプチャのプレースホルダー `$n` は最大10件入力できます。
- 中国語のコンテンツはサポートしていません。入力欄のコンテンツの長さは1024文字以内とすること。

設定例

©2013-2022 Tencent Cloud. All rights reserved.

アクセラレーションドメイン名 `www.test.com` の**アクセスURL書き換え設定**を行う場合は次となります。



実際のアクセス状況は次のとおりです。

- クライアントが `www.test.com/test/a.jpg` をリクエストした場合、CDNノードは `www.test.com/newtest/b.jpg` コンテンツを返します。
- クライアントが `www.test.com/test/a.png` をリクエストした場合、CDNノードは `www.newtest.com/newtest/a.png` コンテンツを返します。

©2013-2022 Tencent Cloud. All rights reserved.

ブラウザのキャッシュ有効期限を設定する

最終更新日：：2021-03-18 15:45:45

機能の概要

ブラウザのキャッシュ有効期限を設定することで、クライアントのブラウザのキャッシュポリシーをカスタマイズして、back-to-origin率を下げることができます。

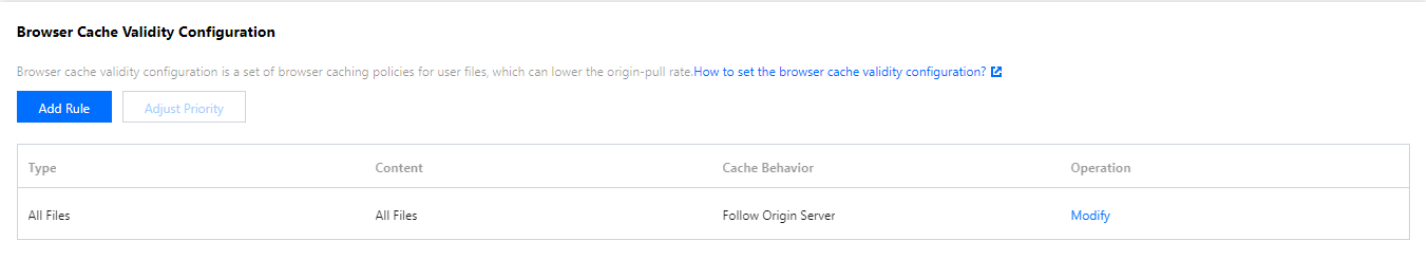
説明：

リソースをリクエストするとき、リクエストされたリソースがブラウザにキャッシュされている場合は直接返されます。ブラウザにキャッシュされていない場合は、リクエストはCDNキャッシュノードに転送されます。リソースがノードにキャッシュされている場合ノードはリソースを返し、キャッシュされていない場合はオリジンサーバーに戻って取り出します。

設定ガイド

設定の確認

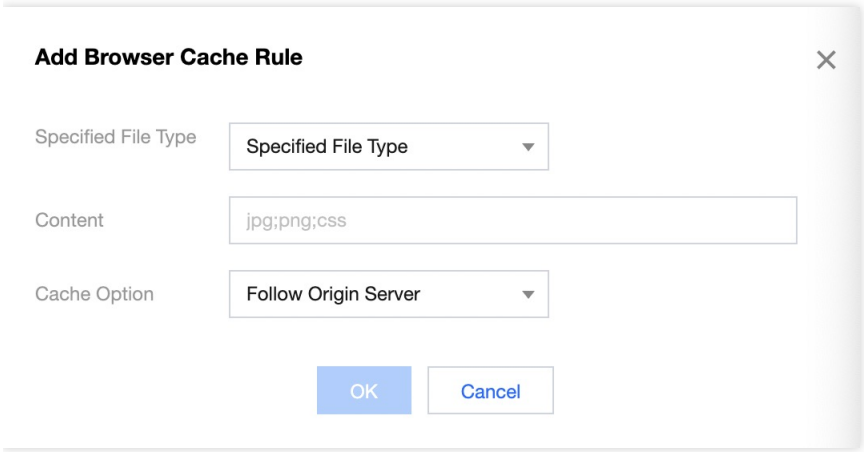
CDNコンソールにログインし、左側のナビゲーションメニューバーで【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。第3欄の【キャッシュ設定】タブで、【ブラウザのキャッシュ有効期限の設定】セクションを見つけます。



ルールの追加

必要に応じてブラウザのキャッシュ有効期限ルールを追加できます。【ルールの追加】をクリックして、ファイルタイプ、ファイルディレクトリ、ファイルパス、ホームページを指定してキャッシュを設定できます。

©2013-2022 Tencent Cloud. All rights reserved.



- オリジンサーバーに従う：オリジンサーバーのCache-Controlヘッダーに従います。
- キャッシュ：ブラウザでのリソースのキャッシュ有効期限を設定します。
- キャッシュなし：ブラウザはリソースをキャッシュしません。

設定の制約

- 一つのドメイン名には最大20のルールを含めることができます。「すべてのファイル」と「ホームページ」のルールは最大1件まで追加することができます。
- 複数のルールが設定されている場合、ルールの優先順位を変更できます。ルールリストの一番下にあるルールの優先順位が最も高くなります。
- 1つのファイルタイプ/ファイルディレクトリ/ファイルパスの各ルールには、最大50グループのコンテンツを入力でき、異なるコンテンツ間は「;」で区切ります。例：ファイルタイプ - jpg;png。
- 中国語コンテンツはサポートされていません。

©2013-2022 Tencent Cloud. All rights reserved.

キャッシュ設定に関するよくある質問

最終更新日：：2021-11-15 14:17:02

キャッシュ有効期限の設定とは何ですか。

キャッシュ有効期限の設定とは、CDNキャッシュノードがユーザーのビジネスコンテンツをキャッシュするために従うべき一連の有効期限ポリシーを指します。
CDNノードにキャッシュされたユーザーリソースは、いずれも「有効期限切れ」の問題に直面しています。リソースの有効期限が切れていない場合は、ユーザーリクエストがノードに到達すると、ノードはリクエストされたリソースをユーザーに直接返し、取得速度を向上させます。リソースの有効期限が切れている場合は、（即ち、設定された有効時間を超えた場合）、ノードはユーザーリクエストをオリジンサーバーに転送します。オリジンサーバーのコンテンツが更新されている場合、コンテンツを再取得してノードにキャッシュしてから、ユーザーに返します。オリジンサーバーのコンテンツが更新されない場合、リソースのキャッシュ時間のみが更新されます。適切なキャッシュ有効期限を設定することで、リソースヒット率を効果的に向上させ、back-to-origin率を低下させ、帯域幅の使用量を削減できます。

ファイルがブラウザキャッシュに保持される期間をどのように制御しますか。

コンソールでブラウザのキャッシュ有効期限を設定できます。詳細については、ブラウザのキャッシュ有効期限をご覧ください。

CDNオリジンサーバ（自分のサーバを使用）が特定のファイルをキャッシュしないようにするには、どうしたらよいですか。キャッシュの有効期限が0秒に設定されている場合、キャッシュしないという意味ですか。

ユーザーは、ディレクトリとファイルのタイプに応じて対応するキャッシュの有効期限を設定することができます。キャッシュ有効期限が0に設定されている場合、CDNノードが該当リソースをキャッシュしません。その場合、ユーザーがCDNノードにアクセスリクエストを送信するたびに、CDNノードはオリジンサーバーから関連リソースを取り出す必要があります。キャッシュ設定の詳細については、ノードキャッシュの設定をご参照ください。

Tencent Cloudはどのようなキャッシュ有効期限の設定をサポートしていますか。

Tencent Cloud CDNサービスは、さまざまなファイルタイプのキャッシュアクションとキャッシュ有効期限ルールの設定をサポートしています。また、カスタムキャッシュルールの優先度を調整することもできます。適切なキャッシュ有効期限ルールを設定することで、リソースヒット率を効果的に向上させ、back-to-origin率を低下させ、帯域幅の使用量を削減できます。リンクをクリックして、 キャッシュ設定についてさらに詳しい解説をご覧ください

CDNのデフォルトのキャッシュ設定は何ですか。

©2013-2022 Tencent Cloud. All rights reserved.

アクセラレーションドメイン名を追加すると、さまざまなアクセラレーションサービスタイプに基づいて、CDNはデフォルトのノードキャッシュ有効期限ルールを追加します。必要に応じて変更できます。

- 静的アクセラレーションが選択されている場合、通常の動的ファイル（php、jsp、asp、aspxなど）はデフォルトでキャッシュされず、他のすべてのファイルはデフォルトでオリジンサーバーに従います。
- ダウンロードアクセラレーションまたはストリーミングVODアクセラレーションが選択されている場合、デフォルトでは、すべてのファイルのキャッシュ有効期限は30日です。

キャッシュの一致ルールとは何ですか。

複数のキャッシュポリシーが設定されている場合、ルールリストの一番下にあるルールの優先順位が最も高くなります。ドメイン名が次のように設定されているとします：

```
All files - 30 days
.php .jsp .aspx - 0 seconds
.jpg .png .gif - 300 seconds
/test/*.jpg - 400 seconds
/test/abc.jpg - 200 seconds
```

ドメイン名が `www.test.com` で、リソースが `www.test.com/test/abc.jpg` の場合、その一致ルールは次のようになります。
1.1番目のルールと一致し、ヒットしました。この場合のキャッシュの有効期限は30日です。
2.2番目のルールと一致し、ヒットしませんでした。
3.3番目のルールと一致し、ヒットしました。この場合のキャッシュの有効期限は300秒です。
4.4番目のルールと一致し、ヒットしました。この場合のキャッシュの有効期限は400秒です。
5.5番目のルールと一致し、ヒットしました。この場合のキャッシュの有効期限は200秒です。

そのため、最終のキャッシュ有効期限が200秒となります。

©2013-2022 Tencent Cloud. All rights reserved.

Back-to-Origin設定
Back-to-Origin of Range 設定

最終更新日：：2023-03-14 15:13:28

ファイルが静的な大容量ファイルで構成されている場合は、Back-to-Origin of Rangeを有効にすると、Back-to-Originファイルの応答性が向上し、大容量ファイルの配信効率が向上します。

機能の説明

Back-to-Origin of Rangeとは、RangeリクエストのBack-to-Originのことで、RangeはHTTPリクエストヘッダーの1つで、指定された範囲内のファイルを取得するために使用されます。Rangeリクエストを使用すると、サーバーにファイルの内容の一部をリクエストできます。例えば、リクエストにHTTPヘッダー「range：bytes=0～999」が含まれる場合、ファイルの最初の1000バイトがユーザーに返されます。
Tencent Cloud CDNでBack-to-Origin of Range設定を有効にすると、デフォルトでBack-to-Origin of Rangeリクエストが含まれます。ユーザーがリクエストしたファイルの一部がノードでキャッシュされていないか、またはキャッシュが期限切れになっている場合、CDNはユーザーのリクエストによりBack-to-Origin of Rangeを行い、ユーザーが必要とするファイルのみをプルしてキャッシュし、ユーザーに返します。Range back-to-origin設定を無効にすると、ユーザーのリクエストにRangeリクエストが含まれていない場合、CDNはback-to-originするときにファイル全体をプルします。
APKインストールパッケージ、オーディオビデオファイルなどの大容量ファイルタイプの場合は、rangeリクエストを使用することで、大容量ファイルの配信効率が効果的に向上し、応答時間が改善され、オリジンサーバーへの負荷が軽減されます。

注意事項

1. Back-to-Origin of Range設定を有効にするには、オリジンサーバーで Rangeリクエストがサポートされている必要があります。そうでない場合、Back-to-Originが失敗する可能性があります。
2. Back-to-Origin of Range設定を有効にすると、リソースはノードのシャードにキャッシュされますが、各シャードのキャッシュの有効期限が全部一致し、ユーザーが指定したキャッシュ有効期限ルールに従います。
3. リソースがすべて静的な小容量ファイルの場合、またはオリジンサーバーがCOSオリジンサーバーであり、かつデータ処理系の機能（画像処理など）をすでに使用している場合は、Back-to-Origin of Rangeを有効にするとback-to-originに影響が生じるおそれがあるため、お勧めしません。
4. リソースがすべて静的な大容量ファイルの場合で、なおかつオリジンサーバーがRangeリクエストをサポートしているか、またはオリジンサーバーがCOSオリジンサーバーであり、かつデータ処理系の機能（画像処理な

©2013-2022 Tencent Cloud. All rights reserved.

ど）を使用していない場合は、配信効率と応答速度を向上させるためにBack-to-Origin of Rangeを有効にすることをお勧めします。

設定についての説明

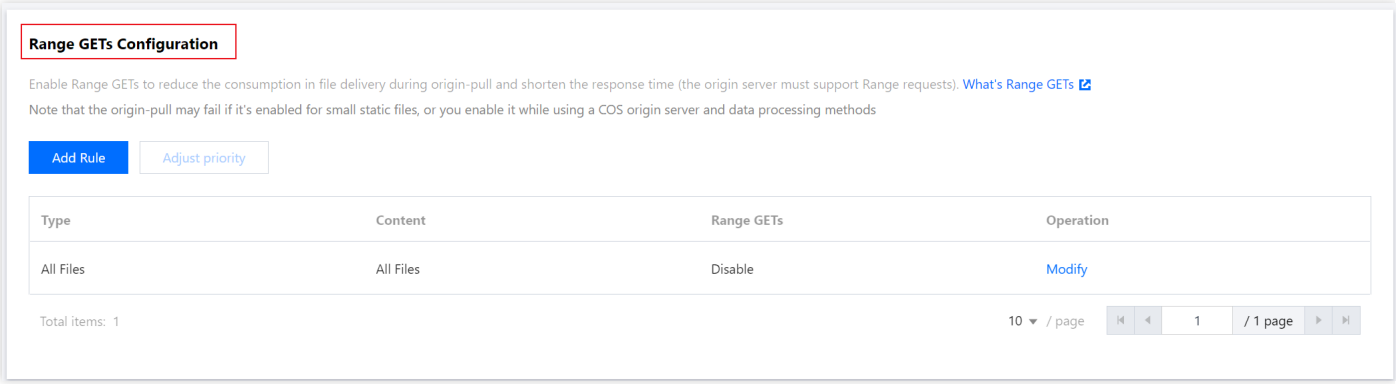
ドメイン名管理の設定

1. CDNコンソールにログインします。

2. 左側のメニューで**ドメイン名管理**をクリックし、ドメイン名管理リストへ進みます。

3. 設定するドメイン名を選択し、**管理**をクリックして、ドメイン名の設定ページへ進みます。

4. 「**Back-to-Origin設定**」をクリックして「Back-to-Origin設定」タブに移動します。タブには、Back-to-Origin設定項目が表示されます。



5. Back-to-Origin設定では、デフォルトですべてのファイルのBack-to-Origin設定が無効になっています。必要に応じて、ファイルに複数のルールを追加するようにカスタマイズできます。また、ファイルの接尾辞、ファイルディレクトリ、フルパスファイルに基づいてBack-to-Origin of Rangeをマッチングすることができます。

設定項目	説明

©2013-2022 Tencent Cloud. All rights reserved.

設定項目	説明
タイプ	すべてのファイル、指定されたファイル接尾辞、ファイルディレクトリ、フルパスファイルを対象に設定できます。 すべてのファイル：すべてのファイルにこのBack-to-Origin of Rangeルールを使用します。デフォルトのルールは削除できません。 ファイル接尾辞：ファイルの接尾辞に従って、Back-to-Origin of Rangeルールを適用します。 ファイルディレクトリ：指定されたファイルディレクトリに従って、Back-to-Origin of Rangeルールを適用します。 フルパスファイル：Back-to-Origin of Rangeルールを適用する特定のパスファイルを指定できます。
内容	選択したファイルタイプによって、次のような内容の入力制約があります。 タイプがファイル接尾辞の場合：ファイル接尾辞の文字列でマッチングすることがサポートされます。複数の場合は「;」で区切ります。 タイプがファイルディレクトリの場合：「/test;/a/b/c」のようなファイルディレクトリの入力がサポートされます。ただし「/」で終わることはできません。複数の場合は「;」で区切ります。 タイプがフルパスファイルの場合：「/index.html;/test/*.jpg」のようなファイルディレクトリの入力がサポートされます。ファイルパスは*でマッチングすることがサポートされます。複数の場合は「;」で区切ります。
Back-to-Origin of Range	有効/無効がサポートされます。 有効：Back-to-Origin of Rangeを有効にすると、Back-to-Originをリクエストする時、Back-to-Origin of Rangeリクエストを使用します。有効にすると、ユーザリクエストにrangeリクエストが含まれていない場合、リクエストファイルが4Mより大きければ、CDNノードではサイズが1Mのシャードでrangeリクエストを Back-to-Originします。ファイルが4Mより小さければ、CDNノードではBack-to-Originを行い完全なファイルを取得します。ユーザリクエストにrangeリクエストが含まれている場合、含まれたrangeリクエストに従って、back-to-originをリクエストします。 無効：Back-to-Origin of Rangeを無効にすると、Back-to-Originをリクエストする時、Back-to-Origin of Rangeリクエストを使用しません。

推奨設定

ファイルサイズが4MBを超える場合は、そのファイルタイプに対してBack-to-Origin of Rangeを有効にすることをお勧めします。ファイルの一部のみが大容量の場合は、ファイルタイプ/ファイルディレクトリ/フルパスファイルでマッチングした一部の大容量ファイルにBack-to-Origin of Rangeを有効にし、他のファイルにBack-to-Origin of Rangeを使用しないように設定することをお勧めします。

設定の制約

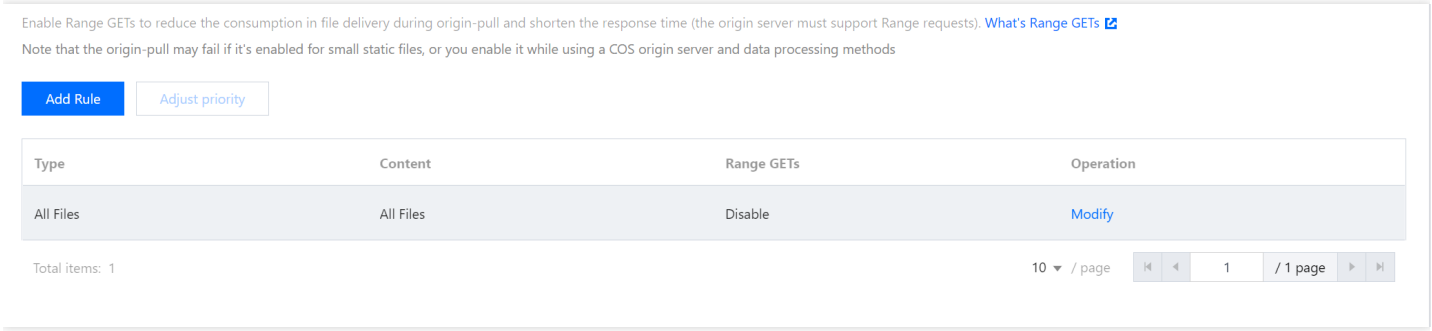
©2013-2022 Tencent Cloud. All rights reserved.

Back-to-Origin of Range設定は、最大20件のルールを設定することをサポートします。ルールの優先順位は、一番下のルールが最も優先順位が高く、一番上のルールが最も優先順位が低い。ユーザーがファイルをリクエストすると、ルールの優先順位に従って順次マッチングします。マッチングに成功すると、優先順位が最も高いルールに従って優先的に実行されます。

設定例

例1

すべてのファイルでBack-to-Origin of Rangeを有効にする必要がある場合、ドメイン名 `cloud.tencent.com` のBack-to-Origin of Rangeは次のように設定されます：

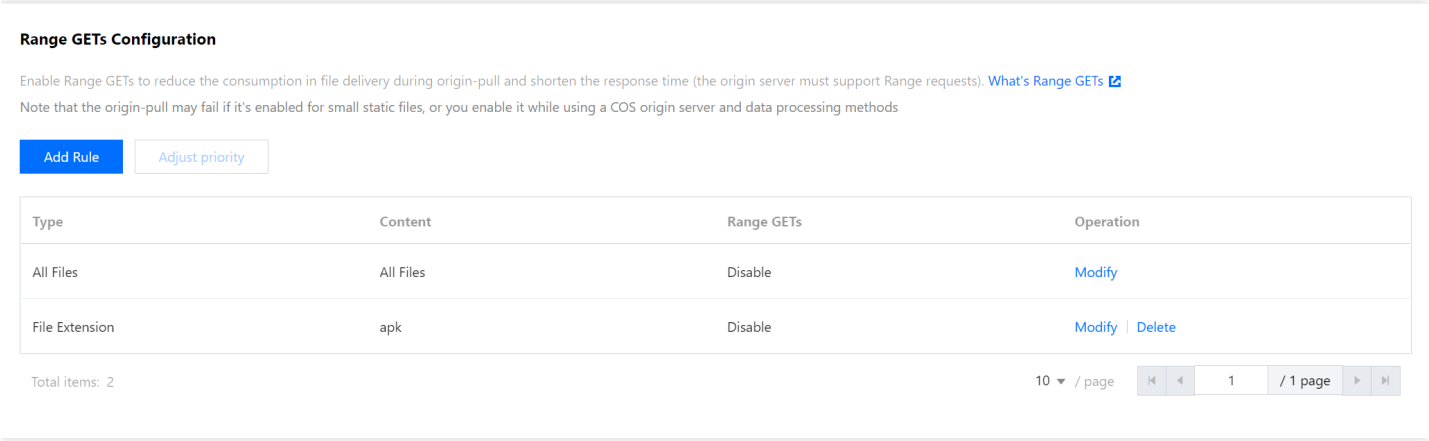


ユーザーAがリソース `http://cloud.tencent.com/test.ap` kをリクエストする場合は、ノードがリクエストを受信し、キャッシュされている `test.apk` ファイルがすでに期限切れであることが判明すると、Back-to-Originリクエストを送信します。ノードBack-to-OriginはRangeリクエストを使用し、シャードごとにリソースを取得してキャッシュします。この時に、ユーザーBも同様に同一ノードに同じファイルのRangeリクエストを送信し、ノードに保存されているシャードがすでにRangeリクエストで指定されたバイトセグメントと一致する場合、リソースはすべてのシャードの取得が完了するまで待つ必要がなく、直接ユーザーに返します。

例2

現在、一部のファイルのみがBack-to-Origin of Rangeを使用する必要がある場合、ドメイン名 `cloud.tencent.com` のBack-to-Origin of Rangeは次のように設定されます：

©2013-2022 Tencent Cloud. All rights reserved.



ユーザーAがリソース `http://cloud.tencent.com/test.apk` をリクエストする場合、下のルールは上のルールよりも優先順位が高いので、ノードリソースがヒットしなかったり、キャッシュが期限切れになったりした場合、このリクエストはBack-to-Origin of Rangeを使用します。ユーザBがリソース `http://cloud.tencent.com/test.jpg` をリクエストし、このルールはすべてのファイルにのみマッチングする場合、そのリクエストにBack-to-Originが発生すると、Back-to-Origin of Rangeが使用されません。

©2013-2022 Tencent Cloud. All rights reserved.

Follow 301/302

最終更新日：：2021-05-25 15:45:01

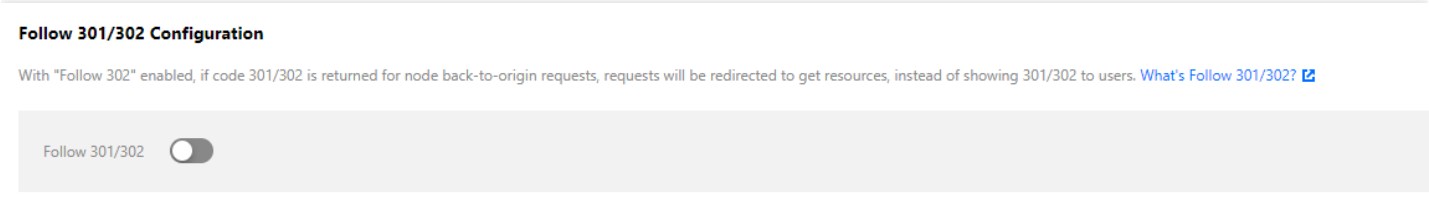
設定の概要

Tencent Cloud CDNは、デフォルトでは301/302ステータスコードをキャッシュしません。オリジンサーバーから301/302リクエストを返すと、CDNノードはデフォルトでクライアントに応答を返し、クライアントは対応するリソースにリダイレクトされアクセスします。

「Follow 301/302 設定」が有効になっている場合は、CDNノードは、back-to-origin中に301/302リダイレクト要求を受信すると、必要なリソースを取得するまでリダイレクトされます（最大3回フォロー可能）。実際のリソースをクライアントに返し、クライアントをリダイレクトする必要はありません。

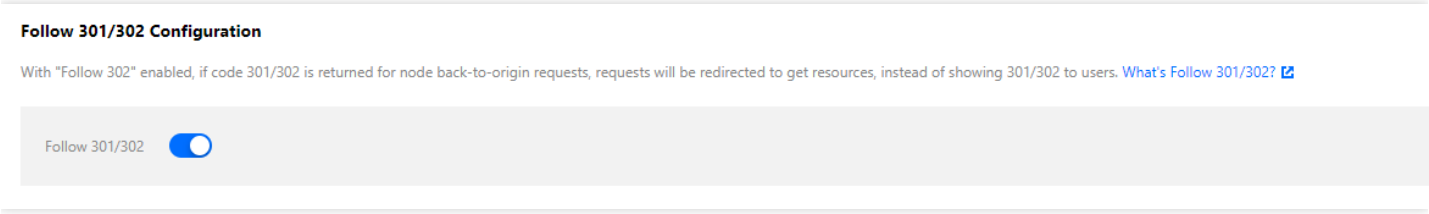
設定ガイド

CDNコンソールにログインし、メニューバーで【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。第4欄の【back-to-origin設定】タブで【Follow 301/302 設定】をを見つけます。この設定はデフォルトで無効になっています。



設定例

ドメイン名 `cloud.tencent.com` の「Follow 301/302 設定」が次のように設定されているとします



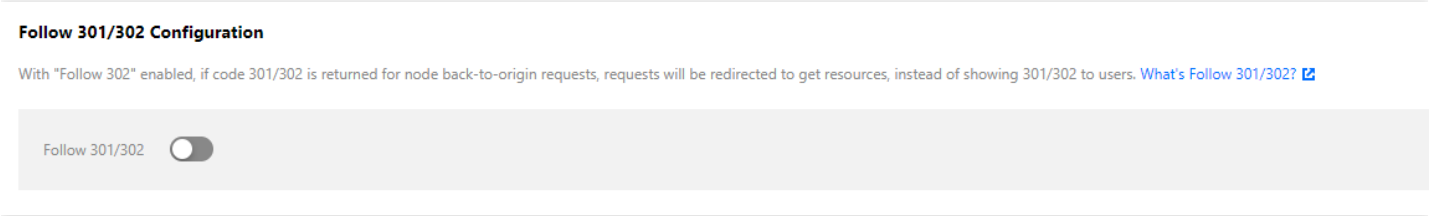
ユーザーAがリソース `http://cloud.tencent.com/1.jpg` をリクエストします。ノードでキャッシュヒット

©2013-2022 Tencent Cloud. All rights reserved.

しない時は、ノードはオリジンサーバーへリクエストを転送してリソースを要求します。オリジンサーバーから返されたHTTP Response ステータスコードが302で、リダイレクト先アドレスがhttp://cloud.tencent.com/1.jpgの場合、次のようになります。

1. 「Follow 301/302 設定」を有効にした後、ノードは301/302ステータスコードを含むHTTP応答を受信すると、リダイレクトアドレスへ直接にリクエストを送信します。
2. 必要なリソースを取得し、ノードにキャッシュしてから、ユーザーに返されます。
3. この時に、ユーザーBも `http://cloud.tencent.com/1.jpg` に対しリクエストを送信すると、直接キャッシュをヒットし、リソースがユーザーに返されます。
4. 「Follow 301/302 設定」を有効にした後、最大3回までのリダイレクトをフォローします。この制限を超えると、301/302ステータスコードがユーザーに返されます。

ドメイン名 `cloud.tencent.com` の301/302リダイレクト設定は以下のとおりです。



ユーザーAがリソース `http://cloud.tencent.com/1.jpg` をリクエストします。ノードでキャッシュヒットしない時は、ノードはオリジンサーバーへリクエストを転送してリソースを要求します。オリジンサーバーから返されたHTTP Response ステータスコードが301/302で、リダイレクト先アドレスがhttp://cloud.tencent.com/1.jpgの場合、次のようになります。

1. ノードはHTTP応答をユーザーに直接返します。
2. ユーザーは `http://xxx.tencent.com/1.jpg` に対しリクエストを送信し、当該ドメイン名がCDNに接続されていない場合、アクセラレーションは有効になりません。
3. この時、ユーザーBも `http://cloud.tencent.com/1.jpg` に対しリクエストを送信すると、上記プロセスが繰り返されます。

©2013-2022 Tencent Cloud. All rights reserved.

back-to-originタイムアウト時間の設定

最終更新日：：2020-07-21 18:51:09

設定シナリオ

Tencent Cloud CDNがリクエストをオリジンサーバーに転送する場合、デフォルトでTCP接続のタイムアウト時間が5秒で、back-to-originのデータロードのタイムアウト時間が10秒です。back-to-origin時間が上記の制限時間を超えると、障害が発生することがよくあります。

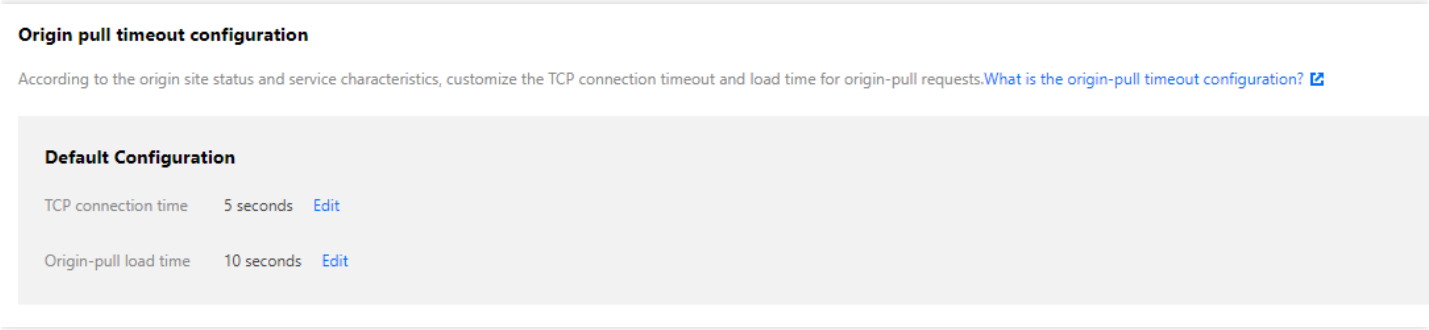
オリジンサーバーのデータ処理状況とネットワークの状況に応じて、back-to-originのTCP接続とデータロードのタイムアウト期間を調整して、back-to-originを正常に完了させることができます。

設定ガイド

設定の確認

CDNコンソールにログインし、左側のナビゲーションメニューバーで【ドメイン管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。【back-to-origin設定】タブで、back-to-originのタイムアウト設定を確認することができます。デフォルトでは以下のようになります。

- TCP接続のタイムアウト時間は5秒です。
- back-to-originの読み込みタイムアウト時間は10秒です。

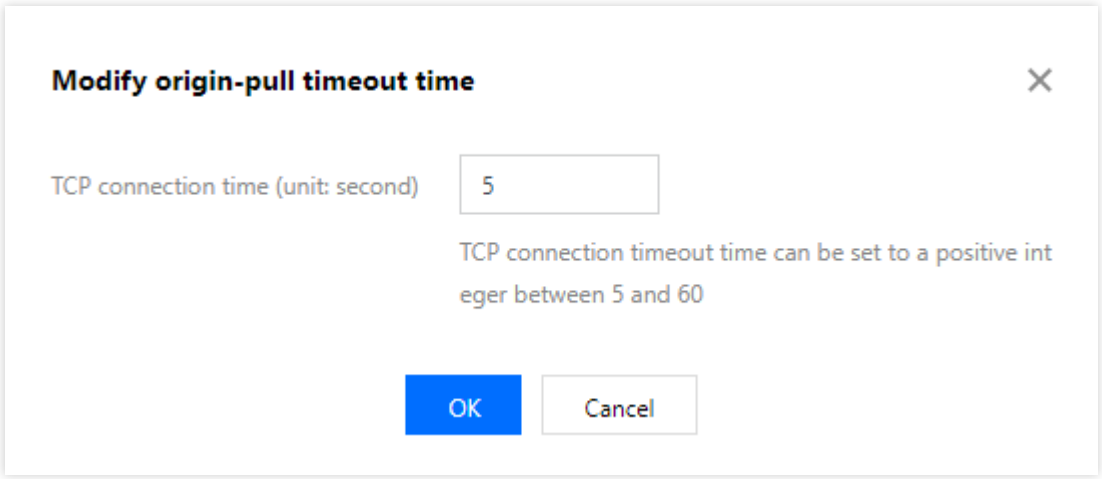


設定の変更

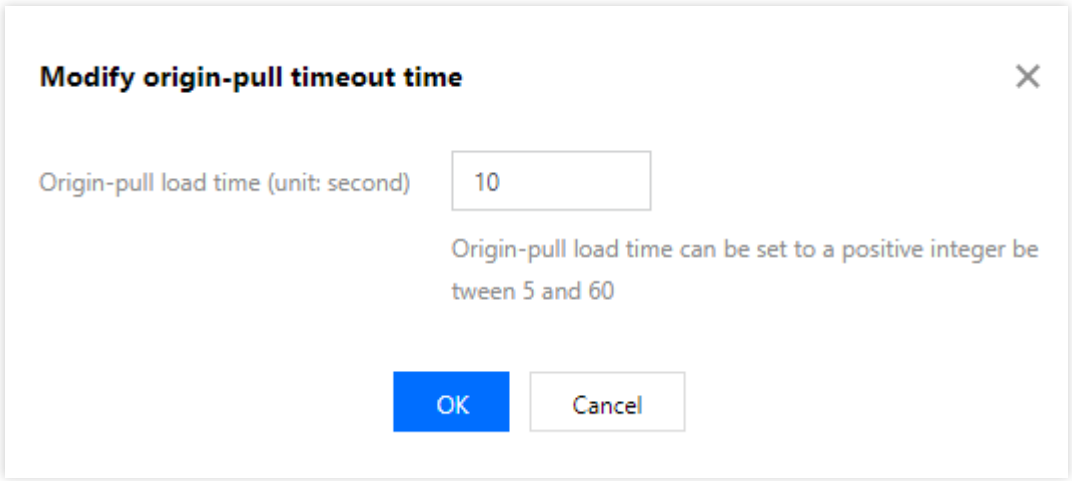
右側の【編集】をクリックして、対応するタイムアウト時間を必要に応じて変更することができます。

©2013-2022 Tencent Cloud. All rights reserved.

- TCP接続のタイムアウト時間は5～60秒に設定できます。



- back-to-originの読み込みタイムアウト時間は5～60秒に設定できます。



アクセラレーションドメイン名がグローバルアクセラレーション用に設定されている場合、設定されたback-to-originタイムアウト時間はグローバルに有効になります。

©2013-2022 Tencent Cloud. All rights reserved.

Back-to-Origin HTTP ヘッダーの設定

最終更新日：：2021-05-19 14:08:25

設定シナリオ

Tencent Cloud CDNは、Back-to-Originリクエストヘッダーの追加をサポートします。

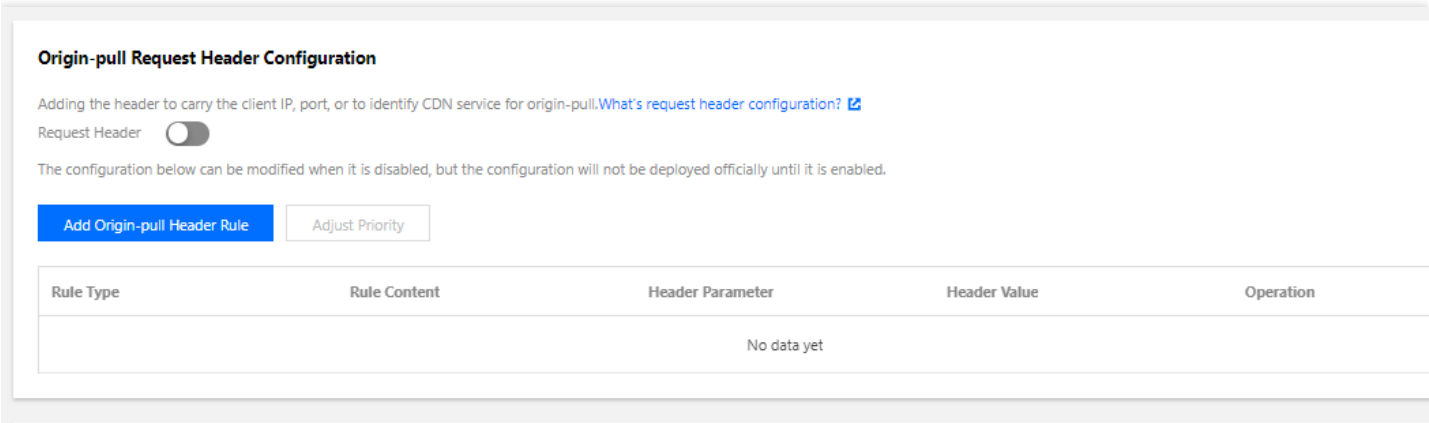
- X-Fiorward-Forヘッダを通じて、実際のクライアントIPをオリジンサーバーに転送することをサポートします。
- X-Forward-Port ヘッダーを通じて実際のクライアントポートをオリジンサーバーに転送することをサポートし、オリジンサーバー側の分析に用います。
- さまざまなカスタムヘッダーの追加をサポートします。

カスタムback-to-originリクエストヘッダーの設定と削除もサポートします。

設定ガイド

設定の確認

CDNコンソールにログインし、左側のナビゲーションウィンドウで【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。【back-to-origin設定】タブを選択して、[Back-to-origin Request Headerの設定]セクションを見つけます。 この機能はデフォルトで無効になっています。



操作タイプ

操作タイプ	説明

©2013-2022 Tencent Cloud. All rights reserved.

操作タイプ	説明
設定	指定されたリクエストヘッダーパラメータの値を設定します。 設定されたヘッダーが存在しない場合、そのヘッダーが追加されます。 back-to-originリクエストヘッダーパラメータがすでに存在する場合、設定された新しいリクエストヘッダーが古いリクエストヘッダーを上書きし、一意になります。
追加	指定されたback-to-originリクエストヘッダーパラメータを追加します。 設定されたヘッダーがすでに存在する場合、追加されたリクエストヘッダーが古いヘッダーを上書きし、一意になります。
削除	指定された応答ヘッダーパラメータを削除します。

注意：

- 最下位の優先度が最上位よりも高い-この相対位置の優先度は、複数のヘッダールールの追加、複数のヘッダールールの削除または複数のヘッダールールの設定など、同じタイプのヘッダー操作に制限されます。
- 一つのback-to-originリクエストヘッダーパラメータに複数のルールが混在している場合は、操作タイプの優先度に従って実行され、その順序は追加>削除>設定となります。例えば、X-CDNヘッダーの追加、削除、設定が同時に存在するルールでは、最初に追加、次に削除、最後に設定という順に実行します。

ヘッダーパラメータ

ヘッダーパラメータ	説明
X-Forward-For	実際のクライアントIPを転送するために使用されます。デフォルト値は$client_ip変数であり、変更できません。
X-Forward-Port	実際のクライアントポートを転送するために使用されます。デフォルト値は$remote_port変数であり、変更できません。
カスタムヘッダー	デフォルトのキーの長さは1〜100文字で、0〜9の数字、a - z、A - Zの英文字、および特殊記号「-」で構成されます。 Valueの長さは1〜1000文字で、漢字はサポートされていません。 一部の標準ヘッダーは、ユーザーが設定、追加、または削除できません。詳細なリストについては、注意事項をご覧ください。

注意：

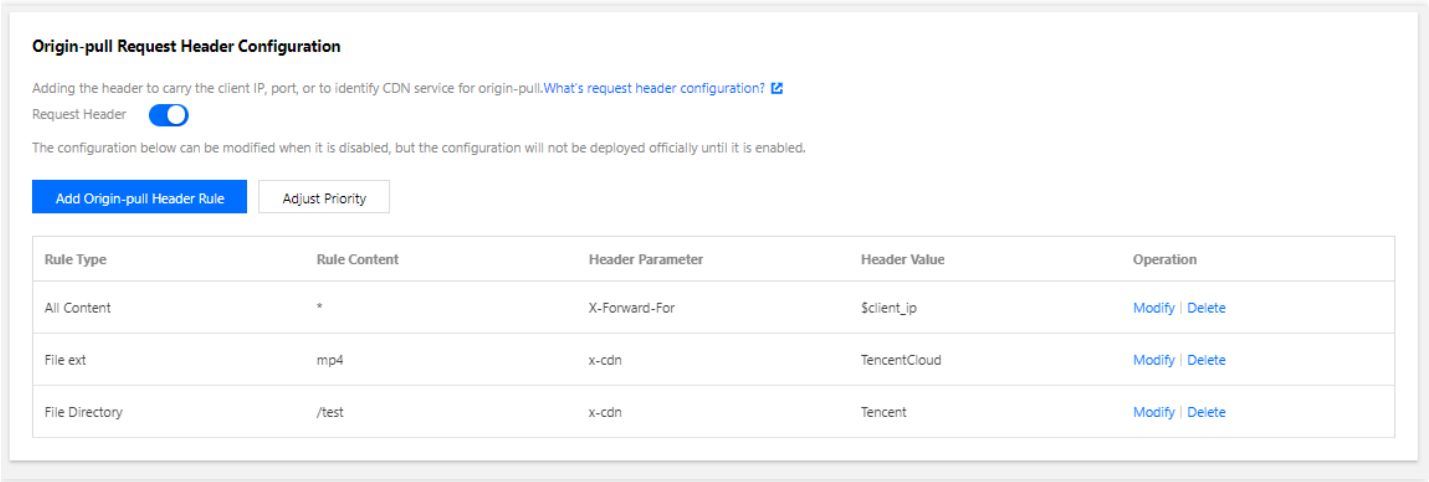
- 最大10のback-to-originリクエストヘッダールールを設定できます。

©2013-2022 Tencent Cloud. All rights reserved.

