ALIBABA CLOUD

Alibaba Cloud

CDN

域名管理

Document Version: 20220531

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.功能概述

阿里雲CDN控制台不僅可以協助您完成網域名稱配置等基本操作，也提供了即時資料分析的資源監控服務。同時您還可以瞭解自己的計費情況，隨時變更計費方式。 通過本文為您可以瞭解CDN控制台介面展示和網域名稱管理功能。

控制台指引

CDN控制台介面展示如下圖所示。

CDN控制台介面說明如下表所示。

序號	地區	說明
1	左側導覽列	CDN網域名稱導覽列。詳細功能介紹，請參見網域名稱管理功能列表。
2	基礎資料	CDN根據您服務的計費方式，展示計費項目中的使用資料。詳細功能介紹，請參見基礎服務計費。
3	熱門服務	CDN為您展示使用頻率高的服務的快速快口。
4	CDN使用指南	您可以查閱CDN相關的使用指南。如果您想瞭解更多，請參考CDN學習路徑。
5	計費方式	您已選擇的計費方式。您也可根據所需快速修改計費方式。詳細功能介紹，請參見基礎服務計費和增值服務計費。
6	資源套件	您已購買的資源套件。詳細功能介紹，請參見。
7	全部網域名稱	您可以通過快速入口對網域名稱進行管理，並執行添加和重新整理預熱操作。
8	其他加速產品	您可以瞭解與CDN相關的其他產品。
9	網域名稱流量排行	您可以瞭解流量排行前五的網域名稱。

網域名稱管理功能列表

CDN網域名稱管理功能列表如下表所示。

功能	參考文檔	說明	預設值
批量複製	批量複製	將某一個加速網域名稱的一個或多個配置，複製到另外一個或多個網域名稱上。	無
設定警示	設定警示	監控CDN網域名稱的頻寬峰值、4xx5xx返回碼佔比、命中率、公網下行流量和QPS監控項。當警示規則被觸發時，阿里雲監控會根據設定通過簡訊和郵件發送警示資訊。	無
標籤管理	綁定标签	標記網域名稱或為網域名稱分組。	無
	使用標籤快速篩選網域名稱，進行分組管理。	無	

功能	參考文檔	說明	預設值
	使用标签筛选数据	使用標籤快速篩選網域名稱，查詢相關資料。	無
基本資料	修改基础信息	修改加速地區。	無
	配置源站	修改來源站點配置。	無
回源設定	回源HOST	修改回源HOST網域名稱。	開啟
	協議跟隨回源	CDN根據設定的協議規則回源。回源使用協議和用戶端訪問資源的協議保持一致。	未開啟
	私人Bucket回源	開通加速網域名稱訪問私人bucket資源內容的許可權。	未開啟
	配置回源SNI	當來源站點IP綁定多個網域名稱，且CDN節點以HTTPS協議訪問來源站點時，設定回源SNI，指明具體訪問網域名稱。	關閉
	配置自定义回源HTTP头	當HTTP請求回源時，可以添加或刪除回源HTTP頭。	關閉
	配置回源请求超时时间	根據實際需求設定CDN回源請求逾時的最長等待時間。當回源請求等待時間超過配置的逾時時間時，CDN節點與來源站點的串連斷開。	30秒
緩衝配置	緩衝到期時間	自訂指定資源的緩衝到期時間規則。	無
	配置状态码过期时间	配置資源的指定目錄或檔案尾碼名的狀態代碼到期時間。	無
	設定HTTP頭	設定HTTP要求標頭，目前提供10個HTTP要求標頭參數可供自行定義取值。	無
	自訂錯誤頁面	根據所需自訂HTTP或者HTTPS響應返回碼跳轉的完整URL地址。	404
	配置重写	對請求的URI進行修改和302重新導向至目標URI。	無
HTTPS安全加速	HTTPS安全加速設定	提供全鏈路HTTPS安全加速方案，僅需開啟安全加速模式後上傳加速網域名稱認證/私密金鑰，並支援對認證進行查看、停用、啟用、編輯操作。	關閉
	HTTP/2	二進位協議帶來更多擴充性、Alibaba Content Security Service性、多工、頭部壓縮等優勢。	未開啟
	強制跳轉	加速網域名稱開啟HTTPS安全加速的前提下，支援自訂設定，將原請求方式進行強制跳轉。	未開啟
	配置TLS	TLS協議版本開啟後，加速網域名稱開啟TLS握手。目前只支援TLSv1.0、TLSv1.1、TLSv1.2和TLSv1.3版本。	關閉
	配置HSTS	HSTS的作用是強制用戶端（如瀏覽器）使用HTTPS與伺服器建立串連。	關閉

功能	參考文檔	說明	預設值
存取控制	Refer防盜鏈	通過配置訪問的Refer黑名單和白名單來實現對訪客身份的識別和過濾，從而限制訪問CDN資源的使用者。	未開啟
	鑒權配置	通過配置URL鑒權來保護使用者網站的資源不被非法網站下載盜用。	未開啟
	IP黑名單	通過配置IP黑名單和白名單來實現對訪客身份的識別和過濾，從而限制訪問CDN資源的使用者。	未開啟
	配置UA黑名单或白名单	通過配置UsageAgent黑名單和白名單來實現對訪客身份的識別和過濾，從而限制訪問CDN資源的使用者。	未開啟
效能最佳化	頁面最佳化	壓縮與去除頁面中無用的空行、斷行符號等內容，有效縮減頁面大小。	未開啟
	智能壓縮	支援多種內容格式的智能壓縮，有效減少您傳輸內容的大小。	未開啟
	Brotli压缩	對靜態文字檔進行壓縮時，可以開啟此功能，有效減小傳輸內容大小，加速分發效果。	未開啟
	過濾參數	當URL請求中攜帶 `?` 和*參數*時，CDN節點在收到URL請求後，判斷是否需要攜帶參數的URL返回來源站點。	關閉
進階配置	頻寬封頂	當統計周期（5分鐘）產生的平均頻寬超出所設定的頻寬最大值時，為了保護網域名稱安全，此時網域名稱會自動下線，所有的請求會回到來源站點。	未開啟
視頻相關設定	Range回源	開啟Range回源功能，可以減少回源流量消耗，並且提升資源回應時間。	關閉
	拖拽播放	開啟拖拽播放功能後，當播放視音頻時，隨意拖拽播放進度，而不影響視音訊播放效果。	未開啟

2.批量複製

功能介紹

您可以將某一個加速網域名稱的一個或多個配置，複製到另外一個或者多個網域名稱上，實現大量設定網域名稱的效果。

> **說明** 您只能選擇狀態為正常啟動並執行網域名稱進行複製。

操作步驟

請確保您已經配置過您想複製配置的網域名稱，否則將無法批量複製。

> **說明** 您無法複製HTTPS認證到其他網域名稱，請您單獨配置。

> **警告** 網域名稱複製後，複製不可回退。請確認該被複製的網域名稱正在服務或已有配置，且流量頻寬較大。請務必確認您的網域名稱複製選擇無誤，謹慎複製。

1. 在 **網域名稱概覽** 頁，選擇您想要複製配置的網域名稱，單擊 **複製配置** 。
2. 勾選您想要複製的配置項，單擊 **下一步** 。

   > **說明** 您無法同時複製來源站點資訊和非來源站點資訊。

3. 勾選您想要的被大量設定的目標網域名稱（您想要應用上一步中複製到的配置的網域名稱），單擊 **下一步** 。

   您也可以輸入關鍵詞尋找網域名稱。

   > **說明** 複製的內容會覆蓋目標網域名稱已經配置的內容，請您謹慎操作，以免造成服務不可用。

4. 在單彈窗中單擊 **確認** ，批量複製成功。

注意事項

- 自訂回源頭為差異複寫。例如，假設您的A網域名稱有2條回源頭配置，您從B網域名稱複製了5條內容，則你會有7條回源頭配置內容。
- HTTP頭為非差異複寫，假設您的A網域名稱配置了cache_control 為private，您的B網域名稱配置為public，複製後，您的cache_control為public。
- 開關類的配置複製，將會覆蓋網域名稱原有的配置。
- Refer黑白名單或IP黑白名單將會覆蓋網域名稱原有配置。

3.設定警示

當您需要監控CDN網域名稱的頻寬峰值、4xx5xx返回碼佔比、命中率、下行流量和QPS等監控項時，您可以直接在阿里雲的CloudMonitor控制台設定警示規則。當警示規則被觸發時，阿里雲監控會根據您設定的簡訊、郵件等通知方式給您發送警示資訊。

操作步驟

1.
2.
3. 在 **域名管理**頁面，單擊 **报警设置**，跳轉到CloudMonitor控制台。
4. 選擇 **CloudMonitor服務 > CDN** ，單擊 **警示規則** 頁簽。
5. 單擊 **建立警示規則** 。
6. 建立針對CDN的警示規則。
7. 單擊 **確定** 。

4.標籤管理

4.1. 什麼是標籤

阿里雲CDN不對標籤進行任何定義，僅嚴格按字串對標籤和網域名稱進行匹配、篩選。標籤可以標記網域名稱，允許企業或個人將相同屬性的網域名稱分類，方便您識別、篩選和管理網域名稱。

使用限制

標籤的使用限制如下：

- 每個標籤都由一個索引值對 `Key:Value` 組成。
- 每個網域名稱最多綁定20個標籤。
- 同一個網域名稱的標籤鍵Key不能重複。如果對一個網域名稱設定2個同Key不同Value的標籤，新值將覆蓋舊值。例如對網域名稱 `test.example.com` 先後設定了標籤 `Key1:Value1` 和 `Key1:Value2` ，則最終 `test.example.com` 只會綁定標籤 `Key1:Value2` 。
- 鍵key不支援 `aliyun` 、 `acs:` 開頭，不允許包含 `http://` 和 `https://` ，不允許為空白字串。
- 值value不允許包含 `http://` 和 `https://` ，允許為空白字串。
- 最大鍵key長度：64個Unicode字元。
- 最大值value長度：128個Unicode字元。
- 區分大小寫。

相關功能

您可以使用標籤，對網域名稱進行如下操作。

功能	說明
綁定標籤	為網域名稱綁定標籤，方便您分類和統一管理
解除綁定標籤	標籤不再適用於管理和檢索網域名稱時，將該標籤與網域名稱解除綁定。
使用標籤管理網域名稱	通過標籤快速篩選網域名稱，進行分組管理。
使用標籤篩選資料	通過標籤篩選某類網域名稱的監控資料（例如，流量頻寬、命中率等）。
案例介紹	舉例為您介紹如何使用標籤進行網域名稱的分組管理。

4.2. 綁定標籤

您可以通過標籤功能為網域名稱綁定標籤，實現標記網域名稱或為網域名稱分組。

操作步驟

1.
2.
3. 網域名稱綁定標籤。

- 單個網域名稱增加標籤
  a. 在 **域名管理**頁面，選擇您需要設定標籤的網域名稱，將游標移動到對應標籤上。
  b. 在懸浮窗內，單擊 **編輯** 。
  c. 在 **编辑标签**對話方塊，您可以 **选择已有标签**或 **新建标签**進行綁定。
  d. 單擊 **確定** 。
- 批量網域名稱增加標籤
  a. 選中您需要批量增加標籤的網域名稱，選擇 **标签管理 > 增加标签**。
  b. 在 **批量新增标签**對話方塊，您可以 **选择已有标签**或 **新建标签**進行綁定。
  c. 單擊 **確定** 。

相關API

您可以調用API介面綁定標籤，請參見 添加資源標籤。

4.3. 解除綁定標籤

如果標籤已經不再適用於您當前某個或多個網域名稱的用途，您可以解除綁定網域名稱標籤。

操作步驟

1.
2.
3. 勾選您需要刪除標籤的網域名稱，選擇 **标签管理 > 删除标签**。
4. 在 **批量删除标签**對話方塊，選擇您需要刪除的標籤，單擊 **確定** 。

API介面

您可以調用API介面解除綁定標籤，請參見 刪除資源標籤。

4.4. 使用標籤管理網域名稱

您可以在網域名稱綁定標籤後，使用標籤快速篩選對應的網域名稱，進行分組管理。

操作步驟

1.
2.
3. 在 **域名管理**頁面，單擊 **选择标签**。
4. 選中需要篩選的標籤（可多選）進行管理。

調用介面

您可以調用API介面查詢網域名稱對應的標籤，從而對網域名稱進行管理，請參見 擷取資源對應的標籤。

4.5. 使用標籤篩選資料

如果您需要查詢部分網域名稱的資料，您可以在網域名稱綁定標籤後，使用標籤快速篩選對應的網域名稱，查詢相關資料。

操作步驟

1.
2. 您可以通過如下兩種方式篩選並查詢資料。

   > 說明 如果您同時選擇多個標籤，則查詢的結果是各個標籤對應網域名稱的交集。

   - 在左側導覽列，選擇 **监控查询 > 资源监控**。
     a. 在 **流量带宽**頁簽，單擊 **选择标签**。
     b. 選中需要篩選的標籤，單擊 **查询**。
   - 在左側導覽列，選擇 **监控查询 > 用量查询**。
     a. 在 **用量查询**頁簽，單擊 **选择标签**。
     b. 選中需要篩選的標籤，單擊 **查询**。

4.6. 案例介紹

本文通過舉例為您介紹如何使用標籤進行網域名稱的分組管理。

某公司在阿里雲CDN擁有100個網域名稱，分屬電商、遊戲、文娛三個部門，服務於營銷活動、遊戲 A、遊戲 B、後期製作等業務。公司有三位營運負責人，分別是張三、李四、王五。

設定標籤

為了方便管理，該公司使用標籤來分類管理對應的網域名稱，定義了下述標籤鍵（Key）和值（Value）。

鍵（Key）	值（Value）
部門	電商、遊戲、文娛
業務	營銷活動、遊戲 A、遊戲 B、後期製作
負責人	張三、李四、王五

將這些標籤的鍵和值綁定到網域名稱上，網域名稱與標籤索引值的關係如下表所示：

網域名稱	Key為部門，Value為	Key為業務，Value為	Key為負責人，Value為
domain1	電商	營銷活動	王五
domain2	電商	營銷活動	王五
domain3	遊戲	遊戲 A	張三
domain3	遊戲	遊戲 B	張三
domain4	遊戲	遊戲 B	張三
domain5	遊戲	遊戲 B	李四
domain6	遊戲	遊戲 B	李四

網域名稱	Key為部門，Value為	Key為業務，Value為	Key為負責人，Value為
domain7	遊戲	遊戲 B	李四
domain8	文娛	後期製作	王五
domain9	文娛	後期製作	王五
domain10	文娛	後期製作	王五

使用標籤

- 如果您想篩選出王五負責的網域名稱，則選擇標籤 **負責人：王五** 。
- 如果您想篩選出遊戲部門中李四負責的網域名稱，則選擇標籤 **部門：遊戲** 和 **負責人：李四** 。

5.基本配置

5.1. 多源優先順序設定

功能介紹

阿里雲CDN支援三種類型回源網域名稱，包括oss回源網域名稱、IP和自訂網域名。其中IP和自訂網域名支援多IP或多網域名稱設定，並支援用在多來源站點情境下，進行回源優先順序設定。

當使用者選擇的回源來源站點類型為IP或自訂網域名時，可設定多個來源站點，並為多來源站點設定優先權。添加多來源站點時，來源站點優先順序為“主”和“備”，優先順序為“主”>“備”。

使用者100%回源流量都將首先回源優先順序高的來源站點，如果某個來源站點健全狀態檢查連續3次都是失敗的話，則100%的流量都將選擇優先順序第二的來源站點回源。如果主動健全狀態檢查成功的話，該來源站點就會重新標記為可用，恢複原來優先順序。當所有來源站點的回源優先順序一樣時，cdn將自動輪詢回源。

來源站點健全狀態檢查：實行主動四層健全狀態檢查機制，每5秒主動健全狀態檢查來源站點一次。

主要支援情境：主備方式切換來源站點

操作步驟

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**基本配置 > 來源站點資訊來源站點配置**，設定來源站點類型、來源站點地址和連接埠（您可以選擇的回源連接埠類型為：80連接埠、443連接埠和自訂連接埠）。
   - 如果您選擇的來源站點資訊為 IP 或 **來源站點網域名稱**，則您仍然按照外網流量標準進行計費。
   - 如果您選擇的來源站點資訊為 **OSS網域名稱**，即從CDN回源OSS，則按照內網的價格計費。OSS價格詳情。
   - 如果選擇網域名稱類型為**來源站點網域名稱**，並設定了一個oss的網域名稱，那麼仍然按照外網流量價格計費。
3. 設定完成後，單擊**確認**，設定成功。