- 有効なタイプは、すべてのファイル、ファイルタイプ、ファイルディレクトリ、および指定されたファイルパスの4つのモードをサポートします。正規表現マッチングは一時的にサポートしていません。

設定例

アクセラレーションドメイン名 `cloud.tencent.com` のback-to-origin Request Headerが次のように設定されているとします。



アクセスされたリソースが `http://cloud.tencent.com/test/test.mp4` の場合、

1. `*` ルールにヒットすると、 `X-Forward-For:$client_ip` ヘッダーが追加され、back-to-origin中に$client_ipを実際のクライアントIPに置き換えます。
2. `.mp4` ファイルタイプおよび `/test` パスにヒットすると、同じヘッダー操作タイプ - 追加であることから、最下位の優先度が最上位より高くなり、 `x-cdn:Tencent` のヘッダーが追加されます。

注意事項

次の標準ヘッダーは、一時的にback-to-origin Request Headerの設定/追加/削除をサポートしていません。

www-authenticate	authorization	proxy-authenticate	proxy-authorization
age	cache-control	clear-site-data	expires
pragma	warning	accept-ch	accept-ch-lifetime
early-data	content-dpr	dpr	device-memory

©2013-2022 Tencent Cloud. All rights reserved.

www-authenticate	authorization	proxy-authenticate	proxy-authorization
save-data	viewport-width	width	last-modified
etag	if-match	if-none-match	if-modified-since
if-unmodified-since	vary	connection	keep-alive
accept	accept-charset	expect	max-forwards
access-control-allow-origin	access-control-max-age	access-control-allow-headers	access-control-allow-methods
access-control-expose-headers	access-control-allow-credentials	access-control-request-headers	access-control-request-method
origin	timing-allow-origin	dnt	tk
content-disposition	content-length	content-type	content-encoding
content-language	content-location	forwarded	x-forwarded-host
x-forwarded-proto	via	from	host
referer-policy	allow	server	accept-ranges
range	if-range	content-range	cross-origin-embedder-policy
cross-origin-opener-policy	cross-origin-resource-policy	content-security-policy	content-security-policy-report-only
expect-ct	feature-policy	strict-transport-security	upgrade-insecure-requests
x-content-type-options	x-download-options	x-frame-options(xfo)	x-permitted-cross-domain-policies
x-powered-by	x-xss-protection	public-key-pins	public-key-pins-report-only

©2013-2022 Tencent Cloud. All rights reserved.

www-authenticate	authorization	proxy-authenticate	proxy-authorization
sec-fetch-site	sec-fetch-mode	sec-fetch-user	sec-fetch-dest
last-event-id	nel	ping-from	ping-to
report-to	transfer-encoding	te	trailer
report-to	transfer-encoding	te	trailer
sec-websocket-version	accept-push-policy	accept-signature	alt-svc
date	large-allocation	link	push-policy
retry-after	signature	signed-headers	server-timing
service-worker-allowed	sourcemap	upgrade	x-dns-prefetch-control
x-firefox-spdy	x-pingback	x-requested-with	x-robots-tag
x-ua-compatible	max-age		

©2013-2022 Tencent Cloud. All rights reserved.

back-to-origin URL書き換え

最終更新日：：2021-08-27 11:36:41

設定シナリオ

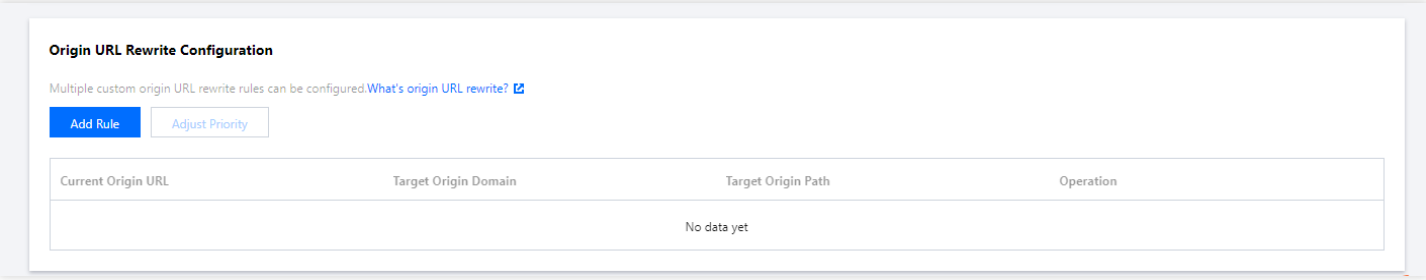
back-to-originリクエストのURLをオリジンサーバーと一致するURLに変更する必要がある場合、Tencent Cloud CDNはback-to-origin URL書き換え設定機能を提供しています。

> 注意：
> ECDNドメイン名は、現時点では、この機能の設定をサポートしていません。

設定ガイド

設定の確認

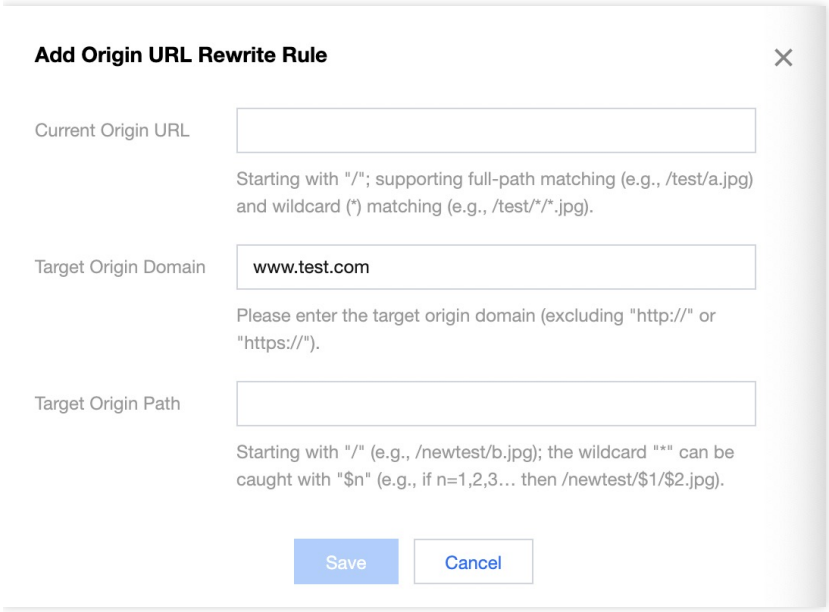
CDNコンソールにログインし、左側のメニューバーで【Domain Management】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定画面に入ります。Tabを【back-to-origin設定】に切り替えると、【Origin URL書き換え設定】が表示されます。



ルールの追加

©2013-2022 Tencent Cloud. All rights reserved.

必要に応じて書き換えルールを追加できます。【ルールの追加】をクリックします。



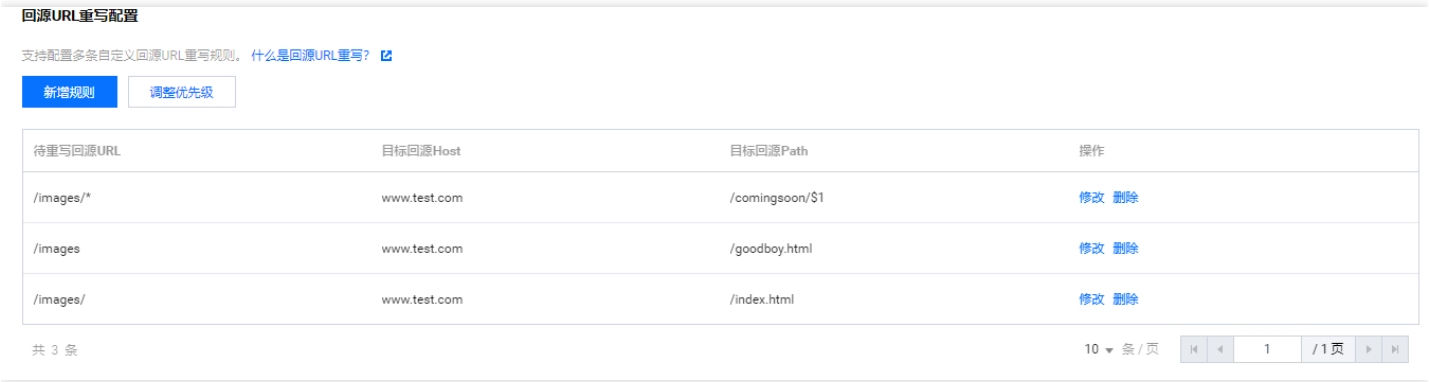
設定の制約

- 1つのドメイン名につき、最大100件の書き換えルールを追加できます。
- 複数あるルールは優先順位を変更できます。下部の優先順位が上部のものよりも高くなります
- 書き換え予定のback-to-origin URL： `/` で始まり、デフォルトはプレフィックス一致で、フルパス一致（例：/test/a.jpg）とワイルドカード `*` 一致（例：/test/*/*.jpg）もサポートします。ファイルディレクトリを指定する場合は、「/」で終わることはできません（例：/test）。
- 目標back-to-origin Host：デフォルトは現在のドメイン名です。修正は可能で、 `http://` または `https://` ヘッダーを含みません。
- 目標back-to-originパス： `/` で始まり（例：/newtest/b.jpg）、ワイルドカード `*` は `$n` でキャプチャできます（n=1,2,3...、例：/newtest/$1/$2.jpg）。ファイルディレクトリを指定する場合は、「/」で終えることはできません（例：/test）。
- ワイルドカード `*` は最大5件入力できます。キャプチャのプレースホルダー `$n` は最大10件入力できます。
- 中国語のコンテンツはサポートしていません。目標back-to-origin Hostは250文字以内とし、その他の入力欄のコンテンツは1024文字以内とします。

設定例：

アクセラレーションドメイン名 `www.test.com` の** back-to-origin URL書き換え設定**を行う場合は次のとおりとなります。

©2013-2022 Tencent Cloud. All rights reserved.



上記設定の場合、実際のback-to-originの状況は次のとおりです。

- back-to-originリクエスト `www.test.com/images/1.jpg` は第1、2、3条のルールにヒットした場合、下部の優先順位が最も高く、実際のback-to-originリクエストは `www.test.com/index.html` になります。
- back-to-originリクエスト `www.test.com/images` は第2条のルールにヒットした場合、実際のback-to-originリクエストは `www.test.com/goodboy.html` になります。

©2013-2022 Tencent Cloud. All rights reserved.

back-to-origin SNI

最終更新日：：2022-08-11 19:26:31

設定シナリオ

オリジンサーバーIPが複数のドメイン名をバインドしている場合、CDNノードがHTTPSプロトコルでオリジンサーバーにアクセスするときに、back-to-origin SNIを設定して、具体的なアクセスドメイン名を明確に指定することができます。

注意：

- back-to-origin SNIは、現時点では中国本土のアクセラレーションドメイン名のみをサポートしています。
- 一部のプラットフォームはアップグレード中のため、この設定機能を開放していません。

設定ガイド

設定の確認

デフォルトの状態では、back-to-origin SNIはオフの状態となっていますので、実際の必要性に応じてご自身で有効化してください。

設定の編集

有効化後、back-to-origin SNIを設定し、具体的なアクセスドメイン名を設定する必要があります。また、設定スイッチを再度オフにすることもできます。スイッチがオフの状態の場合は、下部に具体的な設定が存在していても、現行のネットワークが有効化されることはなく、スイッチがオンになったときのみ現行のネットワークにリリースされます。

©2013-2022 Tencent Cloud. All rights reserved.

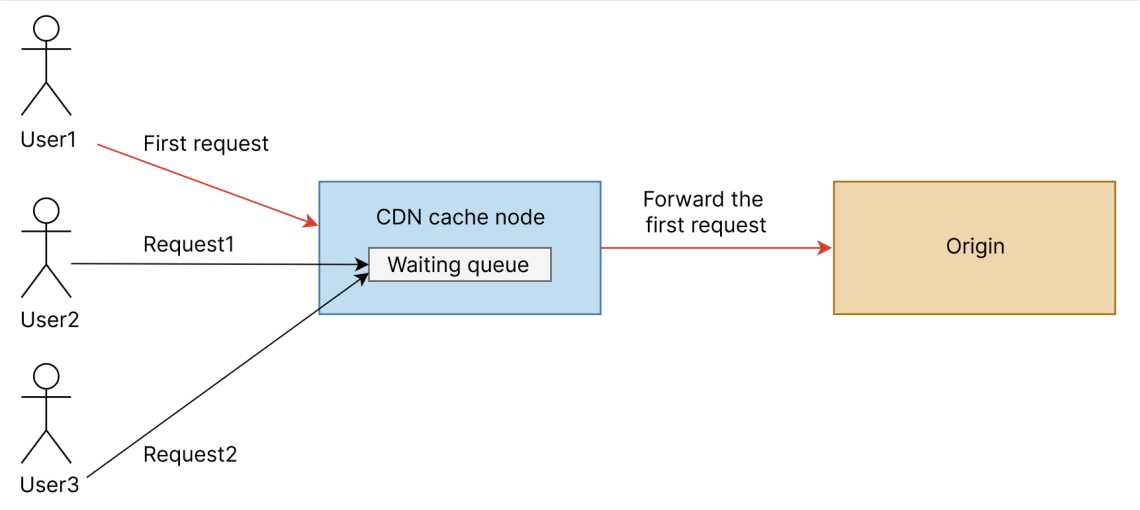
Back-to-Originマージの設定

最終更新日：：2022-12-26 17:49:56

大規模ECセールイベントのような、大量なリソースを必要とし、膨大な並列リクエストが発生する運用シーンでは、Back-to-Originマージを有効にすれば、キャッシュヒット率を向上させ、Back-to-Originの負荷を減らすことができます。

機能説明

複数のユーザーがCDNノードにキャッシングされていない同一リソースを同時に要求すると、リクエストごとにBack-to-Originが発生し、Back-to-Origin帯域幅と接続数が急増します。オリジンサーバーで性能のボトルネックになっている場合、オリジンサーバーの応答が遅くなったり、応答しなかったりして、結果的にユーザビリティが低下する可能性があります。
Back-to-Originマージとは、ノードにキャッシングされていない同一リソースを要求した複数のリクエストが発行された場合、Back-to-Originを1回だけ実行し、他のユーザーにBack-to-Originリクエストの応答を待たせる処理です。この機能はオリジンサーバーの負荷を減らし、ユーザーアクセスのヒット率を向上させることができます。
下図に示すように、3つのユーザーが同時に同じノードに同一リソースを要求すると、マインリクエストに対してBack-to-Originを実行しリソースを取得し、他のサブリクエストが待ちキューに入ります。メインリクエストに対するオリジンサーバーの応答を受信すると、メインリクエストを発行したユーザーにデータを渡し、CDNノードにキャッシングします。同時に、待ちキューにあるすべてのサブリクエストに通知します。これらのサブリクエストはキャッシュからデータを読み取り、サブリクエストを発行したユーザーに応答します。



注意事項

©2013-2022 Tencent Cloud. All rights reserved.

1. ステータスコードが200/206/304の応答だけに対して、Back-to-Originマージを実行します。
2. オリジンサーバーがcache-control: no-cache、no-store、privateまたはpragma：no-cacheなどを返し、指定したCDNノードにキャッシングできない場合、Back-to-Originマージを実行しません。
3. オリジンサーバーがchunkedを返した場合、Back-to-Originマージを実行しません。
4. GETリクエストの場合のみ、Back-to-Originマージを実行します。
5. オリジンサーバーが返したHTTP応答ヘッダーにcontent-lengthとtransfer-encodingのいずれも含まれていない場合、Back-to-Originマージを実行しません。
6. gzipやbrなどの圧縮リクエストの場合、Back-to-Originマージを実行しません。

設定説明

1.CDNコンソールにログインします。
2. 左側のメニューでドメイン名管理をクリックし、ドメイン名管理リストへ進みます。
3. 設定するドメイン名を選択し、管理をクリックして、ドメイン名の設定ページへ進みます。
4. Back-to-Origin設定をクリックしBack-to-Origin設定タブに切り替えると、Back-to-Originマージの設定項目が表示されます。

5. Back-to-Originマージはデフォルトでは無効です。必要に応じて有効にしてください。

設定例

Back-to-Originマージを有効にします。

©2013-2022 Tencent Cloud. All rights reserved.

HTTPS 設定
HTTPS 設定について

最終更新日：：2021-03-04 15:29:30

ドメイン名に既存の証明書を設定する場合は、先に次の内容をご参照ください。Tencent Cloud SSL証明書管理からの証明書を設定する場合は、この手順をスキップできます。

証明書をアップロードする

CA機構によって提供の証明書は一般的に以下の種類があります。CDNサービスは**Nginx**を使っています。

Nginxフォルダーに入り、テキストエディターで「.crt」（証明書）ファイルと 「.key」（プライベートキー）ファイルを開くと、PEMフォーマットの証明書内容及びプライベート内容を確認できます。

証明書

証明書の拡張子は一般的に「.pem」、「.crt」または「.cer」です。テキストエディターで証明書ファイルを開くと、以下に示すような内容が表示されます。
証明書PEMフォーマット：「-----BEGIN CERTIFICATE-----」で始まり、「-----END CERTIFICATE-----」で終わります。その間の内容は1行あたり64文字であり、最後の行の長さが64文字未満にすることができます。

©2013-2022 Tencent Cloud. All rights reserved.

証明書が中間CA機関によって発行された場合、証明書ファイルは複数の証明書で構成されます。サーバー証明書と中間証明書を手動でスプライスしてアップロードする必要があります。スプライスのルールとして、サーバー証明書は1部目に、中間証明書は2部目に、サーバー証明書のコンテンツを中間証明書のコンテンツの前に空白行を入れずに配置して、一般的には、機構が証明書を発行する時に、対応する説明がありますので、ルールの説明をよく確認してください。

- 証明書間に空行があってはなりません
- 証明書はすべてPEMフォーマットです

中間CAにより発行する証明書チェーンのフォーマットは下記の通りです。

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

プライベートキー

©2013-2022 Tencent Cloud. All rights reserved.

プライベートキーの拡張子は一般的に「.pem」または「.key」です。テキストエディターでプライベートキーファイルを開くと、以下に示すような内容が表示されます。
プライベートキー PEM フォーマット：「-----BEGIN RSA PRIVATE KEY-----」で始まり、「-----END RSA PRIVATE KEY-----」で終わります。その間の内容は1行あたり64文字であり、最後の行の長さが64文字未満することができます。

取得したプライベートキーが「-----BEGIN PRIVATE KEY-----」で始まり、「-----END PRIVATE KEY-----」で終わる場合は、openssl ツールで形式を変換することをお勧めします。コマンドは下記の通りです。

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

他の形式をPEM形式に変換する

現在、CDNはPEM形式の証明書をしか対応していません。ほかの形式の証明書はPEM形式に変換する必要があります。openssl ツールで変換を行うことをお勧めします。以下は、証明書形式をPEM形式に変換するためによく使われている方法です。

DERをPEMに変換する

DER形式は通常、Javaプラットフォームで使用されます。
証明書の変換：

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

©2013-2022 Tencent Cloud. All rights reserved.

プライベートキーの変換：

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

P7BをPEMに変換する

P7B形式は通常、Windows ServerおよびTomcatで使用されます。
証明書の変換：

```
openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
```

テキストエディターでoutcertificat.cerを開くと、PEM形式の証明書内容を確認できます。
プライベートキーの変換：プライベートキーは一般的にIISサーバーにエクスポートすることが可能です。

PFXをPEMに変換する

PFX形式は通常、Windows Serverで使用されます。
証明書の変換：

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

プライベートキーの変換：

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

証明書チェーンの補完

プライベート証明書を設定する場合、下図に示すように、**証明書チェーンが補完できない**場合があります。

この場合、CAが発行した証明書（PEM形式）の内容をドメイン名証明書（PEM フォーマット）の末尾に貼り付けることにより、証明書チェーンを補完することができます。またチケットを提出してください。

ホスト証明書

Tencent Cloudは、証明書ホスティングサービス、つまりSSL証明書を提供します。既存の証明書をSSL証明書管理プラットフォームにアップロードしてホスティングを行い、他のクラウド製品に展開できます。 また、証明書を購入して申請することもできます。

Tencent Cloud SSL証明書サービスは、各ユーザーにTrustAsiaが無料で発行した20のDV SSL証明書を提供します。

©2013-2022 Tencent Cloud. All rights reserved.

HTTPS設定ガイド

最終更新日：：2021-06-07 10:55:55

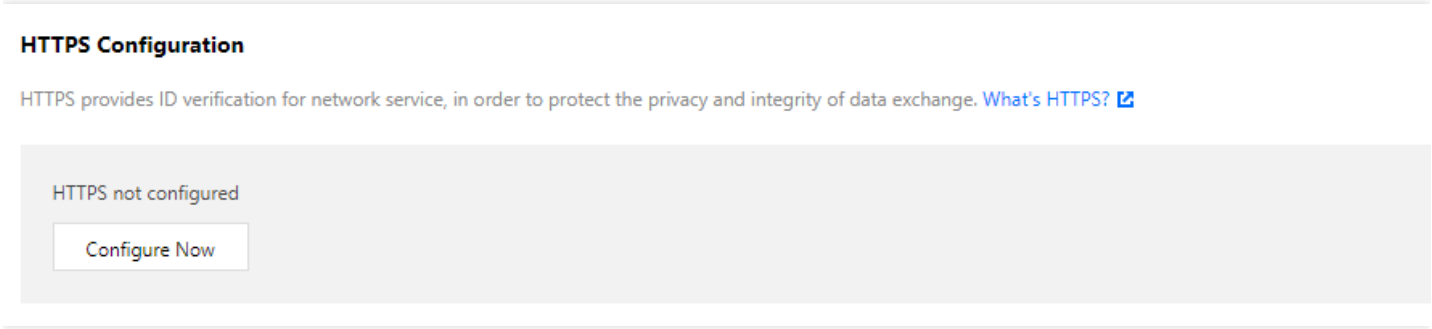
設定シナリオ

Tencent Cloud CDNは、HTTPSアクセラレーションサービスをサポートしています。証明書をアップロードしてデプロイするか、Tencent CloudのSSL証明書管理にホストされている証明書をCDNプラットフォームに直接デプロイし、HTTPSアクセラレーションサービスを有効にして、ネットワーク全体でのデータの暗号化伝送を実現することができます。

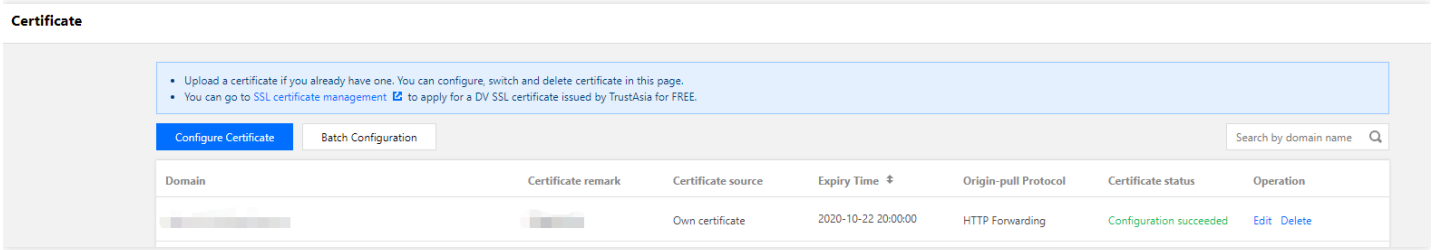
設定ガイド

設定の確認

CDNコンソールにログインし、メニューバーから【ドメイン名管理】を選択し、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面の【HTTPS設定】に進み、指定されたドメイン名のHTTPS設定状況を確認することができます。



左側メニューバーの【証明書管理】画面に移動して、アカウントでHTTPSアクセラレーションが設定されているすべてのドメイン名のリストを確認することもできます。



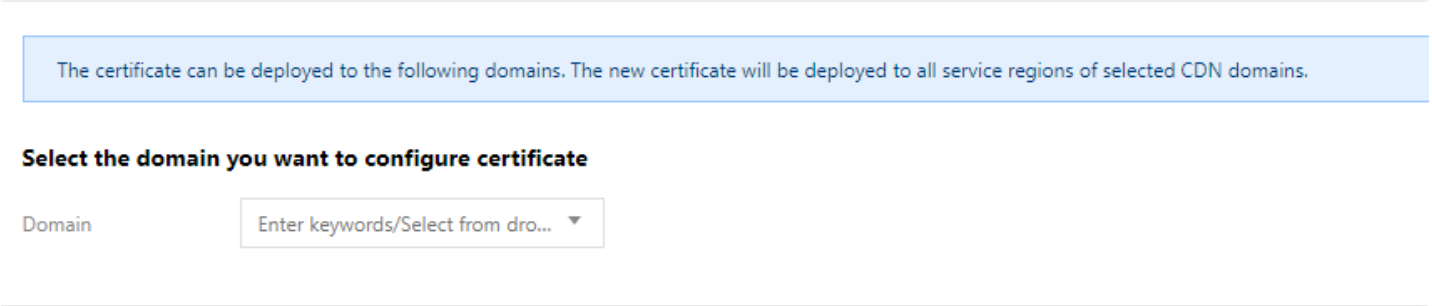
©2013-2022 Tencent Cloud. All rights reserved.

証明書の設定

1. ドメイン名の選択

【証明書管理】メニューバーの【証明書設定】をクリックし、証明書の設定が必要なアクセラレーションドメイン名を選択します。

- アクセラレーションドメイン名のステータスは、「デプロイ中」または「起動済み」である必要があります。無効化ステータスのアクセラレーションドメイン名は、HTTPSアクセラレーションの設定を行えません。
- `.file.myqcloud.com` の拡張子は、Tencent CloudのCloud Object Storageのデフォルトのアクセラレーションドメイン名であり、証明書を設定せずにHTTPSアクセラレーションを直接実行できます。
- `.image.myqcloud.com` の拡張子ドメイン名は、Tencent CloudのCloud Infiniteのデフォルトのアクセラレーションドメイン名であり、証明書を設定せずにHTTPSアクセラレーションサービスを直接実行できます。

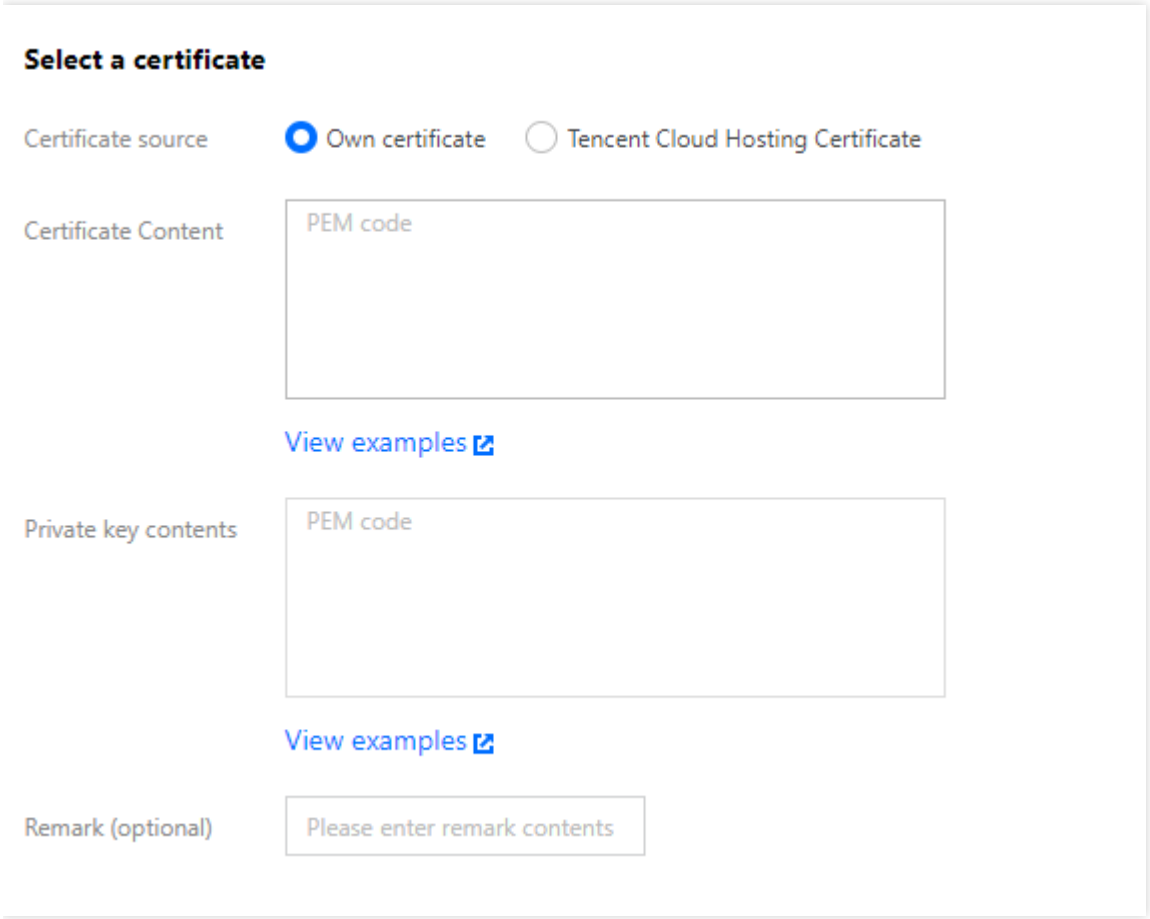


2. 証明書の選択

証明書がある場合は、PEM形式の証明書の内容と秘密鍵を対応する位置に直接貼り付ければ完了です。

- Tencent Cloud CDNは現在、ECC証明書のデプロイをサポートしています。
- 証明書の内容はPEM形式である必要があります。この形式以外の証明書については、PEM形式の変換をご参照ください。
- Tencent Cloudホスト証明書を選択して、ワンクリックで直接デプロイできます。

©2013-2022 Tencent Cloud. All rights reserved.



一括設定

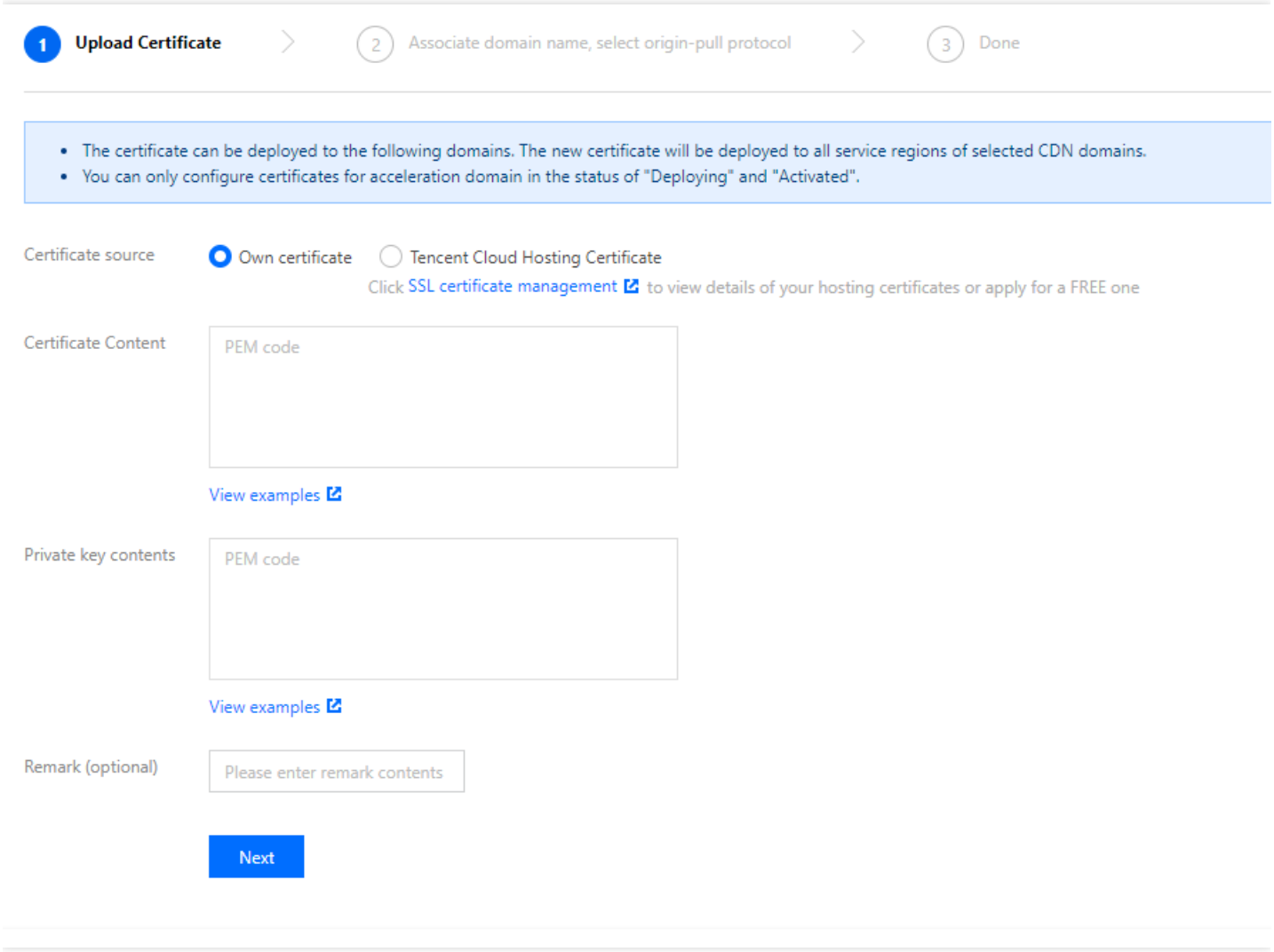
上の【一括設定】をクリックして、証明書をアップロードすることにより、適応したドメイン名を自動的にマッチングさせ、一括設定を行うことができます。

1. 証明書の選択

証明書がある場合は、PEM形式の証明書の内容と秘密鍵を対応する位置に直接貼り付ければ完了です。

- Tencent Cloud CDNは現在、ECC証明書のデプロイをサポートしています。
- 証明書の内容はPEM形式である必要があります。この形式以外の証明書については、PEM形式の変換をご参照ください。
- Tencent Cloudホスト証明書を選択して、ワンクリックで直接デプロイできます。

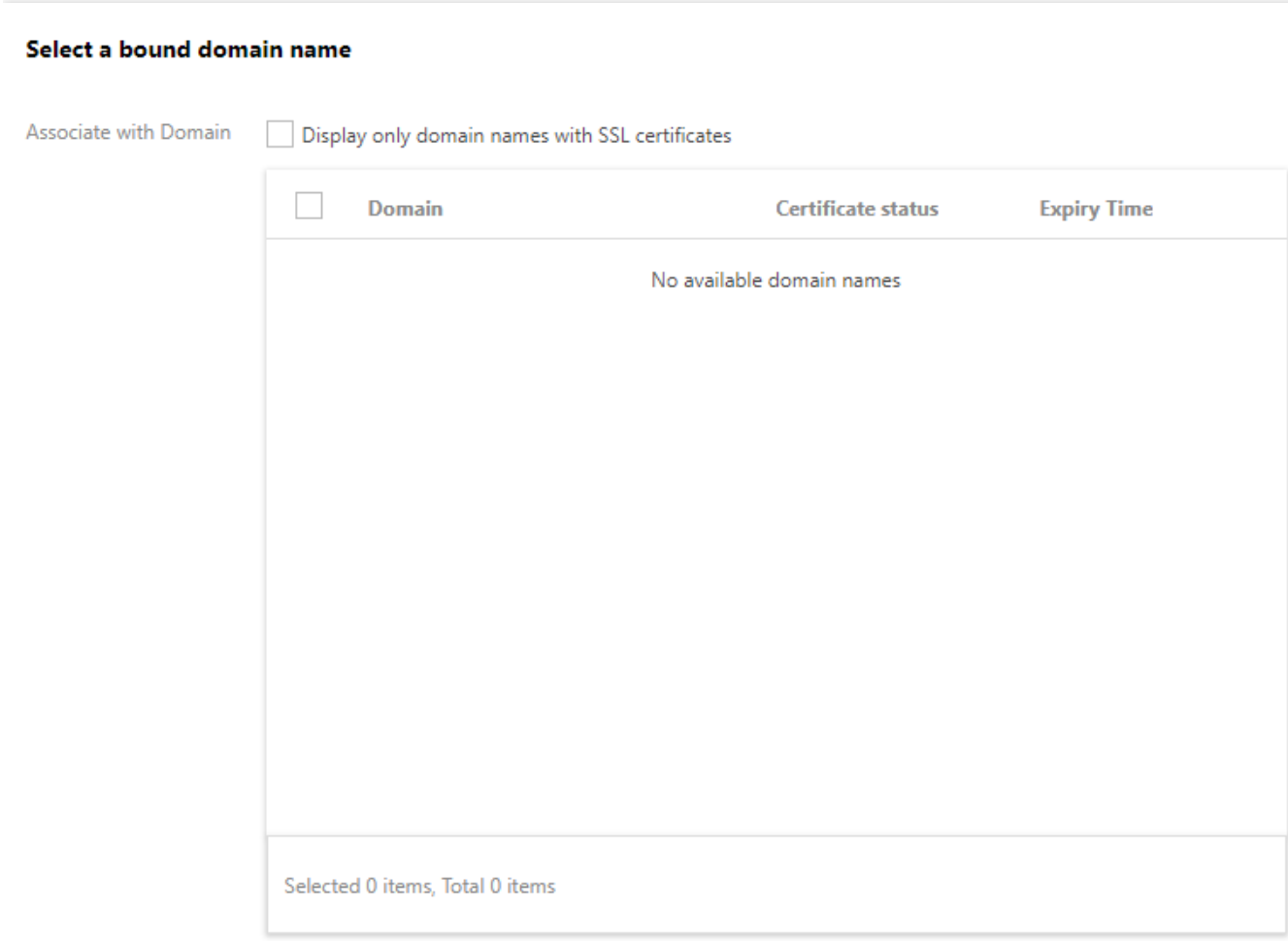
©2013-2022 Tencent Cloud. All rights reserved.



2. ドメイン名の選択

CDNはアップロード/選択された証明書に基づいて、設定が許可されているドメイン名リストと自動的にマッチングします。必要に応じてチェックを入れて選択し、設定することができます。

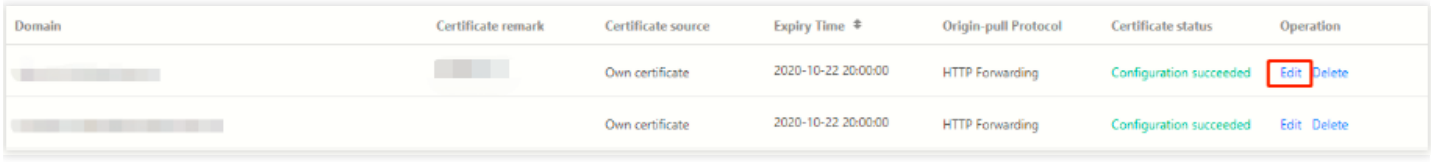
©2013-2022 Tencent Cloud. All rights reserved.



証明書の変更

証明書の修正

証明書の右側の【編集】をクリックし、ドメイン名を指定して証明書を更新することも、再度一括設定して元の証明書の設定を上書きすることもできます。



更新された証明書はネットワーク全体のノードで有効になり、シームレスに切り替わりますので、既存ネットワークのHTTPSサービスには影響を与えません。また、【削除】をクリックして、HTTPSアクセラレーションサービスをキャンセルすることもできます。

証明書の期限切れ

©2013-2022 Tencent Cloud. All rights reserved.

Tencent Cloudは、証明書の有効期限が切れる30日前、15日前、7日前および期限切れ当日に、Short Message Service、電子メールおよび内部メッセージといった形式でユーザーアカウントに期限切れの通知を送信します。現在、SSL証明書についてはアラーム受信者のカスタマイズをサポートしており、メッセージサブスクリプションの設定に進むことができます。

リージョンの特殊設定

アクセラレーションドメイン名サービスエリアがグローバルの場合、設定したHTTPS証明書は中国本土・中国本土以外の両方で有効になります。現時点では、中国本土・中国本土以外で別の証明書はサポートしていません。

ドメイン名に中国本土と中国本土以外の証明書の設定に不一致がある特殊なシナリオの場合、【証明書管理】画面で、中国本土、中国本土以外などのマークを表示して、このドメイン名に以前からのリージョンに関する特殊な設定があることを示せます。

ドメイン名の【高度な設定】には、次の2つの設定も表示されます。

©2013-2022 Tencent Cloud. All rights reserved.

強制リダイレクト

最終更新日：：2021-02-02 17:04:32

設定の概要

Tencent Cloud CDNサービスは、HTTPS/HTTP強制リダイレクトの設定をサポートしています。

- HTTPS Secure Acceleration が CDNドメイン名に対して有効になっている場合、301/302リダイレクト方式を指定して、CDNノードに到達するすべてのHTTPリクエストを強制的にHTTPSにリダイレクトさせることができます。
- また、301/302リダイレクト方式を指定して、CDNノードに到達するすべての HTTPSリクエストを強制的にHTTPにリダイレクトさせることができます。
- リダイレクト時はデフォルトで Response headerをつけません。変更可能です。

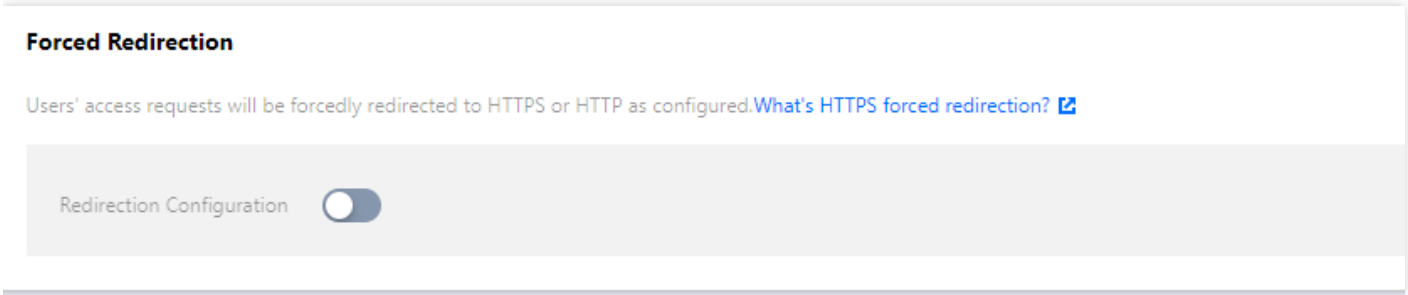
設定ガイド

制限について

HTTPS強制リダイレクトを設定するには、HTTPSアクセラレーションを有効にする必要があります。

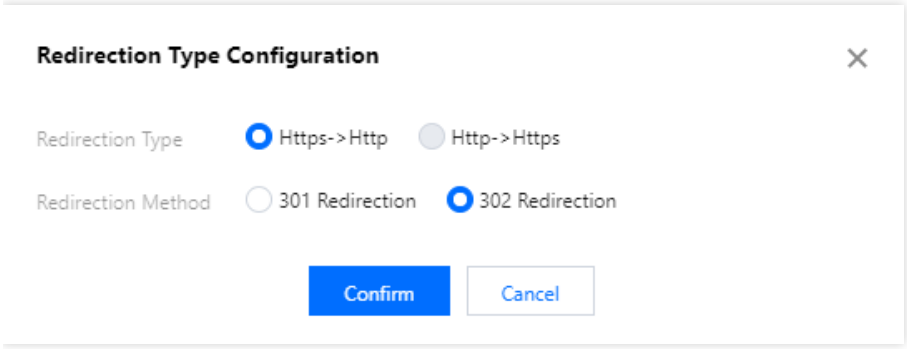
設定方法

CDNコンソールにログインし、左側のサイドバーで【ドメイン管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。【HTTPS設定】タブをクリックし、【強制リダイレクト】セクションを見つけます。この機能はデフォルトで無効になっています。

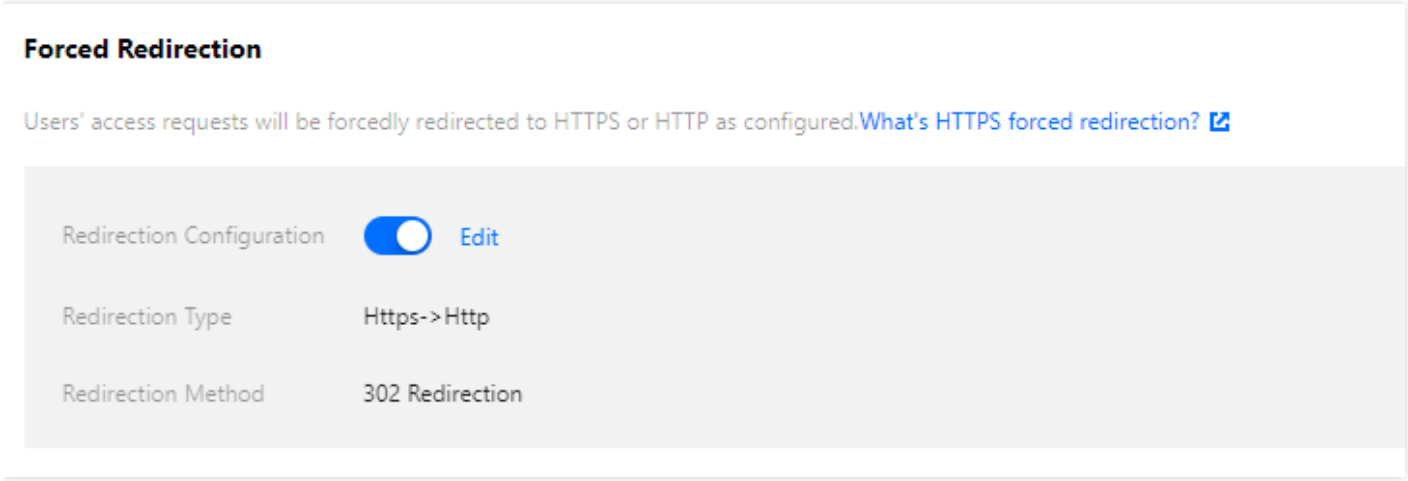


「リダイレクト設定」をオンに切り替えて、リダイレクトタイプ、リダイレクト方式を設定できます。

©2013-2022 Tencent Cloud. All rights reserved.



【OK】をクリックします。



©2013-2022 Tencent Cloud. All rights reserved.

HTTP2.0 設定

最終更新日：：2021-03-18 10:56:00

設定シナリオ

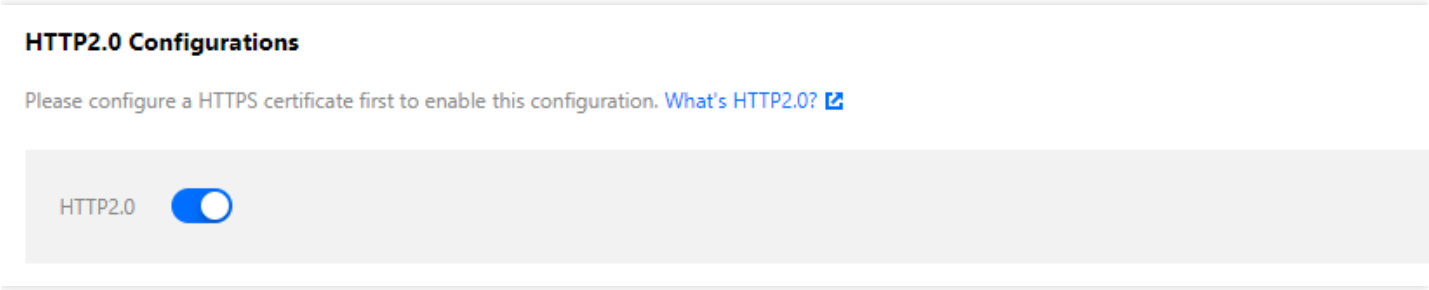
HTTP2.0は HTTPの最新バージョンで、Webパフォーマンスを大幅に向上させ、ネットワークの遅延の大部分を削減します。証明書が設定されてHTTPSアクセラレーションが有効になっているドメイン名は、HTTP2.0プロトコルサポートを有効にできます。

> ⚠ **注意：**
>
> 現在、HTTP2.0アクセスのみがサポートされています。HTTP2.0 back-to-originはサポートされていません。

設定ガイド

設定の確認

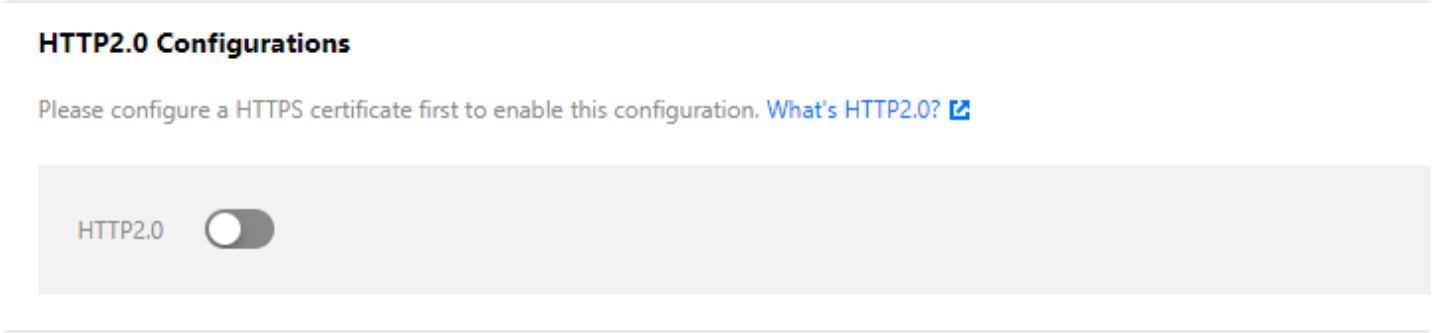
CDNコンソールにログインし、左側のナビゲーションウィンドウで【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定ページに入ります。【HTTPS設定】タブで、【HTTP2.0設定】を見つけます。【HTTP2.0設定】はデフォルトで有効になっています。



設定の変更

オン／オフを切り替えることで、HTTP2.0設定を有効または無効にでき、証明書の設定が削除されると、HTTP2.0の設定は自動的に無効になります。

©2013-2022 Tencent Cloud. All rights reserved.



⚠ 注意：

ドメイン名がグローバルアクセラレーション用に設定されている場合、設定されたHTTP2.0 はグローバルに有効になります。

©2013-2022 Tencent Cloud. All rights reserved.

OCSPステープリング設定

最終更新日：：2021-11-24 15:30:30

設定シナリオ

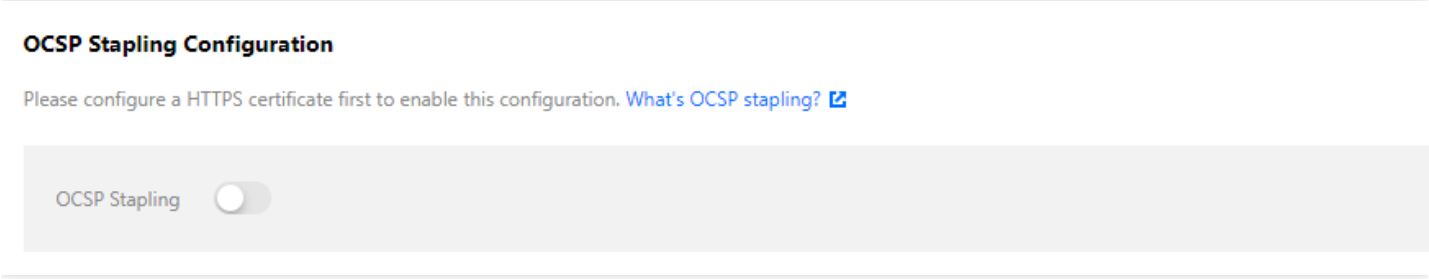
OCSPステープリング（TLS証明書状態クエリ拡張）を有効にすると、サーバーは、TLSハンドシェイク中にユーザー認証用のキャッシュされたオンライン証明書状態プロトコル（OCSP）応答を送信します。ユーザーがデジタル証明書認証機関（CA）にクエリリクエストを送信する必要はありません。OCSPステープリングにより、LSハンドシェイクの効率が大幅に向上し、ユーザー認証時間が短縮されます。

Tencent Cloud CDNは、OCSPステープリング設定を手動で有効または無効にすることができます。

設定ガイド

設定の表示

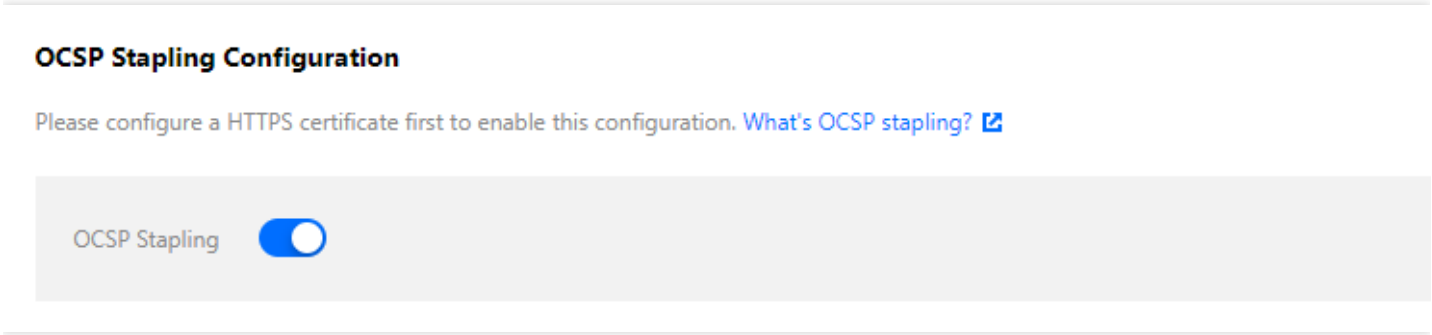
CDNコンソールにログインして、メニューバーから【ドメイン名管理】を選択し、ドメイン名右側の【管理】をクリックすると、ドメイン名設定ページに進むことができ、【Https設定】の中から、【OCSPステープリングの設定】を確認することができます。デフォルトでは無効になっています。



設定の変更

HTTPS加速が設定されたドメイン名は、スイッチをクリックすることで直接オンまたはオフにできます。証明書設定を削除すると、OCSPステープリング設定も無効になります。

©2013-2022 Tencent Cloud. All rights reserved.



注意：
ドメイン名のサービスリージョンがグローバルの場合は、設定したOCSPステープリングがグローバルで有効となります。現在中国本土、中国本土以外を個別に設定することはできません。

©2013-2022 Tencent Cloud. All rights reserved.

HSTS設定

最終更新日：：2021-03-04 18:11:21

概要

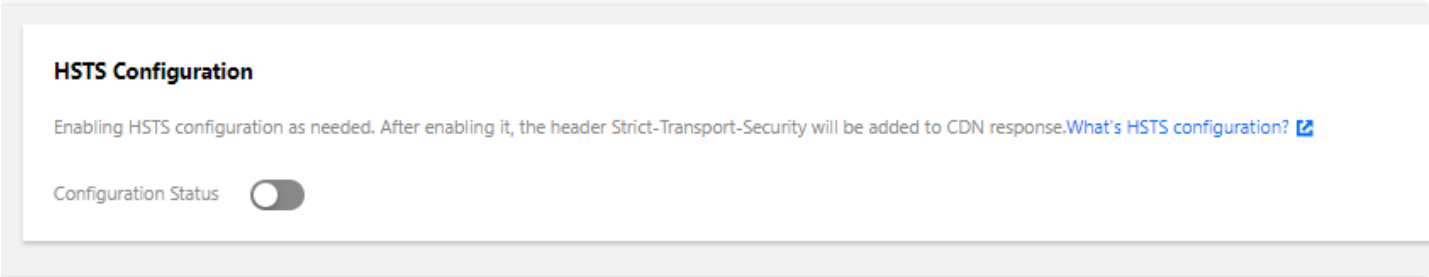
HTTP Strict TransportSecurity （HSTS）は、Institution of Electronics and Telecommunication Engineers（IETE）によって設計されたWebセキュリティポリシーメカニズムです。HSTS はブラウザなどのクライアントに、ドメインはHTTPSのみを使用してアクセスするように指示し、ウェブサイト全体で100%の暗号化を実現するのに役立ちます。

設定の制限事項

- expireTimeの範囲は0〜365日で、秒単位で構成されます。
- サブドメイン名を含めるかどうかを選択することにより、includeSubDomainパラメータを制御できます。
- HSTS設定を有効にするには、HTTPSアクセラレーション設定を最初に完了する必要があります。
- HSTS設定を有効にした後、強制リダイレクトを有効にしてHTTPリクエストをHTTPSリクエストにリダイレクトすることをお勧めします。そうしないと、HTTPリクエストの場合、ブラウザはHTTPリクエストのHSTSキャッシュを作成しません。

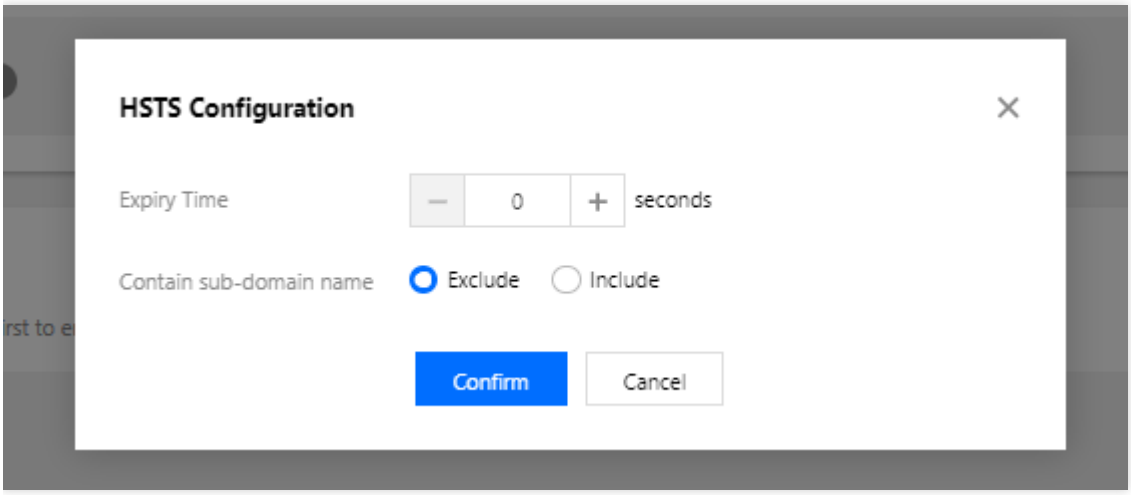
設定ガイド

CDNコンソールにログインし、左のサイドバーメニューで、【ドメイン名管理】を選択して、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定画面に入ります。【HTTPS設定】でHSTS設定モジュールを確認できます。デフォルトでは無効になっています。

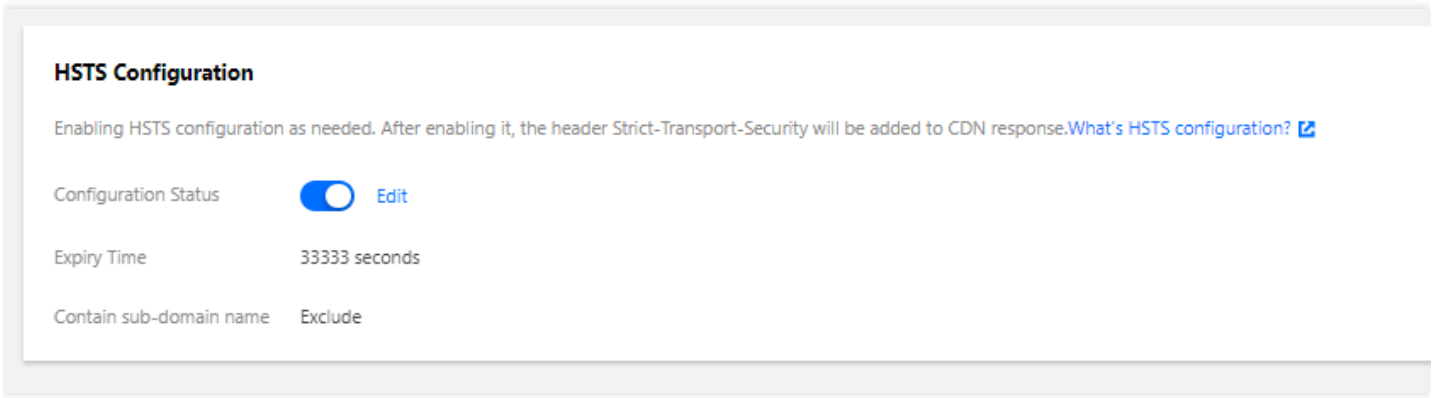


スイッチを「ON」に切り替えて設定します。

©2013-2022 Tencent Cloud. All rights reserved.

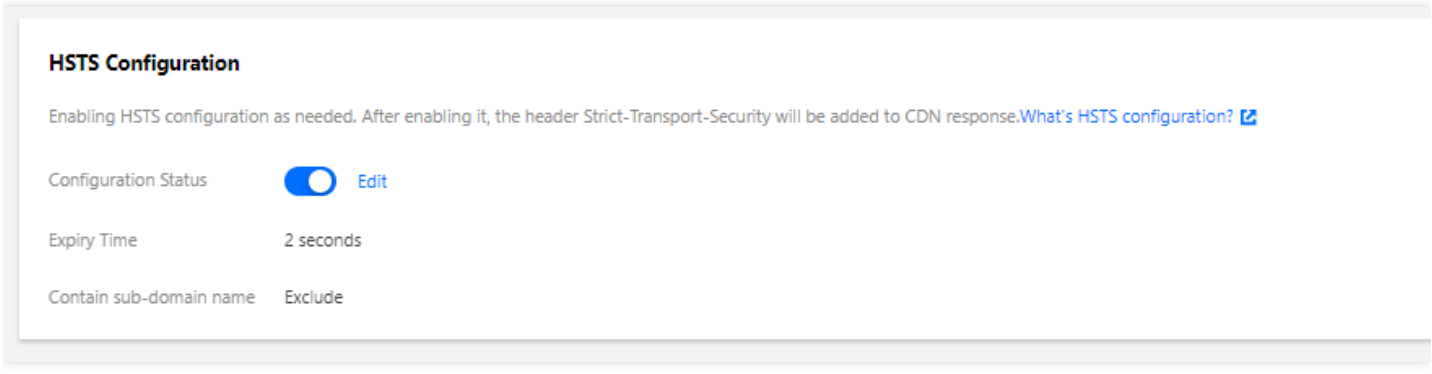


【OK】をクリックした後、設定されたコンテンツに従って応答ヘッダー値を決定し、【編集】をクリックして変更できます。



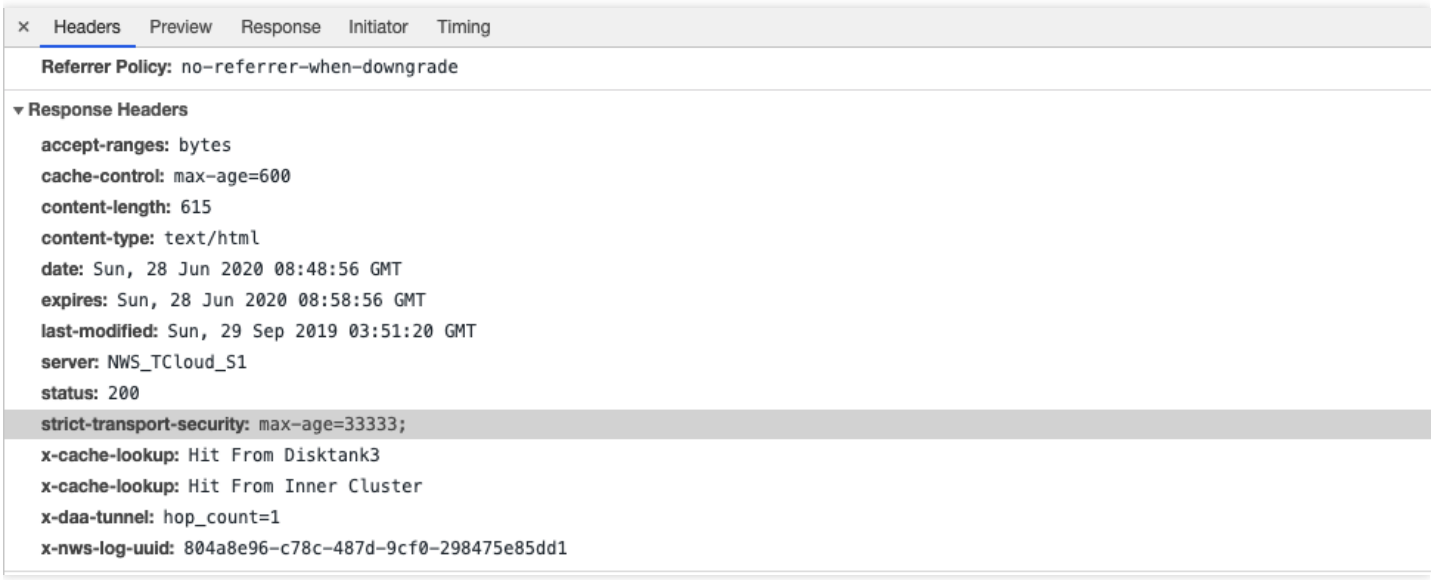
例

ドメイン名 `cloud.tencent.com` のHSTS設定は以下の通りであると仮定する：



©2013-2022 Tencent Cloud. All rights reserved.

応答ヘッダーは以下のとおり：



©2013-2022 Tencent Cloud. All rights reserved.

TLS バージョン設定

最終更新日：：2021-01-20 17:32:07

機能の概要

Tencent Cloud CDNは、デフォルトではTLS 1.0/1.1/1.2が有効、TLS 1.3が無効になっています。必要に応じて指定するTLSのバージョンを有効/無効にできます。

⚠ 注意：

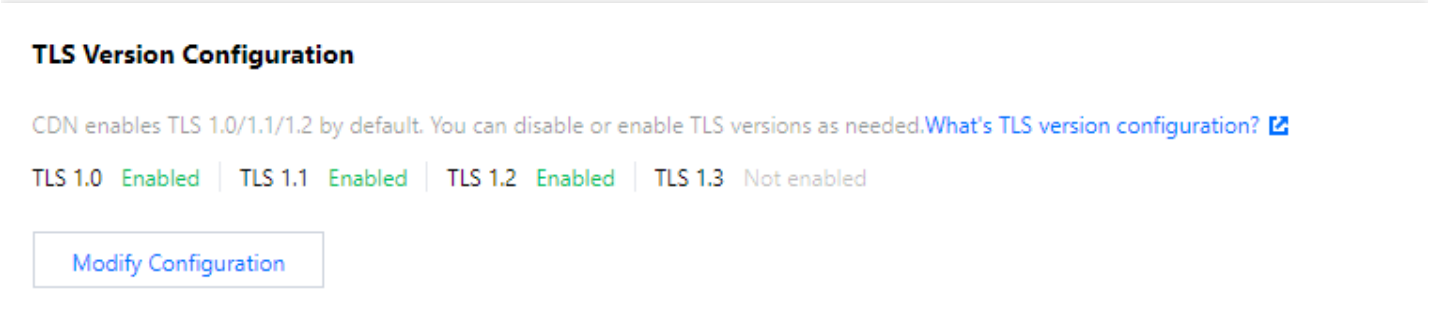
- 設定前にHTTPS証明書の設定が完了していることを確認してください。
- TLSのバージョン設定は、現在中国国外ではサポートしていません。ドメイン名のアクセラレーションリージョンがグローバルである場合、設定変更後は中国国内でのみ有効となります。
- 一部のプラットフォームはアップグレード中のため、この設定機能を開放していません。

設定ガイド

設定の確認

CDNコンソールにログインし、左側のメニューバーで【ドメイン名管理】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定画面に入ります。タブを【HTTPS設定】に切り替えると、【TLSバージョンの設定】が表示されます。

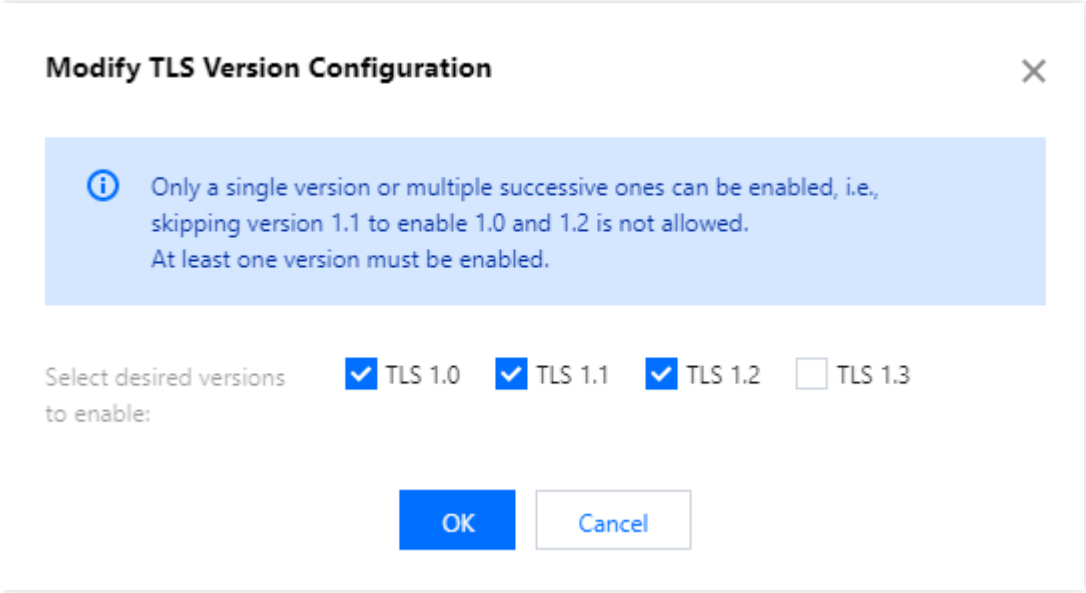
デフォルトの状況では、TLS 1.0/1.1/1.2が有効状態、TLS 1.3が無効状態になっています。



設定の変更

©2013-2022 Tencent Cloud. All rights reserved.

必要に応じてTLSバージョンの有効/無効を指定し、【設定を変更】をクリックしてください。



設定の制約

- 連続または単独のバージョンナンバーのみを有効にできます。例えば、1.0、1.2のみを有効にし、1.1を無効にすることはできません。
- 全てのバージョンを無効にはできません。

©2013-2022 Tencent Cloud. All rights reserved.

QUIC

最終更新日：：2022-01-17 10:53:36

お知らせ

Tencent Cloud Content Delivery Network(CDN)は、2022年1月5日にQUICアクセス機能を正式にリリースします。QUICアクセス機能を有効にすると、生成されたQUICリクエスト数には後払いの従量課金が適用されます。詳細については、課金説明- QUICアクセスリクエスト数の課金をご参照ください。
オンライン課金を行う場合は、あらかじめメッセージをプッシュし、コンソールやドキュメントでお知らせいたしますので、ご確認のほどよろしくお願いいたします。

機能の説明

QUIC（Quick UDP Internet Connectionsは、汎用的なネットワークプロトコルであり、ネットワークセキュリティを保障するとともに、伝送と接続時のレイテンシーも低減し、ネットワークの輻輳を回避することができます。QUICプロトコルを有効にすることで、クライアントがCDNノードにアクセスする際のデータ転送の安全性を確保し、アクセス効率を向上させることができます。

現在、デフォルトでh3 Draft 28、h3-Q050、h3-Q046、h3-Q043、Q046、Q043のバージョンをサポートしています。

操作ガイド

1、QUICの有効化

ドメイン名の追加が完了した後、ドメイン名管理に入り、Tabを【HTTPS設定】に切り替えると、【QUIC】設定が見つかります。デフォルトはオフ状態で、ユーザーにより有効化することができます。
注：有効化する前に、HTTPS証明書を設定してください。

注意：

- 業務タイプの切り替えはリソースプラットフォームのスケジューリングに影響します。QUICプラットフォームに接続した後は、ドメイン名のサービスタイプを再度切り替えないようにすることをお勧めします。
- QUIC back-to-originは現在サポートしておりません。

©2013-2022 Tencent Cloud. All rights reserved.

- 一部のプラットフォームは現在QUICをサポートしていません。プラットフォームのアップグレード中ですのでご期待ください。

設定の制約：

- ストリーミングメディアのVODアクセラレーションサービスタイプのドメイン名は現在QUICをサポートしていません。
- IPv6アクセスを有効にするとQUICを有効にできません。

2、QUICの無効化

コンソールのドメイン名管理 - HTTPS設定-QUICで、QUIC機能を無効にできます。

課金ルール

QUICアクセスは付加価値サービスであり、QUICリクエスト数の回数に応じて課金され、後払いの従量課金が適用されます。詳細については、課金説明をご参照ください。

©2013-2022 Tencent Cloud. All rights reserved.

HTTPSに関してよくある質問

最終更新日：：2021-06-16 11:08:36

HTTPSとは何ですか。

HTTPSとは、ハイパーテキスト転送セキュリティプロトコル（Hypertext Transfer Protocol Secure）である。HTTPプロトコルに基づいてデータを暗号化して安全性を確保するためのプロトコルです。HTTPSを設定する場合、ネットワーク全体でデータの暗号化転送機能を実現するために、ユーザーは、ドメイン名に対応する証明書を提供し、ネットワーク全体のCDNノードにデプロイする必要があります。

CDNサービスはHTTPS設定をサポートしますか。

Tencent Cloud CDNは現在、HTTPS設定を完全にサポートしています。ユーザーは自分の証明書をアップロードしてデプロイするか、または[証明書管理コンソール]（https://console.tencentcloud.com/ssl）にアクセスしてTrustAsiaが無料で提供するサードパーティの証明書を申請することができます。

HTTPS証明書を設定するにはどうすればよいですか。

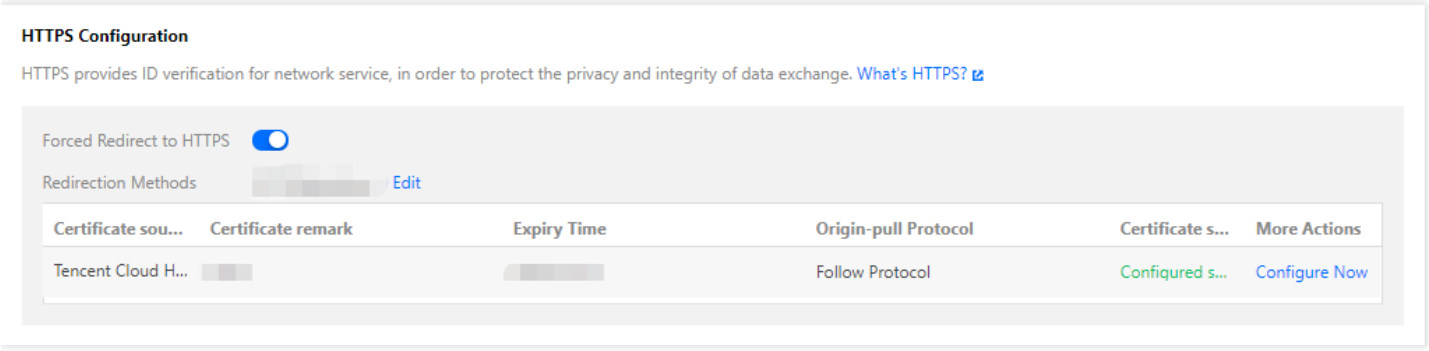
CDNコンソールでHTTPS証明書を設定することができます。詳細については、HTTPS設定をご参照ください。

オリジンサーバーのHTTPS証明書が更新されました。CDNに設定されている証明書は同時に更新する必要がありますか。

必要がありません。オリジンサーバーのHTTPS証明書を更新しても、CDNに設定されている証明書には影響しません。CDNに設定されている証明書の有効期限が近づいているか、すでに切れている場合、HTTPS証明書を更新する必要があります。

ユーザーがHTTPSアクセスのみを許可し、HTTPアクセスを禁止する方法はありますか。

強制リダイレクト機能を使用できます。HTTPS証明書を設定した後、「Http->Https機能」を有効にすることができます。有効にすると、ユーザーがHTTPリクエストを送信しても、HTTPSに強制的にリダイレクトしてアクセスします。

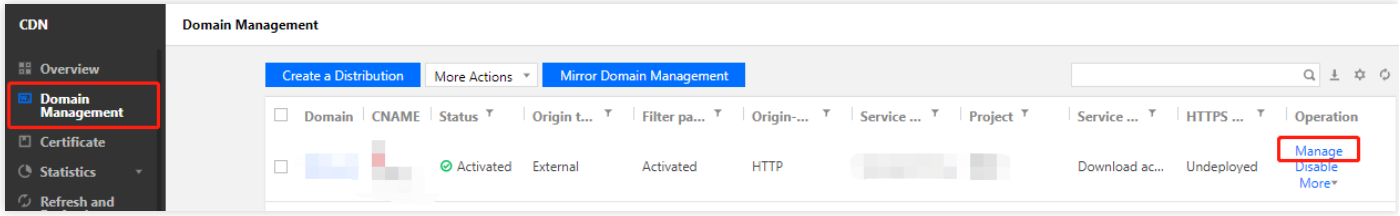


CDNを設定したのに、HTTPSアクセスが機能しないのはなぜですか。

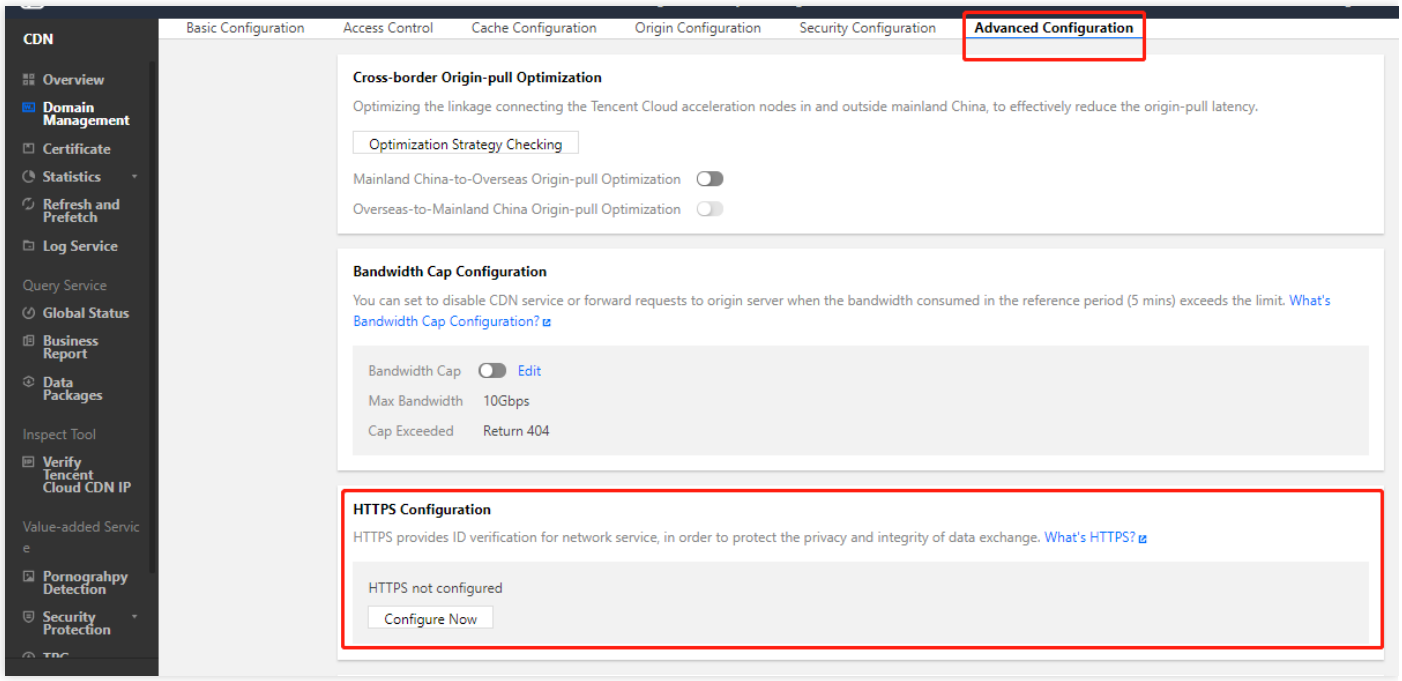
©2013-2022 Tencent Cloud. All rights reserved.

HTTPSアクセスを使用するには、以下の操作を行います。

1. CDNコンソールにログインし、左側のナビゲーションウィンドウで【ドメイン名管理】を選択し、ドメイン名の右側にある【管理】をクリックして、その管理ページに入ります。



2. 【HTTPS設定】をクリックし、HTTPS設定モジュールを見つけて、【設定に進む】をクリックして、証明書管理ページにジャンプし、証明書を設定します。設定手順については、証明書の設定をご参照ください。



証明書が正しく設定されている場合、HTTPSアクセスを有効にできます。

©2013-2022 Tencent Cloud. All rights reserved.

高度な設定
ピーク帯域幅の設定

最終更新日：：2022-11-17 11:31:34

設定シナリオ

悪意のあるユーザーによる大量の帯域幅やトラフィックの盗難によって高額の請求が発生することを心配する場合は、使用量上限設定機能を使用して使用量を制限します。

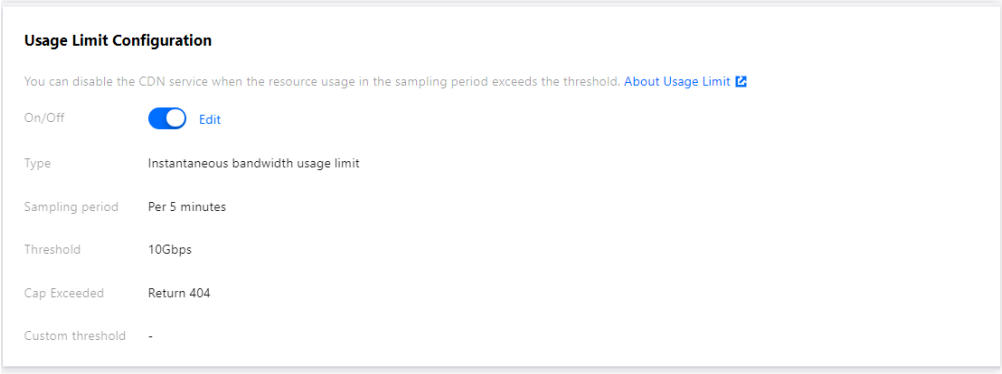
統計周期内に発生した帯域幅またはトラフィックが設定されたアラートのしきい値を超えた場合、CDNがメッセージ通知を送信します。設定されたアクセスしきい値を超えた場合は、CDNサービスを停止して、それ以上のCDNサービス料金が発生しないようにします。

> 注意：
> 使用量上限設定の有効化には遅延（約10分）があり、途中に発生した使用量は通常課金されます。詳細については、攻撃リスク防止プランをご参照ください。

設定ガイド

設定の表示

CDNコンソールにログインし、メニューバーから**ドメイン名管理**を選択し、ドメイン名の右側にある**管理**をクリックすると、ドメイン名設定ページに進み、**高度な設定**で使用量上限の設定を確認することができます。デフォルトでは無効になっていま：

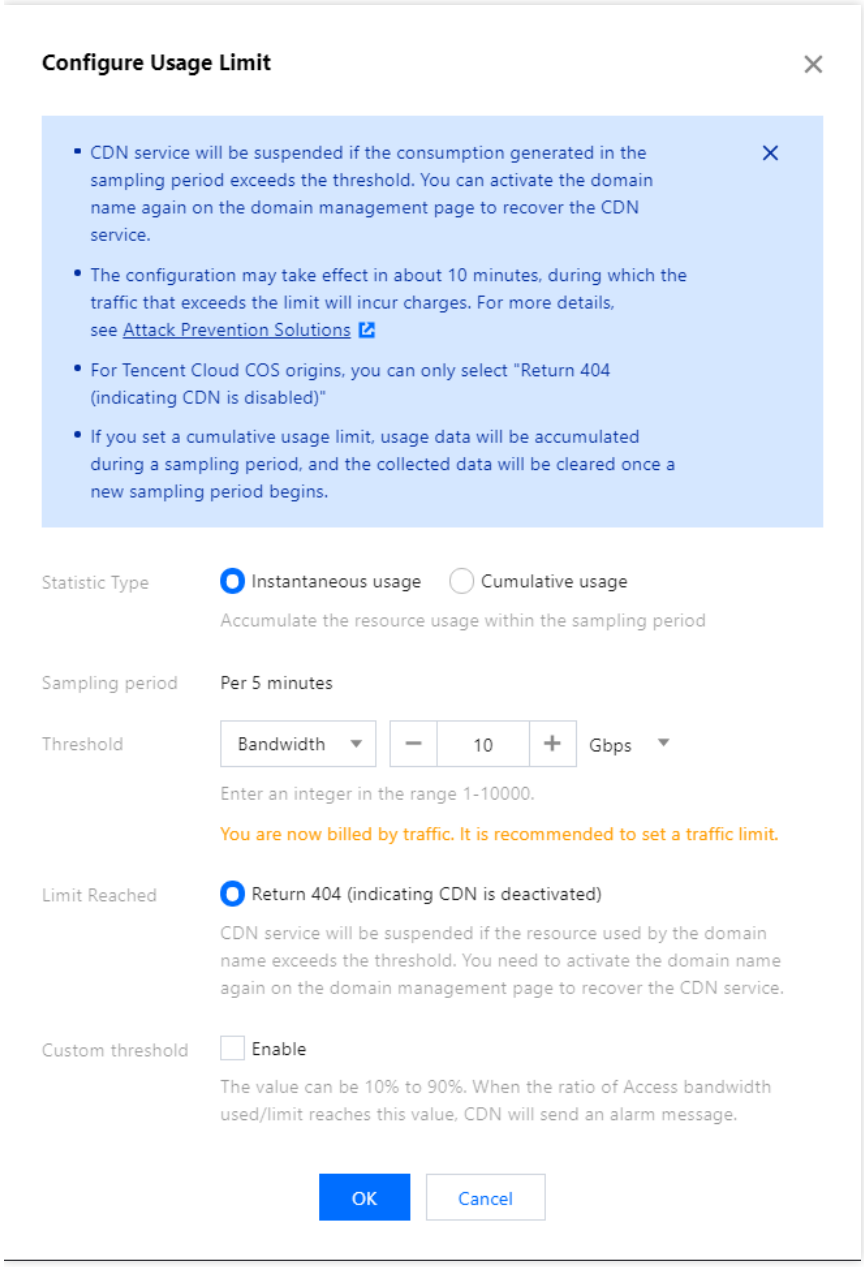


詳細設定

©2013-2022 Tencent Cloud. All rights reserved.

1. 有効にする

[設定スイッチオン]をクリックして、詳細の設定を行います：



- 統計タイプ：
  - 一時的な使用量：5分ごとにトラフィック/帯域幅の使用量を統計的に測定します。
  - 累積使用量：一時的な使用量よりも長い統計期間があり、時間単位/自然日単位のトラフィックの使用量統計をサポートします。

注意：
アクセラレーションタイプがECDN動的加速アクセラレーションおよびECDN動的アクセラレーションのドメイン名は、「累積使用量」の上限設定をサポートしていません。

©2013-2022 Tencent Cloud. All rights reserved.

- 統計サイクル：分（5分ごと）、時間（1時間ごと）、日（当日24時まで）の統計サイクルをサポートします。

注意：

- 統計サイクルの開始時刻は設定時間より前の5分刻みに切り捨てする時刻とします：
  例：09:05:01から09:09:59までルールを設定する場合、09:05:00は統計サイクルの開始時刻です。
- 統計サイクルが「1時間ごと」を選択した場合、（1）設定後の最初の1時間のデータ統計サイクルについて、1時間未満の統計時間になり、（2）次のデータ統計サイクルに入り、1時間ごとに使用量を統計します。
  例：2022-01-13の9:23:10にルールを設定すると、最初のデータ統計サイクルは9:20:00～9:59:59、次回の統計サイクルは10:00:00~10:59:59となります。
- 統計サイクルに「当日24時まで」を選択すると、統計サイクルは2022-01-13の9:20:00から2022-01-13の23:59:59までとなります。

- 上限設定：一時的な使用量の場合はトラフィック/帯域幅の上限設定をサポートし、累積使用量の場合は、トラフィックのみをサポートします。
  - トラフィック上限：統計するドメイン名のトラフィック消費量。トラフィックしきい値はユーザーがこのドメイン名にアクセスするためのトラフィックの上限値です。
  - 帯域幅上限：統計するドメイン名の帯域幅消費量。帯域幅のしきい値はユーザーがこのドメイン名にアクセスするための帯域幅の上限値です。
- 上限解除時間：定期的な解除/永久的な解除禁止をサポートします。
  - 定期的な解除：定期的な解除サイクルは、60分、12時間、24時間、3日間に対応しています。
    例えば、設定したex.comドメイン名がしきい値を超えた後にアクセスが404（CDNサービスオフ）を返します、自動解除時間が60分になります。ドメイン名が設定された累積使用量上限のしきい値を超えると、CDNサービスが停止し、アクセラレーションされたドメイン名がオフラインになります。60分後、ドメイン名を自動的に解除し、ドメイン名のアクセラレーションをオンにします。
  - 永久的な解除禁止：ドメイン名が大規模なトラフィック/帯域幅の攻撃を受けることを心配する場合は、永久的な解除禁止を設定することができます。設定値がしきい値を超えた場合、アクセスは404を返します（CDNサービスをオフにします）。ドメイン名が設定された累積使用量上限のしきい値を超えると、ドメイン名はオフラインになり、自分でコンソールに移動してドメイン名アクセラレーションをオンにする必要があります。
- 閾値を超えた場合：
  - アクセスが404を返します。しきい値を超えた場合、そのドメイン名のCDNサービスを直接オフにします。ドメイン名管理ページで再びドメイン名がオンラインになり、CDNサービスを回復するよう設定します。

©2013-2022 Tencent Cloud. All rights reserved.

注：オリジンサーバーのタイプがCOSソース/サード・パーティのオブジェクトストアでは、アクセスの404返し（CDNサービスのオフ）のみがサポートされています。

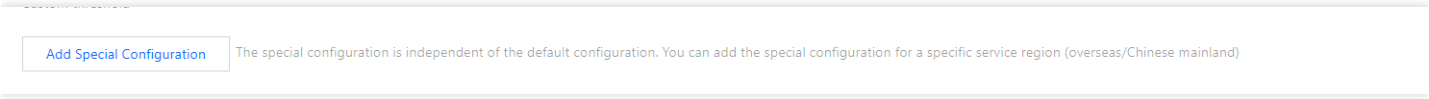
- アラームのしきい値：
  アクセス帯域幅/トラフィックしきい値の比が設定されたパーセンテージ（10%～90%のような10の倍数のみ入力可能）を超えた場合、CDNはアラームメッセージを送信します

注意：

- ドメイン名の帯域幅（トラフィック）がしきい値を超えたことを検出した後、アクセスが404エラーを返します。設定の有効化はネットワーク全体のノードが徐々に配信する必要があるため、有効になるまで遅延が発生する可能性があります。
- アラームのしきい値がオンになっている場合：スキャンの時間単位が5分間であるため、使用量が短期間に急増したり、パーセンテージの設定値が大きくなったりすると、前回のスキャンでパーセンテージのアラームのしきい値がトリガーされず、次のスキャンでアクセスのしきい値に直接達した可能性があります。この場合は、CDNはパーセンテージアラームとアクセスしきい値アラームの2つの通知メッセージを送信します。

2.地域の特別な設定

アクセラレーションドメイン名のサービスリージョンがグローバルアクセラレーションであり、中国国内と中国国外のアクセラレーションリージョンに異なる使用量の上限を設定する場合は、設定の下にある**特別な設定を追加**をクリックして設定できます：



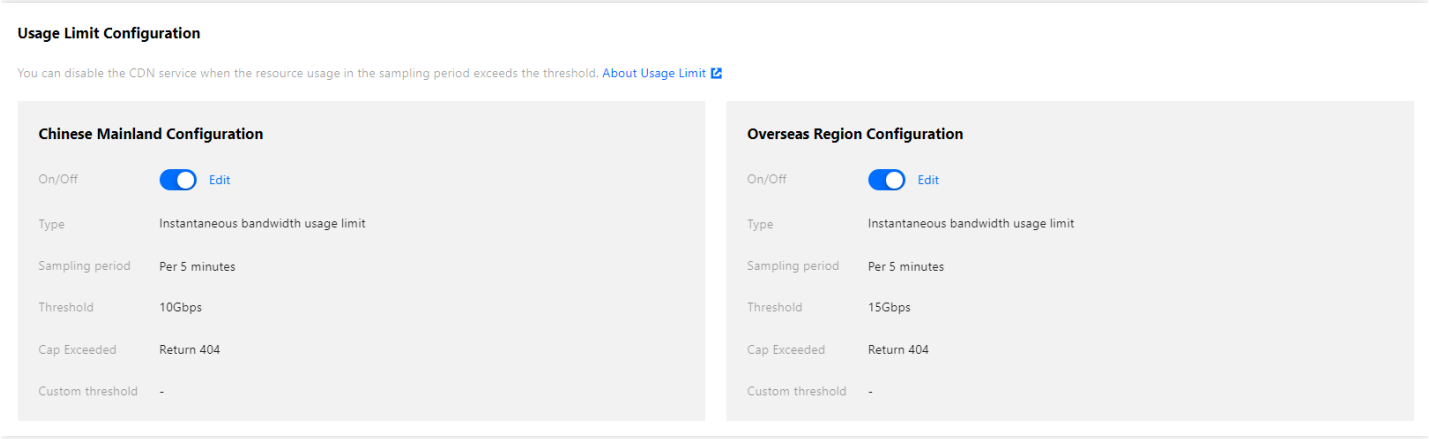
注意：

- 地域の特別な設定が追加された後、削除することはできません。設定を無効にすることができます。
- アクセラレーションタイプがECDN動的アクセラレーションおよびECDN動的アクセラレーションのドメイン名では「リージョンの特別設定」をサポートしません。

設定例

アクセラレーションドメイン名 `cloud.tencent.com` がグローバルアクセラレーションドメイン名である場合、新しいリージョンの特別設定（中国国外）の使用量の上限は以下の通りです：

©2013-2022 Tencent Cloud. All rights reserved.