> **說明**
>
> - 多源優先順序的設定只支援IP和來源站點網域名稱類型，OSS網域名稱不支援多源優先順序功能；您可以根據實際需求，選擇適合自己的來源站點類型及設定合理的優先順序。
> - 直播加速不支援來源站點設定。

設定自訂連接埠

您可以在開通白名單後，設定自訂連接埠。自訂連接埠支援範圍為0-65535。

- 當您的靜態或動態通訊協定設定為**跟隨**時，無法設定自訂連接埠。
- 如果您通過OpenAPI，設定自己的回源協議為**跟隨**，請確保您的回源協議和自訂連接埠均能正常使用。
- 當您通過連接埠設定了回源協議（HTTP或HTTPS）和**自訂連接埠**時，則無論您在控制台如何設定，回源都將按照連接埠的配置進行。

5.2. 切換加速地區

當您需要變更加速網域名稱的CDN服務涵蓋範圍時，您可以通過切換加速地區功能實現。

操作步驟

1.
2.
3.
4. 在 **基础信息** 地區，單擊 **修改**。
5. 在 **加速区域** 對話方塊，選擇您需要切換的加速地區。

參數	說明
仅中国内地	如果選擇 **仅中国内地**，代表全球使用者訪問均會調度至中國內地加速節點進行服務（海外使用者的訪問流量將會被調度至華東電信的CDN節點）。同時需要工信部備案。網域名稱備案方法，請參見 數量限制。
全球	如果選擇 **全球**，全球使用者訪問將會擇優調度至最近的加速節點進行服務。同時需要工信部備案。網域名稱備案方法，請參見 數量限制。
全球（不包含中国内地）	如果選擇 **全球（不包含中国内地）**，全球使用者訪問均會調度至中國香港、中國澳門、中國台灣以及其他國家和地區的加速節點進行服務（中國內地使用者將會被調度至日本、新加坡和中國香港的CDN節點）。該選項無需工信部備案。

6. 單擊 **确定**。

5.3. 配置來源站點

阿里雲CDN支援的來源站點類型包括OSS網域名稱、IP、來源站點網域名稱和Function Compute網域名稱，每種來源站點類型都支援配置多個來源站點地址，多來源站點情境下，支援設定來源站點的主備優先順序和權重，實現負載平衡。本文介紹如何新增或修改來源站點資訊及來源站點的健全狀態檢查策略。

新增或修改來源站點資訊

1.
2.
3.
4. 在 **源站信息** 地區，根據業務需求，選擇新增或修改來源站點配置。
   - 單擊 **新增来源站点资讯** ，可以增加來源站點。
   - 單擊已有源你好站資訊後面的 **编辑** ，可以修改已有來源站點配置。

> **說明** 以下三種情境下的計費詳情，請參見 OSS價格詳情 。
>
> - 來源站點資訊選擇 IP或 **源站域名**，則OSS上產生的流量費用將按照外網流出流量的價格計費。
> - 來源站點資訊選擇 **源站域名**，並設定了一個OSS的網域名稱，則OSS上產生的流量費用仍按照外網流出流量的價格計費。
> - 來源站點資訊選擇 **OSS域名**，即從CDN回源OSS，則OSS上產生的流量費用將按照CDN回源流出流量的價格計費。

參數	說明
加速域名	注意事項如下： ○ 加速網域名稱一般使用子網域名稱或泛網域名稱，且僅支援全英文小寫網域名稱，不支援中文網域名稱加速。 樣本：您的網域名稱是 `example.com`，加速網域名稱可以是 `example.com` 的子網域名稱，例如 `cdntest.example.com`。 ○ 支援泛網域名稱加速，例如 `*.example.com`。泛網域名稱加速規則，請參見 泛網域名稱加速規則 。 **說明** ■ 泛網域名稱和子網域名稱必須在同一個帳號下。您添加網域名稱時CDN會進行檢查，如果泛網域名稱或子網域名稱被添加到不同帳號，系統會報錯。如果您無法自行解決，請 提交工單處理。 ■ 如果泛網域名稱未被添加到任何CDN帳號下，則支援在多個帳號下添加不同的子網域名稱。 ○ 加速網域名稱不允許重複添加。 如果出現網域名稱已被添加到其他雲產品（例如ApsaraVideo for VOD、ApsaraVideo for Live、全站加速等）中的提示，您可以 提交工單 處理。 ○ 每個阿里雲帳號最多可以添加50個加速網域名稱。 如果您網域名稱的總頻寬日均峰值大於50 Mbps，且業務無風險，可 申請增加網域名稱個數。 ○ 加速內容必須合法且符合CDN業務規範。詳細資料，請參見 網域名稱准入標準。
业务类型	**业务类型**配置後不允許修改，需謹慎選擇。 ○ 圖片小檔案：適用於電商類、網站類、遊戲圖片類等小型的靜態資源加速情境。 ○ 大檔案下載：適用於大於20 MB的靜態檔案加速情境。 ○ 視音頻點播：適用於音頻或視頻檔案加速情境。 ○ 全站加速 ：適用於含有大量動態和靜態內容混合，且多為動態資源請求的加速情境。 當業務類型選擇 **全站加速**時，您需根據介面提示，前往全站加速控制台添加網域名稱並進行相關配置。

參數	說明
加速区域	選擇加速地區。加速地區為 **仅中国内地** 或 **全球** 時，加速網域名稱必須備案，您可以登入 阿里雲ICP代備案管理系統 完成備案。由於工信部備案系統存在資料延遲，剛完成備案的網域名稱請在8小時後再配置。 **說明** 不同的加速地區價格不一樣，請根據您的實際需求選擇。計費詳情，請參見 CDN定價 。 ○ **仅中国内地**：全球使用者訪問均會調度至中國內地加速節點進行服務（海外使用者的訪問流量將會被調度至華東電信的CDN節點）。 ○ **全球**：全球使用者訪問將會擇優調度至最近的加速節點進行服務。 ○ **全球（不包含中国内地）**：全球使用者訪問均會調度至中國香港、中國澳門、中國台灣以及其他國家和地區的加速節點進行服務（中國內地使用者將會被調度至日本、新加坡和中國香港的CDN節點）。

5. 單擊 **确认**，完成配置。

來源站點的健全狀態檢查策略

阿里雲CDN節點支援對來源站點進行四層（TCP）健全狀態檢查。通過健全狀態檢查來判斷來源站點的可用性，避免來源站點異常導致回源擷取資源失敗。

當使用者對同一個來源站點IP和連接埠發起四層串連請求，連續兩次出現不可用（串連失敗或逾時等）時，CDN會從回源地址清單中剔除該來源站點IP並將該IP加入dead table中，與此同時，系統會根據來源站點優先順序從高到低的順序進行重試，如果來源站點優先順序相同，會根據來源站點的權重大小按比例重試；當某個來源站點IP地址出現連續兩次不可用時，將會啟動5秒定時任務，每隔5秒進行TCP四層串連探測，檢測TCP四層串連是否成功，如果串連成功，則將該來源站點IP恢複到可用列表中。

說明

- 重試是IP地址層級的，如果來源站點是網域名稱，只有網域名稱下的所有IP都串連失敗後才會訪問備來源站點。
- 重試時系統會自動過濾dead table中停用來源站點。

5.4. IPv6配置

本文介紹阿里雲CDN IPv6功能在控制台的操作步驟，通過開啟IPv6開關，IPv6的用戶端請求將支援以IPv6協議訪問CDN，CDN也將攜帶IPv6的用戶端IP資訊訪問您的來源站點。

背景信息

阿里雲CDN大部分節點已經支援接收IPv6協議的請求，開啟IPv6後，當您的使用者處於IPv6環境，且就近的CDN節點也支援IPv6請求時，用戶端可以通過IPv6協議訪問CDN節點。當使用者就近地區的CDN節點不支援IPv6協議時，用戶端仍可以以IPv4協議訪問CDN節點。

說明 目前海外、中國香港、中國澳門和中國台灣節點不支援IPv6配置。

操作步驟

1.
2.
3.
4. 在 **基本配置** 地區，找到IPv6功能。
5. 開啟 **IPv6开关**。

   開啟IPv6功能後，您可以在用戶端通過IPv6協議訪問CDN節點，阿里雲CDN節點也將攜帶IPv6協議資訊訪問您的來源站點。

6.內容回源設定

6.1. 回源概述

當您通過用戶端請求訪問資源時，如果CDN節點上未緩衝該資源，則會到來源站點擷取，如果是靜態資源直接緩衝到CDN節點，如果是動態資源則透傳給客戶；或者您部署預熱任務給CDN節點時，CDN節點收到預熱任務以後主動回來源站點擷取所需資源同時緩衝到CDN節點。您可以根據業務的實際需要來配置回源相關功能。

如果您遇到如下情境，您可以通過豐富的回源配置功能，對網域名稱執行相關操作。

功能	說明	文檔連結
自訂CDN節點回源時需要訪問的具體伺服器網域名稱 。	當您的來源站點的同一個IP地址上綁定了多個網域名稱或網站，您可以通過配置HTTP要求標頭中的HOST資訊，來指定CDN節點回源時需要訪問的網站。CDN在回源過程中會根據HOST資訊去對應網站擷取資源。	回源HOST
設定回源協議類型（跟隨、HTTP或HTTPS） 。	當您通過用戶端請求訪問資源時，如果CDN節點上未緩衝該資源，則會根據您配置的協議跟隨規則到來源站點擷取資源。	協議跟隨回源
OSS私人Bucket回源 。	當您的來源站點為OSS且Bucket設定為私人時，必須先開啟阿里雲OSS私人Bucket回源開關對CDN授權，才能實現CDN回源至私人OSS Bucket訪問資源，從而有效防止資源盜鏈。	私人bucket回源授權
指定CDN回源時具體訪問的網站 。	如果您的來源站點IP綁定了多個網域名稱，當CDN節點以HTTPS協議訪問您的來源站點時，您可以設定回源SNI，指明具體訪問網域名稱。	配置回源SNI
設定CDN回源請求的最長等待時間 。	CDN加速節點的回源請求逾時等待時間預設為30秒，您可以根據實際需求設定CDN回源請求的最長等待時間。當回源請求等待時間超過配置的逾時時間時，CDN節點與來源站點的串連斷開。	配置回源請求逾時時間
指定是否由CDN節點代替使用者處理302狀態代碼的內容 。	CDN節點未配置回源302跟隨時，收到來源站點返回的302狀態代碼將直接轉寄給使用者。配置回源302跟隨功能後，CDN節點會代替使用者直接處理302狀態代碼的內容。	配置回源302跟隨
添加、修改或刪除回源HTTP要求標頭 。	HTTP請求回源時，您可以添加或刪除回源HTTP頭。	配置回源HTTP要求標頭
	當您需要改寫使用者回源請求中的HTTP Header時，可以通過配置回源HTTP要求標頭參數實現。	配置回源HTTP要求標頭（新）
添加、修改或刪除回源HTTP回應標頭 。	當您需要改寫使用者回源響應中的HTTP Header時，可以配置功能。	配置回源HTTP回應標頭
回源URI改寫 。	當您需要改寫回源請求中的URI時，可以配置回源URI改寫功能。	改寫回源URI

功能	說明	文檔連結
配置回源參數改寫（忽略、添加、刪除、保留、修改等） 。	當使用者請求URL中攜帶的參數資訊與您需要發送給來源站點的參數資訊不一致時，您可以配置多個回源參數改寫規則，實現忽略、添加、刪除、保留、修改等多種操作。	改寫回源參數

6.2. 回源HOST

功能介紹

使用回源HOST，您可以自訂CDN節點回源時所需訪問的具體伺服器網域名稱。您可以選擇三種網域名稱類型：*加速網域名稱*、*來源站點網域名稱*或*自訂網域名*。

> **說明** 如果您的一個IP來源站點綁定了多個網域名稱或網站，就需要指定**回源HOST**回到的具體網域名稱，否則回源會失敗。

回源HOST的預設值為：

- 如果來源站點是 **IP**類型，回源HOST預設為*加速網域名稱*。
- 如果來源站點是 **OSS來源站點**類型，回源HOST預設為*來源站點網域名稱*。

來源站點和回源HOST的區別：

- 來源站點： 來源站點決定了回源時，請求到的具體IP。
- 回源HOST：回源HOST決定了回源請求訪問到該IP上的具體網站。

> **說明** 目前不支援SNI回源。

配置引導

1. 進入CDN**網域名稱管理**頁，選擇網域名稱，單擊**管理**。
2. 單擊**內容回源**。
3. 在**回源HOST**項，單擊**修改配置**。
4. 開啟**回源HOST**，並選擇**網域名稱類型**。單擊**確定**，配置成功。

執行個體

例一

如果你的來源站點是標題來源站 `www.a.com` ，且將回源HOST設定為 `www.b.com` ， 則實際回源的是 `www.a.com` 解析到的IP網站 `www.b.com` 。

例二

如果您的來源站點是IP來源站點 `1.1.1.1` ，且將回源HOST設定為 `www.b.com` ，則實際回源的是 `1.1.1.1` 對應的主機上的網站 `www.b.com` 。

6.3. 協議跟隨回源

功能介紹

開啟該功能後，回源使用協議和用戶端訪問資源的協議保持一致，即如果用戶端使用 HTTPS 方式請求資源，當節點上未緩衝該資源時，會使用相同的 HTTPS 方式回源擷取資源；同理類似 HTTP 協議的請求。

> **說明** 來源站點需要同時支援 80 連接埠和 443 連接埠，否則有可能會造成回源失敗。

配置說明

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**回源配置 > 靜態協議跟隨回源**開啟功能。
3. 您可以選擇跳轉類型：**跟隨**、**HTTP**或**HTTPS**。

6.4. 私人bucket回源授權

功能介紹

私人bucket回源授權是指若加速網域名稱想要回源至該使用者帳號下標記為私人的bucket時，需要首先進行授權，授權成功並開啟授權配置後，使用者開啟了私人bucket授權的網域名稱有許可權訪問私人bucket。

您可以配合使用cdn提供的refer防盜鏈功能，鑒權等功能，有效保護您的資源安全。

> **警告**
> - 授權成功並開啟了對應網域名稱的私人bucket功能，該加速網域名稱可以訪問您的私人bucket內的資源內容。開啟該功能前，請根據實際的業務情況，謹慎決策。若您授權的私人bucket內容並不適合作為CDN加速網域名稱的回源內容，請勿授權或者開啟該功能。
> - 若您的網站有攻擊風險，請購買高防服務，請勿授權或開啟私人bucket功能。

操作步驟

如何開啟私人bucket回源授權？

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**回源配置 > 私人Bucket回源設定**中，開啟該功能。
3. 單擊**立即授權**。
4. 授權成功，為該網域名稱開啟私人bucket回源配置，單擊**確定**。
5. 設定成功。

如何關閉私人bucket回源授權？

> **說明** 若您的加速網域名稱正在使用私人bucket做為來源站點進行回源，請不要關閉或刪除私人bucket授權。

1. 進入**存取控制 > 角色管理**。
2. 刪除**AliyunCDNAccessingPrivateOSSRole**授權。
3. 私人bucket授權刪除成功。

6.5. 配置回源SNI

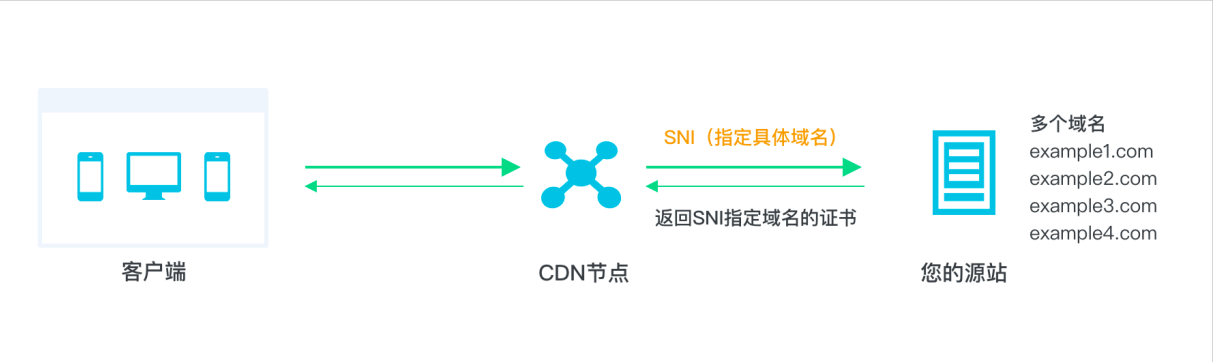
如果您的來源站點IP綁定了多個網域名稱，且CDN回源協議為HTTPS時（443連接埠回源），需配置回源SNI，來指明所請求的具體網域名稱，並使伺服器根據該網域名稱正確地返回對應的認證。