- 国内外の設定は相互に影響しません。リージョンの特別設定に「中国国外」を選択すると、初期設定は中国国内で有効になります。国内トラフィックが統計サイクル（5分）内に4GBに達した場合、すべての国内からのリクエストは404を返し、海外サービスに影響を与えません。海外トラフィックが統計サイクル（その日の24時まで）内に11GBに到達すると、すべての海外からのリクエストは404を返し、国内サービスに影響を与えません。
- ドメイン名のアクセラレーションリージョンの切り替え：グローバルアクセラレーションドメイン名を中国国内アクセラレーションドメイン名に切り替えた場合、使用量上限の海外設定はデフォルトでオフになり、編集できません。

3. 設定を無効にする

使用量上限スイッチを切り替えて、この機能を無効にすることができます。スイッチがオフの場合、下位に既に設定が存在しても実稼働環境では有効になりません。再びスイッチをオンに切り替えると、ネットワーク全体で設定が有効になる前に、先に設定の2回目の確認が行われます。

©2013-2022 Tencent Cloud. All rights reserved.

HTTPレスポンスヘッダーの設定

最終更新日：：2021-08-27 11:36:42

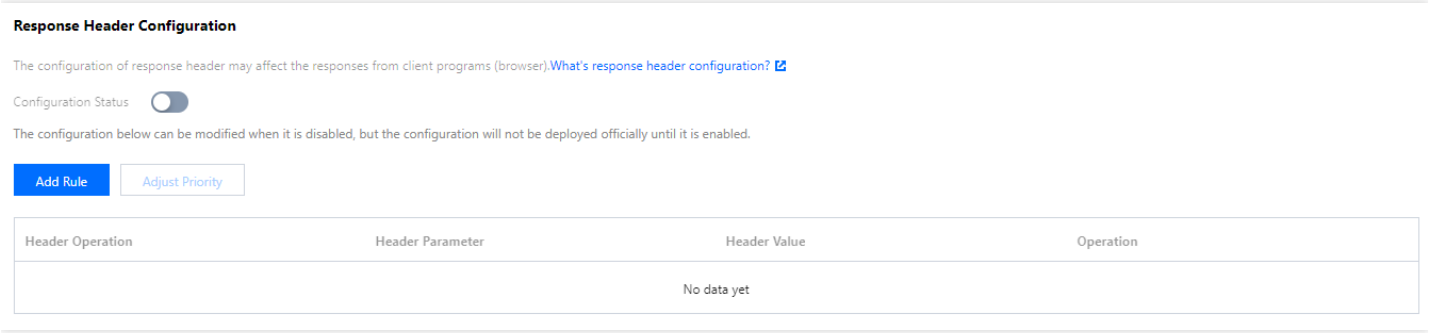
設定シナリオ

ユーザーがサービスリソースをリクエストする時に、返された**応答メッセージ**にカスタムヘッダーを追加して、オリジン間リソース共有などを実現できます。
応答ヘッダーの設定は、ドメイン名に関連するものです。このため、いったん有効に設定すると、ドメイン名の下にある任意のリソースの応答メッセージが有効になります。応答ヘッダーの設定はクライアント（ブラウザなど）の応答動作にのみ影響し、CDNノードのキャッシュ動作までは影響しません。

設定ガイド

設定の確認

CDNコンソールにログインし、メニューバーから【ドメイン名管理】を選択して、ドメイン名の右側の【管理】をクリックすると、ドメイン名設定ページに入ることができ、【高度な設定】でレスポンスヘッダーの設定を確認できます。デフォルトの状態では無効になっており、【ルールの追加】をクリックするとHTTPレスポンスヘッダールールを設定できます：



操作タイプ

操作タイプ	説明

©2013-2022 Tencent Cloud. All rights reserved.

操作タイプ	説明
設定	指定したレスポンスヘッダーパラメータの値を設定後の値に変更します。 設定したヘッダーが存在しない場合は、そのヘッダーを追加します。 重複するヘッダーパラメータが複数存在する場合は、すべて変更すると同時に、1個のヘッダーに統合します。つまり、ルールを【x-cdn: value1の設定】に設定するとき、リクエストに複数のx-cdn ヘッダーが含まれる場合は、複数のヘッダーをすべて変更して1個のヘッダーのx-cdn: value1に統合します。
削除	指定したレスポンスヘッダーのパラメータを削除します。

注意：

- 一部のヘッダーはお客様個人での設定/削除はサポートしていません。リストの詳細はドキュメント 注意事項をご参照ください。
- HTTPレスポンスヘッダーの設定ルールは最大10個まで設定できます。
- 複数のルールで優先度を変更できます。最下部の優先度が最上部よりも高くなっています。同じヘッダーのパラメータが複数の条項のルールを設定した場合は、最下部のものを有効にします。つまり、最下部のものが最優先の条項になります。

ヘッダーパラメータ

ヘッダーパラメータ	説明
Access-Control-Allow-Origin	リソースのクロスドメインの権限問題を解決することに使用します。ドメイン値はそのリソースドメインへのアクセスを定義しています。ソースリクエストHostがドメイン名の設定リストにある場合は、対応する値を戻りヘッダーに直接入力します。ワイルドカード「*」を設定して、すべてのドメインによるリクエストを許可することもできます。詳細は Access-Control-Allow-Origin一致パターンの概要をご参照ください。 「*」 の入力、または複数のドメイン名 / IP / ドメイン名と IPの組み合わせ入力（ `http://` または `https://` を必ず含めてください。入力見本： `http://test.com,http://1.1.1.1` 、 カンマ区切りとする）（注意：最大1000字まで入力可能）をサポートします。
Access-Control-Allow-Methods	クロスドメインが許可するHTTPリクエスト方法の設定に使用します。同時に複数の方法を設定することができます。例：Access-Control-Allow-Methods: `POST, GET, OPTIONS` 。

©2013-2022 Tencent Cloud. All rights reserved.

ヘッダーパラメータ	説明
Access-Control-Max-Age	プレリクエストする有効時間の指定に使用します。単位は秒。 非シンプルクロスドメインリクエストは、正式に通信する前に、HTTP クエリーリクエストを一度追加する必要があり、これを「プレリクエスト」と呼びます。このクロスドメインリクエストが安全に受信可能かを確認するために使用します。以下のリクエストが非シンプルクロスドメインリクエストと見なされた場合： GET、HEADまたはPOST以外の方式で起動するか、またはPOSTを使用しますが、リクエストデータのタイプはapplication / x-www-form-urlencoded、 multipart / form-data、text / plain以外のデータタイプになります。例えば、application / xml またはtext / xmlになります。 カスタマイズしたリクエストヘッドを使用して：Access-Control-Max-Age: `1728000` にすると、1728000秒（20日）以内に、そのリソースのクロスドメインアクセスに対してその他のプレリクエストを再発信しなくなることを示します。
Access-Control-Expose-Headers	どのヘッダーが応答する一部としてクライアントに公開できるかを指定するために使用します。 デフォルトでは、Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragmaの6種類のヘッダーのみクライアントに公開できます。 クライアントをその他のヘッダー情報にアクセスさせたい場合は、以下の設定を行うことができます。複数のヘッダーを入力する場合は、“,” を用いて区切ります。例： `Access-Control-Expose-Headers: Content-Length,X-My-Header` は、クライアントがContent-LengthおよびX-My-Headerの2つのヘッダー情報にアクセスできることを示しています。
Content-Disposition	ブラウザのダウンロードを有効にするために用います。同時にデフォルトでダウンロードするファイル名を設定できます。 サーバーは、クライアントのブラウザにファイルを発信するとき、ブラウザがサポートするファイルタイプがTXT、JPG などのタイプの場合は、デフォルトでブラウザを直接使用して開きます。ユーザー保存を提示したい場合はContent-Dispositionフィールドの設定によってブラウザでのデフォルト動作をカバーできます。通常での設定は次のとおりです。 `Content-Disposition：attachment;filename=FileName.txt`

Content-Language	ページで使用する言語コードを定義するのに用います。通常の設定は次のとおりです。
	`Content-Language: zh-CN`
	`Content-Language: en-US`

©2013-2022 Tencent Cloud. All rights reserved.

ヘッダーパラメータ	説明
カスタマイズ	カスタマイズHeaderの追加、カスタマイズkey-valueの設定をサポートします。 カスタマイズヘッダーパラメータ：英文字の大文字、小文字、数字および-（ハイフン）で構成します。1 ～ 100字まで対応します。 カスタマイズヘッダーの値：1 ～ 1000字まで。中国語はサポートしていません。

Access-Control-Allow-Origin一致パターンの概要

マッチング方式	ドメイン値	説明
完全一致	*	* を設定する時、応答してヘッダーを追加し `Access-Control-Allow-Origin:*`

固定一致	`http://cloud.tencent.com`
	`https://cloud.tencent.com`
	`http://www.b.com`
		ソース `https://cloud.tencent.com` カトにヒットした場合、レスポンスしてヘッダ追加します： `Access-Control-Allow-Origin: https://cloud.tencent.com` ソースが `https://www.qq.com` でリストヒットしない場合、レスポンスに変化はありん。

セカンダリ汎用ドメイン名に一致	`http://*.tencent.com`	ソース `https://cloud.tencent.com` トにヒットした場合、レスポンスしてヘッダ追加します： `Access-Control-Allow-Origin: https://cloud.tencent.com` ソースが `https://cloud.qq.com` でリヒットしない場合、レスポンスに変化はありん。
ポートに一致	`https://cloud.tencent.com:8080`	ソースが `https://cloud.tencent.com:8080` てトにヒットした場合、レスポンスしてヘッダ追加します： `Access-Control-Allow-Origin:https://cloud.tencent.com:` ソースが `https://cloud.tencent.com` ストにヒットしない場合、レスポンスに変化りません。

注意：

©2013-2022 Tencent Cloud. All rights reserved.

特別なポートがある場合は、リストに関連情報を入力する必要があります。任意のポートへの対応はサポートしないため、指定する必要があります。

注意事項

この機能は以下のヘッダーをサポートしていません。つまり以下のヘッダーは有効になりません。

```
Date
Expires
Content-Type
Content-Type
Content-Length
Transfer-Encoding
Cache-Control
If-Modified-Since
Last-Modified
Connection
Connection
ETag
Accept-Ranges
Age
Authentication-Info
Proxy-Authenticate
Retry-After
Set-Cookie
Vary
WWW-Authenticate
Content-Location
Content-MD5
Content-Range
Meter
Allow
Error
```

©2013-2022 Tencent Cloud. All rights reserved.

SEOの設定

最終更新日：：2021-08-11 14:21:55

設定シナリオ

SEO設定はドメインがCDNに接続された後、CDNのIPアドレスの頻繁な変更によりドメイン名検索結果の重みに影響が出る問題を解決するための機能です。IPアドレスへのアクセスが検索エンジンに属するかどうかを識別することにより、直接back-to-originしてリソースへのアクセスを選択することができ、検索エンジンの重みの安定性を確保することができます。

注意：

- 検索エンジンIPが頻繁に更新されることで、Tencent Cloud CDNは検索エンジンIPの大多数を識別できることを保証できます。
- SEO設定機能はドメイン名のオリジンサーバータイプを 外部オリジンサーバー とした時に使用できます。SEO設定機能を有効にした後、ドメイン名に複数のオリジンサーバーアドレスがある場合は、デフォルトのback-to-originアドレスは最初に追加されたオリジンサーバーアドレスになります。
- 中国本土以外は現時点ではサポートしていません。ドメイン名のアクセラレーションリージョンが中国本土以外の場合は、SEO設定の有効化をサポートしていません。ドメイン名のアクセラレーションリージョンがグローバルの場合は、SEO設定を有効にした後、中国本土のみ有効となります。

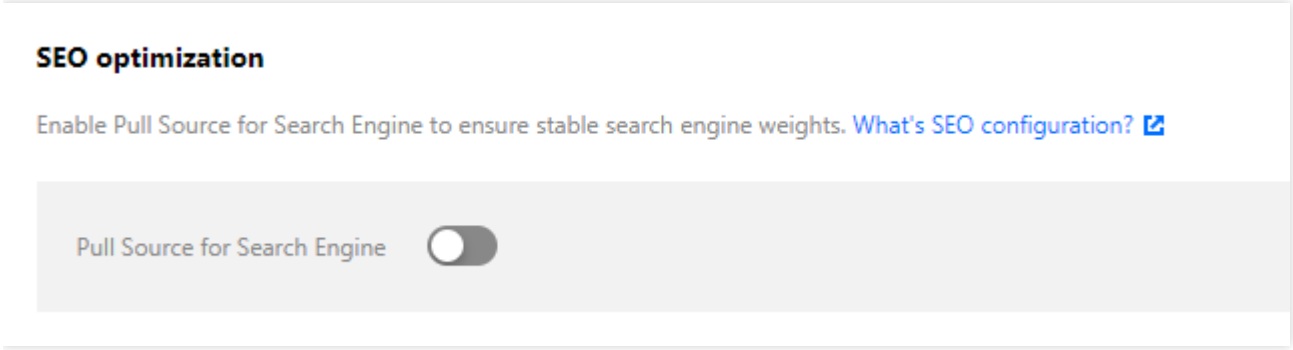
設定ガイド

設定の確認

CDNコンソールにログインし、メニューバーから【ドメイン名管理】を選択し、ドメイン名の右側にある【管理】をクリックすると、ドメイン名設定ページに進み、【高度な設定】の中でSEO設定を確認することができま

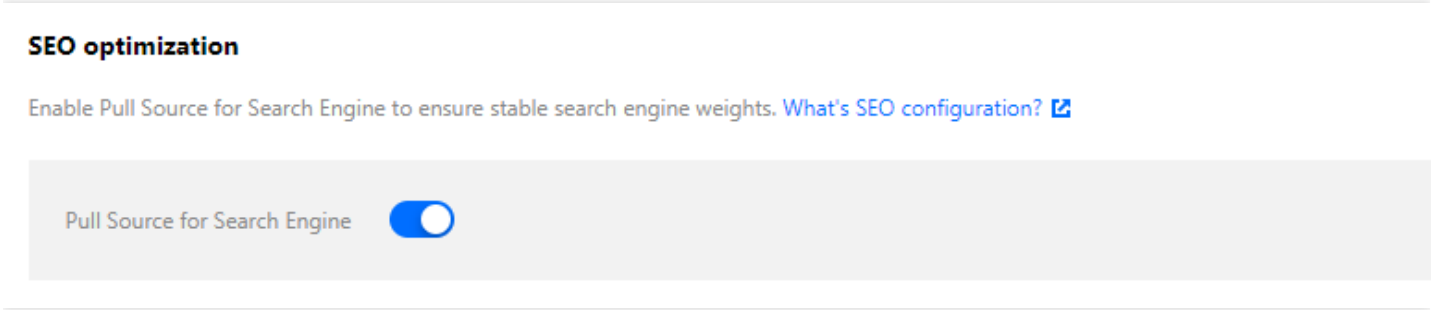
©2013-2022 Tencent Cloud. All rights reserved.

す。デフォルトでは無効になっています。



設定の変更

SEO設定スイッチにより、サービスの有効化または無効化の操作を自分で行うことができます。



©2013-2022 Tencent Cloud. All rights reserved.

インテリジェント圧縮

最終更新日：：2022-01-27 14:34:05

設定シナリオ

インテリジェント圧縮設定により、CDNはコンテンツを返すときに設定されたルールに従ってリソースをGZIP圧縮またはBrotli圧縮し、転送されるコンテンツのサイズを効果的に削減して、オーバーヘッドを削減します。

注意：

- ドメイン名のアクセラレーションリージョンがグローバルである場合は、インテリジェント圧縮設定が有効化された後、グローバルに有効となります。中国本土と中国本土以外の設定が一致しない場合については、現状ではサポートしていません。
- 中国本土以外のアクセラレーションリージョンでは、現状ではContent-Typeタイプおよびbrotli圧縮方式をサポートしていません

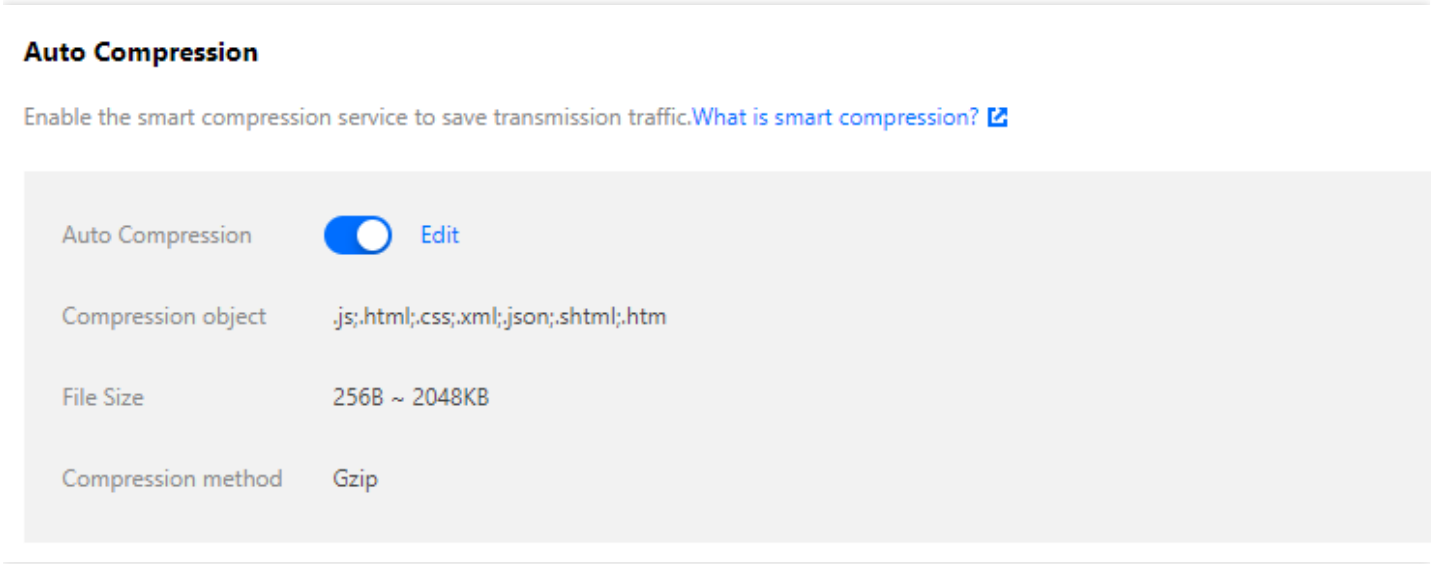
設定ガイド

設定の表示

CDNコンソールにログインし、メニューバーから**ドメイン名管理**を選択し、ドメイン名の右側にある**管理**をクリックすると、ドメイン名設定ページに進み、**高度な設定**でインテリジェント圧縮設定を確認することができます。デフォルトでは有効になっています。

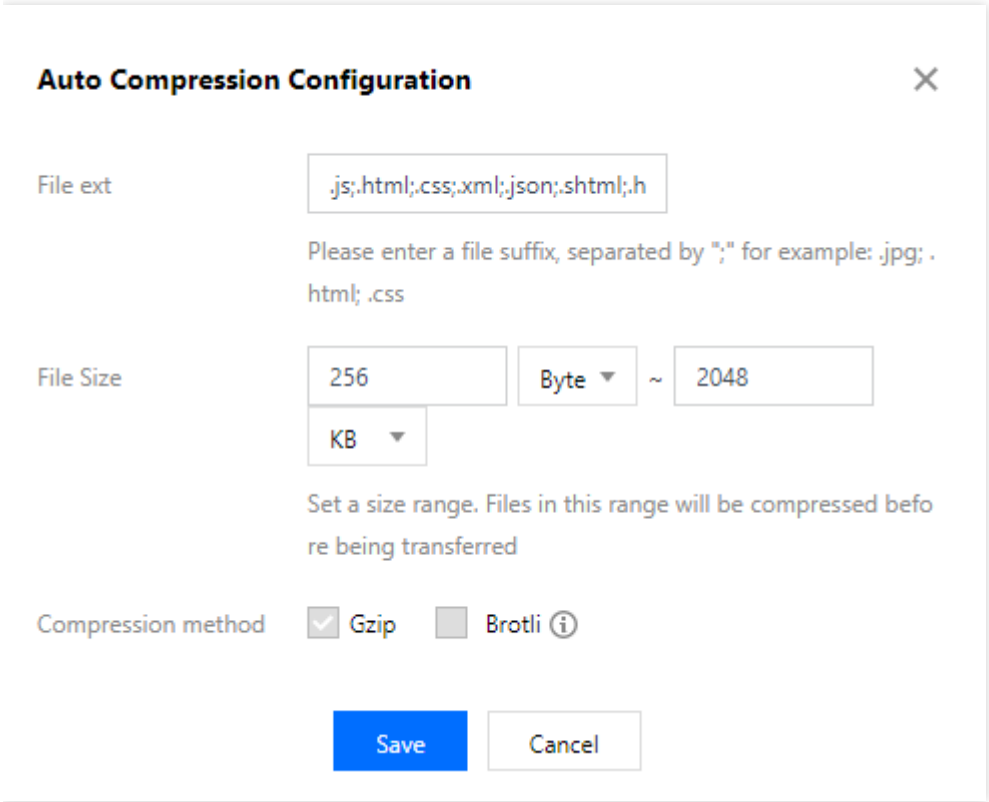
- アクセラレーションドメイン名に接続した後、ファイル拡張子が.js、.html、.css、.xml、.json、.shtml、.htmで、サイズは256Byte～2048KB範囲内のリソースは、デフォルトでGzipで圧縮されます。

©2013-2022 Tencent Cloud. All rights reserved.



設定の変更

操作列の**変更**をクリックすると、圧縮ルールを変更できます。



設定の制約

- タイプはデフォルトではファイル拡張子となっており、全ファイル、Content-Typeタイプに追加できます。
- ファイル拡張子タイプのコンテンツ全体の長さは200文字以内とします。

©2013-2022 Tencent Cloud. All rights reserved.

- ファイルContent-Typeタイプのコンテンツはデフォルトではtext/html、text/xml、text/plain、text/css、text/javascript、application/json、application/javascript、application/x-javascript、application/rss+xml、application/xmltext、image/svg+xml、image/tiffとなっており、必要に応じて設定できます。100組以内とし、それぞれの組のコンテンツは「;」で区切ります。各組のコンテンツは50文字以内とします。
- 一部のプラットフォームではアップグレード中のため、現在はContent-Typeタイプおよびbrotli圧縮方式を利用できません。

説明：

- 以下の構成は、クローズ状態でも変更できますが、現在のネットワークには公開されていません。このスイッチがオンになっている場合にのみ、現在のネットワークに構成が配信されます。
- Gzip圧縮とBrotli圧縮の両方を選択した場合、リクエスト圧縮ヘッダーに従って、対応する圧縮ファイルが返されます。
- Brotli圧縮のみが有効になっている場合、リクエスト圧縮ヘッダーがBrotli圧縮をサポートしていないと、圧縮は有効にならず、元のリソースが返されます。

©2013-2022 Tencent Cloud. All rights reserved.

カスタムエラーページ

最終更新日：：2021-05-25 15:41:03

機能の概要

カスタムエラーページの設定機能は、必要に応じて指定されたエラーステータスコードのリクエストを指定された宛先URLにリダイレクトすることをサポートします。

現在サポートされているステータスコードは次のとおりです。

- 4XX：400,403,404,405,414,416,451
- 5XX：500,501,502,503,504

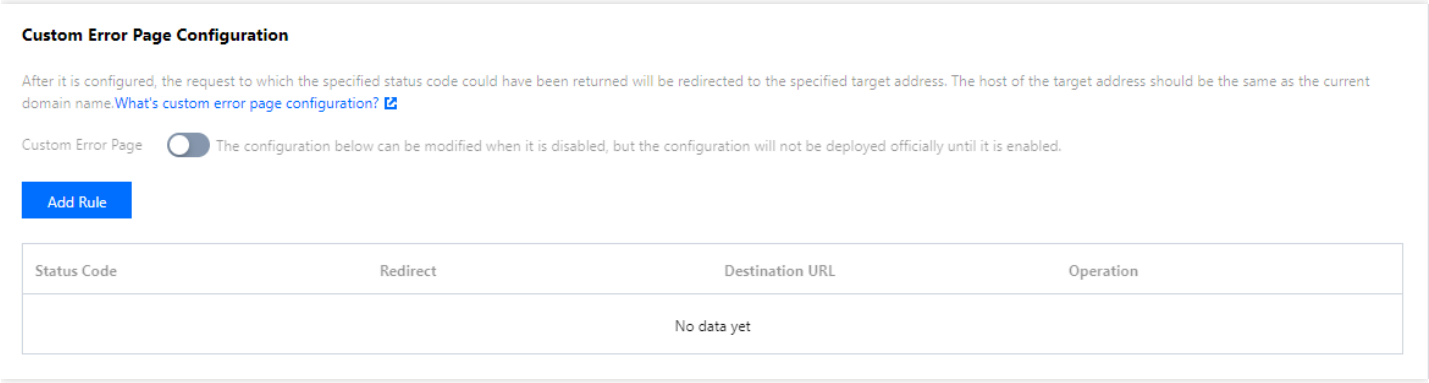
> 注意：
>
> - 一部のプラットフォームはアップグレード中のため、現在この設定機能をサポートしていません。
> -

設定ガイド

設定の確認

CDNコンソールにログインし、左側のメニューバーで【ドメイン名管理】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定画面に入ります。【高度な設定】で【カスタムエラーページの設定】セクションを見つけます。

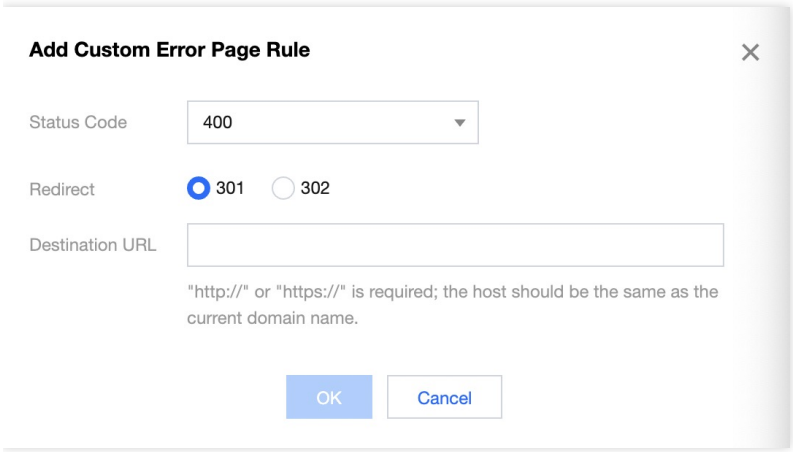
カスタムエラーページの設定はデフォルトで無効になっています。



©2013-2022 Tencent Cloud. All rights reserved.

ルールの追加

【ルールの追加】をクリックして、必要に応じてカスタムエラーページルールを追加できます。



設定の制約事項

- 一つのステータスコードにつき一つのルールを追加することができ、繰り返しルールを設定することができません。
- リダイレクト：301または302を選択できます。
- 宛先URL： `http://` または `https://` が含まれている必要があります。
- コンテンツには最大1,024文字を含めることができ、中国語はサポートされていません。

©2013-2022 Tencent Cloud. All rights reserved.

POSTリクエストサイズ設定

最終更新日：：2021-08-03 10:07:42

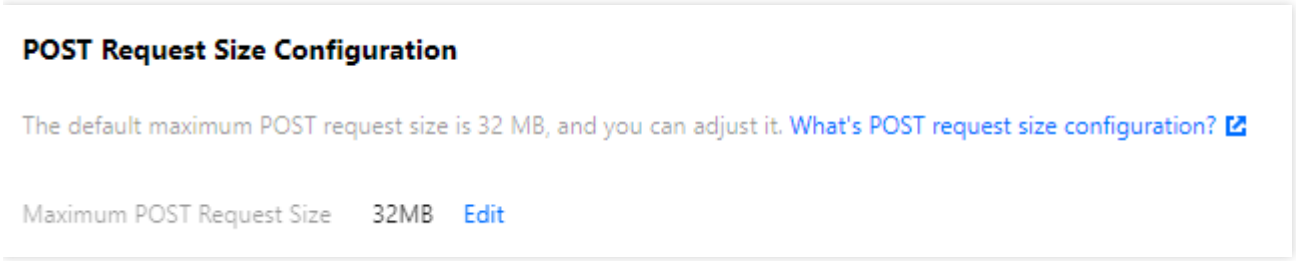
機能説明

Tencent Cloud CDNのPOSTリクエストのサイズの上限、すなわち、リクエストbodyのサイズの上限は、デフォルトで32MBです。実際の業務の状況に応じてこの上限を調整することができます。

設定ガイド

設定の確認

CDNコンソールにログインし、左側メニューバーで【Domain Management】を選択し、ドメイン名操作列の【管理】をクリックして、ドメイン名設定ページに入ります。Tabを【高度な設定】に切り替えると、【POSTリクエストサイズ設定】が見つかります。最大**200MB**まで調整可能です。



注意：
一部のプラットフォームにはPOSTリクエストのサイズ制限がありません。またドメイン名では現在この機能をサポートしていません。

©2013-2022 Tencent Cloud. All rights reserved.

画像の最適化

最終更新日：：2022-07-22 17:27:50

設定シナリオ

大量の画像配信にTencent Cloud CDNを使用すると、画像の最適化を有効にして、要件を満たす画像リクエストのwebp、guetzli、tpg形式の画像を自動的に圧縮できます。これにより、画像によって生成されるダウンリンクトラフィックを効果的に削減し、コストを削減できます。

設定ガイド

CDNコンソールにログインし、メニューバーから**ドメイン名管理**を選択し、ドメイン名の右側にある**管理**をクリックすると、ドメイン名設定ページに進み、オリジンサーバーがCOSである場合、**画像の最適化**メニューバーを表示できます：

- 関連する設定は、オリジンサーバーがCOSで、バージョンがCOS V5である場合にのみ、実行できます。
- Cloud Infiniteサービスをまだ有効にしていない場合は、このページをワンクリックするだけで、Cloud Infiniteサービスを有効にしてから、画像処理に関連する設定を実行できます。
- Cloud Infiniteサービスを有効にしている場合は、直接設定できます。

> 説明：
> Cloud Infiniteは、Tencent Cloudが提供する安全で安定した効率的なクラウドデータ処理サービスであり、Webp、Guetzli、TPGなどの画像処理により一定量のCloud Infinite料金が発生されます。課金説明の確認をクリックしてください。

Webp適応

Webp適応画像圧縮機能を有効にした後、以下の条件を満たすリクエストは、Webpによって処理された画像が直接返されます。以下の条件を満たさない場合は、元の画像が返されます：

- HTTPリクエストヘッダーのacceptヘッダーにimage/webpが含まれています。
- 画像のサフィックスはjpg、jpeg、bmp、gif、pngです。

> 注意：
> - Webp画像圧縮によって発生された料金は、Cloud Infinite-基本的な画像処理料金に起因します。

©2013-2022 Tencent Cloud. All rights reserved.

- 処理された画像の元の画像サイズは20MBを超えてはならず、幅と高さは30000画素を超えてはならず、合計画素は1億画素を超えてはなりません。処理された画像の幅と高さは9999画素を超えてはなりません。
- アニメーション画像の場合、元の画像の幅高さフレーム数は1億画素を超えず、GIFのフレーム数は300フレームに制限されます。

Guetzli適応

Guetzli画像圧縮は、Cloud Infiniteによって開始された視覚的なロスレス圧縮サービスであり、JPG画像を高い比率で圧縮し、ユーザーのダウンロードトラフィックを節約し、ユーザーのダウンロード速度を高め、ユーザーエクスペリエンスを向上させることができます。これは、一部の色域と画像の詳細に対する人間の目の鈍感さを利用し、視覚効果に影響を与えることなく詳細情報を選択的に破棄し、同じ視覚効果の下で元の画像と比較して画像トラフィックの約35%〜50%を節約します。

Guetzli適応画像圧縮機能を有効にした後、以下の条件を満たすリクエストは、Guetzliによって処理された画像が直接返されます：

- HTTPリクエストヘッダーのacceptヘッダーにimage/guetzliが含まれています。
- 画像のサフィックスはjpg、jpegです。

注意：

- Guetzli画像圧縮によって発生された料金は、Cloud Infinite-Guetzli圧縮料金に起因します。
- Guetzliを有効にすると、画像に初めてアクセスしたときに元のJPG画像が返され、同時に非同期Guetzli処理が開始されます。処理が完了した後、画像を再度リクエストすると、圧縮された結果画像が取得されます。
- 現在のGuetzli画像圧縮サービスは、品質qが70を超え、画素数が400万画素未満のJPG画像のみを処理します。

TPG適応

TPG圧縮は、Tencent Cloud Cloud Infiniteが提供する高度な画像圧縮機能です。この機能を使用すると、指定した形式の画像をTPG形式にトランスコードできます。これにより、画像のサイズが大幅に減少し、画像のトラフィックが大幅に削減され、ページのロード速度が向上します。

TPG適応画像圧縮機能を有効にした後、以下の条件を満たすリクエストは、TPGによって処理された画像が直接返されます。

- HTTPリクエストヘッダーのacceptヘッダーにimage/tpgが含まれています。
- 画像のサフィックスはjpg、jpeg、bmp、gif、png、webpです。

©2013-2022 Tencent Cloud. All rights reserved.

注意：
TPG 画像圧縮によって発生された料金は、Cloud Infinite-高度な画像圧縮料金に起因します。

注意事項

適応画像圧縮機能を有効にすると、URLにアクセスするためのキャッシュキーが変更されますが、**キャッシュ設定-キャッシュキールール設定**のキャッシュキールールの優先度が高くなります。
たとえば、jpgタイプのファイルで画像の最適化を有効にしている場合、リクエストURL `http://www.test.com/a.jpg?colour=red` は `http://www.test.com/a.jpgxxxxxx?colour=red` に変更されます。**キャッシュ設定-キャッシュキールール設定**には、すべてのファイル-すべてのパラメータを無視するという優先度がより高いと、設定されている場合、すべてのパラメータを無視すると有効になり、リクエストURLは最終的に `http://www.test.com/a.jpgxxxxxx` に変更されます。

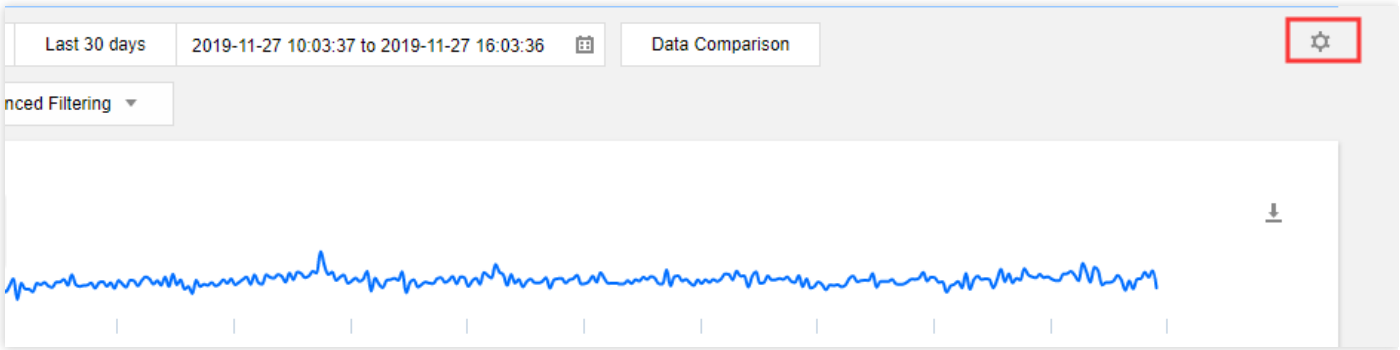
©2013-2022 Tencent Cloud. All rights reserved.

統計分析
リアルタイム監視
パネル構成

最終更新日：：2020-03-17 18:06:57

リアルタイム監視ページの新しいバージョンでは、必要に応じて指標パネルの調整がサポートされているため、監視対象となる指標の監視曲線を簡単に表示できます。

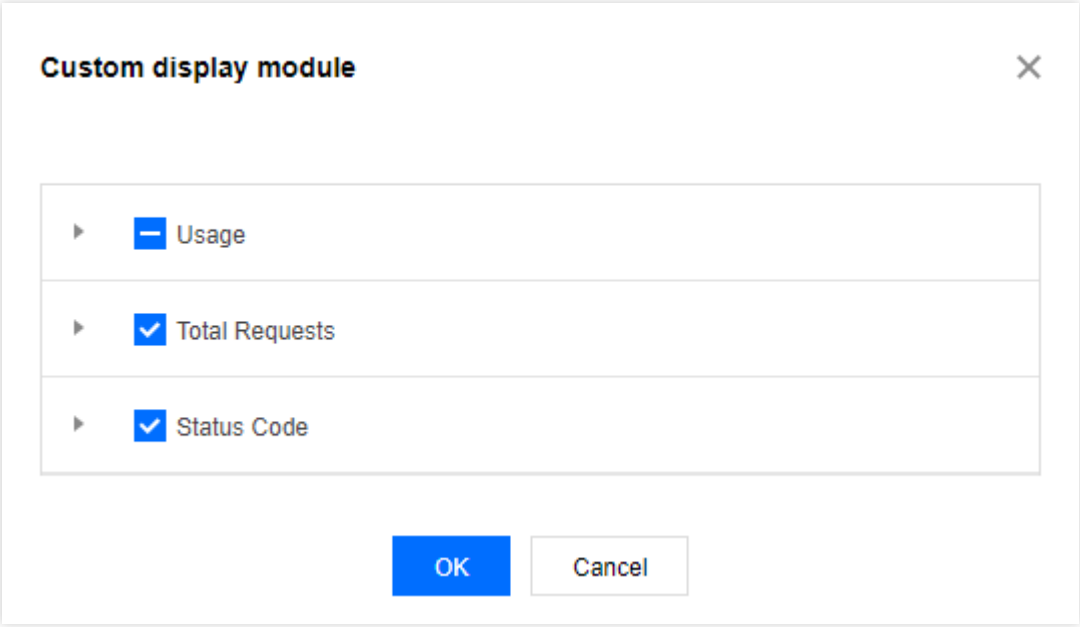
1. CDNコンソールにログインし、左側のディレクトリで【Statistics】>【Realtime Monitoring】をクリックすると、管理ページに入ります。
2. 右側のコンフィグレーションアイコンをクリックして、コンフィグレーションページに入ります。



3. 必要に応じて、全体ビュー画面に表示されるデータ指標を選択します。チェックされた指標は、概要ページに直接表示されます。チェックを外すと、デフォルトでは表示されなくなります。
   リアルタイム監視の【アクセス監視】と【back to origin監視】全体ビュー画面は、それぞれのカスタマイズパ

©2013-2022 Tencent Cloud. All rights reserved.

ネルをコンフィグレーションできます。



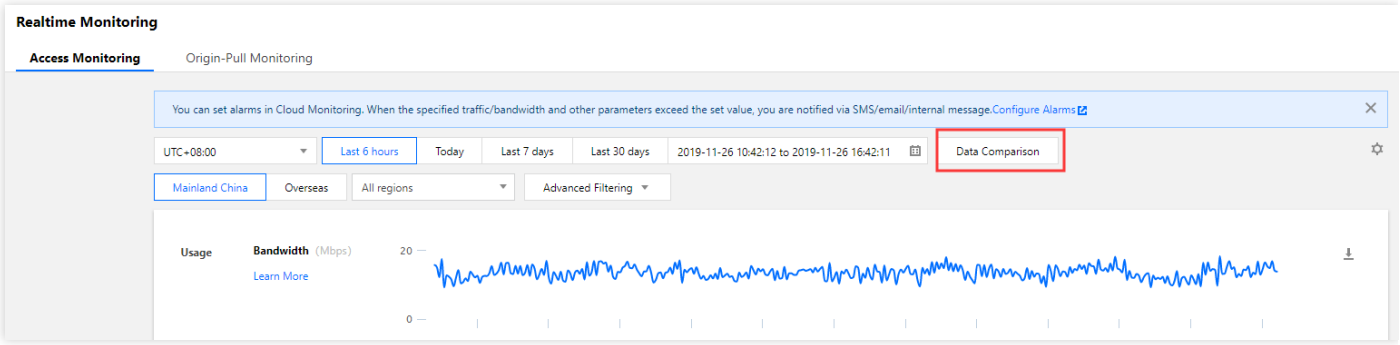
©2013-2022 Tencent Cloud. All rights reserved.

データ比較

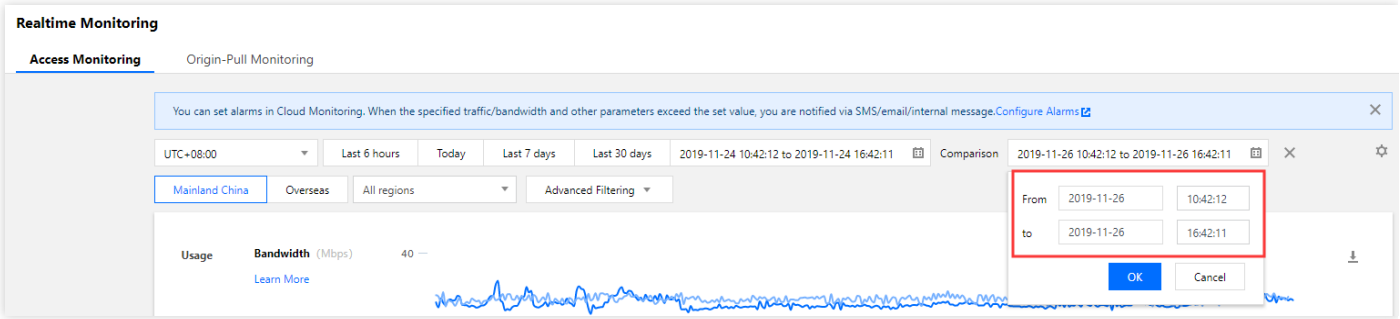
最終更新日：：2020-08-17 17:33:28

新しいバージョンのリアルタイム監視ページのすべてのサブページは、データ曲線の比較機能をサポートしています。

1. CDNコンソールにログインし、左側のディレクトリで【統計分析】>【リアルタイム監視】をクリックすると、管理ページに入ります。
2. 指定された時間帯の監視曲線をクエリーした後、【データ比較】をクリックし、時間帯を指定すると、データを比較表示できるようになります。



ユーザーが使いやすいように、開始日時を指定すると、終了日時がシステムによって自動的に入力されます。終了日時を指定すると、開始日時がシステムによってが自動的に入力され、比較期間の一致が確保されます。



©2013-2022 Tencent Cloud. All rights reserved.

アクセス監視

最終更新日：：2020-11-23 17:45:29

次は新しいバージョンのコンソールの内容です。統計データは古いバージョンよりも充実かつ詳細になり、課金データもこのバージョンに準じるため、新しいバージョンのコンソールのご使用をお勧めします。

指標の説明

概要ページの指標説明

CDNコンソールにログインし、左側のディレクトリで【Statistics】>【Realtime Monitoring】を選択します。管理ページが表示されると、デフォルトでは【アクセス監視】サブページが表示されます。すべてのドメイン名に関する約6時間分の1分間粒度の監視曲線を返します。次の指標が含まれます。

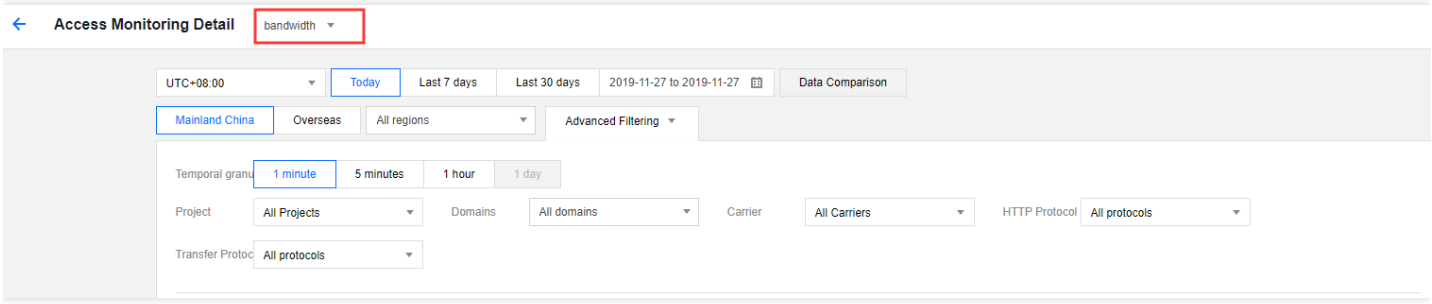
- 帯域幅：1分の総トラフィックを時間（60秒）で割って算出されます。
- トラフィックヒット率：1分以内（ダウンストリームトラフィックの合計-back to originトラフィック）/総ダウンストリームトラフィックで算出されます。
  ＋リクエスト数状態コードの割合：選択された時間帯2XX/3XX/4XX/5XXの割合チャートです。
- リクエスト数状態コード2XX：2XX状態コード監視で、生成された状態コードがすべてカウントされます。
- リクエスト数状態コード3XX：3XX状態コード監視で、生成された状態コードがすべてカウントされます。
- リクエスト数状態コード4XX：4XX状態コード監視で、生成された状態コードがすべてカウントされます。
- リクエスト数状態コード5XX：5XX状態コード監視で、生成された状態コードがすべてカウントされます。

詳細ページのデータ説明

各指標の下にある【詳細を見る】をクリックすると、指標の詳細ページが表示されます。

詳細ページで、左上から指標を速やかに切り替えることもできます。

©2013-2022 Tencent Cloud. All rights reserved.



詳細ページで次のデータを確認することができます。

- 帯域幅：総ピーク帯域幅、リアルタイム帯域幅曲線、ドメイン名帯域幅のランキング（降順）です。
- トラフィック：総トラフィック、リアルタイムトラフィック曲線、ドメイン名トラフィックのランキング（降順）、URLトラフィックのランキング（降順）です。
- トラフィックヒット率：トラフィックヒット率、リアルタイムトラフィックヒット率曲線、ドメイン名トラフィックヒット率のランキング（降順）です。
- リクエスト数：総リクエスト数、リアルタイムリクエスト数曲線、ドメイン名リクエスト数のランキング（降順）、URLリクエスト数のランキング（降順）です。
- 状態コードの割合：2XX、3XX、4XX、5XX状態コードの割合リング図、および各状態コード数と割合の詳細です。
- 状態コード2XX：2XX状態コードのリアルタイム監視曲線、2XX状態コードを構成する各サブ状態コードの監視曲線、2XX状態コードのドメイン名のランクキング（降順）です。
- 状態コード3XX：3XX状態コードのリアルタイム監視曲線、3XX状態コードを構成する各サブ状態コードの監視曲線、3XX状態コードのドメイン名のランクキング（降順）です。
- 状態コード4XX：4XX状態コードのリアルタイム監視曲線、4XX状態コードを構成する各サブ状態コードの監視曲線、4XX状態コードのドメイン名のランクキング（降順）です。
- 状態コード5XX：5XX状態コードのリアルタイム監視曲線、5XX状態コードを構成する各サブ状態コードの監視曲線、5XX状態コードのドメイン名のランクキング（降順）です。

粒度の説明

総覧ページの粒度説明

監視ページには、1分、5分、1時間、1日の粒度曲線の表示オプションを提供します、表示可能な最小の時間粒度は選択された時間帯によって異なります。

- 時間帯 ≤ 6時間の場合、最小の時間粒度は1分となります。1分の粒度監視曲線の現在の遅延は約5～10分です。
- 時間帯が ＞ 6時間で、≤ 24時間の場合、最小の時間粒度は5分となります。5分のデータ遅延は約5～10分です。
- 時間帯が ＞ 24時間で、≤ 31日の場合、最小の時間粒度は1時間となります。
- 時間帯が ＞ 31日の場合、最小の時間粒度は1日となります。

©2013-2022 Tencent Cloud. All rights reserved.

詳細ページの粒度説明

指標の詳細ページに入ると、時間粒度は以下のとおりです。

- 時間帯が ≤ 1日の場合、最小の時間粒度は1分となります。1分の粒度監視曲線の現在の遅延は約5〜10分です。
- 時間帯が ＞ 1日で、 ≤ 31日の場合、最小の時間粒度は5分、1時間、1日（オプション）となります。
- 時間帯が ＞ 31日の場合、最小の時間粒度は1日となります。

> - 現在、1分間の統計粒度でのデータクエリは、中国本土でのみサポートされています。履歴データクエリの最小粒度は5分です。
> - クエリー可能な最大の時間帯は90日です。

集約の説明

データの指標により、1分の粒度が5分、1時間、1日に集約される方法は異なります。

- 帯域幅：CDNサービスが提供する帯域幅監視の最も細かい粒度データは1分のデータです。業界基準によると、課金には一般的に使用されている5分の粒度データは1分のデータAVGから集約されるため、1時間と1日サイクルの帯域幅データは5分の粒度単位でMAXを求めています。
  ＋ トラフィック：5分、1時間、1日サイクルのトラフィックデータは、いずれも1分の粒度トラフィックデータを使用して累積されます。
- トラフィックヒット率：トラフィックヒット率は、1分の結果データを使用して平均を計算する代わりに、依然として選択された時間粒度によって（総ダウンストリームトラフィック-back to originトラフィック）/総ダウンストリームトラフィックという公式で算出されます。
- リクエスト数、状態コード：5分、1時間、1日のデータは、いずれも1分の粒度データを使用して累積されます。

データソースの説明

費用データとログデータ

- 加速ドメイン名ログに記録されている下りバイト数によってカウントされたデータは、アプリケーション層データです。実際のネットワーク転送において生成されたネットワークトラフィックは純粋なアプリケーション層のトラフィックより5%〜15%多くなります。
  - TCP/IPパケットヘッダの消費：TCP/IPプロトコルに基づくHTTPリクエストでは、各パケットのサイズが最大1500バイトであり、TCPとIPプロトコルの40バイトのパケットヘッダが含まれます。パケットヘッダ部分にトラフィックが発生しますが、アプリケーション層にカウントされません。この部分のオーバーヘッドは約3%です。

©2013-2022 Tencent Cloud. All rights reserved.

  - TCP再送信：通常のネットワーク転送中、送信されたネットワークパケットは3%～10%ぐらいがインターネット上で廃棄されます。サーバーは廃棄された部分を再送信しますが、アプリケーション層はこの部分にかかったトラフィックをカウントできません。比率は約3%～7%です。
- 業界標準では、費用に使用されるデータは、一般的にはアプリケーション層のデータに上記のオーバーヘッドを加えます。Tencent Cloud CDNは10%です。ですから、監視画面で表示される費用トラフィック/帯域幅は、ログ計算データの約110%です。
- トラフィック帯域幅以外に、その他の指標はアプリケーション層の統計量です。監視画面で表示されるデータはログデータとわずかな違いがあります。それは主にネットワークの変動の影響を受けて、ノードからログをプルして分析し、またはサーバーへデータをレポートする時、いずれもある程度のデータロスが発生しますので、これは完全に一致しない原因となります。

データソースの説明

+「統計地域」または「キャリア」オプションがスクリーニングされていない場合、クエリーされたデータはすべて費用データとなります。

- 「統計地域」または「キャリア」をスクリーニングした場合、アクセスログ内のclient IPマッチングに基づいて計算する必要があり、クエリーされたデータはすべてログデータとなります。

スクリーニングの説明

- 現時点、「統計地域」と「キャリア」の両方を指定したクエリーはサポートされておらず、省指定によるすべてのキャリアクエリーまたはキャリア指定によるすべての地域クエリーのみがサポートされています。
- back to origin監視は、現時点、「統計地域」と「キャリア」のスクリーニングをサポートしていません。
- back to origin監視は、現時点、HTTPS/HTTPリクエストのスクリーニングをサポートしていません。

©2013-2022 Tencent Cloud. All rights reserved.

back-to-origin監視

最終更新日：：2021-08-06 11:54:30

注意：
ECDNドメイン名は、現時点ではback-to-originデータの照会をサポートしていません。

インジケータの説明

概要ページインジケータの説明

CDNコンソールにログインし、左側のディレクトリで【統計分析】>【リアルタイムモニタリング】を選択して管理ページに移動したら、デフォルトで【アクセス監視】サブページが表示されます。上部の【back-to-origin監視】をクリックすると、back-to-origin監視指標ページに移動し、次のインジケータを含む、すべてのドメイン名の6時間1分粒度の監視曲線に戻ることができます。

- back-to-origin帯域幅：1分間の総back-to-originトラフィックを時間（60秒）で割って計算します。
- back-to-originトラフィック：最終レイヤーアクセラレーションノードの総back-to-originトラフィック。
- back-to-originリクエスト数：最終レイヤーアクセラレーションノードの総back-to-originリクエスト数。
- back-to-origin失敗率：失敗したback-to-originリクエストが総back-to-originリクエストに占める割合。
- back-to-originステータスコードの割合：選択した時間間隔のback-to-originで生成された2XX/3XX/4XX/5XX割合図。
- back-to-originステータスコード2XX：back-to-origin 2XXステータスコードの監視。生成されたステータスコードはすべて統計に組み入れることができます。
- back-to-originステータスコード3XX：back-to-origin 3XXステータスコードの監視。生成されたステータスコードはすべて統計に組み入れることができます。
- back-to-originステータスコード4XX：back-to-origin 4XXステータスコードの監視。生成されたステータスコードはすべて統計に組み入れることができます。
- back-to-originステータスコード5XX：back-to-origin 5XXステータスコードの監視。生成されたステータスコードはすべて統計に組み入れることができます。

次の状況は失敗したback-to-originリクエストにカウントされます。

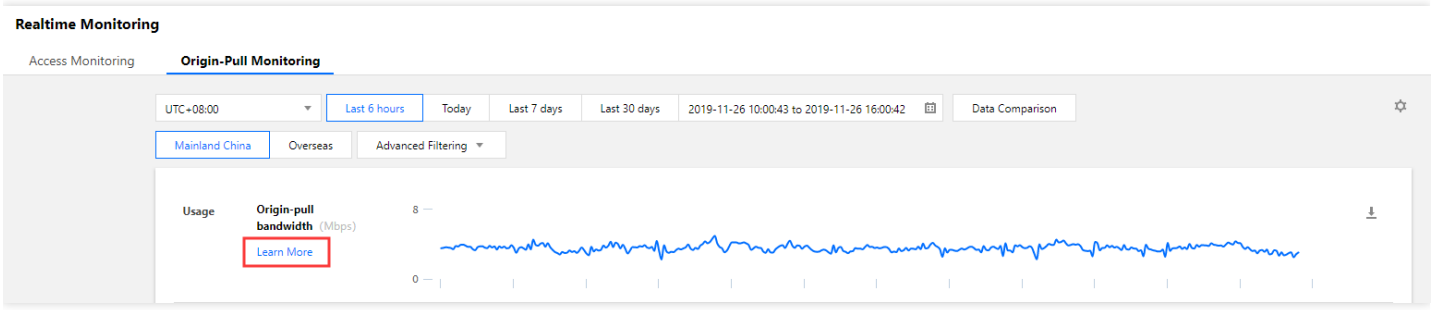
- back-to-originデータ受信時のタイムアウト。
- back-to-originリクエスト送信時のタイムアウト。
- back-to-origin tcp connectのタイムアウト。
- オリジンサーバーによる接続の能動的なシャットダウン。

©2013-2022 Tencent Cloud. All rights reserved.

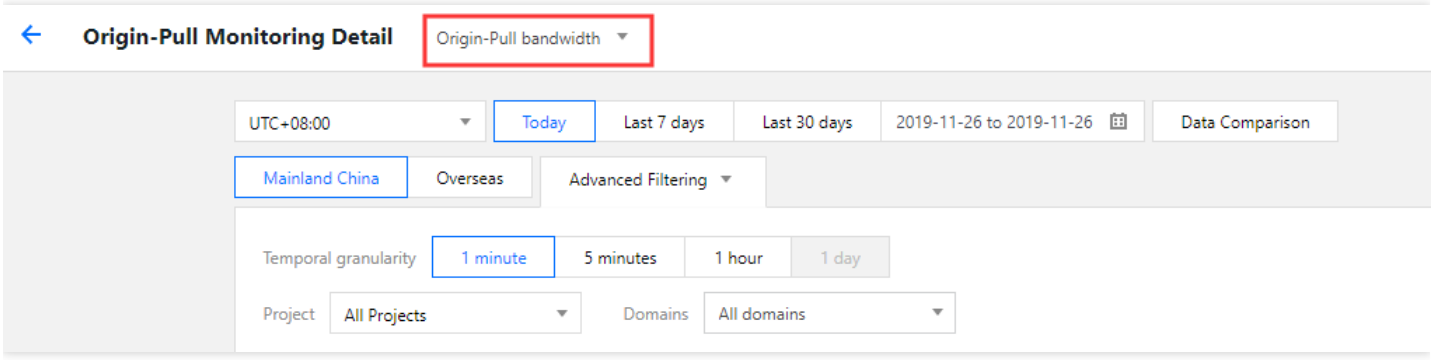
- オリジンサーバーHTTPプロトコルの互換性エラー。

詳細ページデータの説明

各インジケータ下部の【詳細の表示】をクリックすれば、インジケータ詳細ページに移動できます。



詳細ページの左上からインジケータの迅速な切り替えを実行できます。



粒度の説明

概要ページの粒度の説明

監視ページでは、1分、5分、1時間、1日粒度の曲線表示オプションを提供しています。選択した時間間隔によって、表示可能な最小の時間粒度が異なります。

- 時間間隔 ≤ 6時間での最小時間粒度は1分であり、1分粒度監視曲線の現在の遅延は約3分です。
- 時間間隔 ＞ 6時間かつ ≤ 24時間での最小時間粒度は5分で、5分データの遅延は5～10分です。
- 時間間隔 ＞ 24時間かつ ≤ 31日での最小時間粒度は1時間です。
- 時間間隔 ＞ 31日での最小時間粒度は1日です。

詳細ページの粒度の説明

インジケータ詳細ページに移動した場合の時間粒度は次のとおりです。

- 時間間隔 ≤ 24時間での最小時間粒度は1分であり、1分粒度監視曲線の現在の遅延は約3分です。

©2013-2022 Tencent Cloud. All rights reserved.

- 時間間隔 ＞24時間かつ ≤ 31日での最小時間粒度は5分、1時間、または1日です（オプション）。
- 時間間隔 ＞ 31日での最小時間粒度は1日です。

注意：

- 1分粒度データは、新規バージョンがオンラインにならなければ照会できません。履歴データの照会可能な最小粒度は5分です。
- 照会可能な最大時間間隔は直近90日です。

集計の説明

各種データインジケータに応じて、1分粒度から5分、1時間、1日に集計する各種の方法があります。

- back-to-origin帯域幅：CDNが提供する帯域幅監視の最小粒度データは1分データであり、業界標準規格によれば、料金に通常使用される5分粒度データは1分データAVGに基づくことから、1時間、1日サイクルの帯域幅データでは、5分粒度を利用してMAXを計算します。
- back-to-originトラフィック：5分、1時間、1日サイクルのトラフィックデータは、いずれも1分粒度のトラフィックデータを利用して累計します。
- back-to-originリクエスト数：5分、1時間、1日サイクルのトラフィックデータは、いずれも1分粒度のリクエスト数を利用して累計します。
- back-to-origin失敗率：選択した時間粒度に基づき、総back-to-origin失敗数 / 総back-to-originリクエスト数で計算します。
- back-to-originステータスコード：5分、1時間、1日サイクルのステータスコードデータは、いずれも1分粒度のステータスコードデータを利用して累計します。

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコードに関する説明

最終更新日：：2023-03-14 15:13:28

以下でCDN内部のステータスコードの意味を説明します：

ステータスコード	意味	推奨する対処方法
0	リクエストに対するレスポンスのステータスコードを取得する前にリクエストが終了しました	クライアントが早めにリクエストを自発的に切断したか、Back-to-Originに失敗したを確認してください。
400	HTTPリクエストの構文エラーサーバーで解決できません	リクエストの構文が正しいかを確認してください。
403	リクエストが拒否されました	refererブラックリスト/ホワイトリスト、IPブラックリスト/ホワイトリスト、認証設定などのアクセス制御機能が設定されているかを確認してください。
404	サーバーが正しい情報を返すことができません	オリジンサーバーが正常に動作しているか、またはオリジンサーバーの情報、ホストヘッダーの設定が変更されたかを確認してください。詳しくは、CDNドメイン名の404エラーが発生した場合の対処方法をご参照ください。
413	POSTの長さが制限を超えています	クライアントのPOSTのコンテンツサイズを確認してください（デフォルトのサイズ制限は32MBです）。
414	URLの長さが制限を超えています	URLのデフォルトのサイズ制限は2KBです。
423	ループバックリクエスト	Back-to-Originの301/302追従設定、設定したHTTPS　Back-to-Origin方法、オリジンサーバーrewriteの対処方法を確認してください。
499	クライアントが自発的に接続を切断しました	クライアントのステータスまたはタイムアウトの設定を確認してください。
502	ゲートウェイエラー	オリジンサーバーが正常に動作しているかを確認してください。
503	COS頻度制御がトリガーされました	キャッシュ設定またはCOSオリジンサーバーがno-cache/no-storeを返しているかを確認してください。

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコード	意味	推奨する対処方法
504	ゲートウェイタイムアウト	公式サイトにお問い合わせください。
509	CC攻撃のためロックされました	ロックを解除するには、お問い合わせまたはチケットを提出してください。
514	IPアクセス頻度制限を超えました	CDNコンソールでIPアクセス頻度制限の設定を確認してください。
524	プラットフォームへのアクセス負荷が上限を超えました	業務リクエストが短時間で大量に発生すると、プラットフォームへのアクセス負荷が上限を超えます。業務量を見積もってTencent Cloudに伝えてください。質問等があればアフターサービスにお問い合わせください。
531	HTTPSリクエストのback-to-originドメイン名解決エラー	オリジンサーバーのドメイン名解決設定を確認してください。
532	HTTPSリクエストのback-to-originサーバーとの接続の確立に失敗しました	オリジンサーバー443ポートのステータスおよび証明書の設定またはオリジンサーバーの可用性を確認してください。
533	HTTPSリクエストのback-to-originサーバーとの接続がタイムアウトしました	オリジンサーバー443ポートのステータスおよび証明書設定またはオリジンサーバーの可用性を確認してください。
537	HTTPSリクエストのオリジンサーバーのデータ受信がタイムアウトしました	業務オリジンサーバーの安定性を確認してください。
538	HTTPSリクエストのSSLハンドシェイクに失敗しました	オリジンサーバープロトコルとアルゴリズムの互換性を確認してください。
539	HTTPSリクエストの証明書の検証に失敗しました	オリジンサーバーの証明書の設定が正常かどうかを確認してください（期限切れではないか、証明書リンクが完全かどうかなど）。
540	HTTPSリクエストの証明書ドメイン名検証に不合格となりました	オリジンサーバーの証明書が正常に設定されているかどうかを確認してください。
562	HTTPSリクエストの接続の確立に失敗しました	お問い合わせに連絡してX-NWS-LOG-UUID情報を提供するか、またはチケットを提出して原因を調査してください。

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコード	意味	推奨する対処方法
563	HTTPSリクエスト接続がタイムアウトしました	お問い合わせに連絡してX-NWS-LOG-UUID情報を提供するか、またはチケットを提出して原因を調査してください。
564	HTTPSリクエストのback-to-originに失敗しました	HTTP back-to-origin方式に設定している場合は、オリジンサーバーの負荷および帯域幅の使用率をチェックするか、またはオリジンサーバーのアクセス制限を確認してください。 プロトコル追従方式に設定している場合は、オリジンサーバー443ポートのステータスおよび証明書の設定を確認してください。 調査の結果、オリジンサーバーに異常がない場合は、お問い合わせに連絡してX-NWS-LOG-UUID情報を提供するか、またはチケットを提出して原因を調査してください。
563	HTTPSリクエスト接続がタイムアウトしました	お問い合わせに連絡してX-NWS-LOG-UUID情報を提供するか、またはチケットを提出して原因を調査してください。

以下はHTTPプロトコルのレスポンスステータスコードの定義です。

ステータスコード	意味
100	サーバーはリクエストヘッダーを受信しました。クライアントはリクエストボディを継続してよいです（例えば、POSTリクエストなど、リクエストボディを送信する必要がある場合）。また、リクエストが完了している場合、レスポンスを無視してよいです。サーバーはリクエストが完了した後、クライアントに最終的なレスポンスを送信する必要があります。サーバーがリクエストヘッダーをチェックするには、クライアントは最初のリクエストに100-continueをヘッダーとするExpectを送信する必要があります。なお、本文を送信する前に、100 Continueステータスコードを受信しなければなりません。レスポンスステータスコード
101	サーバーはクライアントのリクエストを理解し、Upgradeメッセージヘッダーを通して、クライアントに異なるプロトコルでリクエストを完了させることを通知します。このレスポンスの最後の空行を送信した後、サーバーはUpgradeメッセージヘッダーに定義されているプロトコルに切り替えます。新しいプロトコルに切り替えるメリットがある場合のみ、上記の処理が行われます。例えば、古いバージョンを使用することに比べ、新しいHTTPバージョン（HTTP/2など）に切り替える方がメリットがある場合、または、リアルタイムかつ同期性のあるプロトコル（WebSocketなど）に切り替えてこのような特徴を利用するリソースを転送する場合。

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコード	意味
102	WebDAVリクエストにファイル操作関連のサブリクエストが複数含まれている場合、リクエストが完了するまで時間がかかります。このコードは、サーバーがリクエストを受信し処理しているが、レスポンスを提供できないことを示します。これにより、クライアントのタイムアウトを防ぎ、リクエスト紛失として扱います。
103	最終的なHTTPメッセージの前にレスポンスヘッダーを返します。
200	リクエストが成功したことを示します。リクエストしたレスポンスヘッダーまたはデータボディはこのレスポンスとともに返されます。GETリクエストの場合、リソースが読み込まれ、メッセージ本文で転送されます。POSTリクエストの場合、動作の状態または動作により得られた結果がメッセージ本文で転送されます。
201	リクエストは成功し、その結果新たなリソースが作成され、そのURIがLocationヘッダーにて返されます。必要なリソースをタイムリーに作成できなかった場合、'202 Accepted'を返すべきです。
202	サーバーはリクエストを受信したが、まだ処理していません。このリクエストは最終的には実行される可能性と実行されない可能性両方あります。また、処理開始時に禁止される可能性もあります。
203	サーバーはトランスフォーミングプロキシ（ネットワークアクセラレーションなど）です。リクエストはトランスフォーミングプロキシによって元のサーバーの200（OK）レスポンスからペイロードが変更されました。
204	サーバーはリクエストを正常に処理したが、コンテンツを返しませんでした。Captive Portal機能では、Wi-FiデバイスがWeb認証が必要なWi-Fiアクセスポイントに接続する時、HTTP 204レスポンスを作成できるサイトにアクセスし、204レスポンスを受信した場合、Web認証を行う必要がありません。204レスポンスを受信しなかった場合、ウェブページブラウザが起動し、Web認証画面が表示され、認証を行ってログインします。
205	サーバーはリクエストを正常に処理したが、コンテンツを返しませんでした。204レスポンスと違い、このレスポンスはクライアントにドキュメントビューをリセットするように指示します。
206	サーバーは一部のGETリクエストを正常に処理しました。FlashGet、迅雷のようなHTTPダウンロードツールは全部このレスポンスを使用し、レジューム対応ダウンロード、ラージ文書を分割して同時にダウンロードする方法を実装します。
207	次のメッセージボディはXMLメッセージです。これまでのサブリクエスト数によって、一連の独立したレスポンスステータスコードを含む可能性があります。
208	DAVにバインディングしているメンバーはすでに（マルティステータス）レスポンスより前の部分に列挙されているため、今回は含まれていません。

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコード	意味
226	サーバーはリソースへのリクエストを処理しました。１つ以上の動作により得られた結果を示します。
300	リクエストされたリソースに対して、複数のレスポンスがあります。レスポンスごとにより具体的なアドレス及びブラウザとの交渉情報があります。ユーザーまたはブラウザは、優先アドレスを選択しリダイレクトを実行できます。
301	恒久的に移動されました。リクエストされたリソースのURIが永遠に変更されました。レスポンスで新しいURIが与えられます。ブラウザは新しいURIに自動的にリダイレクトします。将来のリクエストで新しいURIを使用してください。
302	一時的に移動します。301と似ています。ただし、リクエストされたリソースのURIが一時的に変更されました。クライアントは将来のリクエストでも同じURIを使用してください。
303	現在のリクエストのレスポンスは別のURIから取得できます。レスポンスがPOST（またはPUT/DELETE）にてレスポンスを受信した場合、クライアントはサーバーがデータを受信しているとして扱い、独立したGETメッセージを使用しリダイレクトを発行してください。
304	リクエストヘッダーのIf-Modified-SinceパラメータまたはIf-None-Matchパラメータに指定したバージョン以降、リソースが変更されていません。この場合、クライアントに以前キャッシングされたコピーがあるため、リソースを再転送する必要がありません。
305	リクエストされたリソースは指定したプロキシからアクセスしなければなりません。指定したプロキシが所在するURIの情報はLocationドメインによって提供されています。受信側は独立したリクエストを重複して送信し、このプロキシを経由してリソースにアクセスします。
306	新しいバージョンの仕様書では、306ステータスコードはもう使用されていません。このコードは、最初に「将来のレスポンスで指定したプロキシを使用する必要がある」ということを意味します。
307	この場合、リクエストは別のURIと重複しますが、将来のリクエストで元のURIを使用してください。302と異なり、元のリクエストを再送信する場合、リクエストのメソッドを変更してはいけません。例えば、始めのリクエストでPOST を用いた場合は、次のリクエストでもPOSTを使用しなければなりません。
308	リクエストとすべての将来のリクエストは別のURIを使用してください。307と308は、302と301の処理を繰り返すが、HTTPメソッドを変更してはいけません。例えば、フォームを永遠にリダイレクトされたリソースにサブミットすれば、処理が順調に行われる可能性があります。

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコード	意味
401	403 Forbiddenと似ています。401は未認証を意味します。つまり。ユーザには必要な資格情報を持っていません。
405	リクエスト行に指定したリクエストメソッドは、同じリソースのリクエストに使用できません。このレスポンスは、Allowヘッダーを返し、現在のリソースが受け付けられるリクエストメソッドのリストを示す必要があります。
406	リクエストされたリソースのコンテンツがリクエストヘッダーに与えられた条件を満たさないため、レスポンスボディを生成できず、このリクエストを受け入れられません。
407	401と似ていますが、クライアントがプロキシーサーバーで認証を行わなければなりません。
408	リクエストタイムアウト。HTTP仕様書により、クライアントはサーバーのアイドル状態でリクエストの送信を完了しなかった場合、いつでもこのリクエストを変更せずにサブミットできます。
409	サーバに既に存在しているデータが競合しているためリクエストを完了できません。例えば、複数の同期更新の間に編集の矛盾が発生しています。
410	リクエストされたリソースを使用できなくなりました。リソースが意図的に削除された場合、またはリソースをクリアすべきな場合、このステータスコードを返します。410を受信した後、ユーザはリソースを改めてリクエストしないでください。ほとんどのサーバーはこのステータスコードではなく、404を使用します。
411	サーバーはContent-Lengthヘッダーが定義されていない場合このリクエストを拒否しました。リクエストのメッセージボディの長さを表す有効なContent-Lengthを追加した後、クライアントはこのリクエストを改めてサブミットできます。
412	サーバー認証で、リクエストのヘッダーフィールドに与えられた1つ以上の前提条件満たしていません。このステータスコードは、クライアントがリソースを取得する時に、リクエストのメタデータ（リクエストのヘッダーフィールドにあるデータ）に前提条件を設定することを許可します。これにより、このリクエストのメソッドがリクエストの意図しないリソースに使用されることを防ぎます。
415	現在リクエストされたメソッドとリソースに対して、リクエストに設定されているインターネットメディアタイプはサーバーがサポートするフォーマットではないため、リクエストを拒否しました。例えば、クライアントはsvgフォーマットの画像をアップロードしましたが、サーバーがサポートするフォーマットはjpgです。
416	サーバーはクライアントがリクエストしたファイルの部分を提供できません。例えば、クライアントがリクエストしたファイルの一部はファイルの最後を超えています。

©2013-2022 Tencent Cloud. All rights reserved.

ステータスコード	意味
417	サーバーはリクエストヘッダーExpectに指定した内容と適合しません。または、このサーバーはプロキシサーバーであり、現在のルーターの次のノードでExpectの内容と適合しません。
500	汎用エラーメッセージ。サーバーで予期しない事態が発生し、リクエストを処理できません。具体的なエラーメッセージが提供されていません。
501	サーバーは現在のリクエストが必要とするある機能をサポートしません。サーバーはリクエストのメソッドを識別できず、リソースに対するリクエストをサポートしません。
505	サーバーはリクエストに使用されているHTTPバージョンをサポートしません。または、リクエストに使用されているHTTPバージョンへのサポートを拒否します。これは、サーバーがクライアントと同じバージョンを使用できない、または使用したくないことを意味します。レスポンスにバージョンをサポートしない理由と、サーバーがサポートするプロトコルの情報を含めるべきです。
508	サーバーは、リクエストの処理中に無限ループを検出しました。
510	リソースの取得に必要とするポリシーと適合しません。

©2013-2022 Tencent Cloud. All rights reserved.

データ分析

最終更新日：：2021-11-08 12:34:24

クライアントがユーザー分布と使用状況を理解しやすいよう、アクセスログを利用してユーザーソースを分析し、データ分析ページで各種グラフの表示を提供します。

CDNコンソールにログインし、左側のディレクトリで【統計分析】>【データ分析】をクリックし、データ分析ページに移動します。

- 照会できる最大時間間隔は31日で、履歴データは90日間保持されます。
- 照会できる最も古い履歴データは、この照会実行した日から3か月以内のデータです。

> 注意：
> 現時点では、ECDNドメイン名は独立IPアクセス数の照会とアクセスのユーザーエリア分布表示をサポートしていません。

データの概要

指定したレポートディメンションに基づいて、さまざまなデータの概要を表示します。
異なる課金方法で表示される概要データは、それぞれに異なります。
トラフィック課金時の表示：総トラフィック、平均トラフィックヒット率およびリクエスト数。
帯域幅課金時の表示：ピーク帯域幅、back-to-originのピーク帯域幅およびリクエスト数。

アクセスユーザーのエリア分布

指定したレポートの次元に基づいて、対応するエリアのトラフィック分布図を表示します。クライアントがビジネスユーザーの地理的分布を把握しやすいよう、ソースクライアントIPを介して訪問者が所在する省を特定し、マップとリストを表示します。中国本土では省ごとに集計し、中国本土以外ではエリアごとに集計します。

トラフィック

指定したレポートディメンションに従って、対応するトラフィック曲線を表示します。課金トラフィックまたはback to originトラフィック曲線の表示を選択できます。

©2013-2022 Tencent Cloud. All rights reserved.

帯域幅

指定したレポートの次元に基づいて、対応するトラフィック曲線を表示します。帯域幅の課金またはback-to-origin帯域幅曲線の表示を選択でき、ピーク帯域幅曲線をサポートします。

リクエスト数

指定したレポートディメンションに応じて、リクエスト数の曲線を表示します。

エラーコード

指定したレポートディメンションに従って、対応するエラーコードの数と割合を表示します。

TOP10 URL

指定したレポートの次元に基づいて、対応するTOP10のURLを表示し、使用量またはリクエスト数でランク付けすることを選択できます。

TOP10項目

指定したレポートの次元に基づいて、対応するTOP10項目を表示します。

TOP10ドメイン名

指定したレポートの次元に基づいて、対応するTOP10ドメイン名を表示します。

独立IPアクセス数

独立IPアクセス数は、指定の時間サイクルに従い、ログ内のアクセスソースクライアントIPを重複排除して計算されます。
時間間隔が1日以下である場合は、5分粒度の重複排除されたIP数曲線が提供されます。
ドメイン名の状況は、1日のDAUの重複を排除して計算され、マルチドメイン名/プロジェクト/アカウントの状況は、各ドメイン名のDAUの5分粒度に従って累積されます。

©2013-2022 Tencent Cloud. All rights reserved.

注意：
過去30日間のデータの照会のみをサポートします。

ユーザーのキャリア分布

クライアントがビジネスユーザーのキャリアを把握しやすいよう、ソースクライアントIPを介して訪問者のキャリアを識別し、円グラフ、リストを表示します。

©2013-2022 Tencent Cloud. All rights reserved.

統計に関するよくあるご質問

最終更新日：：2020-12-04 17:12:00

アクセス監視の帯域幅データはどのように統計されていますか。

各CDNノードはリアルタイムでトラフィックデータを収集し、コンピューティングセンターに報告してドメイン名の総トラフィックデータに集計します。時間の期間によって、総トラフィックを使用時間で割って帯域幅統計を表示します。

例

- 1分間に発生したトラフィックの合計は6MBである場合、対応する帯域幅は（6 * 8）/60 = 0.8Mbpsとなります。
- 帯域幅課金には5分間粒度のデータで決済すると、対応する帯域幅の値=5分間粒度の総トラフィック÷300秒となります。

監視情報のトラフィックとログによって計算されたトラフィックに違いがあるのはなぜですか、違いは何ですか。

アクセラレーションドメイン名のログに記録されているダウンストリームバイトによって統計されたトラフィックデータは、アプリケーション層のデータです。実際のネットワーク転送において生成するネットワークトラフィックは純粋なアプリケーション層のトラフィックよりも約5〜15%多くなります。

- TCP/IPヘッダーによる消費：TCP/IPプロトコルに基づくHTTPリクエストでは、各パケットのサイズは最大1500バイトであり、TCPとIPプロトコルの40バイトのヘッダーが含まれます。ヘッダー部にトラフィックが生成しますが、アプリケーション層に統計されません。この部分のオーバーヘッドは約3%です。
- TCP再送信：ネットワークを介した通常のデータ転送中に、送信されるネットワークパケットの約3%〜10%はインターネット上で廃棄されます。サーバーは廃棄された部分を再送信しますが、アプリケーション層はこの部分にかかったトラフィックを統計できません。このタイプのトラフィックは、総トラフィックの約3%〜7%を占めます。

業界標準では、課金可能なトラフィックは、一般的にアプリケーション層でカウントされたトラフィックとオーバーヘッドの合計です。Tencent Cloud CDNは10%を占めるため、監視トラフィックがログによって計算されるトラフィックの110%程度となります。

トラフィックのヒット率はどのように計算しますか。

CDNは、デフォルトではユーザーにL2キャッシュ(エッジレイヤー、中間レイヤー)を有効にし、CDNのいずれかのレイヤーにヒットされ、リクエストに応答すると、CDNノードにヒットしていること見なされます。
トラフィックヒット率=（総ダウンストリームトラフィック-back-to-originトラフィック）/総ダウンストリームトラフィック。

©2013-2022 Tencent Cloud. All rights reserved.

トラフィックのヒット率が低い問題を解決するにはどうすればよいですか。

- キャッシュ更新が行われたかどうかを確認します。キャッシュ更新により、ノードで指定されたコンテンツがクリアされ、一時的にトラフィックヒット率が低下します。
- オリジンサーバーに新しいリソースが追加されているかどうかを確認します。オリジンサーバーに新しいリソースが多い場合、CDNノードでback-to-originが発生して、トラフィックヒット率が低下する可能性があります。
- オリジンサーバーに異常がないかどうかを確認します。オリジンサーバーに障害が発生すると、5XXまたは4XXエラーが多くなった場合、トラフィックのヒット率に影響を与えます。
- キャッシュの有効期限ポリシーが正しく設定されているかどうかを確認します。コンソールの「キャッシュ設定」ページで「キャッシュの有効期限設定」セクションを表示します。キャッシュの有効期限ポリシーの優先順位は上から下へ、低から高へであり、即ち、下部のキャッシュポリシーは上部のキャッシュポリシーよりも優先されます。
- Range back-to-originが有効になっているかどうかを確認します。コンソールの「back-to-origin設定」ページで「Range back-to-origin」セクションを表示します。Range back-to-originが無効になっている場合、 back-to-origin時にファイル全体を引き出しますため、 back-to-originトラフィックが増加し、ヒット率が低下します。
- フィルターパラメーターが有効になっているかどうかを確認します。コンソールの「アクセス設定」ページで「フィルターパラメーター」セクションを表示します。フィルターパラメーターが無効になっている場合、フルパスに基づいてキャッシュが実行されます。同じリソースが異なるパラメーターによって要求される場合、マッチングできないと複数回キャッシュされるため、トラフィックの命中率に影響を与えます。

ステータスコード統計にはすべてのステータスコードが含まれていますか。

はい。CDN統計分析の新しいバージョンが公開されると、オリジンサーバーで生成されたステータスコードさえあれば、対応する監視曲線が生成されます。トラブルシューティングのプロセスが容易になります。

省別、キャリア別の統計データはどのように計算しますか。

省別、キャリア別の統計データは、アクセスログのクライアントIPに基づいて計算されます。単純なログ計算を採用しているので、累積された課金対象データは、「すべての省」、「すべてのキャリア」が選択された場合の課金対象データとは異なります。詳細については、上記の質問2をご参照ください。

CDN back-to-originトラフィックはどのように生成されますか。

CDN back-to-originトラフィックは、次の3つの状況で生成されます。
1.要求されたリソースはCDNノードにキャッシュされず、オリジンサーバーからプルされます。
2. 手動で更新されたオリジンサーバーはノードと同期されます。
3. オリジンサーバーは自動更新されます。

CDNトラフィックに異常があるか、DDoSまたはCC攻撃を受けている場合はどうすればよいですか。

©2013-2022 Tencent Cloud. All rights reserved.

ビジネストラフィックがそれほど量に到達しないと思われる場合は、ログをダウンロードして、ビジネスのアクセス状況に基づいて関連するアクセス制限を設定できます。CDNではご利用のビジネスロジックを認識しないため、デフォルトではアクセス要求を制限することがありません。したがって、ビジネス状況に基づいて制限を設定する必要があります。詳細については、ログのダウンロードをご参照ください。

悪意のあるリクエストやWebサイトへのCC / DDoS攻撃を回避するために、次の設定を行うことを強くお勧めします。

1. リンク不正アクセス防止の設定：ビジネスリソースのアクセス元を制御し、ユーザーのHTTPリクエストヘッダーのrefererフィールドの値にアクセス制御ポリシーを設定することにより、アクセス元を制限し、悪意のあるユーザーからの盗用を防ぎます。詳細については、リンク不正アクセス防止の設定をご参照ください。
2. IPブラックリスト/ホワイトリストの設定：悪意のあるIPからの盗用や攻撃などの問題を解決するために、ビジネスニーズに応じて、ユーザーリクエストのソースIPにフィルタリングポリシーを設定できます。詳細については、IPブラックリスト/ホワイトリストの設定をご参照ください。
3. IPアクセス制限の設定：クライアントIPに対して、ノードごとの1秒あたりのアクセス回数を制限することにより、CC攻撃から防御できます。設定を有効にすると、QPS制限を超えるリクエストに対して514エラーが返されます。頻度制限を低く設定すると、通常の高頻度ユーザーの利用に影響する場合があるため、実際の業務状況やユースケースに応じて、適切なしきい値を設定してください。詳細については、IPアクセス制限の設定をご参照ください。
4. 帯域幅上限の設定：ドメイン名の帯域幅の上限を設定できます。特定の統計期間（5分）内にドメイン名で発生した帯域幅が指定されたしきい値を超えると、ユーザーの設定に従って、すべてのアクセス要求がオリジンサーバーに転送されるか、直接CDNサービスを無効にして、すべてのアクセス要求が404エラーが返されます。詳細については、帯域幅上限の設定をご参照ください。

APIを使用してデータをクエリーするのに遅延が発生しますか。遅延はどのくらいですか。

APIを使用してデータをクエリーするのには一定の遅延が発生します。アクセスデータや課金データなどのリアルタイムデータのクエリーには約5〜10分の遅延があり、ランキングデータなどの分析系のクエリーには約30分の遅延があります。データは、午前3時頃にバックエンドで調整されます。

©2013-2022 Tencent Cloud. All rights reserved.

更新予熱
キャッシュ更新

最終更新日：：2022-06-17 10:31:21

機能の説明

Content Delivery Network (CDN)は基本的なキャッシュ構成機能を提供しています。サービスタイプやディレクトリ、具体的なURL等各種のルールにより、キャッシュ期限切れ期間を設定することにより、定期的にノードのキャッシュリソースをクリアし、オリジンサーバーが最新のリソースを再度プルしキャッシュする目的を果たします。

また、CDNはキャッシュ更新機能を提供しています。URLまたはディレクトリを一括指定して更新操作を行うことができます：

- URLを更新する：CDNのすべてのノードにおける対応するリソースのキャッシュを削除します。
- ディレクトリの更新：「変更されたリソースの更新」モードを選択すると、ユーザーがマッチングしているディレクトリ配下のリソースにアクセスする時に、back-to-originを行ってリソースのLast-Modify情報を取得します。現在のキャッシュリソースと一致している場合、直接キャッシュされたリソースを戻しますが、一致しない場合は、back-to-originを行って新しいリソースをプルし、再度キャッシュします。「すべてのリソースの更新」モードを選択すると、ユーザーがマッチングしているディレクトリ配下のリソースにアクセスする時に、直接back-to- originを行って新しいリソースをプルしてユーザーに戻し、再度これをキャッシュします。

> 説明：
> 更新が完了した後、ノード上の対応するリソースには有効なキャッシュがありません。ユーザーがアクセス要求を再度開始すると、ノードは必要なリソースをオリジンサーバーから取得し、ノード上にキャッシュします。このため、大量の更新タスクをサブミットすると、非常に多くのキャッシュがクリアされて、back-to-originリクエストが激増し、オリジンサーバーに大きな負荷がかかります。

ユースケース

新しいリソースのリリース

古いリソースがオリジンサーバー上で同じ名前の新しいリソースによって上書きされた場合、ネットワーク全体のユーザーがノードのキャッシュの影響を受け、古いリソースにアクセスしてしまうことを避けるために、対応するリソースのURL / ディレクトリをサブミットして更新し、ネットワーク全体のキャッシュをクリアにします。こ

©2013-2022 Tencent Cloud. All rights reserved.

れにより、 ネットワーク全体のユーザーがリソースの最新バージョンに直接アクセスすることが可能となります。

不正なリソースの削除

オリジンサーバーに不正なリソース（ポルノ、薬物、ギャンブル関係など）が見つかった場合、オリジンサーバーでそれらを削除しても、ノードにキャッシュがあるため、アクセスが可能となります。ネットワーク環境を守るために、URLの更新によってキャッシュされたリソースを削除すれば、不正なリソースのタイムリーな削除を保証できます。

操作ガイド

CDN コンソールにログインし、左側のディレクトリの**更新やプリフェッチ**をクリックし、ページに入ってから必要に応じて**URL 更新**および**ディレクトリ更新**をサブミット：

- CDN と ECDN ドメイン名のURL / ディレクトリはどちらの形式もサポートしています。
- サブミットは、内容の入力とtxtファイルのアップロードいずれもサポートしています。

内容規範

まず、送信する内容が基準を満たしていることをご確認ください：

- URLに、１行につき１つのプロトコル標識 http:// または https:// が含まれている （例：http://www.test.com/test.html）。
- 終了あるいはロック状態、あるいは現在のアカウントを接続していないドメイン名をサブミットしないようにご注意ください。
- ファイルアップロード時のサブミット形式を選択したら、ファイル形式が txt であり、サイズが10M以内であることをご確認ください。
- `http://*.test.com/` 形式の URL はサポートされていません。
- 接続先のアクセラレーションドメイン名が汎ドメインであっても、対応するサブドメインをサブミットしてください。
- URL更新に際して、ワイルドカード付きのURLを含むサブミットはサポートされていません。
- URLに中国語が含まれている場合、URL Encodeをオンにして、エンコードしてください。

サブミット制限

- **URLの更新**：
  各アカウントの１日あたりのURL更新制限は10000個までとなります。中国以外でアクセラレーションを有効に

©2013-2022 Tencent Cloud. All rights reserved.

している場合、中国国内の制限と関係なく、中国国外での1日のURL更新制限が10000個となります。
- 手動で内容を入力するサブミット形式を選択した場合、一回あたりに1000個までサブミット可能です。
- ファイルのアップロードによるサブミット形式を選択した場合、１回あたりの制限はなく、サブミット回数が直接残り回数から差し引かれます。

> 説明：
> URL更新量が多く、URL更新の1日の割り当ての残りが少ない（1000未満など）場合、Tencent Cloud CDNは、コンソールによる1日の割り当ての自動ワンクリック追加をサポートします（50,000個に追加するなど）。
>
> - 割り当ての追加はすぐに有効になりますので、その時点でページを更新し、追加ボタンを頻繁にクリックしないでください。
> - 1度のみの追加をサポートします。例えば、今回、1日の割り当てを50,000まで追加した場合、残りの割り当てが少なくなっても、50,000を超える割り当ての追加はサポートされません。
> - 異なる地域での制限の開放は、互いに独立しています。

- **ディレクトリの更新**：
  各アカウントの１日あたりのディレクトリ更新制限は100個までとなります。中国以外でアクセラレーションを有効にしている場合、中国国内の割り当て量と関係なく、中国国外での1日のディレクトリ更新制限が100個となります。
  - 手動で内容を入力するサブミット形式を選択した場合、一回あたりに20個までサブミット可能です。
  - ファイルのアップロードによるサブミット形式を選択した場合、１回あたりの制限はなく、サブミット回数が直接残り回数から差し引かれます。

更新タスクをサブミットするとき、デフォルトではURLのドメイン名の所属するアクセラレーションドメイン名はすべて更新されます。ドメイン名のアクセラレーションエリアがグローバルのとき、中国国内と中国国外どちらの割り当て量も消費されます。

操作の詳細については、操作記録をご参照ください。

サブユーザー権限の設定

URL更新、ディレクトリ更新及びクエリ更新レコードが権限システムに接続され、リソース（ドメイン名）次元権限構成がサポートされています。詳しくは 権限構成 をご参照ください。

ユースケース

©2013-2022 Tencent Cloud. All rights reserved.