背景信息

SNI（Server Name Indication）是對SSL/TLS協議的擴充，允許伺服器在單個IP地址上承載多個SSL認證，可解決一個HTTPS伺服器擁有多個網域名稱但是無法預知用戶端到底請求的是哪一個網域名稱的服務的問題。開啟SNI後，在用戶端發起TLS握手請求時，伺服器會根據配置的SNI資訊從指定的網域名稱擷取資源，同時返回正確的認證給用戶端。

> 注意
>
> - 來源站點的服務端需要支援CDN節點發起的TLS握手請求包含的SNI資訊的解析能力。
> - 如果加速網域名稱配置了多個來源站點，通過控制台配置SNI功能，所有來源站點地址會共用一個回源SNI值，那麼回源請求都會指向SNI值對應的網域名稱。如果您希望不同的來源站點，配置不同的SNI值，您可以 申請。

回源SNI的工作原理如下圖所示。



回源SNI的工作流程如下：

1. 當CDN節點以HTTPS協議訪問來源站點時，需要在SNI中指定訪問的具體網域名稱。
2. 來源站點接收到請求後，根據SNI中記錄的網域名稱，返回對應網域名稱的認證。
3. CDN節點收到認證，與伺服器端建立安全連線。

操作步驟

1.
2.
3.
4.
5. 在 **配置**頁簽下找到 **回源SNI**，單擊 **修改配置**。
6. 在 **回源SNI**對話方塊，開啟 **回源SNI开关**，輸入您希望用戶端從哪個網域名稱擷取資源的網域名稱名稱（例如：cdn.console.aliyun.com）。

> 說明 回源SNI配置的值只能是精確網域名稱，不能是泛網域名稱。

7. 單擊 **确认**，完成配置。

相關文檔

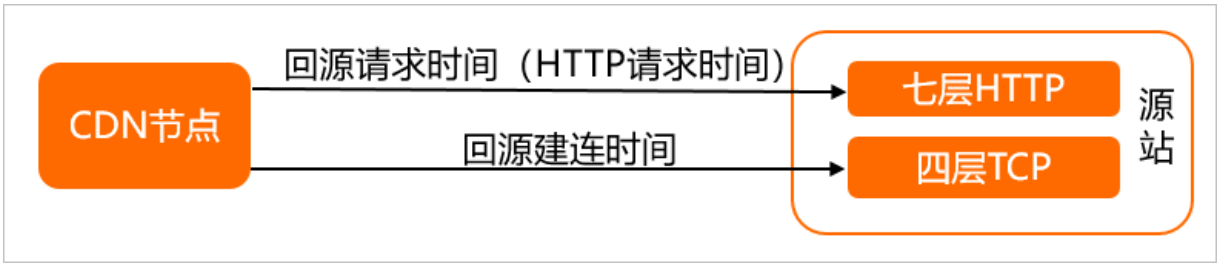
- 大量設定網域名稱

6.6. 配置回源請求逾時時間

阿里雲CDN回來源站點請求資源時，預設請求逾時時間為30秒，若逾時，會出現回源失敗的情況。您可以根據來源站點資料處理速度及網路情況，合理配置回源請求逾時時間，保障正常回源。通過本文，您可以瞭解配置回源請求逾時時間的操作步驟。

背景信息

回源請求時間指的是，CDN回源時，七層HTTP請求時間，不包括回源建連時間（即四層TCP連線時間）。



操作步驟

1.
2.
3.
4.
5. 在 **回源HTTP请求超时时间** 地區，單擊 **修改配置**。
6. 在 **回源HTTP请求超时时间** 對話方塊，設定 逾時時間 。
7. 單擊 **确认** 完成配置。

相關文檔

- 大量設定網域名稱

6.7. 配置回源302跟隨

CDN節點未配置回源302跟隨時，收到來源站點返回的302狀態代碼將直接轉寄給使用者。配置回源302跟隨功能後，CDN節點會代替使用者直接處理302狀態代碼的內容，可減少處理流程，加快使用者擷取資源的速度。

前提條件

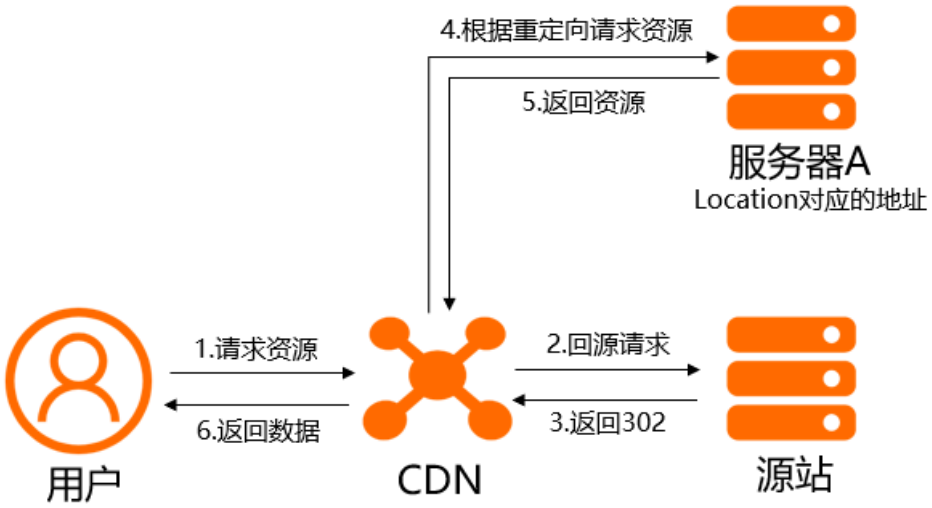
使用者來源站點使用了302重新導向方式去實現商務邏輯。

背景信息

302是HTTP協議中的一個狀態代碼，代表已存在的資源被臨時改變了位置，導致使用者無法訪問到對應的資源。基於此情況，伺服器通常會在訊息回應標頭中加入Location參數，當用戶端接收到帶有Location頭的響應時，會跳轉到Location對應的地址去請求資源。

工作原理

回源302跟隨功能指CDN節點回源請求資源時，如果收到來源站點返回的302狀態代碼，將由CDN節點代替使用者直接處理302狀態代碼的內容，即直接跳轉到來源站點302響應中的Location地址去擷取資源，不會直接返回302狀態代碼給使用者。



1. 使用者向CDN節點請求訪問 `http://example.com/test.jpg` 檔案。
2. CDN節點上未緩衝該檔案，CDN節點回來源站點請求該檔案。
3. 來源站點收到請求後，向CDN節點返回302狀態代碼，Location地址指向 `http://www.example.com/test.jpg` 。
4. CDN節點收到來源站點的響應後，直接向Location地址 `http://www.example.com/test.jpg` 發起請求。
5. CDN節點擷取到所需資源後，緩衝到CDN節點上。
6. CDN節點將擷取到的資源返回給使用者。

此時，如果其他使用者再請求訪問 `http://example.com/test.jpg` 檔案，會直接在CDN節點命中緩衝並返回給使用者。

操作步驟

1.
2.
3.
4. 在指定網域名稱的左側導覽列，單擊 **回源配置**。
5. 在 **配置** 頁簽，找到 **回源302跟隨** 。
6. 開啟 **回源302跟隨** 開關。
7. 配置回源302跟隨。

參數	描述

參數	描述
回源次數上限	○ 回源次數上限 指在一次使用者請求過程中，CDN節點可以回源訪問來源站點的最大次數。回源次數上限預設值為2，最小值為1，最大值為6。 ○ 回源302跟隨次數上限=回源次數上限-1 指在一次使用者請求過程中，CDN節點可以跟隨Location地址跳轉訪問的最大次數，超出限制將直接返回302狀態代碼給使用者。回源302跟隨次數上限預設值為1，最小值為0，最大值為5。
302跟隨保留參數	○ 保留：302跟隨時保留原請求參數回目標來源站點，將特定的參數資訊傳遞給Location地址對應的伺服器。 ○ 不保留：302跟隨時不保留原請求參數回目標來源站點。
302跟隨保留要求標頭	○ 保留：302跟隨時保留原要求標頭回目標來源站點，將要求標頭資訊傳遞給Location地址對應的伺服器。 ○ 不保留：302跟隨時不保留原要求標頭回目標來源站點。

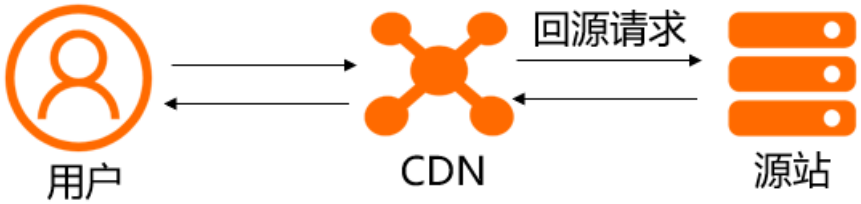
8. 單擊 **確定** ，完成配置。

6.8. 配置回源HTTP要求標頭

HTTP訊息頭準確描述了正在擷取的資源、伺服器或用戶端的行為，定義了HTTP事務中的具體巨集指令引數。如果您的回源商務邏輯需要通過配置HTTP要求標頭來實現時，可以閱讀本文瞭解如何添加、修改或刪除回源HTTP要求標頭。

背景信息

HTTP訊息頭是指在超文字傳輸通訊協定 (HTTP)（ Hypertext Transfer Protocol，HTTP）的請求和響應訊息中，協議頭部的組件。在HTTP訊息頭中，按其出現的上下文環境，分為通用頭、要求標頭、回應標頭等。



說明 目前CDN提供了新版的配置回源HTTP要求標頭功能，具體操作，請參見 配置回源HTTP要求標頭（新）。

操作步驟

1.
2.
3.

4.
5. 單擊 **回源HTTP请求头**頁簽。
6. 單擊 **添加**。
7. 在 **回源HTTP请求头**頁面，選擇 **自定义回源头**，設定 **自訂參數** 和 **取值**。

   如果要修改或刪除已添加的參數，可以單擊對應參數巨集指令清單下的 **修改**或 **删除**。
8. 單擊 **确认**。

後續操作

當您在配置 **回源HTTP请求头**時，如果選擇 **参数**為 **自訂參數** ，則配置自訂參數後，系統可能報錯，如下圖所示。原因是您配置的欄位是內部保留欄位，請您重新設定。

相關文檔

- 大量設定網域名稱

6.9. 配置回源HTTP要求標頭（新）

如果您需要改寫使用者回源請求中的HTTP Header，可以通過配置回源HTTP要求標頭實現。可根據您的實際業務需求，選擇增加、刪除、變更或替換回源HTTP要求標頭。

背景信息

HTTP要求標頭是HTTP的請求訊息頭的組成部分之一，可攜帶特定請求參數資訊並傳遞給伺服器。

當CDN節點上沒有緩衝使用者請求的內容時，CDN節點會回來源站點拉取資源，來源站點可擷取到CDN節點回源要求標頭中攜帶的資訊。為了便於來源站點識別使用者資訊，您可以配置回源HTTP要求標頭（新）功能，改寫使用者回源請求中的HTTP Header資訊，攜帶特定的參數資訊給來源站點。例如，通過X-Forward-For頭部攜帶真實用戶端IP至來源站點。

> **說明**
>
> - 回源請求指使用者請求中通過CDN回源的HTTP訊息。回源HTTP要求標頭配置只會影響通過CDN回源的HTTP訊息，對於CDN節點直接響應給使用者的HTTP訊息不做修改。
> - 不支援對泛網域名稱配置回源HTTP要求標頭。

操作步驟

1.
2.
3.
4.
5. 單擊 **回源HTTP要求標頭（新）** 頁簽。
6. 單擊 **添加**。
7. 配置回源HTTP要求標頭資訊。

> **注意** 當不同的操作方式同時作用於同一個回源要求標頭參數時，會存在操作衝突。此時按照操作類型的優先順序來執行，優先順序順序為 **替換** > **增加** > **變更** 和 **刪除** 。例如，當增加和刪除操作同時作用於同一個參數時，會先增加再刪除。

- 增加要求標頭參數

配置項	樣本	說明
请求头操作	增加	在回源HTTP請求中增加指定的要求標頭參數。
自定义请求头参数	自訂回源要求標頭	選擇 **自定义回源请求头** 或選擇已經預設好的要求標頭參數。
定义请求头名称	x-code	自訂要求標頭名稱為x-code。
请求头值	key1, key2	一個要求標頭參數中可以配置多個值，多個值用英文逗號（,）分隔。
是否允许重复	允許	■ **允许**：可以添加重複的要求標頭參數。例如 `x-code:key1` ， `x-code:key2` 。 ■ **不允许**：添加同一個要求標頭參數，新值將覆蓋舊值。例如先添加 `x-code:key1` ，再添加 `x-code:key2` ，最終的值為 `x-code:key2` 。

- 刪除要求標頭參數

配置項	樣本	說明
请求头操作	刪除	刪除所有與要求標頭參數名稱匹配的參數值，無論是否有重複的要求標頭參數。
请求头操作	自訂回源要求標頭	選擇 **自定义回源请求头** 或選擇已經預設好的要求標頭參數。
请求头操作	x-code	自訂要求標頭名稱為x-code。

- 變更要求標頭參數

配置項	樣本	說明
请求头操作	變更	當要求標頭參數不存在重複時，可以正常變更參數，如果有多個重複的要求標頭參數，則不允許變更。

配置項	樣本	說明
自定义请求头参数	自訂回源要求標頭	選擇 **自定义回源请求头** 或選擇已經預設好的要求標頭參數。
自定义请求头名称	x-code	自訂要求標頭名稱為x-code。
请求头变更为	key1, key3	一個要求標頭參數中可以配置多個值，多個值用英文逗號（,）分隔。

- 替換要求標頭參數

配置項	樣本	說明
请求头操作	替換	當要求標頭參數不存在重複時，可以正常替換參數，如果有多個重複的要求標頭參數，則不允許替換。
自定义请求头参数	自訂回源要求標頭	選擇 **自定义回源请求头** 或選擇已經預設好的要求標頭參數。
自定义请求头名称	x-code	自訂要求標頭名稱為x-code。
查找	key	Regex尋找需要替換的參數值。
替换为	abc	Regex替換需要替換的參數值。
匹配	匹配所有	■ **匹配所有**：所有匹配上的值都會被替換。例如 `x-code:key1,key2,key3` ，正則匹配值key替換為abc，替換後的結果為 `x-code:abc1,abc2,abc3` 。 ■ **仅匹配第一个**：只有第一個匹配上的值會被替換。例如 `x-code:key1,key2,key3` ，正則匹配值key替換為abc，替換後的結果為 `x-code:abc1,key2,key3` 。

8. 單擊 **确定** 请求头变更为。

相關文檔

- 大量設定網域名稱

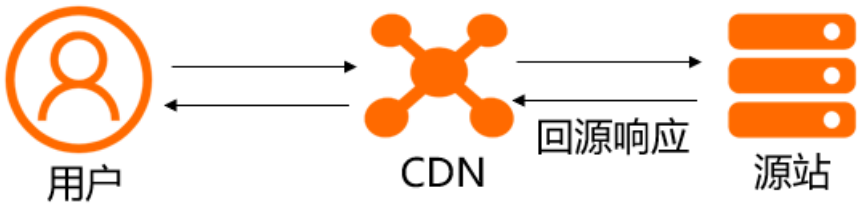
6.10. 配置回源HTTP回應標頭

如果您需要改寫使用者來源站點響應報文中的HTTP Header，可以通過配置回源HTTP回應標頭實現。可根據您的實際業務需求，選擇增加、刪除、變更或替換回源HTTP回應標頭。