ディレクトリ更新-変更されたリソースを更新する

アクセラレーションドメイン名がpurge-test-1251991073.file.myqcloud.comであり、オリジンサーバーがTencent CloudのCloud Object Storage（COS）です。オリジンサーバーのリソースは下記の通りです：

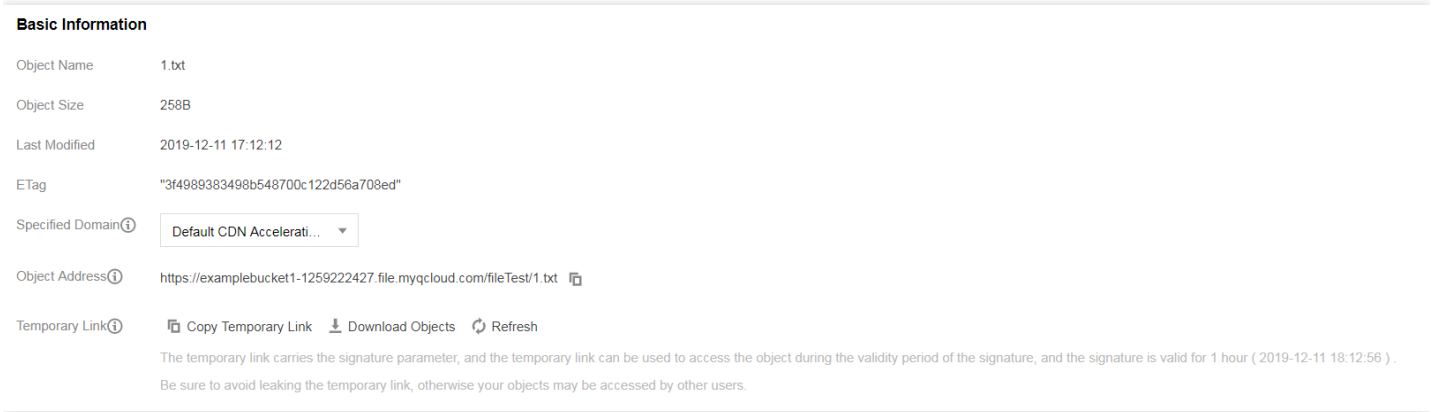
1．それぞれリソース1.txt と2.txtのアクセスリクエストを送信し、X-Cache-Lookup: Hit From Distank3およびServer: NWS_SPMid により、ヒットしたノードを判定することができます。ノードより直接リソースを返します：

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt -sv
*   Trying 14.215.85.233...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (14.215.85.233) port 80 (#0)
> GET /fileTest/1.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:20:46 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:30:46 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: 72e4a2dbd2e9e5304c17d2beb0bf39d5
< X-NWS-LOG-UUID: 5673286006122774168 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

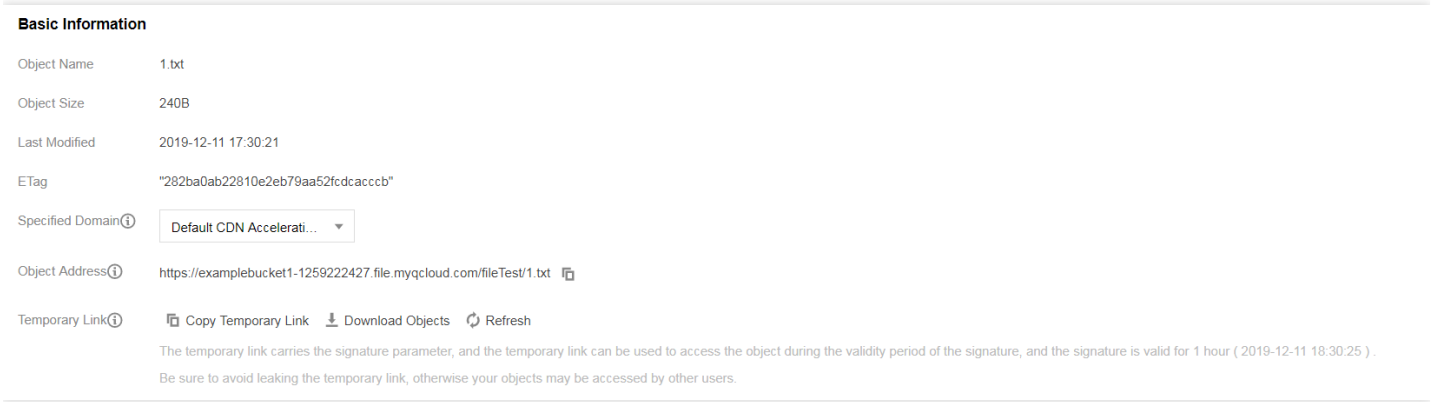
©2013-2022 Tencent Cloud. All rights reserved.

```
[redacted] curl http://purge-test-1251991073.file.myqcloud.com/fileTest/2.txt -sv
*   Trying 14.215.85.233...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (14.215.85.233) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:22:03 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:32:03 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: e7112793c4a1bdde407954fb943e43fb
< X-NWS-LOG-UUID: 14628995741359757299 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

2. オリジンサーバーで同名ファイルの1.txtを差し替え、ファイル修正時間が変更されます。2.txtはそのままにします：



©2013-2022 Tencent Cloud. All rights reserved.



3. この際に、再度リクエストを送信します。キャッシュはまだ期限切れになっていないため、リソース1.txtへのアクセスが古い内容のままです：

```
[redacted] curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt -sv
*   Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:34:19 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:44:19 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: 72e4a2dbd2e9e5304c17d2beb0bf39d5
< X-NWS-LOG-UUID: 5673286006122774168 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

4. ディレクトリ更新をサブミットし、【変更されたリソースを更新する】を選択し、更新が完了するまで待ちます：

5. 更新した後に、ファイル1.txt Last-Modifiedに変更があったため、リクエストはオリジンサーバーに直接転送されます。ファイル2.txtは変更がなかったため、ディレクトリ更新タスクがサブミットされた後でも、ヒットして戻されます：

©2013-2022 Tencent Cloud. All rights reserved.

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt -sv
*   Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/1.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: tencent-cos
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:33:22 GMT
< Last-Modified: Wed, 04 Sep 2019 23:24:17 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 23
< X-NWS-UUID-VERIFY: 6a4ea0410342aee319550d46b866cd37
< Accept-Ranges: bytes
< ETag: "325daac4e71e82db89ee26922d7435b7"
< x-cos-request-id: NWQ2ZmQ5NDJfMjZiMjU4NjRfMzY0Yl81MmU1YWI=
< X-Daa-Tunnel: hop_count=2
< X-NWS-LOG-UUID: 14013390993447302634 2107abdde3874148ff95a672f195831b
< X-Cache-Lookup: Hit From Upstream
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/2.txt -sv
*   Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:34:19 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:44:19 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: e7112793c4a1bdde407954fb943e43fb
< X-NWS-LOG-UUID: 1690084127387779050 2107abdde3874148ff95a672f195831b
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

©2013-2022 Tencent Cloud. All rights reserved.

キャッシュプリフェッチ

最終更新日：：2021-01-18 14:18:44

機能概要

ドメイン名でContent Delivery Network（CDN）を立ち上げた後、初期状態では、ネットワーク全体のCDNアクセラレーションノード上にはドメイン名リソースのキャッシュはありません。ノードのキャッシュはユーザーのリクエストでトリガーされ、ユーザーのリクエストがCDNアクセラレーションノードに届いた時に、ノード上にキャッシュリソースがない、またはキャッシュリソースが既に期限切れの場合、CDN中間層ノードまでback-to-originして取得し、中間層にもキャッシュがなくまたはリソースが期限切れの場合は、ユーザーのオリジンサーバーまでback-to-originしてプルします。

Tencent Cloud CDNではリソースのプリフェッチ機能を提供しています。ユーザーのリクエストでトリガーさせる必要がなく、CDNコンソールでリソースリストをサブミットし、指定リソースはアクセラレーションノードにロードされます。

- ノードにコンテンツをロードする時、そのキャッシュの同名のリソースが期限切れになっていない場合は、リソースのロードを行いません。同名のファイルを更新する時は、先にネットワーク全体の更新を行うことをお薦めします。
- ノードにリソースをロードする時はback-to-originで必要なコンテンツをプルします。このため大量のプリフェッチタスクをサブミットした後、オリジンサーバーの帯域幅が増加します。
- ネットワーク全体のアクセラレーションドメイン名はデフォルトの状態では2層アクセラレーション構造となっています。中国国内のリージョンのプリフェッチは、リソースはデフォルトで中国国内の中間層ノードにロードされ、中国国外のリージョンのプリフェッチは、リソースはデフォルトで中国国外のエッジノードにロードされます。

> 注意：
>
> 中国国外のリージョンのプリフェッチでは、リソースはデフォルトで中国国外のエッジノードにロードされ、発生するエッジ層のトラフィックは課金トラフィックに計上されます。

適用ケース

インストールパッケージのリリース

©2013-2022 Tencent Cloud. All rights reserved.

新バージョンのインストールパッケージまたはレベルアップパッケージのリリース前に、事前にリソースをCDNアクセラレーションノードでプリフェッチします。正式なサービスの開始後は、膨大なユーザーのダウンロードリクエストにはグローバルアクセラレーションノードが直接レスポンスし、ダウンロードスピードをアップすると同時に、オリジンサーバーの負荷を大幅に引き下げます。

イベントオペレーション

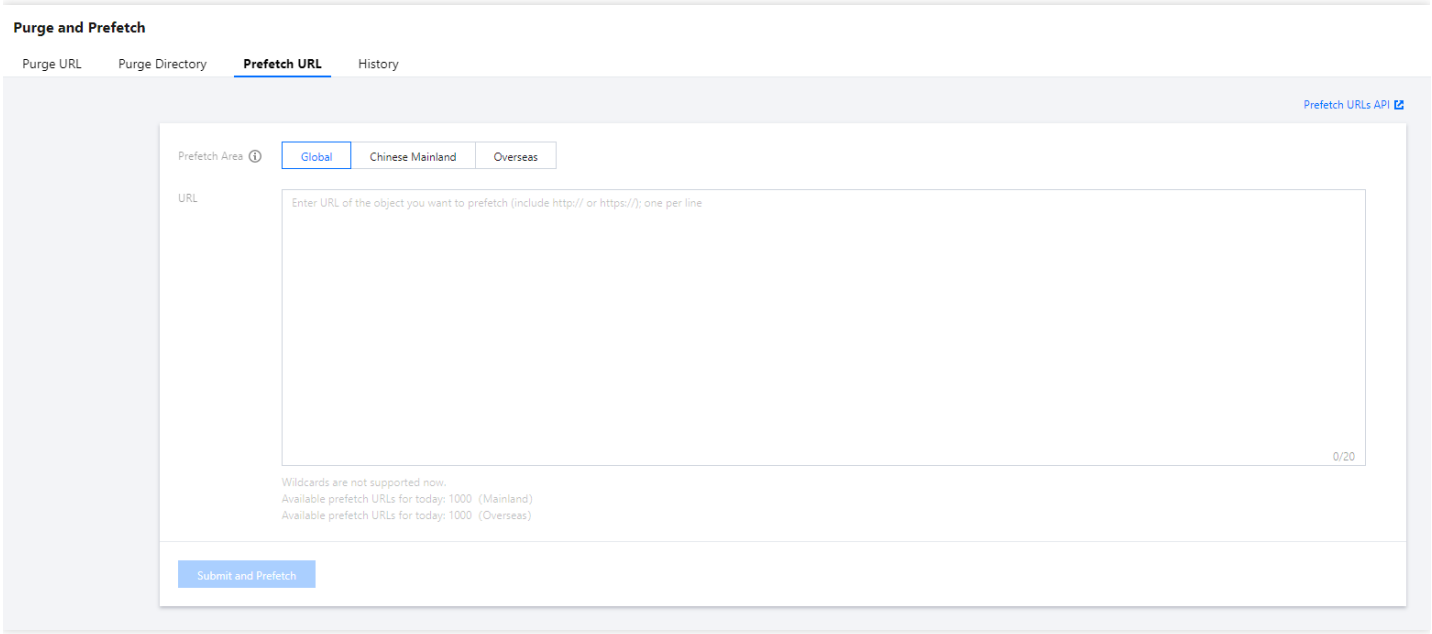
運用するイベントのリリース前に、事前にイベントページに関連する静的リソースをCDNアクセラレーションノードでプリフェッチします。イベントの開始後、ユーザーアクセスの中の全ての静的リソースはいずれもアクセラレーションノードからレスポンスされ、大量の帯域幅のストックがユーザーサービスの可用性を保証し、ユーザーエクスペリエンスを向上させます。

操作ガイド

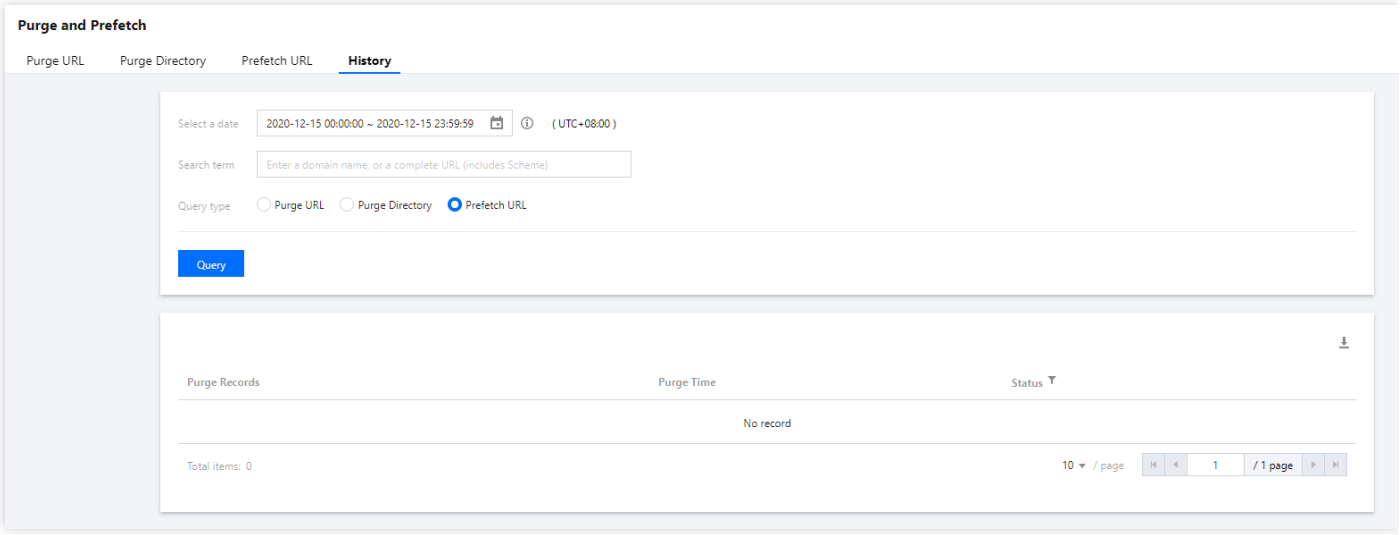
利用方法

1. CDN コンソールにログインし、左側のディレクトリの【パージとプリフェッチ】をクリックし、ページに入ってから必要に応じて【URL更新】をサブミットします。
2. プリフェッチタスクをサブミットする場合、プリフェッチリージョンの指定をサポートします。
   - アクセラレーションドメイン名を国内のアクセラレーションにすると、【中国国内】のアクセラレーションの指定のみサポートします。
   - アクセラレーションドメイン名を国外のアクセラレーションにすると、【中国国外】のアクセラレーションの指定のみサポートします。
   - アクセラレーションドメイン名をグローバルアクセラレーションにすると、【グローバル】、【中国国内】、【中国国外】のアクセラレーションの指定をサポートします。

©2013-2022 Tencent Cloud. All rights reserved.



3. 【操作履歴】をクリックし、時間周期、キーワードを指定してプリフェッチタスクのクエリーを行うことができます。ドメイン名の指定によるクエリー、または完全なURLの指定によるクエリーをサポートしています。



注意事項

プリフェッチ制限

- １つのアカウントの1日あたりの各アクセラレーションリージョンにおけるURLプリフェッチ上限枠は1000件であり、1回にサブミットできるURLプリフェッチ上限枠は20件です。グローバルタイプのプリフェッチの後は、国内、国外のプリフェッチ割り当てが同時に消費されます。
- プリフェッチタスクをサブミットする際に、 `http://` または `https://` プロトコル識別子を付け加える必要があります。

©2013-2022 Tencent Cloud. All rights reserved.

- `http://*.test.com` 形式のURLのプリフェッチはサポートしていません。
- パスに中国語が入っているURLはプリフェッチできません。

サブユーザー権限の設定

- プリフェッチURL、プリフェッチ履歴のクエリーは現在すでに最新の権限システムに接続され、リソース（ドメイン名）の権限設定をサポートしています。
- アサイン方法は 権限設定 をご参照ください。

©2013-2022 Tencent Cloud. All rights reserved.

レコードの操作

最終更新日：：2023-03-14 15:13:28

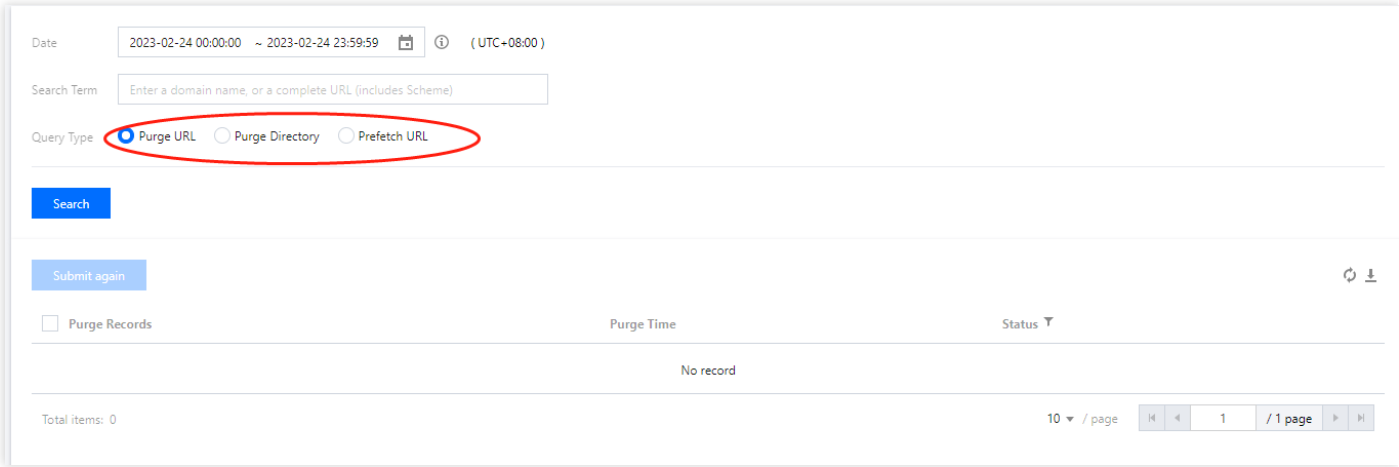
機能説明

更新やプリフェッチタスクを送信した後、**操作レコード**ページで、リソースを更新・プリフェッチした詳細なレコードとステータスを確認できます。

操作ガイド

利用方法

1. CDNコンソールにログインし、左側のディレクトリで**更新やプリフェッチ**をクリックし、**操作レコード**をクリックします。
2. 時間周期、ドメイン名/URL、タスクタイプを指定して検索します。指定したドメイン名での検索がサポートされます。また、指定した完全なURL Purge/ディレクトリ/ホットスタンバイURLでの検索もサポートされます。



利用説明

コンソールには、1回で最大10000個の操作レコードを完全なExcel形式でエクスポートできます。更新タスクが多い場合、タスクを分けてから一括検索してエクスポートしてください。

©2013-2022 Tencent Cloud. All rights reserved.

更新とプリフェッチのよくあるご質問

最終更新日：：2021-09-23 15:58:19

更新・プリフェッチ機能を使用する必要があるのはどのような場合ですか。

- 更新：お客様のオリジンサーバーにリソースの更新や、不正なリソースを削除する必要性、ドメイン名の設定変更があった場合は、ネットワーク全体のユーザーがノードのキャッシュの影響を受けて古いリソースにアクセスしてしまったり、古い設定の影響を受けたりすることを避けるために、タスクの更新を提出することで、ネットワーク全体のユーザーが最新のリソースにアクセスまたは正常にアクセスすることが可能となります。詳細な説明についてはキャッシュ更新をご参照ください。
- プリフェッチ：運用するイベントまたはインストールパッケージ/アップグレードパッケージのリリースなどがある場合は、プリフェッチタスクを提出し、事前に静的リソースをCDNアクセラレーションノードにプリフェッチすることで、オリジンサーバーの負荷を低減し、ユーザーサービスの可用性およびユーザーエクスペリエンスを向上させることができます。詳細な説明については、キャッシュプリフェッチをご参照ください。

更新とプリフェッチはどう違うのですか。

-更新後、このリソースはネットワーク全体のCDNノード上のキャッシュが削除されます。ユーザーリクエストがノードに到達すると、ノードがオリジンサーバーに戻って対応するリソースを引き取り、ユーザーに返してノードにキャッシュするため、ユーザーが最新のリソースを取得することが保証します。
-予熱後、このリソースはネットワーク全体のCDNノードに事前にキャッシュされます。ユーザーはリクエストがノードに到達すると、ノードでリソースを直接取得することができます。

更新・プリフェッチには何が必要ですか。有効になるまでにどのくらい時間がかかりますか。

- キャッシュ更新
  –URL更新：毎日のURL更新数が最大10000個を超えず、更新ごとに提出されるURL数が1000個を超えず、更新タスクが有効になるまで約5分かかります。ファイルに設定されているキャッシュ期限切れ時間が5分以下である場合は、更新ツールを使用せず、タイムアウトの更新を待つことをお勧めします。
  -ディレクトリ更新：毎日のディレクトリ更新数が最大100個を超えず、更新ごとに提出されるURLディレクトリ数が20個を超えず、更新タスクが有効になるまで約5分かかります。フォルダに設定されているキャッシュ期限切れ時間が5分以下である場合は、更新ツールを使用せず、タイムアウトの更新を待つことをお勧めします。
- リソースのプリフェッチ
  - URLのプリフェッチ：1日あたりのURLプリフェッチ数は最大1000個までです。プリフェッチごとに送信されるURL数は20個以下で、プリフェッチタスクが有効になるまでの時間はプリフェッチファイルのサイズに依存し、約5分から30分かかります。

CDN加速ノードのキャッシュ内容はリアルタイムで更新されますか。

©2013-2022 Tencent Cloud. All rights reserved.

現在、CDN アクセラレーションノード上のキャッシュコンテンツはリアルタイムで更新されません。CDN ノードはコンソールで設定されたキャッシュの有効期限の設定 に基づきキャッシュを更新します。特定ファイルのコンテンツをリアルタイムで更新したい場合は、キャッシュ更新で実行することができます。

更新・プリフェッチの記録を確認するにはどうすれば良いですか。

CDNコンソールで更新・プリフェッチの記録を確認することができます。詳細については、操作の記録をご参照ください。

プリフェッチ時にカスタムリクエストヘッダーのプリフェッチを追加できますか。

この機能は現在サポートされていません。

©2013-2022 Tencent Cloud. All rights reserved.

ログサービス
ログのダウンロード

最終更新日：：2023-06-27 14:46:07

お知らせ：
CDN公式サイト共通ログフィールド - HTTPプロトコル識別子（オフラインログの14番目フィールド）に「HTTP/3」の値を追加します。この変更は2021-09-13にカナリアリリースされますが、コンソールおよびインターフェースのデータ監視統計には影響しません。オフラインのログダウンロードパッケージを使用してデータ統計を行っている場合は、具体的な影響に注意しながら確認し、必要に応じて調整してください。ご理解、ご協力のほど、宜しくお願いいたします。

バックグラウンド：QUICアクセス機能がベータ版テスト中です。詳細については、QUICをご参照ください。

機能の説明

ドメイン名をContent Delivery Network（CDN）に接続した後、すべてのユーザー側リソースリクエストが応答を実施するためにCDNノードにスケジューリングされます。ノードがリソースをキャッシュしている場合、コンテンツは直接返されます。CDNノードがこれらリソースをキャッシュしていない場合、リクエストはドメイン名設定のオリジンサーバーにパススルーされ、必要なリソースがプルされます。

CDNノードは大部分のユーザーリクエストに応答することから、クライアントがユーザーアクセスを分析しやすいよう、CDNはネットワーク全体のアクセスログを1時間ごとの粒度でパッケージ化し、デフォルトで30日間保存すると同時に、ダウンロードサービスを提供します。

説明：

- 現時点では、ノードアクセスログのみを提供し、back-to-originログは提供していません。
- ECDNドメイン名のオフラインログは、現時点では、サブリージョンの照会をサポートしていません。ECDNオフラインログフィールドの説明については、ECDN製品ドキュメントをご参照ください。

ユースケース

©2013-2022 Tencent Cloud. All rights reserved.

アクセス行動分析

クライアントは、アクセスログをダウンロードすることで、必要に応じて人気のあるリソースの分析、アクティブユーザーの分析などを行うことができます。

サービス品質のモニタリング

アクセスログをダウンロードすることで、CDNノード全体のサービス状況を把握し、平均応答時間、平均ダウンロードスピードなどの指標を計算することができます。

操作ガイド

利用方法

CDNコンソールにログインし、左側のディレクトリの【ログサービス】をクリックすると、アクセスログの照会を実行するためのドメイン名、時間を選択できます。複数ログパッケージの選択、ローカルへの一括ダウンロードをサポートしています。

注意：

- デフォルトでは、アクセスログは時間単位でパッケージ化されます。特定の時間内にドメイン名のリクエストがない場合、その時間間隔のログパッケージは生成されません。
- 同じドメイン名の中国本土以外のアクセスログは中国本土のアクセスログとは別にパッケージ化されており、ログデータパッケージの命名形式は「時間-ドメイン名-アクセラレーションリージョン」です。
- アクセスログは各CDNアクセラレーションノードから収集されるため、レイテンシーに違いがあります。通常、ログパッケージは約30分のレイテンシーで照会とダウンロードができ、ログパッケージは継続的に追加され、通常は約24時間で安定します。
- ドメイン名の過去のアクセスログは30日以内のログパッケージのみを保存します。次のガイドに従い、SCF関数を利用して、ログパッケージをCOSに転送し、永続的にストレージすることができます。

フィールドの説明

ログ内の対応するフィールドの順序（左から右へ）とその定義を下表に示します。

順序	ログコンテンツ
1	リクエスト時間
2	クライアントIP
3	ドメイン名

©2013-2022 Tencent Cloud. All rights reserved.

順序	ログコンテンツ
4	リクエストパス
5	このアクセスのバイト数サイズ（ファイル自体のサイズとリクエストheaderのサイズを含みます）
6	中国本土のログは省番号を表し、中国本土以外のログはエリア番号を表します（マッピングテーブルについては以下をご参照ください）。
7	中国本土のログはキャリア番号を表し、中国本土以外のログは一律-1とします（マッピングテーブルについては以下をご参照ください）。
8	HTTPステータスコード
9	Referer情報
10	応答時間（ミリ秒）とは、ノードがリクエストを受信した後、すべての戻りパケットに応答し、それが再びクライアントに到達するまでにかかる時間を指します。
11	User-Agent情報
12	Rangeパラメータ
13	HTTP Method
14	HTTPプロトコル識別
15	HIT/MISSをキャッシュし、CDNエッジノードヒット、親ノードヒットのいずれにもHITとマークします
16	クライアントがCDNノードとの接続を確立するために使用するポートで、ない場合は、-とします

リージョン / キャリアマッピングテーブル

中国本土の省のマッピング

リージョンID	地域	リージョンID	地域	リージョンID	地域
22	北京	86	内モンゴル	146	山西
1069	河北	1177	天津	119	寧夏
152	陝西	1208	甘粛	1467	青海
1468	新疆	145	黒龍江	1445	吉林

©2013-2022 Tencent Cloud. All rights reserved.

リージョンID	地域	リージョンID	地域	リージョンID	地域
1464	遼寧	2	福建	120	江蘇
121	安徽	122	山東	1050	上海
1442	浙江	182	河南	1135	湖北
1465	江西	1466	湖南	118	貴州
153	雲南	1051	重慶	1068	四川
1155	チベット	4	広東	173	広西
1441	海南	0	その他	1	香港マカオ台湾
-1	中国本土以外				

中国本土のキャリアのマッピング

キャリアID	キャリア	キャリアID	キャリア	キャリアID	キャリア
2	チャイナテレコム	26	チャイナユニコム	38	CERNET
43	長城ブロードバンド	1046	チャイナモバイル	3947	中国鉄通
-1	中国本土以外のキャリア	0	その他キャリア		

中国本土以外の地区のマッピング

リージョンID	地区	リージョンID	地域	リージョンID	地域
2000000001	アジア太平洋1区（サービス地区）	765	スロバキア	1613	アンゴラ
2000000002	アジア太平洋2区（サービス地区）	766	セルビア	1617	コートジボワール
2000000003	アジア太平洋3区（サービス地区）	770	フィンランド	1620	スーダン
2000000004	中東（サービス地区）	773	ベルギー	1681	モーリシャス

©2013-2022 Tencent Cloud. All rights reserved.

リージョンID	地区	リージョンID	地域	リージョンID	地域
2000000005	北米（サービス地区）	809	ブルガリア	1693	モロッコ
2000000006	ヨーロッパ（サービス地区）	811	スロベニア	1695	アルジェリア
2000000007	南米（サービス地区）	812	モルドバ	1698	ギニア
2000000008	アフリカ（サービス地区）	813	マケドニア	1730	セネガル
-20	アジア（クライアント地区）	824	エストニア	1864	チュニジア
-21	南米（クライアント地区）	835	クロアチア	1909	ウルグアイ
-22	北米（クライアント地区）	837	ポーランド	1916	グリーンランド
-23	ヨーロッパ（クライアント地区）	852	ラトビア	2026	中国台湾
-24	アフリカ（クライアント地区）	857	ヨルダン	2083	ミャンマー
-25	オセアニア（クライアント地区）	884	キルギス	2087	ブルネイ
35	ネパール	896	アイルランド	2094	スリランカ
57	タイ	901	リビア	2150	パナマ
73	インド	904	アルメニア	2175	コロンビア
144	ベトナム	921	イエメン	2273	モナコ
192	フランス	926	ベラルーシ	2343	アンドラ
207	イギリス	971	ルクセンブルク	2421	トルクメニスタン
208	スウェーデン	1036	ニュージーランド	2435	ラオス

©2013-2022 Tencent Cloud. All rights reserved.

リージョンID	地区	リージョンID	地域	リージョンID	地域
209	ドイツ	1044	日本	2488	東ティモール
213	イタリア	1066	パキスタン	2490	トンガ
214	スペイン	1070	マルタ	2588	フィリピン
386	アラブ首長国連邦	1091	バハマ	2609	ベネズエラ
391	イスラエル	1129	アルゼンチン	2612	ボリビア
397	ウクライナ	1134	バングラデシュ	2613	ブラジル
-	-	1158	カンボジア	2623	コスタリカ
417	カザフスタン	1159	中国マカオ	2626	メキシコ
428	ポルトガル	1176	シンガポール	2639	ホンジュラス
443	ギリシャ	1179	モルディブ	2645	エルサルバドル
471	サウジアラビア	1180	アフガニスタン	2647	パラグアイ
529	デンマーク	1185	フィジー	2661	ペルー
565	イラン	1186	モンゴル	2728	ニカラグア
578	ノルウェー	1195	インドネシア	2734	エクアドル
669	アメリカ	1200	中国香港	2768	グアテマラ
692	シリア	1233	カタール	2999	アルバ
704	キプロス	1255	アイスランド	3058	エチオピア
706	チェコ	1289	アルバニア	3144	ボスニア・ヘルツェゴビナ
707	スイス	1353	ウズベキスタン	3216	ドミニカ
708	イラク	1407	サンマリノ	3379	韓国

©2013-2022 Tencent Cloud. All rights reserved.

リージョンID	地区	リージョンID	地域	リージョンID	地域
714	オランダ	1416	クウェート	3701	マレーシア
717	ルーマニア	1417	モンテネグロ	3839	カナダ
721	レバノン	1493	タジキスタン	4450	オーストラリア
725	ハンガリー	1501	バーレーン	4460	中国大陸
726	ジョージア	1543	チリ	-15	アジアその他
731	アゼルバイジャン	1559	南アフリカ	-14	南米その他
734	オーストリア	1567	エジプト	-13	北米その他
736	パレスチナ	1590	ケニア	-12	ヨーロッパその他
737	トルコ	1592	ナイジェリア	-11	アフリカその他
759	リトアニア	1598	タンザニア	-10	オセアニアその他
763	オマーン	1611	マダガスカル	-2	中国本土以外その他

中国本土以外のキャリアのマッピング

キャリアID	キャリア
-1	中国本土以外のキャリア

注意事項

アクセスログの第5フィールドに記録されたバイト数に基づいて集計し、計算したトラフィック/帯域幅データはCDN課金トラフィック/帯域幅データと一致しません。原因は次のとおりです。

- アクセスログに記録できるのはアプリケーション層のデータのみです。実際のネットワーク伝送では、発生するネットワークトラフィックは純粋なアプリケーション層トラフィックより5〜15%多くなります。これは2つの部分で構成されています。
  - TCP/IPヘッダーの消費：TCP/IPプロトコルのHTTPリクエストに基づき、各パケットのサイズは最大1500バイトであり、TCPおよびIPプロトコルの40バイトのヘッダーが含まれます。ヘッダー部分はトラフィックを

©2013-2022 Tencent Cloud. All rights reserved.

発生させますが、アプリケーション層によって合計されることはありません。この部分の費用は3%前後になります。

- TCP再送：正常なネットワーク伝送プロセスにおいては、送信されるネットワークパケットの3〜10%前後がインターネットによって消失します。消失後は、サーバーが消失部分を再送します。この部分のトラフィックアプリケーション層も集計できません。占有率は約3〜7%になります。

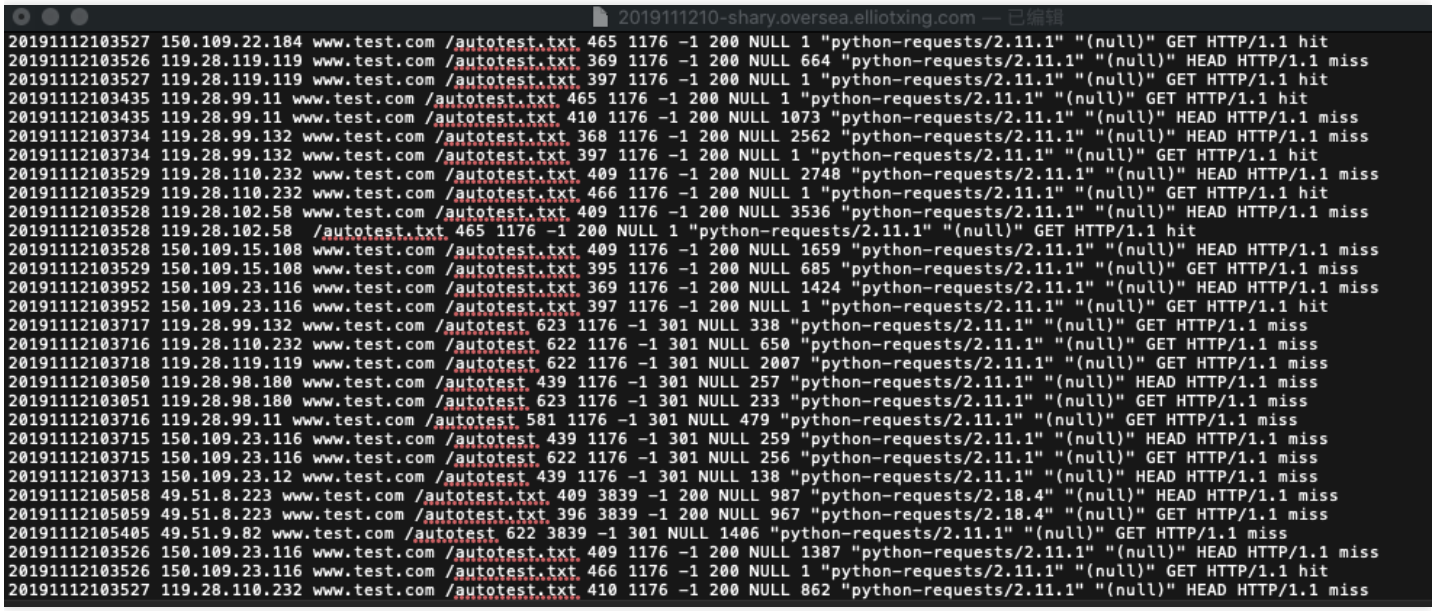
- 業界標準では、課金用トラフィックは一般にアプリケーション層のトラフィックに上述の料金を加算したものになります。Tencent Cloud CDNは10%を取得するため、監視トラフィックはログから計算されるトラフィックの約110%となります。

ユースケース

中国本土のアクセスログの例

```
20170719174306 10.10.10.10 www.test.com /test.png 77487 3 2 0 NULL 1408 "Mozilla/
20170719174407 10.10.10.10 www.test.com /test2.png 72488 5 2 200 NULL 13569 "Mozi
20170719174520 10.10.10.10 www.test.com /test3.png 74864 4 2 200 NULL 9474 "Mozil
20170719174544 10.10.10.10 www.test.com /test4.png 81453 2 2 200 NULL 9218 "Mozil
20170719174532 10.10.10.10 www.test.com /test5.png 54678 7 2 200 NULL 9041 "Mozil
```

中国本土以外のアクセスログの例



©2013-2022 Tencent Cloud. All rights reserved.

リアルタイムログ

最終更新日：：2021-11-08 12:36:33

お知らせ：
CDN公式サイト一般ログフィールド - HTTPプロトコル識別子（リアルタイムログprotoフィールド）に「HTTP/3」の値を追加します。この変更は2021-09-13にカナリアリリースされますが、コンソールおよびインターフェースのデータ監視統計には影響しません。オフラインのログダウンロードパッケージを使用してデータ統計を行っている場合は、具体的な影響に注意を払って確認し、必要に応じて調整してください。ご理解、ご協力のほど、宜しくお願いいたします。

バックグラウンド：QUICアクセス機能がベータ版テスト中です。詳細については、QUICをご参照ください。

機能の説明

Content Delivery Network（CDN）は、アクセスログをリアルタイムで収集してプッシュすることにより、ログデータをすばやく検索して分析できます。ユーザーはCDNコンソールからワンストップですばやくアクセスして、ログの収集、ログの保存からログの検索など、安定した高信頼性の包括的なログサービスを利用することができます。

説明：

- リアルタイムログサービスはすでにすべてリリースされています。コンソールからルートアカウントを用いてセルフアクティベーションすることで使用できます。使用前に、まずCloud Log Service（CLS）をアクティブ化する権限を付与する必要があります。
- リアルタイムログサービスは、現時点では、中国本土以外でのログの配信をサポートしていません。
- リアルタイムログサービスは、ルートアカウントのアクティブ化のみをサポートしています。
- CDNとECDNドメイン名を同じログトピックの下に混在させることはできません。

ユースケース

この機能を使用すると、ユーザーアクセスをリアルタイムで表示および分析できます。

©2013-2022 Tencent Cloud. All rights reserved.

基本概念

ログセット

ログセット（Logset）は、CLSのプロジェクト管理単位であり、異なるプロジェクトのログを区別するために使用されます。1つのログセットは、1つのプロジェクトまたはアプリケーションに対応します。CDNログセットには、以下の基本的な属性情報があります。

- ログセット名:cdn_logset
- リージョン：ログセットが属する リージョン
- 保存時間:現在のログセット内のデータの保存期間
- 作成日時:ログセットの作成日時

ログトピック

ログトピック（Topic）は、CLSの基本的な管理単位です。1つのログセットには、複数のログトピックを含めることができます。1つのログトピックは、1種類のアプリケーションまたはサービスに対応します。異なる端末上の同種類のログを同じログトピックに収集することをお勧めします。たとえば、1つのビジネスプロジェクトには、操作ログ、アプリケーションログ、アクセスログの3種類のログがある場合、ログの種類ごとにログトピックを作成できます。

CLSシステムは、ログトピックを単位として、ユーザーの異なるログデータを個別に管理します。各ログトピックには、異なるデータソース、インデックスルール、および配信ルールを設定できるため、ログトピックはCLSがログデータをを構成および管理するための基本単位です。ログトピックを作成した後、ログを効果的に収集し、検索、分析、配信などの機能を利用するには、関連ルールを設定する必要があります。

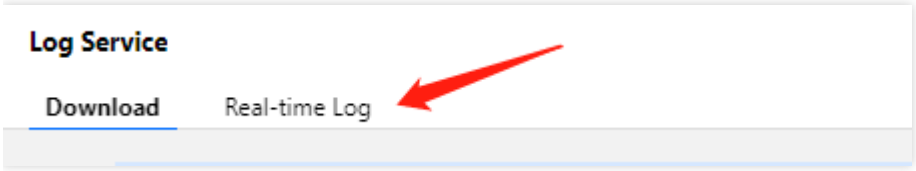
ログトピックの機能は次のとおりです。

- ログを収集してトピックを記録します。
- ログトピックに基づいてログを保存および管理します。
- ログトピックに基づいてログを検索および分析します。
- ログトピックに基づいてログを他のプラットフォームに配信します。
- ログトピックからログをダウンロードして使用します。

操作ガイド

CDNコンソールにログインし、左側のナビゲーションメニューバーで【ログサービス】をクリックして、【リアルタイムログ】を選択すると、リアルタイムログのページに入り、リアルタイムログ配信の作成を開始します。

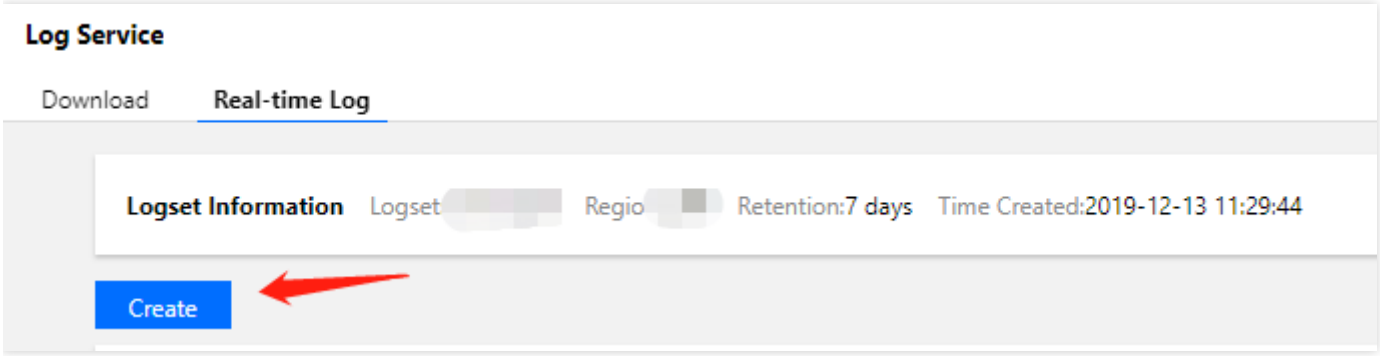
©2013-2022 Tencent Cloud. All rights reserved.