背景信息

HTTP回應標頭是HTTP的響應訊息頭的組成部分之一，可攜帶特定響應參數資訊並傳遞給用戶端。

當CDN節點上沒有緩衝使用者請求的內容時，CDN會回來源站點拉取資源，來源站點收到CDN的請求後會給出響應。為了便於使用者識別來源站點的響應資訊，您可以配置回源HTTP回應標頭功能，改寫使用者來源站點響應報文中的HTTP Header資訊。例如，改寫回源回應標頭中Content-Type參數的值，然後再傳遞給用戶端，以確保用戶端解析正常（如果來源站點返回的Content-Type值有誤，用戶端直接解析將出現亂碼，因此需要在CDN上改寫）。



> **說明**
> - 回源響應指來源站點收到CDN節點的請求後，返回給CDN節點的HTTP訊息。回源HTTP回應標頭配置只會影響來源站點響應給CDN節點的HTTP訊息，對於CDN節點直接響應給使用者的HTTP訊息不做修改。
> - 不支援對泛網域名稱配置回源HTTP回應標頭。

操作步驟

1.
2.
3.
4.
5. 單擊 **回源HTTP响应头** 頁簽。
6. 單擊 **添加**。
7. 配置回源HTTP回應標頭資訊。

> **注意** 當不同的操作方式同時作用於同一個回源回應標頭參數時，會存在操作衝突。此時按照操作類型的優先順序來執行，優先順序順序為 **替換** > **增加** > **變更** 和 **刪除** 。例如，當增加和刪除操作同時作用於同一個參數時，會先增加再刪除。

- 增加回應標頭參數

配置項	樣本	說明
响应头操作	增加	在回源HTTP請求中增加指定的回應標頭參數。
自定义响应头参数	自訂緩衝回應標頭	選擇 **自訂緩衝回應標頭** 或選擇已經預設好的回應標頭參數。
自定义响应头名称	x-code	自訂回應標頭名稱為x-code。
响应头值	key1	一個回應標頭參數中可以配置多個值，多個值用英文逗號（,）分隔。
	key1，key2	

配置項	樣本	說明
是否允许重复	允許	■ **允许**：可以添加重複的回應標頭參數。例如 `x-code:key1`，`x-code:key2`。 ■ **不允许**：添加同一個回應標頭參數，新值將覆蓋舊值。例如先添加 `x-code:key1`，再添加 `x-code:key2`，最終的值為 `x-code:key2`。

- 刪除回應標頭參數

配置項	樣本	說明
响应头操作	刪除	刪除所有與回應標頭參數名稱匹配的參數值，無論是否有重複的回應標頭參數。
自定义响应头参数	自訂緩衝回應標頭	選擇 **自訂緩衝回應標頭** 或選擇已經預設好的回應標頭參數。
自定义响应头名称	x-code	自訂回應標頭名稱為x-code。

- 變更回應標頭參數

配置項	樣本	說明
响应头操作	變更	當回應標頭參數不存在重複時，可以正常變更參數，如果有多個重複的回應標頭參數，則不允許變更。
自定义响应头参数	自訂緩衝回應標頭	選擇 **自訂緩衝回應標頭** 或選擇已經預設好的回應標頭參數。
自定义响应头名称	x-code	自訂回應標頭名稱為x-code。
响应头变更为	key1，key3	一個回應標頭參數中可以配置多個值，多個值用英文逗號（,）分隔。

- 替換回應標頭參數

配置項	樣本	說明
响应头操作	替換	當回應標頭參數不存在重複時，可以正常替換參數，如果有多個重複的回應標頭參數，則不允許替換。
自定义响应头参数	自訂緩衝回應標頭	選擇 **自訂緩衝回應標頭** 或選擇已經預設好的回應標頭參數。

配置項	樣本	說明
自定义响应头名称	x-code	自訂回應標頭名稱為x-code。
查找	key	Regex尋找需要替換的參數值。
替換为	abc	Regex替換需要替換的參數值。
匹配	匹配所有	■ **匹配所有**：所有匹配上的值都會被替換。例如 `x-code:key1,key2,key3` ，正則匹配值key替換為abc，替換後的結果為 `x-code:abc1,abc2,abc3` 。 ■ **仅匹配第一个**：只有第一個匹配上的值會被替換。例如 `x-code:key1,key2,key3` ，正則匹配值key替換為abc，替換後的結果為 `x-code:abc1,key2,key3` 。

8. 單擊 。

相關文檔

- 大量設定網域名稱

6.11. 改寫回源URI

為了避免回源請求URI與來源站點URI不匹配導致的回源失敗，您可以通過配置回源URI改寫功能將回源請求URI修改為與來源站點匹配的URI，從而提升回源命中率。通過本文您可以瞭解配置重寫規則的操作步驟。

注意事項

- 單個網域名稱可以配置的 **回源URI改寫** 規則數量上限是50個。
- 規則改寫按照規則列表從上到下順序執行的，此順序可能會影響您的改寫結果。
- **回源URI改寫** 功能與 **重寫** 功能的區別在於， **重寫** 功能的作用位置是在CDN邊緣節點上面，會影響CDN內部鏈路，也會改寫緩衝key，而 **回源URI改寫** 功能的作用位置是在CDN回源節點上面，不影響CDN內部鏈路，不改寫緩衝key。
- **回源URI改寫** 功能在配置執行規則的情況下，對URL中參數的改寫可能會與 **網域名稱管理 > 效能最佳化** 頁簽下的 過濾參數（可保留指定參數） 或 過濾參數（可刪除指定參數） 功能相衝突，這三個功能同時配置的時候，需要注意避免配置衝突。

配置回源URI

1.
2.
3.
4. 在指定網域名稱的左側導覽列，單擊 **回源配置**。
5. 單擊 **回源URI改写** 頁簽。
6. 單擊 **添加**。
7. 根據您的需求，配置需要改寫的URI、目標URI和執行規則。

參數	樣本	說明
需要改寫的URI	^/hello$	以正斜線（/）開頭的URI，不含http://頭及網域名稱。支援PCRERegex。
目標URI	/hello/test	以正斜線（/）開頭的URI，不含http://頭及網域名稱。
執行規則	空	如果配置了多條規則，在匹配執行當前規則後，繼續匹配後續規則。
	break	◦ 如果配置了多條規則，若請求的URI匹配了當前規則，匹配執行完當前規則後，剩餘規則將不再匹配。 ◦ 只修改URI部分，不修改URL的參數，不影響 **回源參數改寫** 功能對URL中參數的改寫。
	enhance break	◦ 如果配置了多條規則，若請求的URI匹配了當前規則，匹配執行完當前規則後，剩餘規則將不再匹配。 ◦ 對URI中參數的改寫可能會與 回源參數改寫 功能對URL中參數的改寫相衝突，這兩個功能同時配置的時候，需要注意避免配置衝突。

8. 單擊 **確定**，使改寫規則開始執行和生效。

   您也可以在 **回源URI改寫** 頁面的規則列表中，單擊 **修改** 或 **刪除** ，對當前配置的規則進行相應操作。

範例

- **範例一：執行空規則。**

待改寫URI	^/hello$
目標URI	/index.html
執行規則	空
結果說明	原始請求：`http://domain.com/hello` 改寫後的回源請求：`http://domain.com/index.html` 該請求將會繼續匹配 **回源URI改寫** 規則列表中其餘的規則。

- **範例二：執行break規則。**

待改寫URI	^/hello.jpg$
目標URI	/image/hello.jpg
執行規則	break
結果說明	原始請求：`http://domain.com/hello.jpg` 改寫後的回源請求：`http://domain.com/image/hello.jpg` 該請求將不再繼續匹配 **回源URI改寫** 規則列表中其餘的規則。

- **範例三：執行enhance break規則。**

待改寫URI	^/hello.jpg?code=123$
目標URI	/image/hello.jpg?code=321
執行規則	enhance break
結果說明	原始請求：`http://domain.com/hello.jpg?code=123` 改寫後的回源請求：`http://domain.com/image/hello.jpg?code=321` 該請求將不再繼續匹配 **回源URI改寫** 規則列表中其餘的規則。

- **範例四：在檔案名稱是變數的情況下對根目錄添加URI首碼。**

  例如：將包含/xxx的URI（xxx代表任意檔案名稱，例如：/hello.jpg、/hello.html等等）改寫為/image/xxx，即對根目錄下的任意檔案的URI都插入路徑/image。

待改寫URI	^(.*)$ **說明** ^(.*)$代表任一字元，()代表的是一個分組，可以在目標URI中通過$1來調用分組的變數內容。
目標URI	/image$1 **說明** $1表示Regex中第一對圓括弧中的運算式匹配到的內容，$2是第二個小括弧裡面的內容，依此類推。
執行規則	break
結果說明	○ 原始請求：`http://domain.com/hello.jpg` 改寫後的回源請求：`http://domain.com/image/hello.jpg` ○ 原始請求：`http://domain.com/hello.html` 改寫後的回源請求：`http://domain.com/image/hello.html` 該請求將不再繼續匹配 **回源URI改寫** 規則列表中其餘的規則。

- **範例五：在檔案名稱是變數的情況下對指定目錄添加URI首碼。**

  例如：將包含/live/xxx的URI（xxx代表任意檔案名稱，例如：/live/hello.jpg、/live/hello.html 等等）改寫為/image/live/xxx，即對目錄/live下的任意檔案的URI都插入路徑/image。

待改寫URI	^/live/(.*)$
目標URI	/image/live/$1
執行規則	break

結果說明	○ 原始請求：`http://domain.com/live/hello.jpg` 改寫後的回源請求：`http://domain.com/image/live/hello.jpg` ○ 原始請求：`http://domain.com/live/hello.html` 改寫後的回源請求：`http://domain.com/image/live/hello.html` 該請求將不再繼續匹配 **回源URI改寫** 規則列表中其餘的規則。

相關文檔

- 大量設定網域名稱

6.12. 改寫回源參數

如果使用者發起的原始請求URL中攜帶的參數與需要發送給來源站點的參數不一致，您可以通過回源參數改寫功能改寫回源請求URL中攜帶的參數。實現忽略所有參數、添加參數、刪除參數、保留參數、修改參數等操作。

背景信息

回源參數改寫，改寫的是回源請求URL的查詢參數，支援配置多個改寫規則，優先順序為 **添加參數** > **刪除參數** > **忽略參數**和 **仅保留** > **修改參數**。當不同的改寫規則作用於同一個參數時，只有高優先順序的規則會生效。

> 說明 **忽略參數**和 **仅保留**參數互斥，不要同時配置這兩個參數。

衝突說明

回源參數改寫 與 回源URI改寫 的 `enhance break` 規則、以及 過濾參數（可保留指定參數） 和 過濾參數（可刪除指定參數） 功能可能會衝突，配置時注意避免，且後配置的功能生效。

> 說明
> - **回源參數改寫** 是在CDN回源節點上完成，不影響CDN的內部鏈路，且不改寫緩衝key。
> - **過濾參數（可保留指定參數）** 和 **過濾參數（可刪除指定參數）** 是在CDN邊緣節點上完成，會影響CDN的內部鏈路，且會改寫緩衝key。

操作步驟

1.
2.
3.

4. 在指定網域名稱的左側導覽列，單擊 **回源配置**。
5. 單擊 **回源參數改写** 頁簽。
6. 開啟 **使用回源參數改写** 開關。
7. 配置需要改寫的回源參數。

   根據實際業務需求，按照介面提示配置不同的改寫操作，您也可以在一種操作類型的文字框中添加多個參數。更多資訊，請參見 操作範例 。
8. 單擊 **确认**，改寫操作開始執行和生效。

   您也可以在 **回源參數改写** 頁面，單擊 **修改配置**，修改已配置的規則。

範例一：忽略所有參數

配置項	填寫樣本
忽略參數	開啟
添加參數	無
刪除參數	無
僅保留	無
修改參數	無
結果說明	原始請求：`http://domain.com/index.html?code1=1&code2=2&code3=3` 改寫後的回源請求：`http://domain.com/index.html`

範例二：保留指定參數

配置項	填寫樣本
忽略參數	無
添加參數	無
刪除參數	無
僅保留	code2
修改參數	無
結果說明	原始請求：`http://domain.com/index.html?code1=1&code2=2&code3=3` 改寫後的回源請求：`http://domain.com/index.html?code2=2`

範例三：添加參數+刪除參數+修改參數

配置項	填寫樣本
忽略參數	無

配置項	填寫樣本
添加參數	code4=4
刪除參數	code2
僅保留	無
修改參數	code3=0
結果說明	原始請求：`http://domain.com/index.html?code1=1&code2=2&code3=3` 改寫後的回源請求：`http://domain.com/index.html?code1=1&code3=0&code4=4`

相關文檔

- 大量設定網域名稱

7.節點緩衝設定

7.1. 緩衝概述

您使用CDN加速靜態資源時，CDN會將來源站點上的資源緩衝到距離用戶端最近的CDN節點上。當您訪問該靜態資源時，可直接從CDN的緩衝節點上擷取，有效避免通過較長的鏈路回源，提高資源訪問效率。

預設緩衝時間

如果您的來源站點和CDN控制台上均沒有配置緩衝策略，此時將遵循阿里雲CDN的預設緩衝規則。CDN的預設緩衝時間最短為10秒，最長為3600秒，您可以在CDN控制台修改預設緩衝時間。具體操作，請參見 緩衝配置。

> **說明** 設定的緩衝時間長短會導致回源流量不一樣，回源費用也有所不同，建議根據不同的業務需求設定緩衝時間長度。設定的緩衝時間過短，會導致CDN頻繁回源，從而增加來源站點的流量消耗。

- 預設緩衝時間計算方法：t=（curtime-last_modified）×0.1。
- 預設緩衝時間取值範圍：[10,3600]。

參數說明如下：

- t：預設緩衝時間，單位為秒。
- curtime：目前時間。
- last_modified：伺服器上資源的最後修改時間。

舉例說明如下：

- 當對象 `last-modified` 為 `20140801 00:00:00`，目前時間為 `20140801 00:01:00` 時，（curtime-last_modified）×0.1=6s，則預設緩衝時間為10s，因為最小緩衝時間為10s。
- 當對象 `last-modified` 為 `20140801 00:00:00`，目前時間為 `20140802 00:00:00` 時，（curtime-last_modified）×0.1=8640s，則預設緩衝時間為3600s，因為最大緩衝時間為3600s。
- 當對象 `last-modified` 為 `20140801 00:00:00`，目前時間為 `20140801 00:10:00` 時，（curtime-last_modified）×0.1=60s，則預設緩衝時間為60s。

預設緩衝規則

- 如果來源站點返回的資料中沒有 `last-modified` 回應標頭，有 `ETag`，則認為該對象為靜態資源，CDN會將其預設緩衝時間設定為10秒。
- 如果來源站點返回的資料中沒有 `last-modified` 回應標頭，也沒有 `ETag`，則認為該對象為動態資源，CDN會將其預設緩衝時間設定為0，即不緩衝，每次都回源擷取資源。

> **說明** `ETag` 表示資源標識。

緩衝相關功能

通過緩衝配置功能，您可以對網域名稱執行如下操作。

功能	說明

功能	說明
緩衝配置	您可以針對靜態資源配置指定目錄和檔案尾碼名的緩衝到期時間，使其在CDN上按照緩衝規則進行緩衝。
配置狀態代碼到期時間	您可以配置資源的指定目錄或檔案尾碼名的狀態代碼到期時間。
配置自訂HTTP回應標頭	您可以配置資源緩衝到期的HTTP訊息頭。
自訂錯誤頁面	您可以根據所需自訂HTTP或HTTPS響應狀態代碼跳轉的完整URL地址。
配置URI重寫規則	您可以對請求的URI進行修改，實現302重新導向到目標URI。
自訂Cachekey	您可以將訪問同一個檔案的一類請求轉化為統一的Cachekey，避免不同請求緩衝為不同檔案的問題，降低回源頻率。
配置跨域資源共用	您可以通過自訂HTTP回應標頭功能配置跨域資源共用。

7.2. 緩衝配置

功能介紹

- 該功能可以針對不同**目錄路徑**和**檔案名稱尾碼**的資源進行快取服務器行為的設定，使用者可自訂指定資源內容的緩衝到期時間規則。
- 支援使用者自訂緩衝策略優先順序。
- Cache的預設緩衝策略。

> 說明
> - 用於設定檔到期時間，在此配置的優先順序會高於來源站點配置。如果來源站點未配置cache配置，支援按目錄、檔案尾碼兩種方式設定（支援設定完整路徑緩衝策略）。
> - CDN的緩衝是有可能由於熱度較低被提前剔除出CDN節點的。

注意事項

- 對於不經常更新的靜態檔案，建議將緩衝時間設定為1個月以上（eg：圖片類型，應用下載類型）；
- 對於需要更新並且更新很頻繁的靜態檔案，可以將緩衝時間設定短些，視業務情況而定（eg：js,css等）；
- 對於動態檔案（eg：php|jsp|asp），建議設定緩衝時間為0s，即不緩衝；若動態檔案例如php檔案內容更新頻率較低，推薦設定較短緩衝時間；
- 建議來源站點的內容不要使用同名更新，以版本號碼的方式方步，即採用img-v1.0.jpg、img-v2.1.jpg的命名方式。

操作步驟

1. 進入CDN網域名稱概覽頁，選擇網域名稱進入**網域名稱管理**頁面，緩衝配置。
2. 單擊**修改配置**，可以管理緩衝規則，添加、修改、刪除。
3. 單擊**添加**，增加緩衝規則，按目錄或者按檔案尾碼。

4.