ログトピックの新規作成

【新規】をクリックして、ログ トピックを作成します。

> 注意：
> 1つのログセットにつき、最大500のログトピックを作成できます。

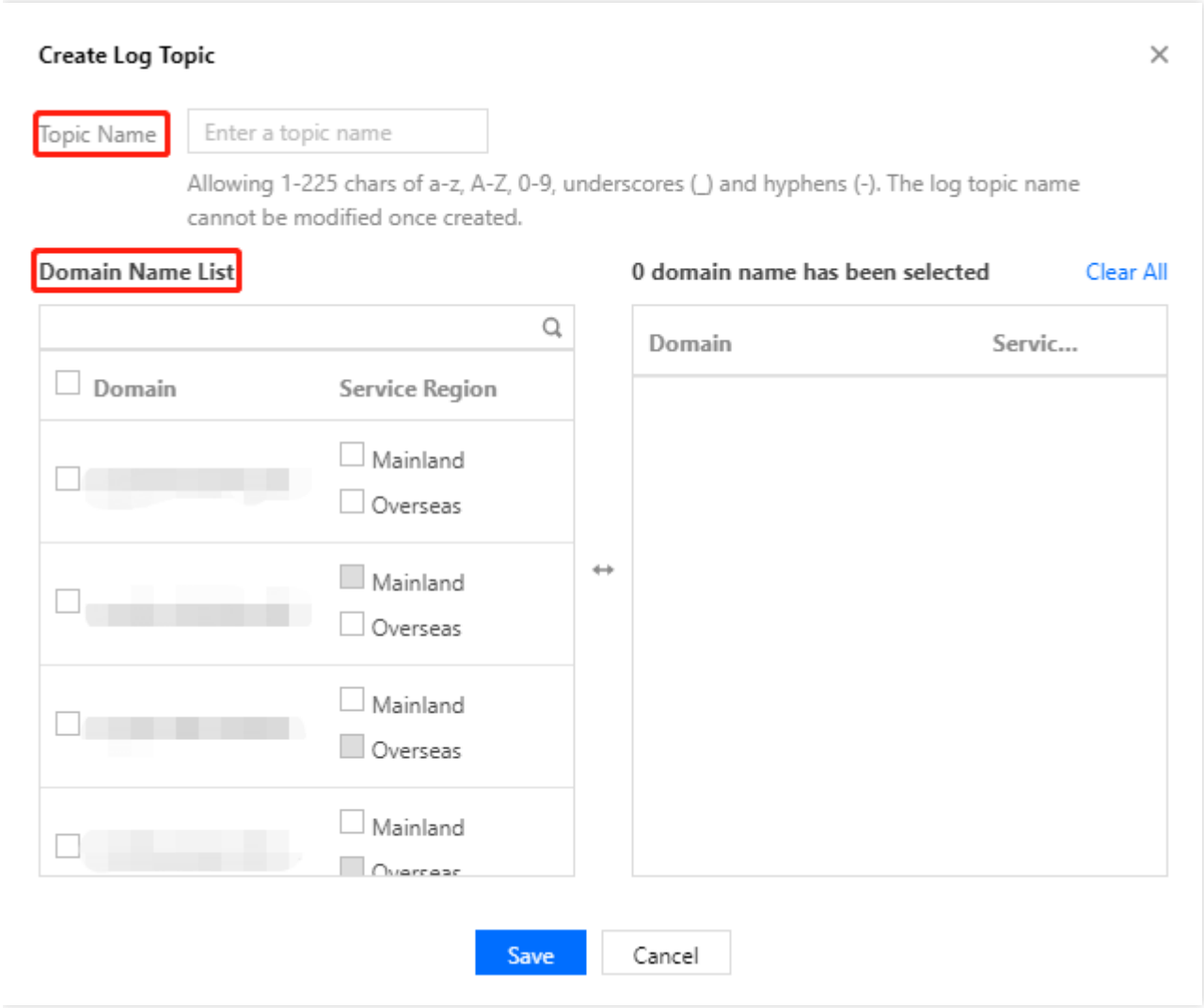


ログトピックの設定

新しいログトピックの名前を記入し、ドメイン名をログトピックにバインドします。

> 注意：
>
> - 新規作成するログトピックの名前は、既存のログトピックの名前と同じにすることはできません。
> - 1つのドメイン名あたり、1 つのログトピックにのみバインドできます。
> - 設定情報が保存されてから、設定が有効になるまでに約15分かかります。

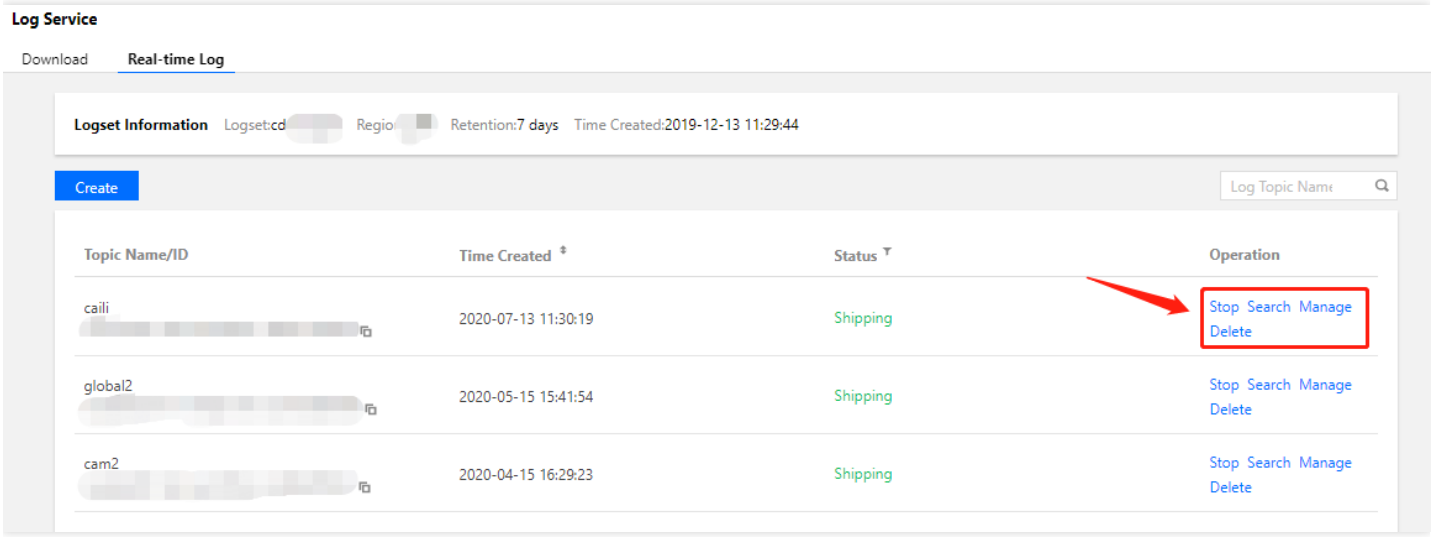
©2013-2022 Tencent Cloud. All rights reserved.



ログトピックの管理

ログトピックを設定した後は、ログトピックを管理できるようになります。ログトピックへのログ配信の停止/開始、当該ログトピックでのログの検索、ログトピックの管理、およびログトピックの削除を行うことができます。

©2013-2022 Tencent Cloud. All rights reserved.



ログ配信の停止/開始

ログトピックへのログ配信を手動で停止/開始することができます。

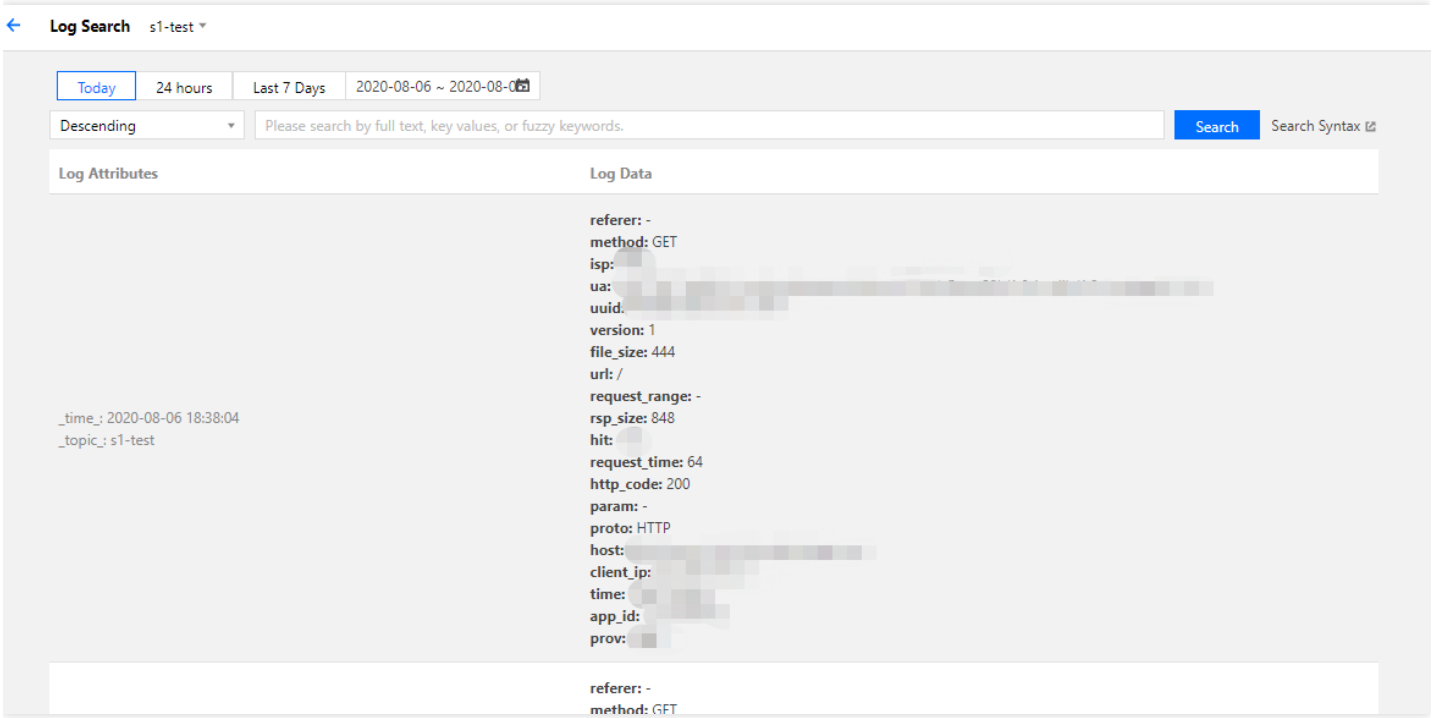
> 注意：
>
> - 停止すると、当該ログトピックにバインドされているドメイン名のすべてのログは当該トピックに配信されなくなり、すでに配信されているログは保持されます。有効になるまでに約5～15分かかります。
> - 開始すると、当該ログトピックにバインドされているドメイン名のすべてのログは引き続き当該トピックに配信され、有効になるまでに約5～15分かかります。

検索

ログトピックでログを検索します。検索するログトピックを選択し、【検索】をクリックすると、ログ検索画面に入ります。

- 期間の選択：本日、24時間（過去7日間から1日を選択）、および過去7日間に記録されたログデータを検索できます。
- ソート: ログ時間に基づいて、ログを昇順または降順で並べ替えることができます。
- 検索：全文検索、キー値検索、あいまい検索をサポートしています。詳細については、検索構文をご参照ください。さらに多くの検索および分析機能については、Cloud Log Service（CLS）に移動するとご利用いただけます。

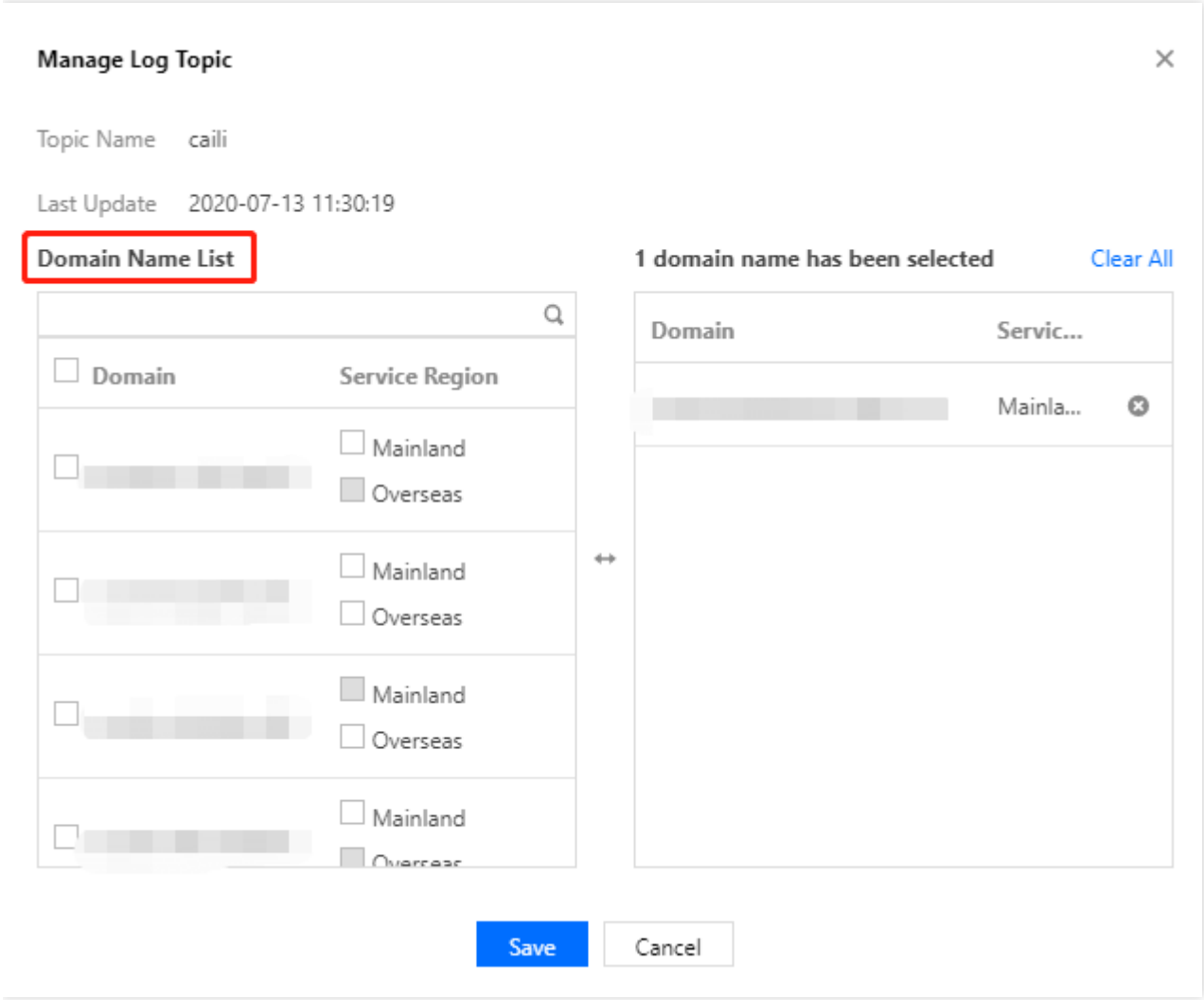
©2013-2022 Tencent Cloud. All rights reserved.



管理

作成したログトピックを管理し、それにバインドされているドメイン名のリストを更新できます。
新しい設定が有効になるまでに約5〜15分かかります。

©2013-2022 Tencent Cloud. All rights reserved.



削除

ログトピックを手動で削除することができます。
ログトピックが削除されると、当該ログトピックにバインドされているドメイン名のすべてのログは当該トピックに配信されなくなり、すでに配信されているすべてのログは消去されます。有効になるまでに約5〜15分かかります。

ログデータの説明

ログフィールド	生ログのタイプ	ログサービスタイプ	説明
app_id	Integer	long	Tencent Cloudアカウント APPID
client_ip	String	text	クライアント IP
file_size	Integer	long	ファイルサイズ

©2013-2022 Tencent Cloud. All rights reserved.

ログフィールド	生ログのタイプ	ログサービスタイプ	説明
hit	String	text	キャッシュヒット/ミス。CDNエッジサーバーと親ノードの両方のヒットがヒットとしてマークされます。
host	String	text	ドメイン名
http_code	Integer	long	HTTPステータスコード
isp	String	text	キャリア
method	String	text	HTTP Method
param	String	text	URLが保持するパラメータ
proto	String	text	HTTP プロトコル識別子
prov	String	text	キャリア所在省
referer	String	text	Referer 情報、つまりHTTPソースアドレス
request_range	String	text	Rangeパラメータ、つまりリクエスト範囲
request_time	Integer	long	応答時間（ms）。ノードがリクエストを受信してからすべてのパケットに応答してクライアントに到達するまでの時間を示します。
request_port	String	long	クライアントとCDNノードが接続を確立するポート。なしの場合は以下となります。 -
rsp_size	Integer	long	返されるバイト数
time	Integer	long	リクエスト時間、UNIX タイムスタンプ、単位：秒。
ua	String	text	User-Agent情報

©2013-2022 Tencent Cloud. All rights reserved.

ログフィールド	生ログのタイプ	ログサービスタイプ	説明
url	String	text	リクエストパス
uuid	String	text	一意のリクエスト ID
version	Integer	long	CDN リアルタイムログのバージョン

©2013-2022 Tencent Cloud. All rights reserved.

サービスクエリー
ネットワーク全体状態のモニタリング

最終更新日：：2020-07-03 15:54:19

機能概要

Content Delivery Network（CDN）は、中国本土の各省のキャリアと中国本土以外の各地域の遅延と可用性状態をリアルタイムで監視できます。 CDNは、世界中に展開されたノードに基づいて、監視ファイルへリクエストを送信して、これらのリクエストに対する応答データを収集します。お客様はネットワーク全体のリアルタイム状態の概要と詳細をCDNコンソールで確認できます。

> ネットワーク全体の状態監視は、ビジネスの実際のサービス状態ではなく、CDNプラットフォームのサービス状態を監視します。

操作ガイド

CDNコンソールにログインし、左側のナビゲーションメニューバーで【ネットワーク全体の状態監視】をクリックすると、ネットワーク全体の監視ページが表示されます。

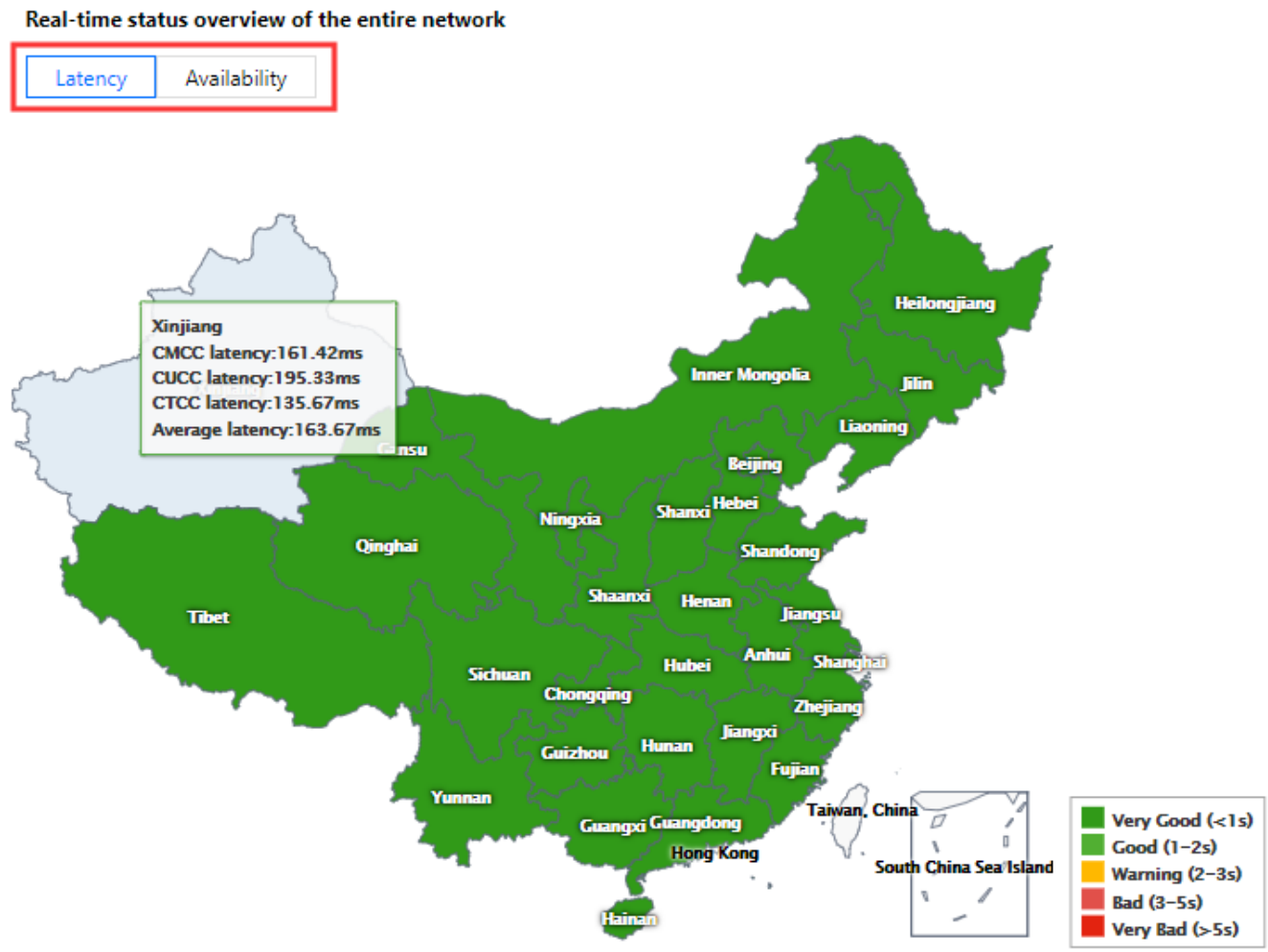
ネットワーク全体リアルタイム状態の概要

ネットワーク全体のリアルタイム状態の概要ページで、中国本土の各省のキャリアと中国本土以外の各地域の遅延と可用性状態の概要を表示できます。 地図上のエリアにカーソルを合わせると、対応するエリアのデータが表示されます。

> 図表のリアルタイムデータは毎分更新されます。

©2013-2022 Tencent Cloud. All rights reserved.

1.中国本土



画像には、チャイナモバイル、チャイナユニコン、チャイナテレコムを含む3つの主要なキャリアのデータが表示されます。平均遅延または可用性を計算する場合、中小規模のキャリアのデータが含まれます。

2.中国本土以外

ネットワーク全体の状態の詳細

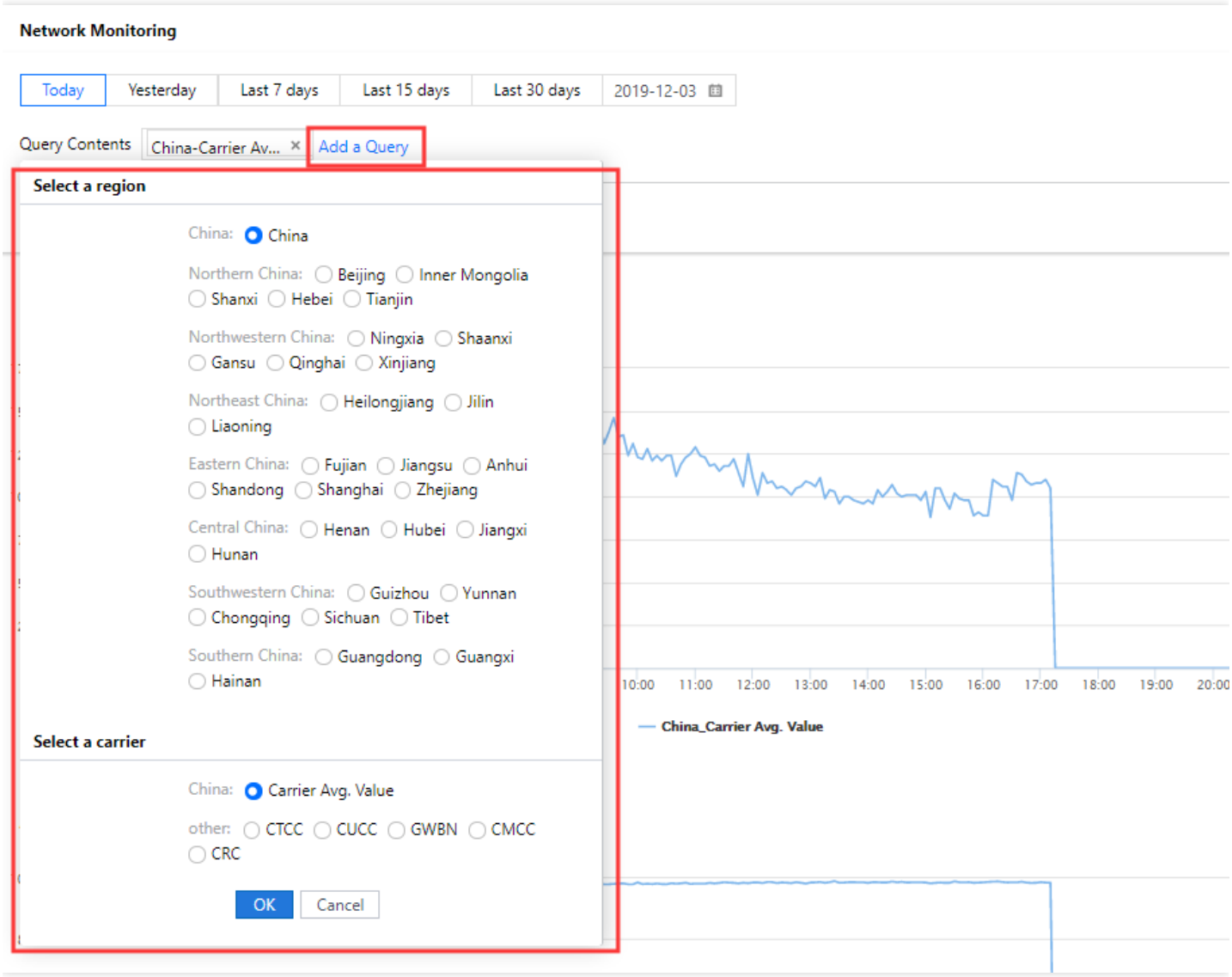
ネットワーク全体の状態の詳細で、中国本土が指定された期間、地域とキャリア、および中国本土以外が指定された期間と地域の遅延履歴および可用性曲線を表示できます。

期間：過去30日間のアクセス統計をクエリできます。クエリーできる期間は最大30日です。

©2013-2022 Tencent Cloud. All rights reserved.

1.中国本土

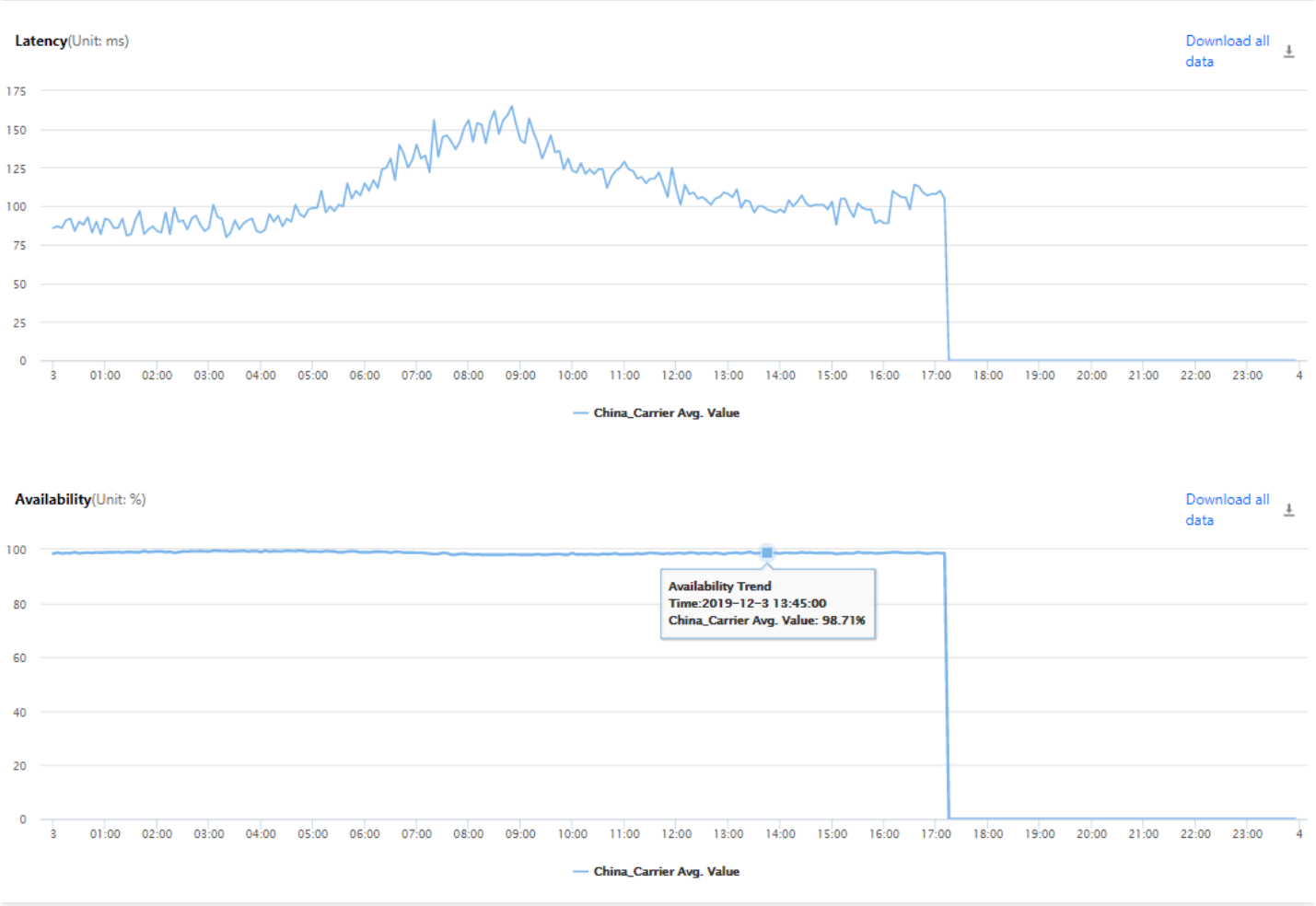
一度に複数のクエリ条件を追加して、複数の曲線を表示できます。



2.中国本土以外

©2013-2022 Tencent Cloud. All rights reserved.

一度に複数の地域を選択して、複数の曲線を表示できます。



©2013-2022 Tencent Cloud. All rights reserved.

トラフィックパッケージ管理

最終更新日：：2020-02-22 21:37:34

課金方式が**トラフィック料金**の場合、より優遇な方法としては、トラフィックパケットを購入して費用を差し引くことをおすすめします。ユーザーは、トラフィックパッケージの残高を把握するために、CDNコンソールで使用状況を確認できます。CDNサービスの通常の使用に影響を与えないように直ちに補充してください。

1. CDNコンソールにログインします。
2. 左側のメニューで【高度なツール】>【トラフィックパッケージ管理】を選択すると、管理ページが表示されます。
3. 既存のトラフィックパッケージおよび期限切れのトラフィックパッケージの購入と使用状況を確認できます。

©2013-2022 Tencent Cloud. All rights reserved.

IP所有権のクエリ

最終更新日：：2021-04-15 18:03:53

機能の説明

Content Delivery Network（CDN）はIP所有権クエリツールを提供します。このツールを介して指定されたIPがTencent Cloud CDNグローバルアクセラレーションノードであるかどうか、およびIPのアクセラレーションサービスエリア、省、キャリア情報をクエリできます。

該当するシナリオ

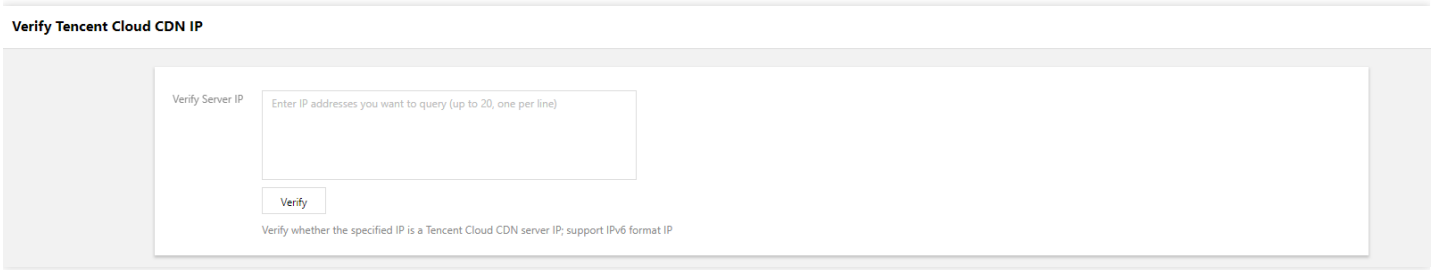
このツールは、様々なトラブルシューティングに使用できます。不正アクセスされた疑いがある場合は、次の方法でアクセスされたIPを照会できます。

- このIPがTencent Cloud CDNノードに属していない場合は、ドメイン名の名前解決時に問題が起きている可能性があります。DNSサービスプロバイダーでCNAME構成が正しいかどうかを確認してください。
- このIPがTencent Cloud CDNノードに属している場合は、ノードのサービスのステータスをチェックすることにより、ノードのアクティブ化/非アクティブ化によるリクエスト中断につながったかどうかを確認できます。

操作ガイド

クエリ方式

CDN コンソールにログインし、左側のディレクトリの【診断ツール】>【IP 帰属クエリ】を選択し、機能ページに入ります。



ご利用時のお約束

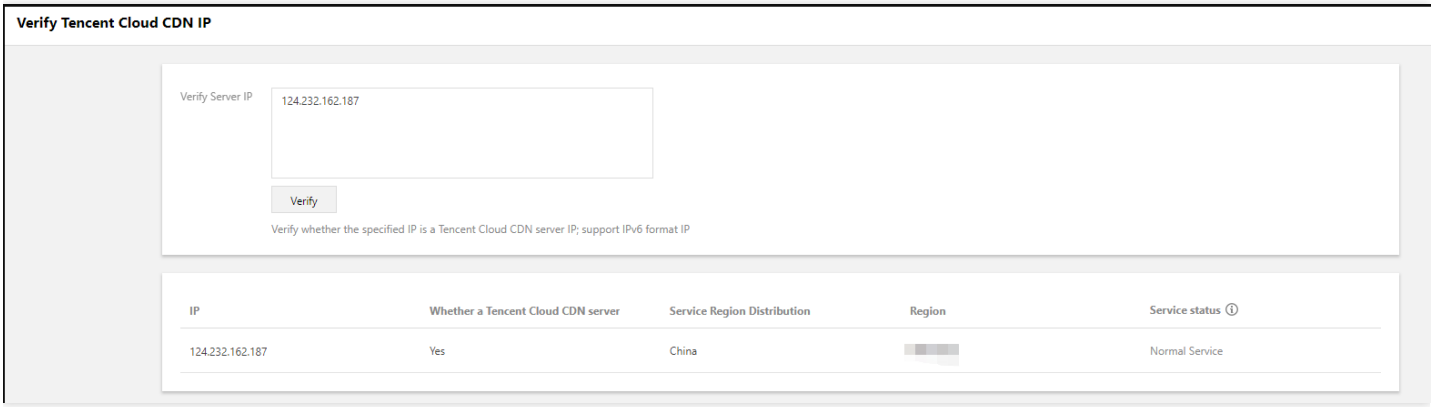
- テキストボックスに検証する複数のIPアドレスを1行に1つずつ入力します。
- 一度に最大20個のIPアドレスを検証できます。

©2013-2022 Tencent Cloud. All rights reserved.

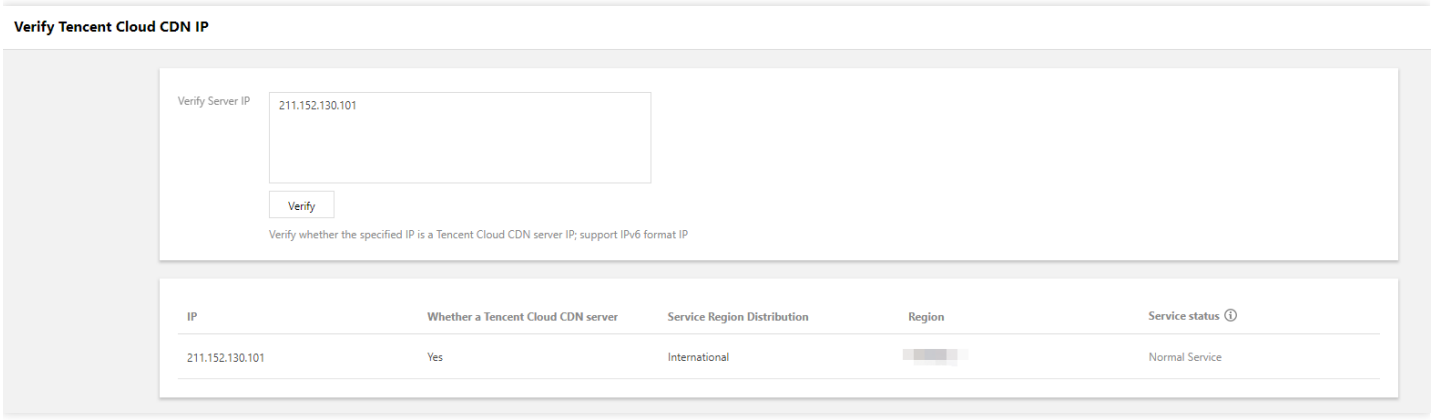
- IPv4とIPv6アドレスの検証をサポートします。
- グローバルアクセラレーションノードの検証をサポートしています。中国本土のノードの場合、対応する省のキャリアのデータが返されます。中国本土以外のノードの場合、対応する国/地域のデータが返されます。
- **過去3時間**のノードのサービスステータスを確認できます。オンライン/オフラインのステータス変更があった場合は、対応する操作時間を照会できます。

ユースケース

IP所有権が中国本土に帰属する場合



IP所有権が中国本土以外に帰属する場合



©2013-2022 Tencent Cloud. All rights reserved.

back-to-originノードクエリー

最終更新日：：2023-03-14 15:13:28

機能説明

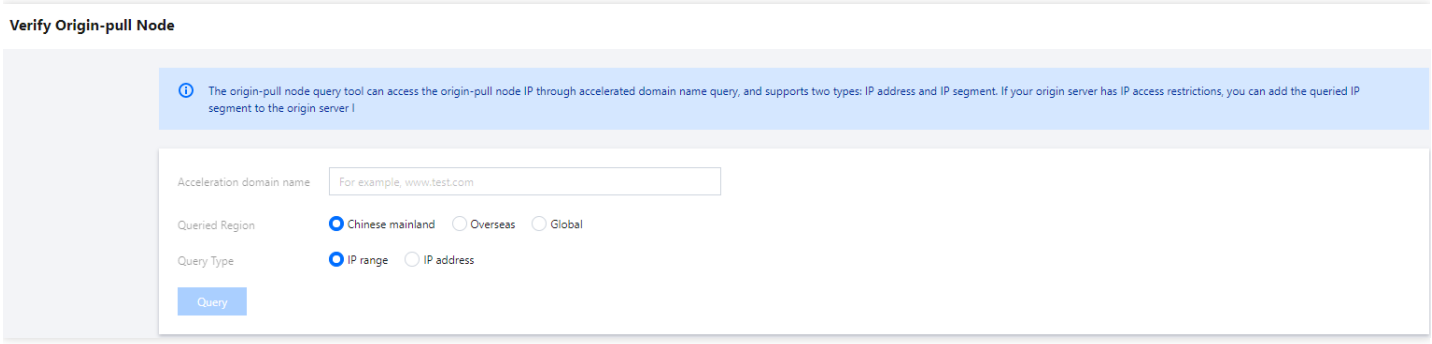
Tencent Cloud CDNでは、アクセラレーションドメイン名のBack-to-OriginノードIP（IPレンジタイプとIPアドレスタイプ）を検索できます。

ユースケース

業務でアクセス制御が必要。

操作ガイド

CDNコンソールにログインし、左側のメニューで**サービス検索** > **Back-to-Originノード検索**を選択します。



使用説明：

- CDNに導入し有効になっている正しいアクセラレーションノード名を入力してください。
- リージョンを検索する時、アクセラレーションドメイン名に対応するアクセラレーションリージョンを選択してください。
- 必要に応じて、検索タイプを選択してください。
- 中国本土以外では、通信事業者の情報がサポートされていません。
- 検索結果をローカルにダウンロードできます。

©2013-2022 Tencent Cloud. All rights reserved.

自己診断ツール

最終更新日：：2021-10-26 15:59:56

CDNは自己診断ツールを提供します。いずれかのURLへの異常なアクセスを発見した場合、このツールは自己検出を実行する上で役立ちます。自己検出プロセスには、アクセスドメイン名のDNS解決の検出、リンク品質の検出、ノードステータスの検出、オリジンサーバーの検出やデータアクセスの一致性など、一連の診断項目が含まれており、問題の特定を支援し、解決策を提供します。

> 注意：
> 診断用のリソースURLは、お客様のアカウントでアクセスした、ステータスが**起動済み**のドメイン名である必要があります。診断で発生する帯域幅は、課金帯域幅に計上されます。診断の対象となるリソースは200MBytes以下にすることをお勧めします。

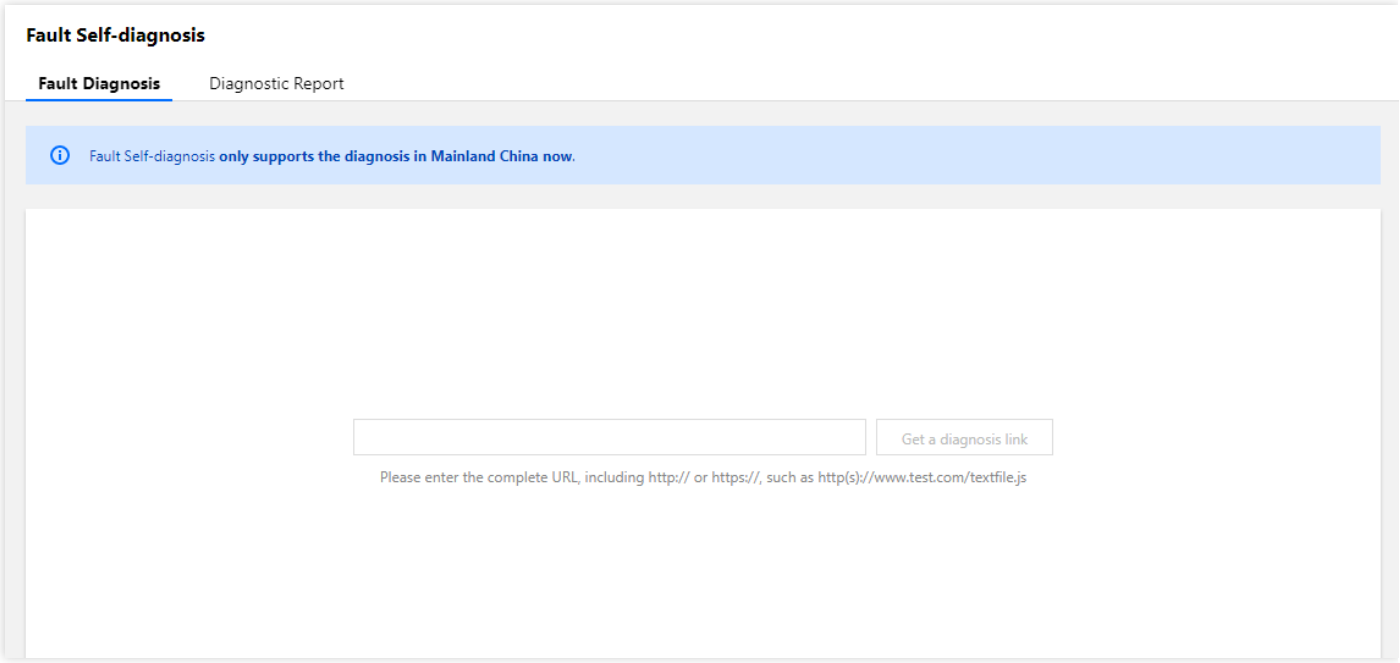
障害診断

診断フロー

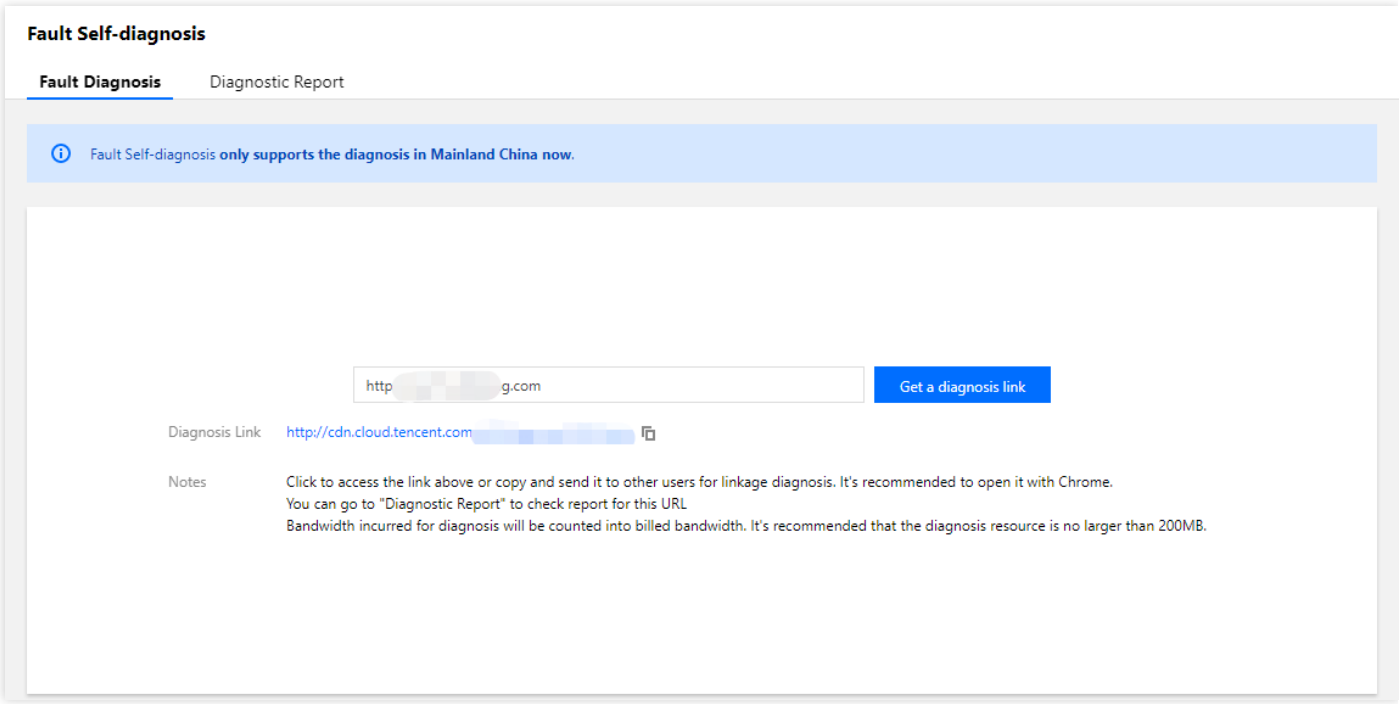
いずれかのリソースURLに異常なアクセスが発見された場合、**障害診断**を介して検出を開始することができます。手順は次のとおりです。

1. CDNコンソールにログインし、左側メニューバーから【診断ツール】>【自己診断ツール】を選択します。
2. 「障害診断」画面で、診断したい異常なURLを入力します。URLに、 `http://` または `https://` というプレフィックスを付けて入力する必要があります。

©2013-2022 Tencent Cloud. All rights reserved.

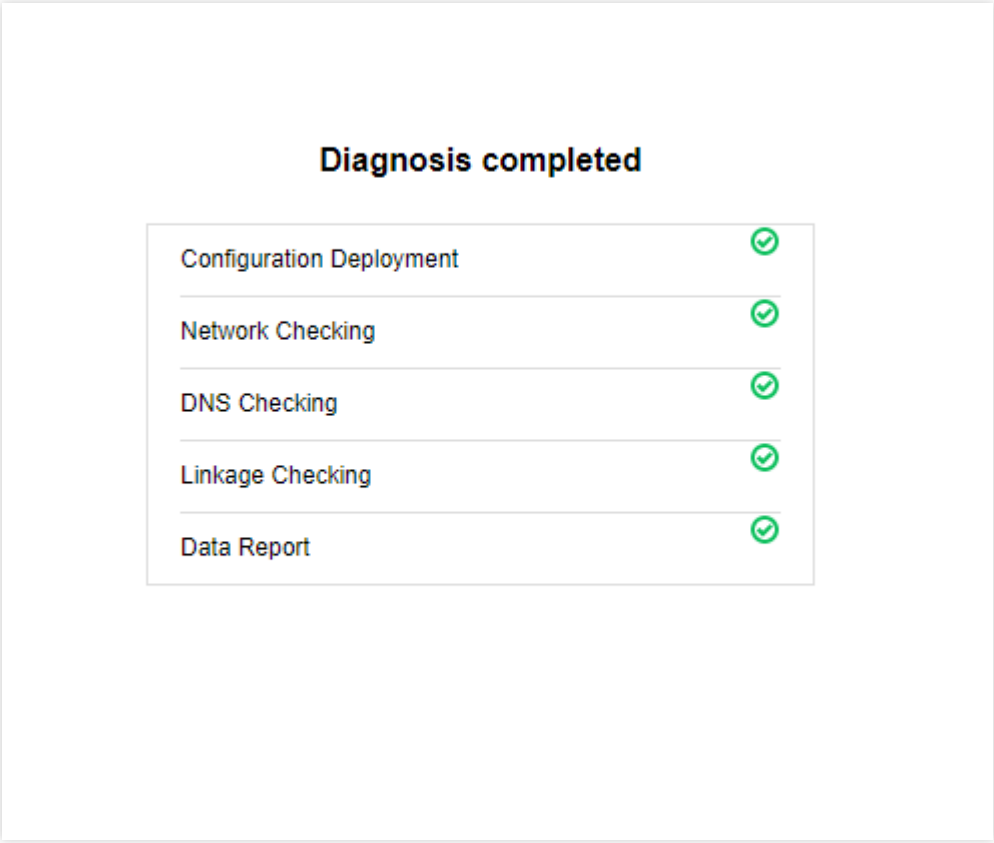


3. URLを入力後、【診断リンクの生成】をクリックすると、診断リンクのアドレスが画面に表示されます。



4. 診断リンクをクリックすると、新しい診断画面が開き、診断情報の収集が開始されます（診断プロセス中に検出画面を閉じないでください。診断が終了したら、この画面は手動で閉じることができます）。

©2013-2022 Tencent Cloud. All rights reserved.



5. 診断リンクを他者に送信して、ローカル側の障害を検出することもできます。検出が完了したら、ブラウザの画面は手動で閉じる必要があります。

注意：

- 各URLで生成される診断リンクの有効期間は24時間で、障害診断は10回までクリックすることができます。
- 「診断レポート」画面で、生成された利用可能な診断リンクを再度コピーすることができます。

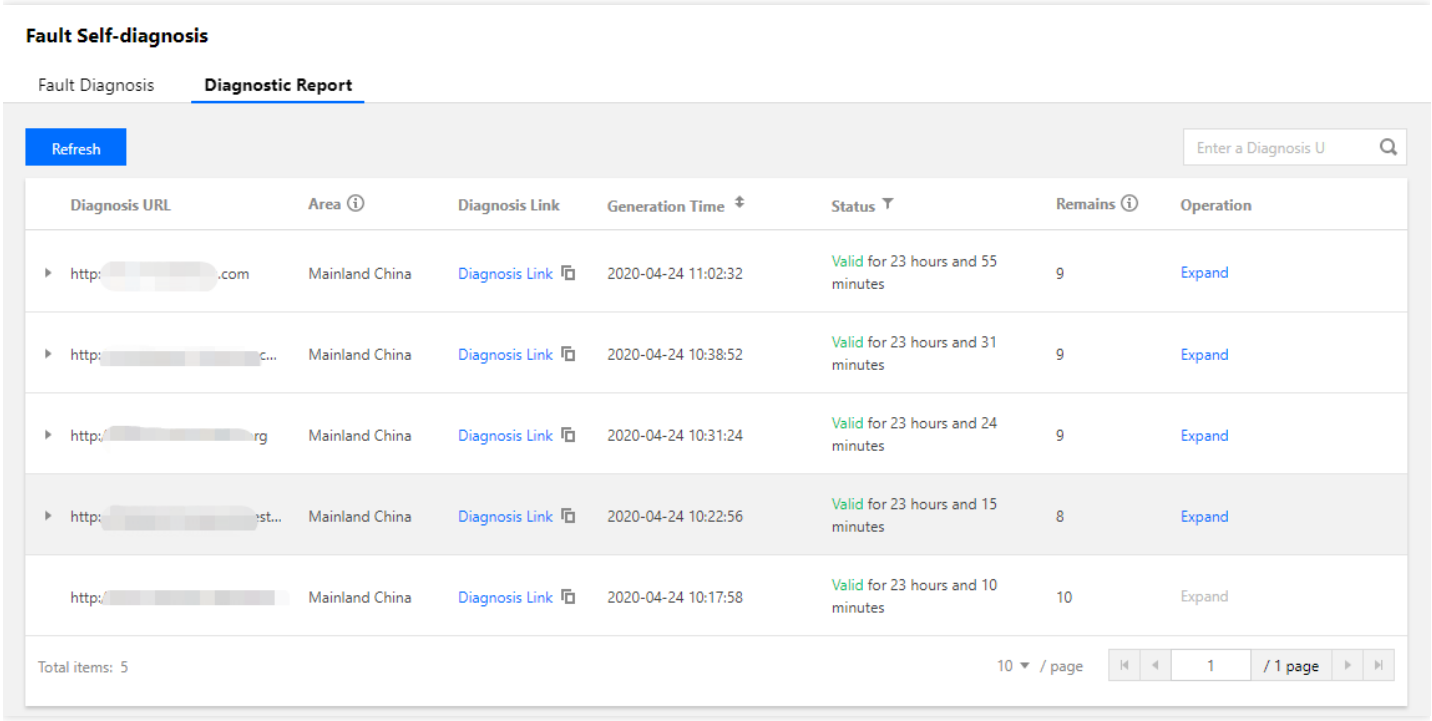
診断レポート

レポートの確認

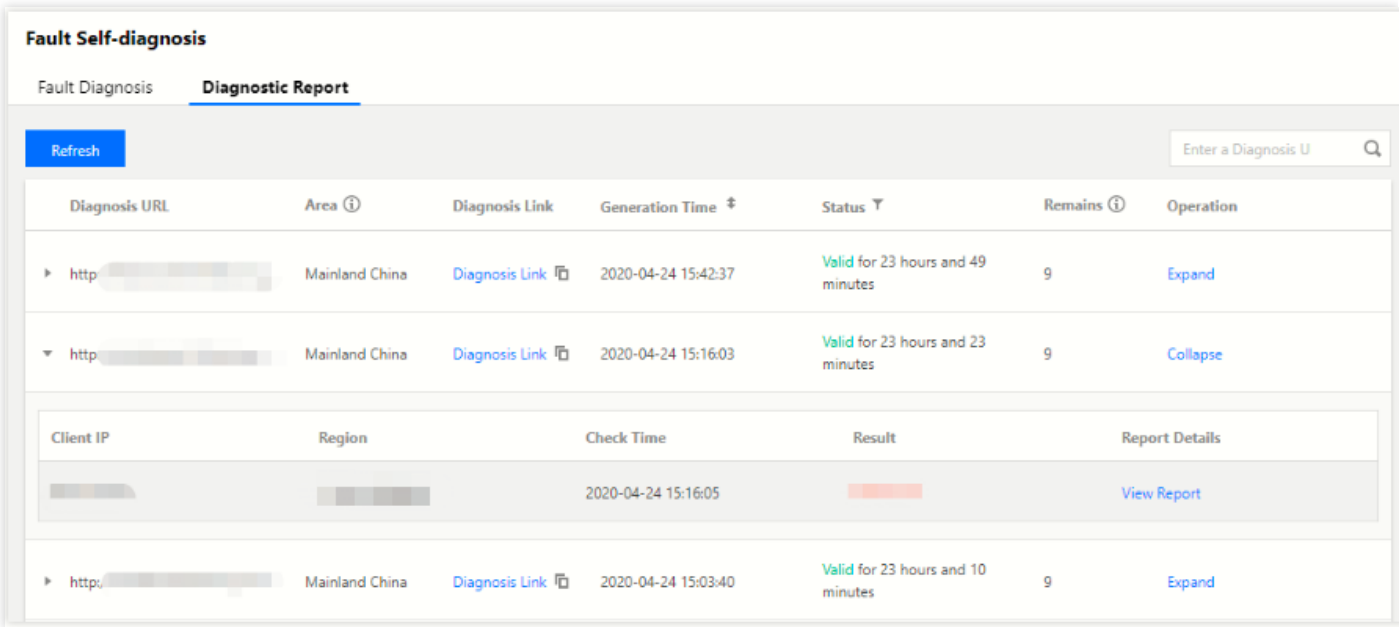
1. 診断が完了したら、【診断レポート】をクリックして画面に進むと、生成された診断レポートが時系列でテーブルに表示され、リストが順番に表示されます。
   - 診断リンクのURLを生成します。
   - URLに対応する診断リージョン。
   - URLに対応する診断リンク。

©2013-2022 Tencent Cloud. All rights reserved.

- 診断リンクの生成時間。
- 診断リンクの生成ステータス。
- 診断リンクで利用可能な診断回数。



2. 操作バーの【展開】をクリックすると、それぞれの診断で生成されたレポートと結果を確認することができます。



3. 診断レポートではそれぞれの手順の検出に基づいて、次のように全体的な判定が行われます。

©2013-2022 Tencent Cloud. All rights reserved.

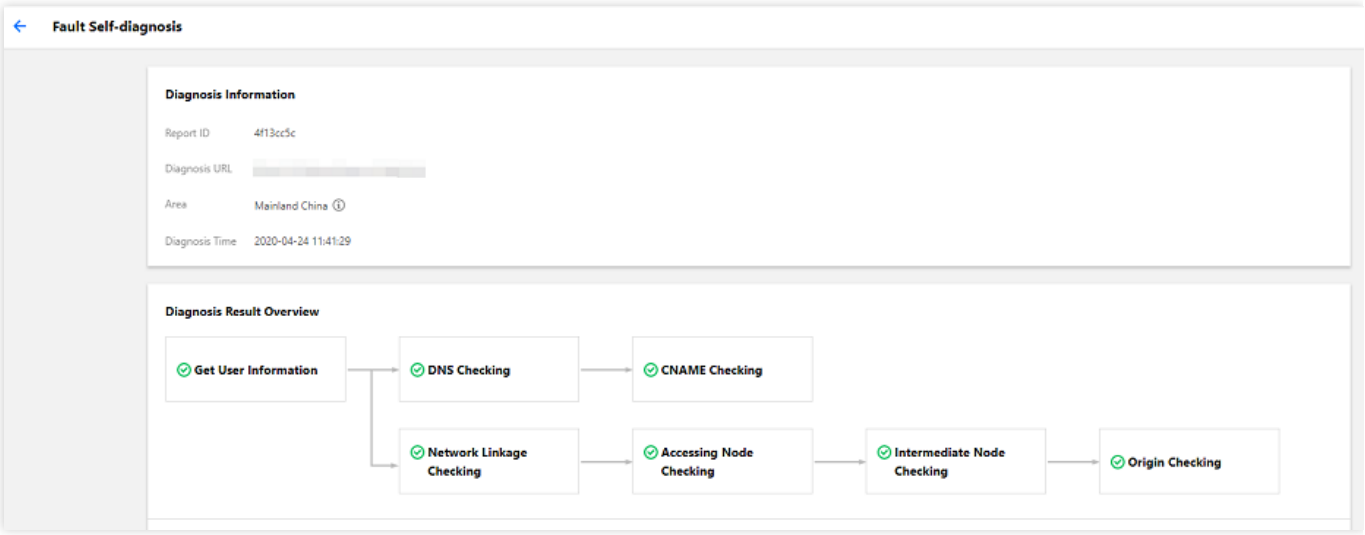
- 正常
- 異常
- 診断画面が異常終了する（ほとんどの場合、診断が完了していない状態で診断画面を閉じることによって生じます）。

4. 右側の【レポートの確認】をクリックすると、診断の詳細と異常な状況への推奨する対処方法が表示されます。

レポートの解読

1. レポートの最初の部分には、次のような診断情報が表示されます。

- 診断レポートID。
- 診断が必要なURL。
- 診断をトリガーする時間。

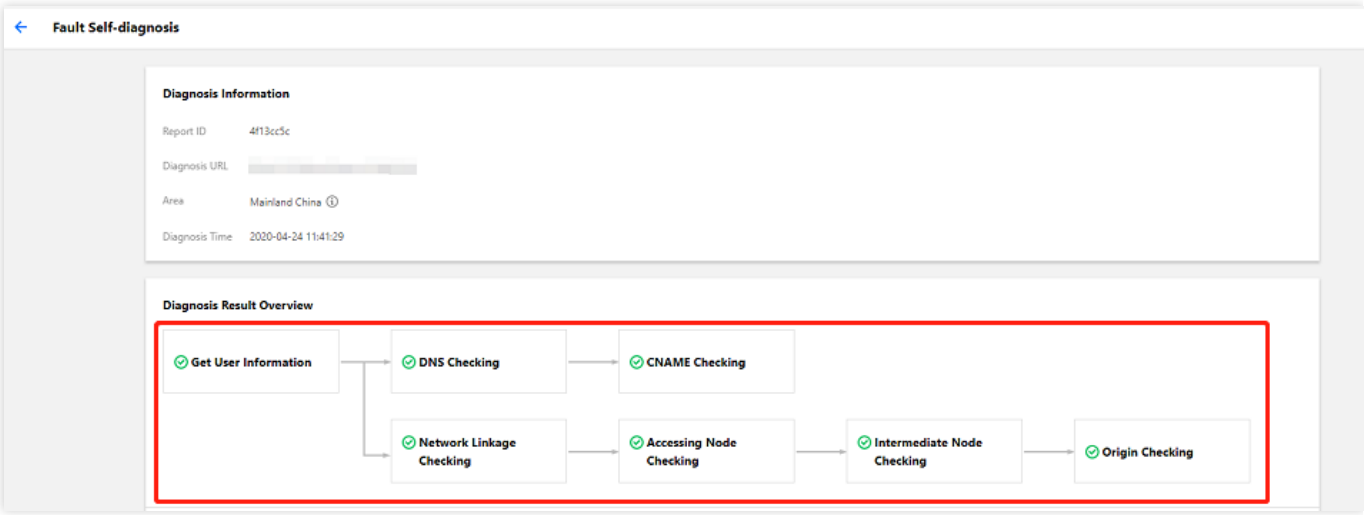


2. レポートの2番目の部分には、診断プロセスの概要と各モジュールの結果が表示されます。異常なモジュールを直感的に発見することができます。診断モジュールには次の事項が含まれます。

- クライアント情報の検出結果。
- DNSの検出結果。
- CNAMEの検出結果。
- ネットワークリンクの検出結果。
- ノード検出へのアクセス結果。
- back-to-originノードの検出結果。

©2013-2022 Tencent Cloud. All rights reserved.

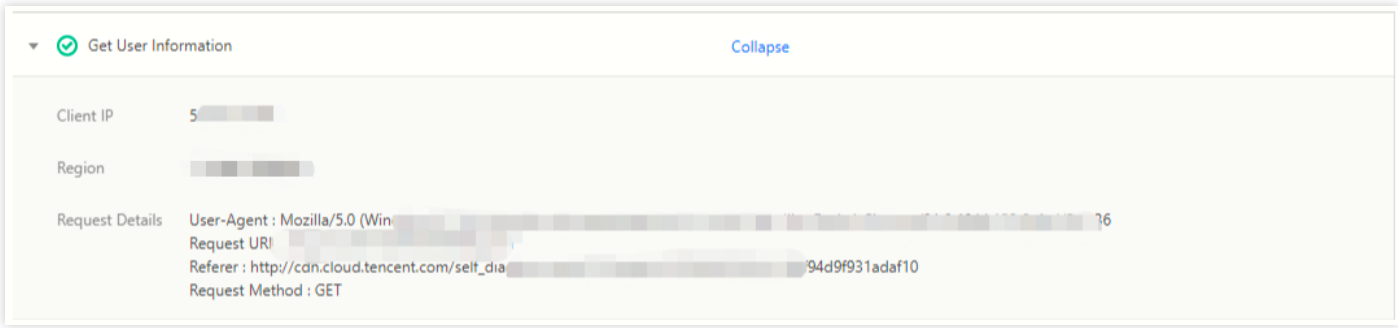
- オリジンサーバーの検出結果。



3. レポートの3番目の部分では、診断結果の詳細な説明を行います。

第1項：クライアント情報

取得したクライアントIP情報、対応する省/キャリア、HTTP/HTTPSリクエストを発信したUser-Agent、Referer、Request Methodなどの情報。クライアント情報の取得に失敗すると、それ以降の部分に対する検出が実行できなくなります。

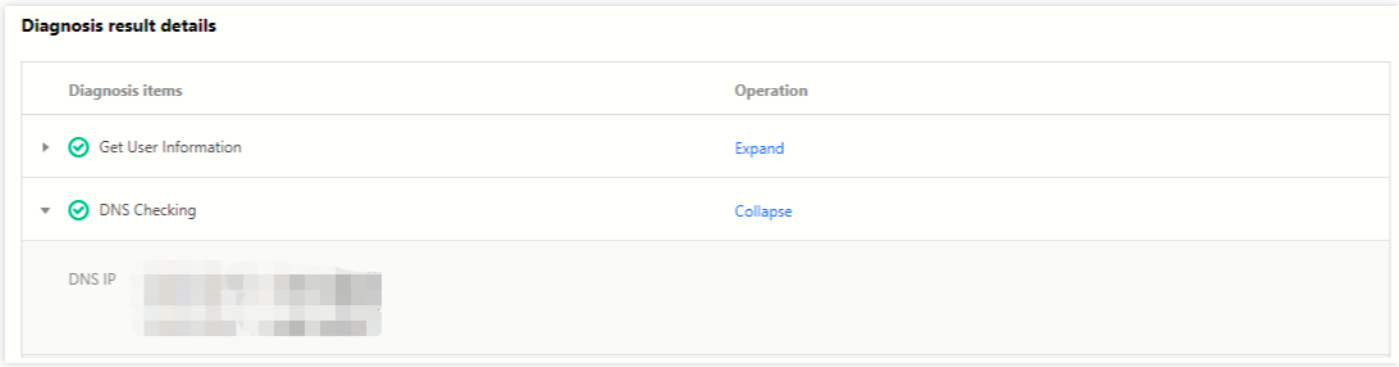


第2項：DNS検出

クライアントのローカルDNS IPを取得し、クライアントIPとDNS IPの帰属が同じであるか確認することによって、ローカルDNSの設定の異常に起因して、最適なアクセラレーションノードのスケジューリングができなく

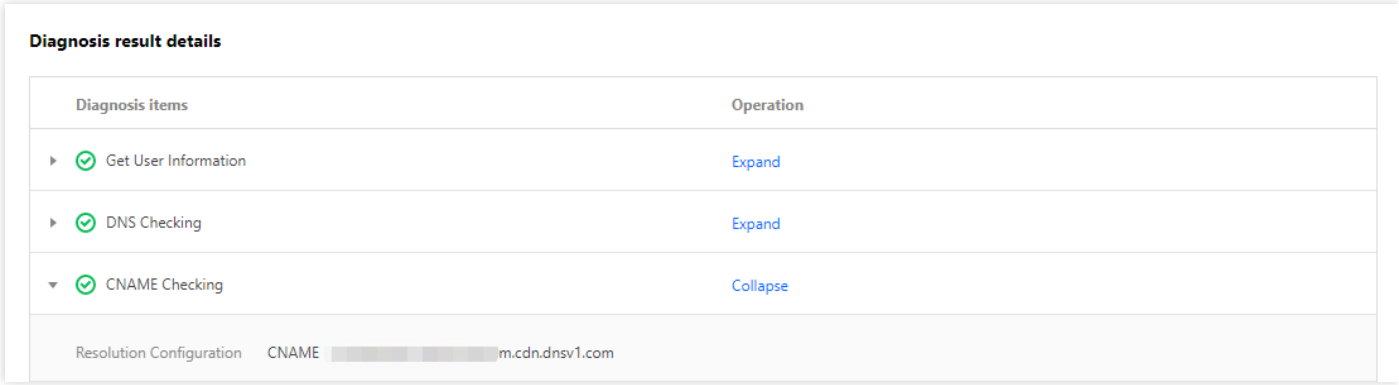
©2013-2022 Tencent Cloud. All rights reserved.

なっているのかどうかを判断することができます。



第3項：CNAME検出

検出ドメイン名のCNAME設定を取得します。ドメイン名のCNAME解決では、正しい*.cdn.dnsv1.com（デフォルト）拡張子ドメイン名として設定する必要があります。設定しない場合、リクエストはCDNノードに到達しません。



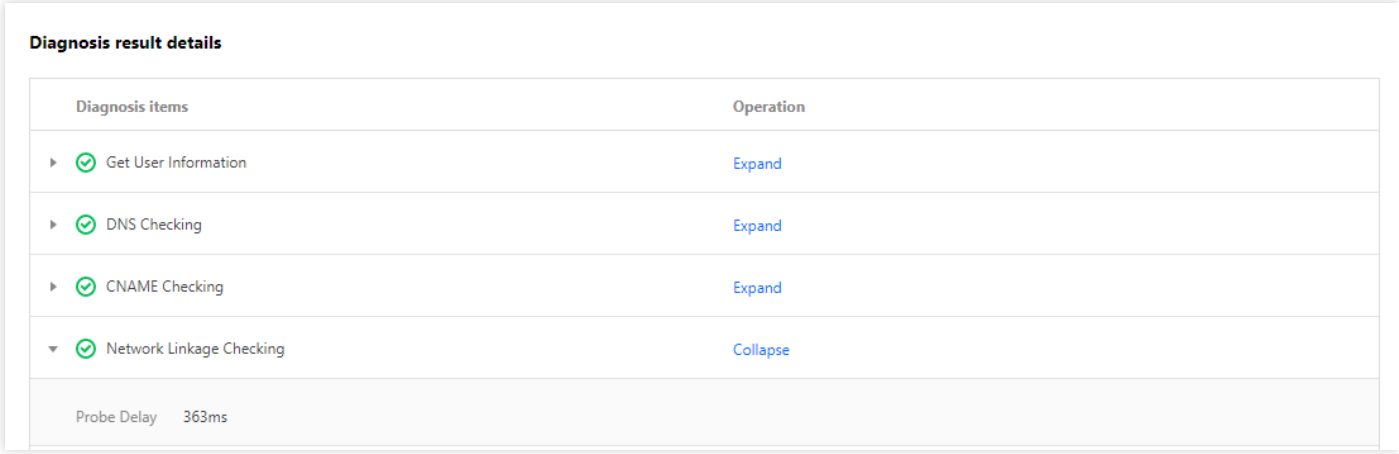
> 注意：
> CNAME設定はチェックされず、リクエストはノードに到達せず、それ以降の検出は実行されなくなります。

第4項：ネットワークリンクの検出

クライアントを介してローカルで複数のインターネットサイトを検出し、クライアントのネットワークステータスを取得します。 ローカルエージェントなどの設定によってサイトにアクセスできない場合、ネットワーク

©2013-2022 Tencent Cloud. All rights reserved.

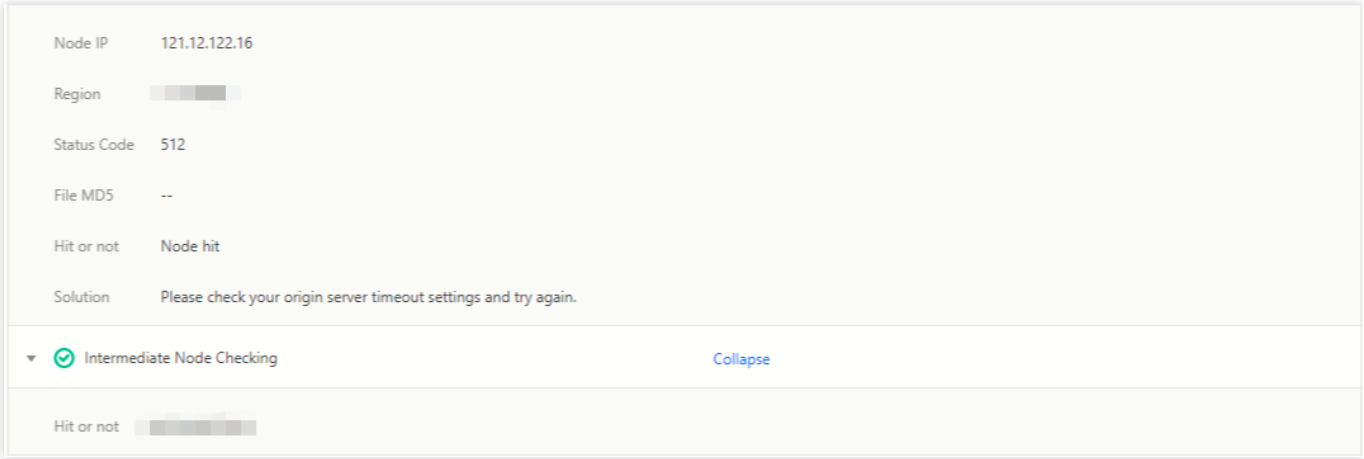
リンクの検出に失敗し、それ以降の検出は実行できなくなります。



第5項：アクセスノード検出

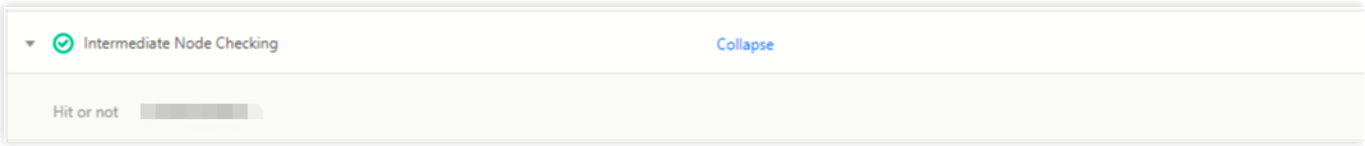
クライアントがリクエストを開始した後、到達したCDNノード情報が収集されます。これには、ノードIP、ノードの省/キャリア、ノードから返されたステータスコード、ヒットステータス、リソースMD5が含まれます。

- ノードがこのリソースをキャッシュしている場合、直接ヒットし、back-to-originノードの検出は実行されません。
- ノードがヒットしない場合、それ以降のback-to-originノードの検出が続行されます。
- URLフィードバックのステータスコードが301、302、504 の場合、ノード検出情報が正常に取得できず、それ以降の検出が実行できなくなります。
- ドメイン名にアクセス制御ポリシーが設定されている場合、アクセスノードは直接403を返し、ヒット状況は**ヒット済み**となります。

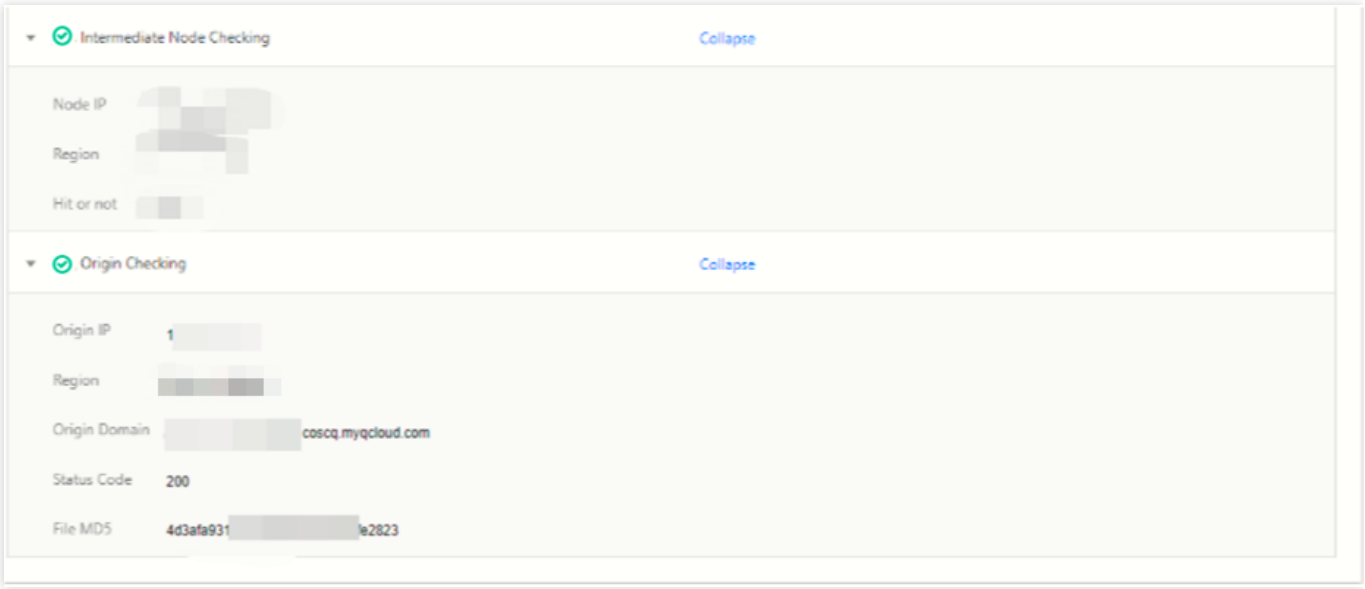


第6項：back-to-originノードの検出

i. リソースがCDNノードによって直接返される場合、この時点で、アクセスノードとback-to-originノードのヒットステータスは、両方とも**ヒット済み**となります。CDNは引き続きオリジンサーバーの検出を実行して、オリジンサーバーから返されたステータスコードと内容がノードと一致しているかどうかを検証しやすくします。



ii. リソースがCDNノードによって直接返されない場合、アクセスノードとback-to-originノードのステータスは両方とも**未ヒット**であり、この時点で内容はオリジンサーバーによって返されます。



iii. この時点で異常なステータス コードが生成された場合、オリジンサーバーのステータスコード、ファイルMD5とアクセスノードモジュールから返されるステータスコード、ファイルMD5を比較することによって、異常がCDNノードか、オリジンサーバーのどちらのせいで発生したか判断し、修復することができます。

説明：
診断レポートで問題を解決できない場合は、チケットを提出するか、またはTencent Cloudの技術者にお問い合わせの上、トラブルシューティングを行うことをお勧めします。

©2013-2022 Tencent Cloud. All rights reserved.

コンテンツのコンプライアンス

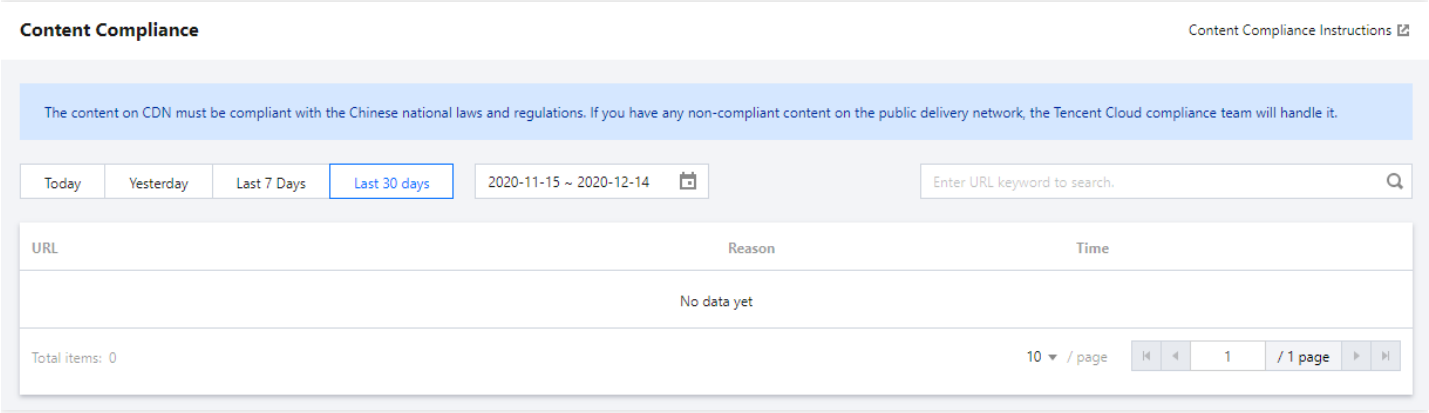
最終更新日：：2021-10-26 16:22:56

機能の概要

Tencent Cloud CDNアクセラレーションコンテンツは、関連する法律、規則、規定に準拠する必要があります。パブリックネットワークから配信されたコンテンツが法律や規則に違反していることは判明した場合、Tencent Cloudコンプライアンスチームがそれを処理します。コンテンツのコンプライアンス機能では、違法コンテンツとコンプライアンスチームによって処理された時間が同時にコンソールに提示されるので参照して確認することができます。

設定の確認

CDN コンソールにログインし、メニューバーから【診断ツール】>【コンテンツコンプライアンス】を選択し、コンテンツコンプライアンス画面に入ります。



©2013-2022 Tencent Cloud. All rights reserved.

クォータ管理

最終更新日：：2022-05-19 10:16:32

機能説明

Content Delivery Network (CDN)のクォータ詳細では、CDNに関連するクォータの上限と使用情報を確認できます。また、業務需要に基づいて一時クォータまたは永続クォータを事前に申請することができます。現在サポートされているクォータには、URL更新クォータ、ディレクトリ更新クォータ、URLプッシュクォータが含まれています。

運用シーン

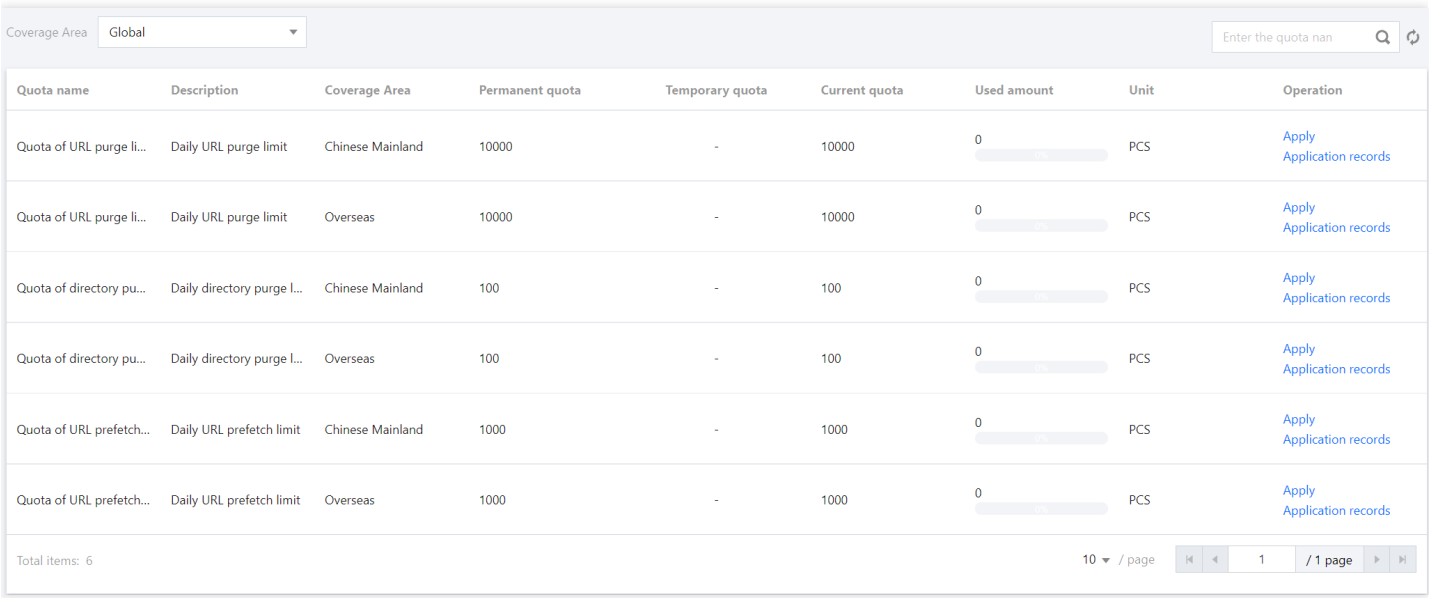
- **一時クォータ**:業務活動や運用シーンにおいて、一時的にクォータを追加する必要がある場合、クォータ管理から必要な時間帯における一時クォータを申請できます。一時クォータの有効期間が過ぎると、現在のクォータは永続クォータに戻ります。
- **永続クォータ**:既存のクォータでは日常の業務需要に対応できない場合、クォータ管理で該当する機能の永続クォータを申請できます。永続クォータの承認に時間がかかるため、一時的な業務需要の場合、一時クォータの申請をお勧めします。

操作ガイド

###クォータの確認
CDNコンソールにログインし、左側のディレクトリで**クォータ管理 > クォータ詳細**をクリックして、クォータ詳細ページに移動します。クォータ詳細ページ、現在のクォータ情報を確認したり、クォータを申請したりできま

©2013-2022 Tencent Cloud. All rights reserved.

す。



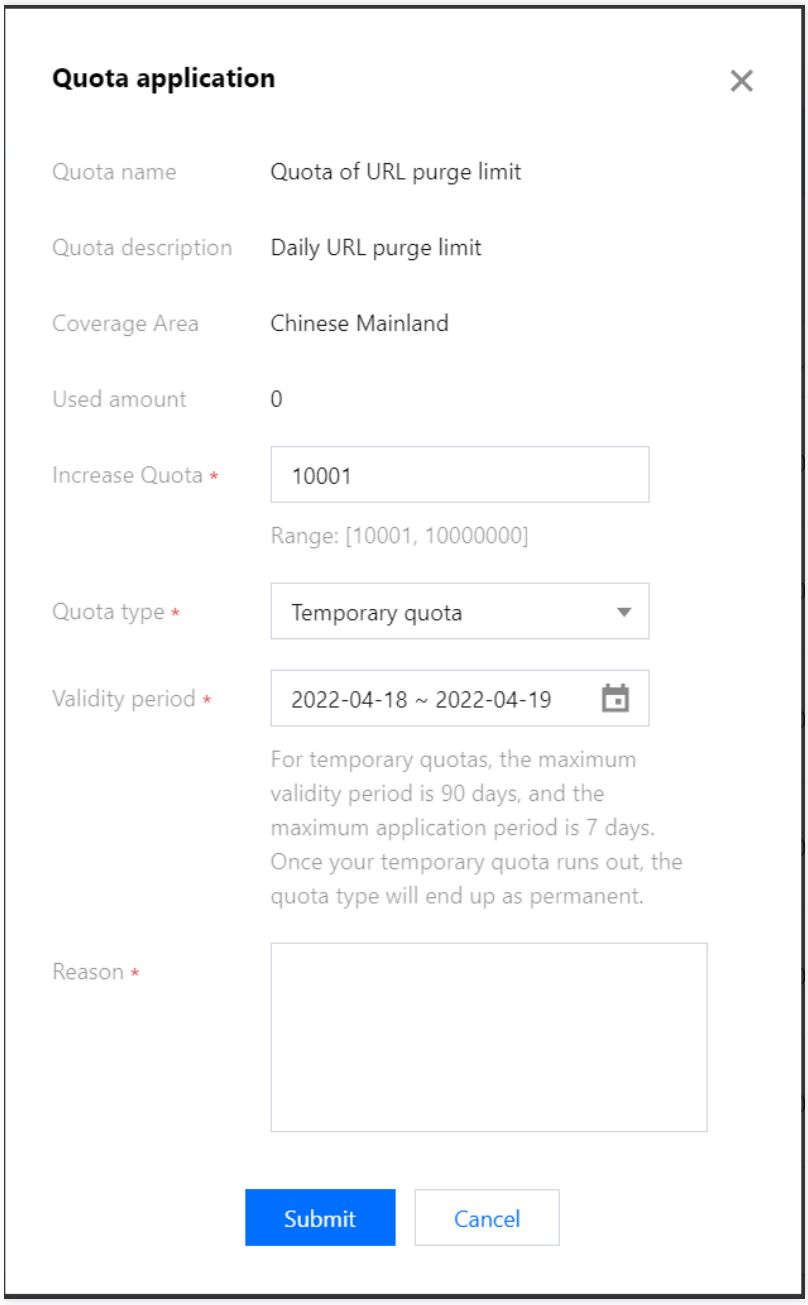
説明：

- 現在のクォータにそのクォータの現在の上限が表示されます。現時点で、有効になっている一時クォータが複数ある場合、現在のクォータに、すべての一時クォータと永続クォータのうちの最大値が表示されます。
- 一時クォータは、開始日の00:00より有効になり、終了日の24:00に無効になります。有効期間が切れると永続クォータに戻ります。
- URL更新クォータ、ディレクトリ更新クォータ、URLプッシュクォータは、全部毎日有効になるクォータであり、使用量が毎日00:00にリセットされます。
- 中国本土と海外のクォータは別々のものであり、上限を引き上げるには個別に申請してください。

クォータの申請

申請 をクリックすると、クォーターの申請ページに移動します。このページで、申請するクォータの情報を入力して提出してください。

©2013-2022 Tencent Cloud. All rights reserved.



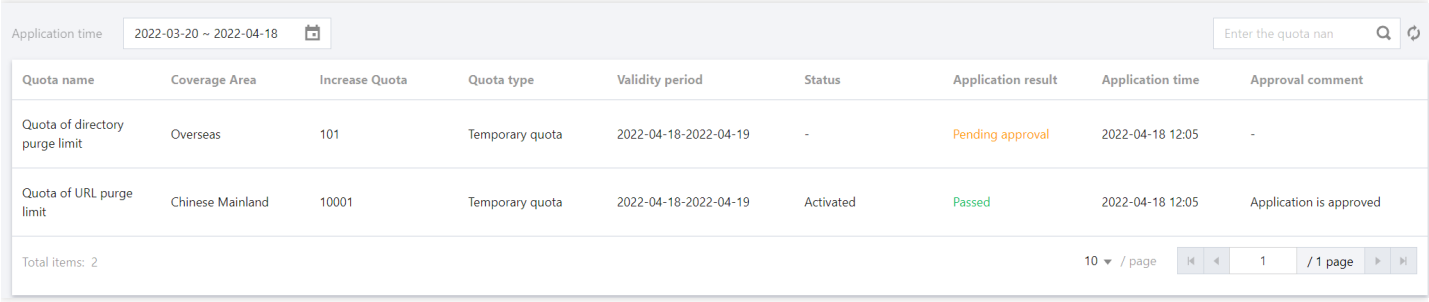
説明：

- 申請するクォータの最小値は、選択されたクォータの「永続クォータ+1」で、最大値は10,000,000です。
- クォータタイプは一時クォータです。一時クォータの発効日は選択可能です。発効日は90日以内の範囲で選択します。最大有効期間は7日です。
- クォータの申請が承認されるように、適切なクォータ値を設定し、申請理由を丁寧に入力してください。

©2013-2022 Tencent Cloud. All rights reserved.

申請履歴

申請履歴または左側のディレクトリで**クォータ管理>申請履歴**をクリックして、申請履歴ページに遷移します。このページでは、申請したクォータの承認情報を確認できます。



説明：

- 申請結果が**承認済み**場合、申請したクォータが承認されています。申請が拒絶された場合、**一時クォータ**を申請するか、申請のクォータ値または理由を変更して改めて申請することをお勧めします。
- 一時クォータの有効期間が過ぎると、状態が期限切れになり、一時クォータが無効になります。現在のクォータは永続クォータまたは他の有効になっている一時クォータになります。

©2013-2022 Tencent Cloud. All rights reserved.

オフラインキャッシュ

最終更新日：：2022-09-29 19:18:34

設定シナリオ

オリジンサーバーが故障し、正常にback-to-originによってリソースを取得できない場合、オフラインキャッシュを有効化すると、CDNを使用してコンテンツをキャッシュすることができます。

- ノードにキャッシュがある場合、キャッシュされたコンテンツを返します。ヒットしたコンテンツが期限切れであっても、オリジンサーバーが回復し、正常にback-to-originされるまで期限切れになったコンテンツに応答します。
- ノードにキャッシュがない場合、通常オリジンサーバーが故障しているというエラーメッセージを返します。

注意：

- オフラインキャッシュは、現時点では中国本土でのみアクセラレーションドメイン名をサポートしています。
- 一部のプラットフォームはアップグレード中のため、この設定機能を開放していません。

設定ガイド

設定の確認

デフォルトの状態では、オフラインキャッシュはオフの状態です。実際の必要性に応じて自身でオン/オフにしてください。

©2013-2022 Tencent Cloud. All rights reserved.