舉例：為加速網域名稱 `example.aliyun.com` 設定三則緩衝配置規則：

- 緩衝策略1：檔案名稱尾碼為jpg、png的所有資源 到期時間為1月，權重設定為90。
- 緩衝策略2：目錄為/www/dir/aaa 到期時間為1小時，權重設定為70。
- 緩衝策略3：完整路徑為/www/dir/aaa/example.php 到期時間為0s，權重設定為80。

則這三個緩衝策略的生效順序是：策略1—>策略3—>策略2。

> **說明**
> - 權重可設定1-99數字越大，優先順序越高，優先生效；
> - 不推薦設定相同的權重，權重相同的兩條緩衝策略優先順序隨機。

7.3. 配置狀態代碼到期時間

您可以針對靜態資源配置指定目錄或檔案尾碼名的狀態代碼到期時間，實現由CDN節點直接響應狀態代碼，減輕來源站點壓力。本文為您介紹如何配置狀態代碼到期時間。

適用情境

正常情況下CDN節點成功從來源站點擷取到所請求的資源，即來源站點響應了2xx狀態代碼時，會按照CDN節點配置的緩衝到期規則進行處理。如果來源站點無法迅速響應所有狀態代碼（例如非2xx狀態代碼），且不希望所有請求全部由來源站點響應，可以配置狀態代碼到期時間，由CDN節點直接響應狀態代碼，減輕來源站點壓力。

> **說明**
> - 對於303、304、401、407、600和601狀態代碼，CDN不進行緩衝。
> - 對於204、305、400、403、404、405、414、500、501、502、503和504狀態代碼，如果來源站點響應了Cache-Control，則遵循來源站點的Cache-Control規則；如果未設定狀態代碼到期時間，緩衝時間預設為1秒。

操作步驟

1.
2.
3.
4.
5. 單擊 **状态码过期时间** 頁簽。
6. 單擊 **添加**，配置狀態代碼到期時間。

類型	注意事項

類型	注意事項
类型	支援 **目录**和 **文件名后缀**這兩種類型，請根據您的實際需求選擇。 **說明** 如果您同時配置了目錄和檔案尾碼名這兩種類型的狀態代碼到期時間，CDN會按照配置的先後順序進行匹配，先配置的類型會優先生效，規則生效後將不會再繼續匹配其他的規則。
地址	○ 類型選擇為 **目錄** ，填寫說明如下： ■ 每次只能添加一條目錄。 ■ 支援輸入目錄的完整路徑，須以正斜線（/）開頭，例如 */directory/aaa* 。 ○ 類型選擇為 **檔案尾碼名** ，填寫說明如下： ■ 支援輸入一個或多個檔案尾碼名，多個檔案尾碼名用半形逗號（,）分隔，例如 `JPG,TXT` 。 ■ 不支援用星號（*）匹配所有的檔案類型。
状态码过期时间设置	○ 支援設定4xx和5xx模糊比對對應的系列狀態代碼的到期時間，單位為秒，多個狀態代碼用半形逗號（,）分隔。例如4xx=10,5xx=15。 ○ 不支援設定2xx和3xx模糊比對對應的系列狀態代碼的到期時間，但支援設定201、302等精確狀態代碼的到期時間，單位為秒。例如201=10,302=15。

7. 單擊 **確定**，完成配置。

   成功配置狀態代碼到期時間後，您可以在 **状态码过期时间**列表中，對當前的配置進行 **修改**或 **操作**操作。

相關API

BatchSetCdnDomainConfig

7.4. 配置自訂HTTP回應標頭

HTTP回應標頭是HTTP訊息頭中的其中一個部分，HTTP訊息頭準確地描述了正在擷取的資源、伺服器或用戶端的行為，定義了HTTP事務中的具體巨集指令引數。通過配置自訂HTTP回應標頭，當您請求加速網域名稱下的資源時，可以在返回的響應訊息中添加您配置的回應標頭，以實現跨域訪問。

背景信息

HTTP訊息頭是指在超文字傳輸通訊協定 (HTTP)HTTP（Hypertext Transfer Protocol）的請求和響應訊息中，協議頭部的組件。在HTTP訊息頭中，按其出現的上下文環境分為通用頭、要求標頭和回應標頭等。

跨域資源共用CORS（Cross-Origin Resource Sharing）簡稱跨域訪問，是HTML5提供的標準跨域解決方案，允許Web應用伺服器進行跨域存取控制，使得跨域資料轉送得以安全進行。

適用情境

當您的業務使用者請求業務資源時，您可以在返回的響應訊息中配置回應標頭，以實現跨域訪問。當CDN收到一個跨域請求時，會讀取CDN上對應的CORS規則，然後進行相應的許可權檢查。CDN會依次檢查每一條規則，使用第一條匹配的規則來允許請求並返回對應的Header。如果所有規則都匹配失敗，則不附加任何CORS相關的Header。

HTTP回應標頭的配置屬於網域名稱維度配置，一旦配置生效，便會對網域名稱下所有資源的響應訊息生效。配置HTTP回應標頭僅影響用戶端（例如瀏覽器）的響應行為，不會影響到CDN節點的緩衝行為。泛網域名稱暫不支援配置自訂HTTP回應標頭。

操作步驟

1.
2.
3.
4.
5. 單擊 **自定义HTTP响应头**頁簽。
6. 單擊 **添加**，配置自訂HTTP回應標頭。

   下面以增加自訂HTTP回應標頭為例，為您介紹配置方法。

參數	說明
响应头操作	您可以增加、刪除、變更和替換指定的回應標頭。
自定义响应头参数	選擇自訂回應標頭參數。詳細資料，請參見 回應標頭參數。
自定义响应头名称	當自訂回應標頭參數選擇為 **自訂** 時，需要配置自訂回應標頭名稱。自訂回應標頭名稱要求如下： ○ 由大小寫字母、短劃線（-）和數字組成。 ○ 長度為1~100個字元。
响应头值	輸入您要設定的回應標頭值。詳細資料，請參見 回應標頭參數。
是否允许重复	○ **允许**：允許重複將會保留來源站點返回的頭，同時會加上一個同名的頭。 ○ **不允许**：如果不允許重複，來源站點返回的頭會被新配置的同名頭覆蓋。

參數	說明
跨域校正	跨域校正預設為關閉狀態，只有在 **响应头操作** 為“增加”， **自定义响应头参数** 為“Access-Control-Allow-Origin”的時候才可以配置。 ○ **開啟** ：開啟狀態下CDN節點將按以下規則對使用者做跨域校正，並根據校正結果響應“Access-Control-Allow-Origin”的值。 ○ **關閉** ：關閉狀態下CDN節點不會校正使用者請求中攜帶的Origin頭，只會固定響應已配置的Access-Control-Allow-Origin值。 **說明** 跨域校正規則： ○ 如果自訂回應標頭參數“Access-Control-Allow-Origin”的值設定為“*”不論使用者請求裡面是否攜帶“Origin”參數，也不論攜帶的“Origin”參數為何值，都固定返回“Access-Control-Allow-Origin:*”。 ○ 如果跨域資源共用的回應標頭值設定了單個或者多個值（多個值之間用“,”分隔）。 ■ 如果使用者要求標頭裡攜帶的“Origin”參數值與被設定的任意一個值精確匹配，就會響應對應的跨域頭。 ■ 如果都沒有精確匹配上，則不響應跨域頭。 ○ 如果跨域資源共用的回應標頭值設定了泛網域名稱，則會校正要求標頭中Origin值是否能匹配上“Access-Control-Allow-Origin”的泛網域名稱。 配置樣本請參見配置跨域資源共用。

7. 單擊 **確定**，完成配置。

   成功配置自訂HTTP回應標頭後，您可以在 **自定义HTTP响应头** 列表中，對當前的配置進行 **修改** 或 **刪除** 操作。

回應標頭參數

回應標頭參數	說明	樣本
自訂	支援添加自訂回應標頭。自訂回應標頭名稱要求如下： • 由大小寫字母、短劃線（-）和數字組成。 • 長度為1~100個字元。	Test-Header
Cache-Control	指定用戶端程式請求和響應遵循的緩衝機制。	no-cache
Content-Disposition	指定用戶端程式把請求所得的內容存為一個檔案時提供的預設的檔案名稱。	examplefile.txt
Content-Type	指定用戶端程式響應對象的內容類型。	image

回應標頭參數	說明	樣本
Pragma	Pragma HTTP 1.0是用於實現特定指令的回應標頭，具有通過請求和響應鏈實現各種效果的功能，可用於相容HTTP 1.1。	no-cache
Access-Control-Allow-Origin	指定允許的跨域請求的來源。填寫星號（*）表示全部網域名稱；您也可以填寫完整網域名稱，例如 `http://www.aliyun.com` 。 **說明** • 回應標頭值支援配置為“*”，表示任意來源。 • 回應標頭值非“*”的情況下，支援配置單個或者多個IP、網域名稱、或者IP和網域名稱混合。相互間用“,”分隔。 • 回應標頭值非“*”的情況下，必須包含協議頭“http:// ”或者“https://”。 • 回應標頭值支援攜帶連接埠。 • 回應標頭值支援泛網域名稱。	• * • http://www.aliyun.com
Access-Control-Allow-Methods	指定允許的跨域要求方法。可同時設定多個方法，多個方法用英文逗號（,）分隔。	POST,GET
Access-Control-Allow-Headers	指定允許的跨域請求欄位。	X-Custom-Header
Access-Control-Expose-Headers	指定允許訪問的自訂頭資訊。	Content-Length
Access-Control-Allow-Credentials	該回應標頭表示是否可以將對請求的響應暴露給頁面。 • 返回true：表示可以暴露。 • 返回其他值：表示不可以暴露。	true
Access-Control-Max-Age	指定用戶端程式對特定資源的預請求返回結果的緩衝時間，單位為秒。	600

相關API

BatchSetCdnDomainConfig

7.5. 自訂錯誤頁面

功能介紹

客戶可以自行定義狀態代碼時返回的頁面，最佳化使用者體驗。提供三種選項：預設頁面、自訂頁面。

以返回碼 404為例：

- 預設值：http 響應返回 404 時，伺服器返回預設 404 Not Found頁面。

- 公益404，http 響應返回 404 時，將會跳轉到即時更新的公益主題 404 頁面，查看公益404頁面。
- 自訂404，http 響應返回 404 時，將會跳轉到自行設計和編輯的 404 頁面，需要自訂跳轉頁的完整URL地址。

注意事項

- 公益 404 頁面屬於阿里雲公益資源，不會造成使用者的任何流量費用，完全免費。
- 自訂頁面屬於個人資源，按照正常分發計費。

操作步驟

1. 進入CDN網域名稱概覽頁，選擇網域名稱進入**網域名稱配置**頁面，設定**自訂錯誤頁面**功能。
2. 單擊**修改配置**，可以查看和管理當前自訂錯誤頁面列表。
3. 單擊**添加**，增加自訂返回碼的頁面內容。

若選擇**自訂 404**選項，將該頁面資源如其他靜態檔案一樣儲存到來源站點網域名稱下，並通過加速網域名稱訪問即可，只需填寫完整的加速網域名稱URL（包含http://）。

例如：加速網域名稱為 `exp.aliyun.com` 404頁面為 `error404.html` ，並將 `error404.html` 頁面儲存到來源站點中選擇“自訂404”，填寫： `http://exp.aliyun.com/error404.html` 即可。

7.6. 配置URI重寫規則

如果您訪問的URI與來源站點URI不匹配，則需要將URI修改為與來源站點匹配的URI。您修改URI中的指定參數時，需要配置URI重寫規則，規則匹配後會302重新導向到目標URI。

適用情境

如果您需要將實際訪問的URI修改為與來源站點匹配的URI，您可以通過配置重寫功能，將實際訪問的URI 302重新導向到目標URI。例如，某些使用者或用戶端仍使用HTTP協議訪問 `www.example.com/hello` ，您配置重寫功能後，所有 `www.example.com/hello` 的請求都會重新導向到 `www.example.com/index.html` 。

操作步驟

1.
2.
3.
4.
5. 單擊 **重写**頁簽。
6. 單擊 **添加**，根據您的實際需求，配置待重寫URI、目標URI和執行規則。

> **說明**
>
> - 單個網域名稱最多可以配置50條重寫規則。
> - 待重寫URI和目標URI均支援Regex，但不支援大括弧（ `{ }` ），配置含有大括弧（ `{ }` ）的規則將不生效。

參數	說明
待重写URI	以正斜線（/）開頭的URI，不含http://頭及網域名稱。支援PCRERegex，例如：^/hello$。
目标URI	以正斜線（/）開頭的URI，不含http://頭及網域名稱，例如：/index.html。
执行规则	支援 **Redirect** 和 **Break** 這兩種規則。 ○ **Redirect** ：如果請求的URI匹配了當前規則，該請求將被302重新導向到目標URI。 ○ **Break** ：如果請求的URI匹配了當前規則，執行完當前規則後將不再匹配剩餘規則。

7. 單擊 **確定**，完成配置。

   成功配置重寫功能後，您可以在 **重写**列表中，對當前的配置進行 **修改**或 **删除**操作。

配置樣本

樣本	待重寫URI	目標URI	執行規則	結果說明
樣本一	/hello	/index.html	Redirect	用戶端請求 `www.domain.com/hello` ，CDN節點將返回302讓用戶端重新請求 `www.domain.com/index.html` 的內容。
樣本二	^/$	/index.html	Redirect	用戶端請求 `www.domain.com/` ，CDN節點將返回302讓用戶端重新請求 `www.domain.com/index.html` 的內容。
樣本三	/hello	/hello/index.html	Redirect	用戶端請求 `www.domain.com/hello` ，CDN節點將返回302讓用戶端重新請求 `www.domain.com/hello/index.html` 的內容。
樣本四	^/hello$	/index.html	Break	用戶端請求 `www.domain.com/hello` ，CDN節點將返回 `www.domain.com/index.html` 的內容，且該請求不再繼續匹配剩餘規則。

相關API

BatchSetCdnDomainConfig

7.7. 自訂Cachekey

通過自訂Cachekey，可以將訪問同一個檔案的一類請求轉化為統一的Cachekey，避免不同請求緩衝為不同檔案的問題，降低回源率。本文為您詳細介紹配置自訂Cachekey功能的操作步驟。

功能介紹

Cachekey是一個檔案在CDN節點上緩衝時唯一的身份ID，每個在CDN節點上緩衝的檔案都對應一個Cachekey。檔案的Cachekey預設為用戶端請求的URL（帶參數）。

情境一：

客戶的不同請求的URL中含有複雜的參數，因此即使多個請求訪問的是同一個檔案，但由於URL參數不同，CDN節點會視為請求不同檔案而將不同請求緩衝成多個檔案，造成回源的請求增加。

可通過自訂Cachekey規則將同一類請求的Cachekey統一，降低回源率。

情境二：

用戶端請求的URL一樣時，CDN將視為請求同一個檔案。但實際上請求的Http Header中攜帶了client欄位區分了用戶端系統，希望請求不同檔案。

此時可通過自訂Cachekey將client欄位的值拼接至Cachekey，兩個請求即可識別為2個不同的Cachekey。

操作步驟

1. 登入 CDN控制台 。
2. 在 **域名管理**頁面，單擊目標網域名稱對應的 **管理** 。
3. 在指定網域名稱的左側導覽列，單擊 **緩存配置**。
4. 在 **自訂Cachekey** 頁簽配置Cachekey。

   > **說明** 支援對URI、參數操作、HTTP HEADER進行修改，同時支援自訂變數，從請求中提取需要的欄位。最終的Cachekey將由URI、參數操作、HTTP HEADER、自訂變數四部分組合而成。

5. 單擊 **確定** 。

樣本

URI

用戶端的請求 `http://yourdomain.com/a/b/test.jpg` 和 `http://yourdomain.com/a/b/c/test.jpg` 將視為請求同一個檔案，該檔案的Cachekey為 `http://yourdomain.com/c/test.jpg` 。

參數操作

用戶端的請求 `http://yourdomain.com/a/b/test.jpg?delete_par=1&modify_par=1` 將按規則添加 `add_par=1` ，刪除 `delete_par` ，將 `modify_par` 的值修改為 `2` ，最終轉化為 `http://yourdomain.com/a/b/test.jpg?modify_par=2&add_par=1` 。

> **注意** 參數操作中，如對同一個變數同時進行了多個操作，則各種操作的生效優先順序：新增>刪除>僅保留>修改。

HTTP Header

用戶端請求的HTTP HEADER的 `User-Agent` 和 `Accept-Language` 的值將被拼接到Cachekey中。例如請求 `http://yourdomain.com/a/b/test.jpg` 中的 `User-Agent=Mozilla/5.0 (Linux; X11)` ， `Accept-Language=en` ，則該請求的Cachekey為： `http://yourdomain.com/a/b/test.jpgMozilla/5.0(Linux;X11)en` 。

自定义变量

樣本一

變數名為 `language` ，來源為 `Request Header` ，來源欄位名為 `Accept-Language` ，匹配規則為 `([%w]+),([%w]+)` ，Variant 運算式為 `$1aa` 。

用戶端的請求 `http://yourdomain.com/a/b/test.jpg` 且攜帶HTTP要求標頭 `Accept-Language=en,ch` ，則匹配規則將匹配到 `en` 賦值給Variant 運算式中的 `$1` 。Variant 運算式還將在末尾拼接上 `aa` ，得到 `enaa` 的變數並取別名為 `language` ，拼接在URL後方形成最終的cachekey: `http://yourdomain.com/a/b/test.jpgenaa` 。

說明 Variant 運算式中的 `$n` 的含義是匹配規則中第 `n` 個括弧所匹配到的內容。例如樣本一中 `Accept-Language=en,ch`，匹配規則為 `([%w]+),([%w]+)`，則 `$1=en`，`$2=ch`。

樣本二

變數名為 `expired`，來源為 `Request Cooike`，來源欄位名為 `a`，匹配規則為 `[%w]+:(.*)`，Variant 運算式為 `$1`。

用戶端的請求 `http://yourdomain.com/a/b/test.jpg` 且攜帶 `Cookie a=expired_time:12635187`，則匹配規則將匹配到 `12635187` 賦值給Variant 運算式中的 `$1` 並取別名為 `expired`，拼接在URL後方形成最終的cachekey: `http://yourdomain.com/a/b/test.jpg12635187`。

樣本三

同時設定URI規則和自訂變數。

URI:

將所有URI符合 `/abc/.*/abc` 的請求都合并成 `/abc`。

自訂變數:

變數名為 `testname`，來源為 `Path`，匹配規則為 `/abc/xyz/(.*)`，Variant 運算式為 `$1`。

用戶端的請求URL `http://yourdomain.com/abc/xyz/abc/test.jpg`，按URI的配置Cachekey將被合并成 `http://yourdomain.com/abc/test.jpg`，然後根據自訂變數的配置該URL將會命中 `/abc/xyz/(.*)`，此時 `$1` 將被賦值為 `abc` 並拼接到Cachekey中，形成最終的cachekey: `http://yourdomain.com/abc/test.jpgabc`，從而達到兩個規則群組合使用，實現更複雜的緩衝邏輯。

注意 自訂Cachekey功能不會修改回源的URL，僅會修改請求的緩衝標識，回源的請求和用戶端發起的請求內容保持一致。

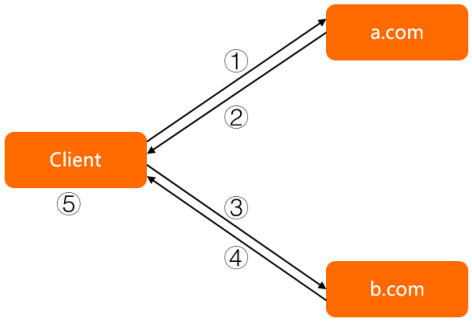
7.8. 配置跨域資源共用

當您需要跨域共用或者訪問資源時，您可以通過自訂HTTP回應標頭來實現。通過本文您可以瞭解跨域共用的概念、配置邏輯和應用案例。

什麼是跨域資源共用

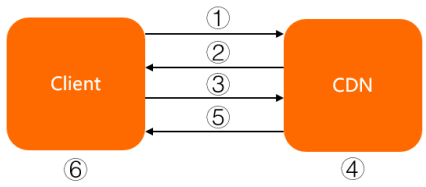
跨域資源共用CORS（Cross-Origin Resource Sharing）簡稱跨域訪問，是HTML5提供的標準跨域解決方案，允許Web應用伺服器進行跨域存取控制，使得跨域資料轉送得以安全進行。

跨域資源共用CORS資料互動示意圖：



1. Client向a.com发出请求，例如：http://a.com/index.html。
2. a.com给Client响应了文件index.html，页面中的链接包含另外一个源站的资源：http://b.com/1.jpg。
3. Client向b.com发出请求：http://b.com/1.jpg。
4. b.com收到请求之后，将会响应跨域头，例如：Access-Control-Allow-Origin: *。
5. Client收到响应，浏览器将会检查跨域响应头的值发现是*，将会允许任意外域访问，于是浏览器就会显示响应结果。

CDN中開啟了跨域共用之後互動示意圖：



1. Client向CDN发出请求，例如：http://a.com/index.html。
2. CDN给Client响应了文件index.html，其中包含另外一个源站的资源：http://b.com/1.jpg。
3. Client向CDN发出请求：http://b.com/1.jpg（其中包含请求头 Origin:http://a.com）。
4. CDN收到请求之后，将会校验用户请求头中Origin的值与CDN上配置的Access-Control-Allow-Origin的值是否匹配（支持单个值或者多个值的精确匹配，也支持泛域名匹配），不匹配的不返回跨域头，只有匹配上的才会返回跨域头。
5. CDN根据校验的结果返回跨域头，例如：Access-Control-Allow-Origin:http://a.com。
6. Client收到响应，浏览器将会检查跨域响应头的值，发现是http://a.com，将会允许外域访问，于是浏览器就会显示响应结果。

開啟跨域資源共用

1.
2.
3.
4.
5. 單擊 **自定义HTTP响应头**頁簽。
6. 單擊 **添加**，配置自訂HTTP回應標頭。
7. 選擇 **增加** 並設定 **自訂回應標頭參數** 為“Access-Control-Allow-Origin”時，您可以開啟 **跨域校正** 功能。

> **說明** 跨域校正預設為關閉狀態，只有在 **响应头操作** 為“增加”，**自定义响应头参数** 為“Access-Control-Allow-Origin”的時候才可以配置。
>
> - **開啟**：開啟狀態下CDN節點將按以下規則對使用者做跨域校正，並根據校正結果響應“Access-Control-Allow-Origin”的值。
> - **關閉**：關閉狀態下CDN節點不會校正使用者請求中攜帶的Origin頭，只會固定響應已配置的Access-Control-Allow-Origin值。

舉例

樣本一：如果跨域資源共用的回應標頭值設定了單個或者多個值（多個值之間用“,”分隔）。

- 如果使用者要求標頭裡攜帶的“Origin”參數值與被設定的任意一個值精確匹配，就會響應對應的跨域頭。
- 如果都沒有精確匹配上，則不響應跨域頭。

CDN上設定：Access-Control-Allow-Origin：http://a.com,https://c.com。

- 如果使用者請求攜帶的origin頭是http://a.com，則CDN節點將會響應Access-Control-Allow-Origin:

http://a.com。

- 如果使用者請求攜帶的origin頭是http://c.com，則CDN節點將會響應Access-Control-Allow-Origin: http://c.com。
- 如果使用者請求攜帶的origin頭是http://x.com，則CDN節點將不會響應Access-Control-Allow-Origin。

樣本二：如果跨域資源共用的回應標頭值設定了泛網域名稱，則會校正要求標頭中Origin值是否能匹配上Access-Control-Allow-Origin的泛網域名稱。

CDN上設定：Access-Control-Allow-Origin：http://*.aliyundoc.com。

- 使用者請求：Origin：http://demo.aliyundoc.com。CDN響應：Access-Control-Allow-Origin: http://demo.aliyundoc.com。
- 使用者請求：Origin：http://demo.example.com。CDN不響應。
- 使用者請求：Origin：https://demo.aliyundoc.com。CDN不響應（協議頭不同，使用者請求的是HTTPS協議，CDN上設定的是HTTP協議）。

8.HTTPS安全加速

8.1. 什麼是HTTPS加速

本文檔介紹了HTTPS安全加速的工作原理、優勢和注意事項。您可以通過開啟HTTPS安全加速，實現用戶端和CDN節點之間請求的HTTPS加密，保障資料轉送的安全性。

什麼是HTTPS？

HTTP協議以明文方式發送內容，不提供任何方式的資料加密。HTTPS協議是以安全為目標的HTTP通道，簡單來說，HTTPS是HTTP的安全版，即將HTTP用SSL/TLS協議進行封裝，HTTPS的安全基礎是SSL/TLS協議。HTTPS提供了身分識別驗證與加密通訊方法，被廣泛用於全球資訊網上安全敏感的通訊，例如交易支付。

根據2017年EFF（Electronic Frontier Foundation）發布的報告，目前全球已有超過一半的網頁端流量採用了加密的HTTPS進行傳輸。

工作原理

在阿里雲CDN控制台開啟的HTTPS協議，將實現用戶端和阿里雲CDN節點之間請求的HTTPS加密。CDN節點返回從來源站點擷取的資源給用戶端時，按照來源站點的配置方式進行。建議來源站點配置並開啟HTTPS，實現全鏈路的HTTPS加密。

HTTPS加密流程如下圖所示。

1. 用戶端發起HTTPS請求。
2. 服務端產生公開金鑰和私密金鑰（可以自己製作，也可以向專業組織申請）。
3. 服務端把相應的密鑰憑證傳送給用戶端。
4. 用戶端解析認證的正確性。
   - 如果認證正確，則會產生一個隨機數（密鑰），並用公開金鑰隨機數進行加密，傳輸給服務端。
   - 如果認證不正確，則SSL握手失敗。

     > **說明** 正確性包括：認證未到期、發行伺服器憑證的CA可靠、發行者認證的公開金鑰能夠正確解開伺服器憑證的發行者的數位簽章、伺服器憑證上的網域名稱和伺服器的實際網域名稱相匹配。

5. 服務端用之前的私密金鑰進行解密，得到隨機數（密鑰）。
6. 服務端用金鑰組傳輸的資料進行加密。
7. 用戶端用金鑰組服務端的加密資料進行解密，拿到相應的資料。

功能優勢

- HTTP明文傳輸，存在各類安全風險：
  - 竊聽風險：第三方可以獲知通訊內容。
  - 篡改風險：第三方可以修改通訊內容。
  - 冒充風險：第三方可以冒充他人身份參與通訊。
  - 劫持風險：包括流量劫持、鏈路劫持、DNS劫持等。
- HTTPS安全傳輸的優勢：

- 資料轉送過程中對您的關鍵資訊進行加密，防止類似Session ID或者Cookie內容被攻擊者捕獲造成的敏感資訊泄露等安全隱患。
- 資料轉送過程中對資料進行完整性校正，防止DNS或內容遭第三方劫持、篡改等中間人攻擊（MITM）隱患。
- HTTPS是主流趨勢：未來主流瀏覽器會將HTTP協議標識為不安全，Google瀏覽器Chrome 70以上版本以及Firefox已經在2018年將HTTP網站標識為不安全，若堅持使用HTTP協議，除了安全會埋下隱患外，終端客戶在訪問網站時出現的不安全標識，也將影響訪問。
- 百度與Google均對HTTPS網站進行搜尋加權，主流瀏覽器均支援HTTP/2，而支援HTTP/2必須支援HTTPS。可以看出來，無論從安全，市場，還是使用者體驗來看，普及HTTPS是未來的一個方向，所以強烈建議您將訪問協議升級到HTTPS。

應用情境

主要將應用情境分為五類，如下表所示 。

應用情境	說明
公司專屬應用程式	若網站內容包含crm、erp等資訊，這些資訊屬於企業級的機密資訊，若在訪問過程中被劫持或攔截竊取，對企業是災難級的影響。
政務資訊	政務網站的資訊具備權威性，正確性等特徵，需預防網路釣魚欺詐網站和資訊劫持，避免出現資訊劫持或泄露引起社會公用的信任危機。
支付體系	支付過程中，涉及到敏感資訊如姓名，電話等，防止資訊劫持和偽裝欺詐，需啟用HTTPS加密傳輸，避免出現下單後，下單客戶會立即收到姓名、地址、下單內容，然後以卡單等理由要求客戶按指示重新付款之類詐騙資訊，造成客戶和企業的雙重損失。
API介面	保護敏感資訊或重要操作指令的傳輸，避免核心資訊在傳輸過程中被劫持。
企業網站	啟用綠色安全標識(DV/OV)或地址欄企業名稱標識(EV)，為潛在客戶帶來更可信、更放心的訪問體驗。

注意事項

HTTPS安全加速功能注意事項，如下表所示。

分類	注意事項

分類	注意事項

配置	• 支援開啟HTTPS安全加速功能的業務類型如下：
	  ○ 圖片小檔案
	  主要適用於各種門戶網站、電子商務類網站、新聞資訊類網站或應用、政府或企業官網網站、娛樂遊戲類網站或應用等。
	  ○ 大檔案下載
	  主要適用於下載類網站和音視頻的應用。
	  ○ 視音頻點播
	  主要適用於各類視音頻網站，如影視類視頻網站、線上教育類視頻網站、新聞類視頻網站、短視頻社交類網站以及音頻類相關網站和應用。
	  ○ 直播流媒體
	  主要適用於互動性線上教育網站、遊戲競技類直播網站、個人秀場直播、事件類別和垂直行業的直播平台等。
	• 支援泛網域名稱HTTPS服務。
	• 支援HTTPS安全加速的啟用和停用。
	  ○ 啟用：您可以修改認證，系統預設相容HTTP和HTTPS請求。您也可以強制跳轉，自訂原請求方式。
	  ○ 停用：停用後，系統不再支援HTTPS請求且不再保留認證或私密金鑰資訊。再次開啟認證，需要重新上傳認證或私密金鑰。詳細說明，請參見HTTPS安全加速設定。
	• 您可以查看認證，但由於私密金鑰資訊敏感，不支援私密金鑰查看。請妥善保管認證相關資訊。
	• 您可以更新認證，但請謹慎操作。更新HTTPS認證後1分鐘內全網生效。

計費	HTTPS安全加速屬於增值服務，開啟後將產生HTTPS請求數計費，詳細計費標準請參見增值服務計費。 **說明** HTTPS根據請求數單獨計費，費用不包含在CDN流量包內。請確保賬戶餘額充足再開通HTTPS服務，以免因HTTPS服務欠費影響您的CDN服務。
認證	• 開啟HTTPS安全加速功能的加速網域名稱，您需要上傳格式均為 `PEM` 的認證和私密金鑰。 **說明** 由於CDN採用的Tengine服務基於Nginx，因此只支援Nginx能讀取的 `PEM` 格式的認證。詳細說明，請參見認證格式說明。 • 上傳的認證需要和私密金鑰匹配，否則會校正出錯。 • 不支援帶密碼的私密金鑰。 • 只支援攜帶SNI資訊的SSL/TLS握手。

相關功能

為了資料轉送的安全，您可以根據實際業務需求，配置相關功能，如下表所示。

功能	說明
HTTPS安全加速設定	實現HTTPS安全加速。
HTTP/2	HTTP/2是最新的HTTP協議，Chrome、 IE11、Safari以及Firefox等主流瀏覽器已經支援HTTP/2協議。
強制跳轉	強制重新導向終端使用者的原請求方式。
配置TLS	保障您互連網通訊的安全性和資料完整性。
設定HSTS	強制用戶端（如瀏覽器）使用HTTPS與伺服器建立串連，降低第一次訪問被劫持的風險。

8.2. 認證格式說明

在您 開啟HTTPS 服務之前，需要配置認證。您可以直接選擇在 阿里雲雲盾 託管或購買的認證，免費認證或自行上傳自訂認證。自訂上傳只支援 `PEM` 格式認證、認證及私密金鑰格式及其他格式轉PEM格式方法。

認證格式要求

CA 機構提供的認證一般包括以下幾種。其中阿里雲CDN使用的是 Nginx （.crt為認證，.key為私密金鑰）：

- 如果認證是通過 root CA機構頒發，則您的認證為唯一的一份。
- 如果認證是通過中級CA機構頒發的認證，則您的認證檔案包含多份認證，需要手工將伺服器憑證與中間認證拼接後，一起上傳。

> **說明** 拼接規則為：伺服器憑證放第一份，中間認證放第二份，中間不要有空行。一般情況下，機構在頒發認證的時候會有對應說明， 請注意規則說明。

樣本

請確認格式正確後上傳。

Root CA機構頒發的認證

認證格式為linux環境下 `PEM` 格式為：

認證規則為：

- 請將開頭 `-----BEGIN CERTIFICATE-----` 和結尾 `-----END CERTIFICATE-----` 一併上傳；
- 每行64字元，最後一行不超過64字元。

中級機構頒發的憑證鏈結：

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

憑證鏈結規則：

- 認證之間不能有空行；
- 每一份認證遵守第一點關於認證的格式說明。

RSA私密金鑰格式要求

rsa私密金鑰規則：

- 本地產生私密金鑰：`openssl genrsa -out privateKey.pem 2048` 其中 `privateKey.pem` 為您的私密金鑰檔案。
- `-----BEGIN RSA PRIVATE KEY-----` 開頭，`-----END RSA PRIVATE KEY-----` 結尾；請將這些內容一併上傳。
- 每行64字元，最後一行長度可以不足64字元。

如果您並未按照上述方案產生私密金鑰，得到如 `-----BEGIN PRIVATE KEY-----` 、

```
-----END PRIVATE
      KEY-----
```

這種樣式的私密金鑰，您可以按照如下方式轉換：

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

然後將 `new_server_key.pem` 的內容與認證一起上傳。

認證格式轉換方式

CDN HTTPS安全加速只支援 PEM 格式的認證，其他格式的認證需要轉換成 PEM 格式，建議通過openssl 工具進行轉換。下面是幾種比較流行的認證格式轉換為 PEM 格式的方法。

DER 轉換為 PEM:

DER格式一般出現在java平台中。

- 認證轉化：

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

- 私密金鑰轉化：

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

P7B 轉換為 PEM:

P7B格式一般出現在windows server和tomcat中。

- 認證轉化：

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

  擷取 `outcertificat.cer` 裡面 `-----BEGIN CERTIFICATE-----` ， `-----END CERTIFICATE-----` 的內容作為認證上傳。

- 私密金鑰轉化：P7B認證無私密金鑰，因此 只需在CDN控制台只需填寫認證部分，私密金鑰無需填寫。

PFX 轉換為 PEM:

PFX格式一般出現在windows server中。

- 認證轉化：

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

- 私密金鑰轉化：

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

免費認證

- 免費認證申請需要5-10分鐘。等待期間，您也可以重新選擇上傳自訂認證或者選擇託管認證。
- 無論您啟用的是自訂認證/託管認證，還是免費認證，都可以相互切換。
- 免費認證有效期間為1年，到期後自動續簽。
- 在您使用過程中，如果關閉Https設定後，再次開啟使用免費認證時，會直接使用已經申請過但未到期的認證。若開啟時認證已到期，會重新申請免費認證。

其他認證相關

- 您可以停用、啟用和修改認證。停用認證後，系統將不再保留認證資訊。再次開啟認證時，需要重新上傳認證或私密金鑰。請參考HTTPS安全加速設定。
- 只支援帶SNI資訊的SSL/TLS“握手”。
- 請確保上傳的認證和私密金鑰匹配。
- 更新認證的生效時間為10分鐘。
- 不支援帶密碼的私密金鑰。

其他認證相關的常見問題，請見更多認證問題。

8.3. HTTPS安全加速設定

功能介紹

HTTPS是以安全為目標的HTTP通道，簡單講是HTTP的安全版。即將HTTP用SSL/TLS協議進行封裝，HTTPS的安全基礎是SSL/TLS。

HTTPS加速優勢：

- 傳輸過程中對使用者的關鍵資訊進行加密，防止類似Session ID或者Cookie內容被攻擊者捕獲造成的敏感資訊泄露等安全隱患。
- 傳輸過程中對資料進行完整性校正，防止DNS或內容遭第三方劫持、篡改等中間人攻擊（MITM）隱患，瞭解更多使用HTTPS防止流量劫持。

阿里雲CDN 提供了HTTPS安全加速方案。您只需要開啟HTTPS後上傳認證和私密金鑰，並支援對認證進行查看、停用、啟用、編輯操作。

> **說明** 如果您有SNI回源的需要，請提交工單。

工作原理

在阿里雲CDN控制台開啟的HTTPS，將實現使用者和阿里雲CDN節點之間請求的HTTPS加密。而CDN節點返回來源站點擷取資源的請求仍按您來源站點配置的方式進行。建議您來源站點也配置並開啟HTTPS，實現全鏈路的HTTPS加密。

以下是HTTPS加密流程：

1. 用戶端發起HTTPS請求。
2. 服務端產生公開金鑰和私密金鑰（可以自己製作，也可以向專業組織申請）。
3. 服務端把相應的密鑰憑證傳送給用戶端。
4. 用戶端解析認證的正確性。
   - 如果認證正確，則會產生一個隨機數（密鑰），並用公開金鑰該隨機數進行加密，傳輸給服務端。
   - 如果認證不正確，則SSL握手失敗。

   > **說明** 正確性包括：認證未到期、發行伺服器憑證的 CA可靠、發行者認證的公開金鑰能夠正確解開伺服器憑證的發行者的數位簽章、伺服器憑證上的網域名稱和伺服器的實際網域名稱相匹配。

5. 服務端用之前的私密金鑰進行解密，得到隨機數（密鑰）。
6. 服務端用金鑰組傳輸的資料進行加密。
7. 用戶端用金鑰組服務端的加密資料進行解密，拿到相應的資料。

注意事項

配置相關

- 支援開啟HTTPS安全加速功能的業務類型包括：圖片小檔案加速、大檔案下載加速、視音頻點播加速、直播流媒體加速。
- 支援泛網域名稱HTTPS服務。
- 支援HTTPS安全加速的**啟用**和**停用**：
  - 啟用：您可以修改認證，系統預設相容使用者的HTTP和HTTPS請求。您也可以自訂對原請求方式設定**強制跳轉**。
  - 停用：停用後，系統不再支援HTTPS請求且將不再保留認證或私密金鑰資訊。再次開啟認證，需要重新上傳認證或私密金鑰。
- 您可以查看認證，但由於私密金鑰資訊敏感，不支援私密金鑰查看。請妥善保管認證相關資訊。
- 你可以更新認證，但請謹慎操作。更新HTTPS認證後1分鐘內全網生效。

計費相關

HTTPS安全加速屬於增值服務，開啟後將產生HTTPS請求數計費，當前計費標準詳見 HTTPS計費詳情。

> **說明** HTTPS根據請求數單獨計費，費用不包含在CDN流量包內。請確保賬戶餘額充足再開通HTTPS服務，以免因HTTPS服務欠費影響您的CDN服務。

認證相關

- 開啟**HTTPS安全加速**功能的加速網域名稱，您需要上傳認證，包含認證和私密金鑰，均為 `PEM` 格式。

  > **說明** 由於CDN採用的Tengine服務基於Nginx，因此只支援Nginx能讀取的認證，即 `PEM` 格式)。具體方法，請看參考認證格式說明及轉化方法。

- 只支援攜帶SNI資訊的SSL/TLS握手。
- 您上傳的認證需要和私密金鑰匹配，否則會校正出錯。

- 不支援帶密碼的私密金鑰。

操作步驟

1. 購買認證。您需要具備匹配加速網域名稱的認證才能開啟HTTPS安全加速。您可以在雲盾控制台快速申請免費的認證或購買進階認證。
2. 登入CDN控制台，進入CDN**網域名稱管理**頁。選擇網域名稱，單擊**管理**。
3. 在**HTTPS設定 > HTTPS認證**，單擊**修改配置**。
4. 在**HTTPS設定**對話方塊中，開啟**HTTPS安全加速**。
5. 選擇認證。您可以選擇的認證類型包括：雲盾、自訂和免費認證。目前僅支援 `PEM` 的認證格式。
   - 您可以選擇雲盾。若認證列表中無當前適配的認證，您可以選擇自訂上傳。您需要在設定認證名稱後，上傳認證內容和私密金鑰，該認證將會在阿里雲雲盾的認證服務中儲存。您可以在**我的認證**裡查看。
   - 您也可以選擇免費認證，即阿里雲的Digicert免費型DV版SSL認證。
6. 驗證認證是否生效。認證生效後（約1小時），使用HTTPS方式訪問資源。如果瀏覽器中出現綠色HTTPS標識，表明當前與網站建立的是私密串連，HTTPS安全加速生效。

> **說明** 關於更換認證：
> - 如果您是免費認證或阿里雲雲盾認證，直接選擇想替換的認證即可。
> - 如果您的自訂認證，請將新認證的名稱和內容填入對應框內，提交資訊即可。

8.4. HTTP/2

功能介紹

HTTP/2也被稱為HTTP 2.0，是最新的HTTP協議。目前，Chrome、 IE11、Safari以及Firefox 等主流瀏覽器已經支援 HTTP/2協議。HTTP/2最佳化了效能，相容了HTTP/1.1的語義，與SPDY相似，與HTTP/1.1有巨大區別。

> **說明** SPDY是Google開發的基於TCP的應用程式層協議，用以最小化網路延遲，提升網路速度，最佳化使用者的網路使用體驗。SPDY並不是一種用於替代HTTP的協議，而是對HTTP協議的增強。新協議的功能包括資料流的多工、請求優先順序以及HTTP前序壓縮，與HTTP/2相似。

HTTP/2的優勢

- 二進位協議：相比於HTTP 1.x 基於文本的解析，HTTP/2將所有的傳輸資訊分割為更小的訊息和幀，並對它們採用二進位格式編碼。基於二進位可以讓協議有更多的擴充性，比如引入了幀來傳輸資料和指令。
- Alibaba Content Security Service：HTTP/2基於HTTPS，因此天然具有安全特性。通過HTTP/2的特性可以避免單純使用HTTPS的效能下降。
- 多工（MultiPlexing）：通過該功能，在一條串連上，您的瀏覽器可以同時發起無數個請求，並且響應可以同時返回。另外，多工中支援了流的優先順序（Stream dependencies）設定，允許用戶端告訴伺服器哪些內容是更優先順序的資源，可以優先傳輸。
- Header壓縮（Header compression）：HTTP要求標頭帶有大量資訊，而且每次都要重複發送。HTTP/2採用HPACK格式進行壓縮傳輸，通訊雙方各自緩衝一份頭域索引表，相同的訊息頭只發送索引號，從而提高效率和速度。

操作步驟

1. 在 **網域名稱管理**頁面，選擇網域名稱，單擊 **配置**。
2. 在 **HTTPS配置 > HTTP/2設定** 欄進行配置。

   > **說明** 開啟HTTP/2前，請確保HTTPS的認證已經配置成功。
   >
   > - 若您是第一次配置HTTPS認證，需要等認證配置完成且生效後，才能開啟HTTP/2。
   > - 若您已經開啟了HTTP/2，但是又關閉了HTTPS認證功能，HTTP/2會自動失效。

3. 開啟後儲存即可。

8.5. 配置OCSP Stapling

OCSP Stapling功能是由CDN伺服器查詢OCSP（Online Certificate Status Protocol）資訊，可以降低用戶端驗證請求延遲，減少等待查詢結果的回應時間。通過本文，您可以瞭解OCSP Stapling功能的使用情境和控制台開啟該功能的操作步驟。

前提條件

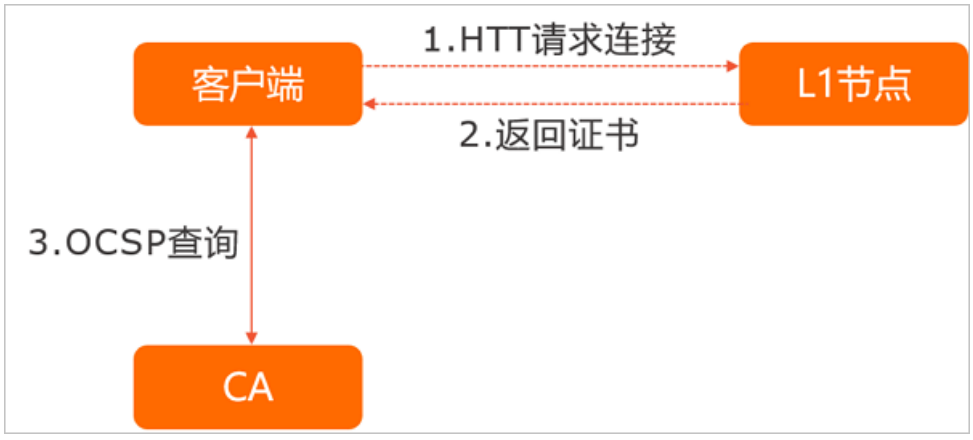
用戶端必須支援OCSP擴充欄位才能使用OCSP Stapling功能，如果用戶端不支援OCSP擴充欄位，則功能無法生效。

> **說明**
>
> - OCSP Stapling功能需要您的業務有一定量的QPS以保證全網觸發，QPS過低可能導致配置無法生效。
> - OCSP Stapling功能預設緩衝時間是1小時，緩衝到期後第一個訪問請求OCSP Stapling將不生效，直到重新擷取OCSP Stapling資訊為止。

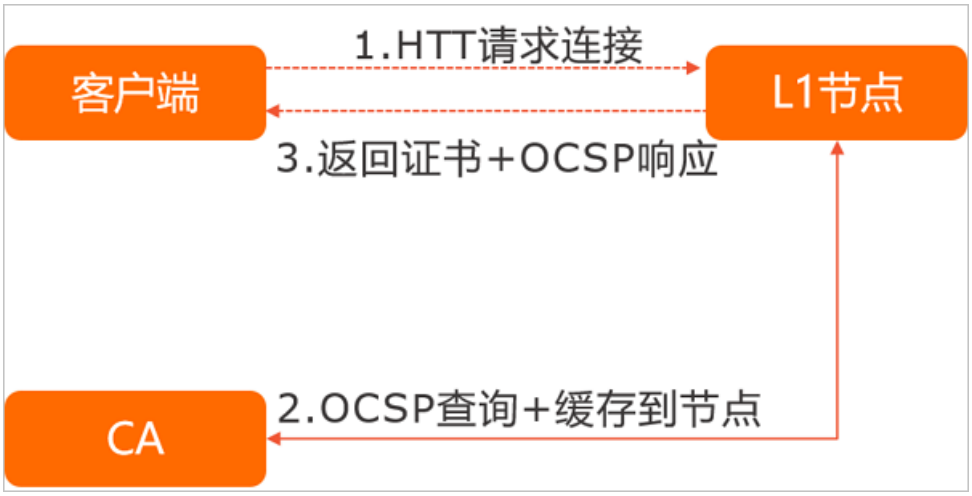
背景信息

OCSP資訊是由數位憑證頒發機構CA（Certificate Authority）提供，用於線上即時驗證認證的合法性和有效性。

使用者痛點：用戶端（瀏覽器）根據認證中的OCSP資訊，將查詢請求發送到CA的驗證地址，檢查此認證是否合法、有效。在網路狀況不佳的情況下，用戶端在等待擷取查詢結果時，會造成長時間的頁面空白，阻塞您終端使用者的後續操作。



解決方案：OCSP Stapling功能將查詢OCSP資訊的工作由CDN伺服器完成。CDN通過低頻次查詢，將查詢結果緩衝到伺服器中（預設緩衝時間60分鐘）。當用戶端向伺服器發起TLS握手請求時，CDN伺服器將認證的OCSP資訊和憑證鏈結一起發送到用戶端。這樣可以避免用戶端驗證會產生的阻塞問題。由於OCSP資訊是無法偽造的，因此這一過程不會產生額外的安全問題。



操作步驟

1.
2.
3.
4.
5. 在 OCSP Stapling 地區，開啟 **開關** 。

8.6. 強制跳轉

功能介紹

- 如果您的加速網域名稱開啟了**HTTPS安全加速**，您可以自訂設定，將終端使用者的原請求方式進行強制跳轉。
- 例如，當您開啟**強制HTTPS跳轉**後，終端使用者發起了一個HTTP請求，服務端返回302重新導向響應，原來的HTTP請求強制重新導向為HTTPS請求，如圖所示：

強制跳轉預設不開啟。開啟後預設設定為：同時支援HTTP和HTTPS方式的請求。

可選項分別是：**預設**、**強制HTTPS跳轉**、**強制HTTP跳轉**。

- **強制HTTPS跳轉**：使用者的請求將強制重新導向為HTTPS請求。
- **強制HTTP跳轉**：使用者的請求將強制重新導向為HTTP請求。

> **說明** 您只有在啟用**HTTPS安全加速**功能後才能設定強制跳轉。同時支援HTTP和HTTPS方式的請求。

操作步驟

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**效能最佳化 > 智能壓縮**開啟功能。

8.7. 配置TLS

為了保障您互連網通訊的安全性和資料完整性，阿里雲CDN提供TLS版本控制功能。您可以根據不同網域名稱的需求，靈活地配置TLS協議版本。通過本文檔，您可以瞭解配置TLS協議的操作方法。

前提條件

背景信息

TLS（Transport Layer Security）即安全傳輸層協議，在兩個通訊應用程式之間提供保密性和資料完整性。最典型的應用就是HTTPS。HTTPS，即HTTP over TLS，就是安全的HTTP，運行在HTTP層之下，TCP層之上，為HTTP層提供資料加解密服務。

操作步驟

1.
2.
3.
4.
5. 在**TLS版本控制**地區，根據所需開啟或關閉對應的TLS版本。

   TLS協議說明如下表所示。

協議	說明	支援的主流瀏覽器
TLSv1.0	RFC2246，1999年發布，基於SSLv3.0，該版本易受各種攻擊（如BEAST和POODLE），除此之外，支援較弱加密，對當今網路連接的安全已失去應有的保護效力。不符合PCI DSS合規判定標準。	○ IE6+ ○ Chrome 1+ ○ Firefox 2+
TLSv1.1	RFC4346，2006年發布，修複TLSv1.0若干漏洞。	○ IE 11+ ○ Chrome 22+ ○ Firefox 24+ ○ Safri 7+
TLSv1.2	RFC5246，2008年發布，目前廣泛使用的版本。	○ IE 11+ ○ Chrome 30+ ○ Firefox 27+ ○ Safri 7+
TLSv1.3	RFC8446，2018年發布，最新的TLS版本，支援0-RTT模式（更快），只支援完全前向安全性金鑰交換演算法（更安全）。	○ Chrome 70+ ○ Firefox 63+

> **說明** 目前TLSv1.0、TLSv1.1和TLSv1.2版本預設開啟。

8.8. 配置HSTS

通過開啟HSTS（HTTP Strict Transport Security）功能，您可以強制用戶端（如瀏覽器）使用HTTPS與伺服器建立串連，降低第一次訪問被劫持的風險。

前提條件

背景信息

當您的網站全站使用HTTPS後，需要將所有HTTP請求的301和302重新導向到HTTPS。如果您在瀏覽器輸入或直接單擊HTTP連結，則伺服器會將該HTTP請求的301和302重新導向到HTTPS。該操作過程可能被劫持，導致重新導向後的請求未發送到伺服器，該問題可以通過HSTS來解決。

HSTS是一個回應標頭：`Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]`，參數說明如下表所示。

參數	說明
max-age	單位是秒。
Strict-Transport-Security	在瀏覽器緩衝的時間，瀏覽器處理網域名稱的HTTP訪問時，若該網域名稱的Strict-Transport-Security沒有到期，則在瀏覽器內部做一次307重新導向到HTTPS，從而避免瀏覽器和伺服器之間301/302重新導向被劫持的風險。
includeSubDomains	選擇性參數。如果指定這個參數，說明這個網域名稱所有子網域名稱也適用上面的規則。
preload	選擇性參數，支援preload列表。

> **說明**
>
> - HSTS生效前，第一次需要將301和302重新導向到HTTPS。
> - HSTS回應標頭在HTTPS訪問的響應中有效，在HTTP訪問的響應中無效。
> - 僅對443連接埠有效，對其他連接埠無效。
> - 僅對網域名稱有效，對IP無效。

操作步驟

1.
2.
3.
4.
5. 在**HSTS**地區，單擊**修改配置**。

   
6. 在**HSTS設定**對話方塊，開啟**HSTS開關**，配置到期時間和包含子網域名稱。

7. 單擊**確定**。

8.9. CDN預設支援的TLS密碼編譯演算法

本文介紹CDN預設支援的TLS密碼編譯演算法。

阿里雲CDN預設支援的TLS密碼編譯演算法列表如下：

```
   TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-C
HACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128
-GCM-SHA256:ECDHE-ECDSA-AES128-CCM8:ECDHE-ECDSA-AES128-CCM:ECDHE-ECDSA-AES128-SHA256:ECDHE-
RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-GCM-SHA384
:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM8:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES
256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-
ARIA256-GCM-SHA384:ECDHE-ARIA256-GCM-SHA384:ECDHE-ECDSA-ARIA128-GCM-SHA256:ECDHE-ARIA128-GC
M-SHA256:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:ECDHE-ECDSA-CAMELLIA12
8-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-GCM-SHA3
84:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA20-POLY1305:DHE-PSK-CH
ACHA20-POLY1305:ECDHE-PSK-CHACHA20-POLY1305:DHE-PSK-AES256-CCM8:DHE-PSK-AES256-CCM:RSA-PSK-
ARIA256-GCM-SHA384:DHE-PSK-ARIA256-GCM-SHA384:AES256-GCM-SHA384:AES256-CCM8:AES256-CCM:ARIA
256-GCM-SHA384:PSK-AES256-GCM-SHA384:PSK-CHACHA20-POLY1305:PSK-AES256-CCM8:PSK-AES256-CCM:P
SK-ARIA256-GCM-SHA384:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256:RSA-PSK-AES12
8-GCM-SHA256:DHE-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-CCM8:DHE-PSK-AES128-CCM:RSA-PSK-ARIA1
28-GCM-SHA256:DHE-PSK-ARIA128-GCM-SHA256:AES128-GCM-SHA256:AES128-CCM8:AES128-CCM:ARIA128-G
CM-SHA256:PSK-AES128-GCM-SHA256:PSK-AES128-CCM8:PSK-AES128-CCM:PSK-ARIA128-GCM-SHA256:ECDH-
RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:AES256-SHA256:CAMELLIA256-SHA256:ECDH-RSA-AES128
-SHA256:ECDH-ECDSA-AES128-SHA256:AES128-SHA256:CAMELLIA128-SHA256:ECDHE-PSK-AES256-CBC-SHA3
84:ECDHE-PSK-AES256-CBC-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC
-SHA:ECDH-RSA-AES256-SHA:RSA-PSK-AES256-CBC-SHA384:DHE-PSK-AES256-CBC-SHA384:RSA-PSK-AES256
-CBC-SHA:DHE-PSK-AES256-CBC-SHA:ECDHE-PSK-CAMELLIA256-SHA384:RSA-PSK-CAMELLIA256-SHA384:DHE
-PSK-CAMELLIA256-SHA384:AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA384:PSK-AES256-CBC-SHA
:PSK-CAMELLIA256-SHA384:ECDHE-PSK-AES128-CBC-SHA256:ECDHE-PSK-AES128-CBC-SHA:SRP-DSS-AES-12
8-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-128-CBC-SHA:ECDH-RSA-AES128-SHA:ECDH-ECDSA-AES128
-SHA:RSA-PSK-AES128-CBC-SHA256:DHE-PSK-AES128-CBC-SHA256:RSA-PSK-AES128-CBC-SHA:DHE-PSK-AES
128-CBC-SHA:ECDHE-PSK-CAMELLIA128-SHA256:RSA-PSK-CAMELLIA128-SHA256:DHE-PSK-CAMELLIA128-SHA
256:AES128-SHA:SEED-SHA:CAMELLIA128-SHA:IDEA-CBC-SHA:PSK-AES128-CBC-SHA256:PSK-AES128-CBC-S
HA:PSK-CAMELLIA128-SHA256:ECDH-ECDSA-AES256-SHA
```

說明 阿里雲控制台無法調整CDN支援的TLS密碼編譯演算法。如果您需要調整密碼編譯演算法，可以 處理。

8.10. HTTPS相關常見問題

HTTPS是以安全為目標的HTTP通道，為CDN的網路內容傳輸提供了更好的保障。用戶端在極速訪問內容的同時，可以更安全有效地瀏覽網站內容。本文為您介紹關於HTTPS的常見問題。

- 什麼是HTTPS?
- 開啟CDN的HTTPS加速後會額外收費嗎?
- 如何配置HTTPS認證?
- 來源站點已經配置了HTTPS，CDN上還需要配置HTTPS嗎?

什麼是HTTPS？

超文本傳輸安全性通訊協定HTTPS（Hypertext Transfer Protocol Secure），是一種在HTTP協議基礎上進行傳輸加密的安全性通訊協定，能夠有效保障資料轉送的安全。HTTP協議以明文方式發送內容，不提供任何方式的資料加密。HTTPS協議是以安全為目標的HTTP通道，簡單來說，HTTPS是HTTP的安全版，即將HTTP用SSL或TLS協議進行封裝，HTTPS的安全基礎是SSL或TLS協議。HTTPS提供了身分識別驗證與加密通訊方法，被廣泛用於全球資訊網上安全敏感的通訊，例如交易支付。當您在阿里雲CDN上配置HTTPS時，需要提供網域名稱對應的認證，並將認證部署在全網CDN節點，實現全網資料加密傳輸。

開啟CDN的HTTPS加速後會額外收費嗎？

會額外收費。開啟CDN的HTTPS加速，實際開啟的是用戶端到CDN邊緣節點這段鏈路的HTTPS。因為SSL協議的握手和內容解密都需要計算，所以會增加CDN伺服器的CPU資源損耗，但不會增加您來源站點伺服器的資源損耗，因為CDN邊緣節點到您來源站點這段鏈路使用的仍然是HTTP協議，不會額外增加您來源站點的損耗。

如果您購買不同類型的認證，則需要額外付費。您也可以登入阿里雲 申請免費認證。免費認證等級為DV，每個加速網域名稱可以申請一個免費認證，認證有效期間為一年，到期後可以免費自動續簽。設定好HTTPS認證後，該網域名稱在CDN上的所有HTTPS請求數會收費。

如何配置HTTPS認證？

您可以在CDN控制台中配置HTTPS認證，具體操作請參見 HTTPS安全加速設定。

來源站點已經配置了HTTPS，CDN上還需要配置HTTPS嗎？

HTTPS是用戶端和服務端的互動，未使用CDN之前，是用戶端直接和來源站點互動，因此來源站點需要配置HTTPS。使用CDN之後，是用戶端和CDN互動，如果您需要以HTTPS的形式訪問CDN，則必須在CDN上配置HTTPS認證。在CDN上配置HTTPS認證的方法，請參見 HTTPS安全加速設定。

來源站點的HTTPS認證更新了，CDN上需要同步更新嗎？

不需要。來源站點的HTTPS認證更新後不會影響CDN上的HTTPS認證，當您在CDN上配置的HTTPS認證將要到期或者已經到期時，您才需要在CDN上更新HTTPS認證。具體操作請參見 HTTPS安全加速設定。

已經配置了HTTPS，為什麼用戶端還是HTTP訪問？

用戶端是以HTTP訪問還是HTTPS訪問完全是用戶端的行為，如果您希望用戶端強制使用HTTPS訪問，可以在CDN上開啟強制HTTPS跳轉。具體操作請參見 強制跳轉。

CDN的免費HTTPS認證申請失敗怎麼辦？

在阿里雲CDN控制台中申請免費HTTPS認證時存在一些限制，這些限制可能導致免費HTTPS認證申請失敗，如果免費HTTPS認證申請失敗，優先建議您前往 SSL認證控制台 申請免費認證並進行部署。

上傳HTTPS認證，提示認證重複怎麼辦？

當您上傳 類型的認證時，如果系統提示認證重複，您需要修改認證名稱後再重新上傳。

配置HTTPS認證時提示“認證格式不對”，如何進行轉換？

HTTPS配置僅支援PEM格式的認證，不同的憑證授權單位對認證內容的上傳有不同的要求，具體格式要求請參見 認證格式說明。如果您的認證格式不是PEM，請完成格式轉換後再上傳，具體請參見 認證格式轉換方式。

開啟HTTPS加速會消耗更多資源或降低訪問速度嗎？

當來源站點開啟HTTPS時，相比於來源站點通過HTTP訪問在計算資源的消耗上會有所增加，主要來自於HTTPS握手過程中對非對稱加解密時的消耗，尤其在高並發情況下資源消耗增長明顯。對稱加解密消耗與HTTP基本一致，因此需要增加Session複用率，但直接通過HTTPS訪問來源站點相比於直接通過HTTP訪問來源站點耗時更長。

通過全站加速進行全鏈路HTTPS訪問時，SSL握手的平均時間會有所縮短，在高並發情況下，對於來源站點Session複用率會有明顯的提高，來源站點資源消耗會有所降低。

- 對於靜態內容：通過邊緣分發的方式，在增加握手時間消耗的同時，減少了傳輸時間的消耗，因此整體訪問上會有所減少，且靜態資源無需回源，減少了來源站點的互動，可以降低來源站點的資源消耗。
- 對於動態內容：在直接選取上比通過傳統公網訪問更加可控且路徑最優，動態請求必須回源，通過全站加速的網路回源，可以增加Session複用率，整體傳輸速度會有所提升。由於動態請求必須回源，因此非對稱加解密必不可少，來源站點的資源消耗會有所增加。但通過全站加速回源形成了全鏈路HTTPS訪問的方式，整體資源消耗上最優。

網站只有登入才需要HTTPS嗎？

不是。您需要從以下幾個方面來分析：

- 從安全方面來看：一些頁面為HTTP，一些頁面為HTTPS，當通過HTTP或不安全的CDN服務載入其他資源（例如JS或CSS檔案）時，網站也存在使用者資訊暴露的風險，而全站HTTPS是防止這種風險最簡單的方法。
- 從效能方面來看：當網站存在HTTPS和HTTP兩種協議時，跳轉需對伺服器進行大量的重新導向，當這些重新導向被觸發時會減慢頁面的載入速度。
- 從全網來看：瀏覽器對HTTPS的支援會更友好，搜尋引擎也對HTTPS的收錄有更好的支援。

常見的HTTP攻擊類型有哪些？

HTTPS只是安全訪問的其中一環，如需全面保證網路安全，則還需要接入WAF、DDoS等防禦能力，以下為常見的HTTP攻擊類型：

- SQL注入：利用現有應用程式，可以將惡意的SQL命令注入到後台資料庫引擎中並執行。也可以通過在Web表單中輸入惡意SQL語句得到一個存在安全性漏洞的網站上的資料庫，而不是按照設計者意圖去執行SQL語句。
- 跨站指令碼攻擊：跨站指令碼攻擊XSS（Cross-site scripting）是最常見和基本的攻擊Web網站的方法。攻擊者在網頁上發布包含攻擊性代碼的資料。當瀏覽者看到此網頁時，特定的指令碼就會以瀏覽者使用者的身份和許可權來執行。通過XSS可以較容易地修改使用者資料、竊取使用者資訊。
- 跨站請求偽造攻擊：跨站請求偽造CSRF（Cross-site request forgery）是另一種常見的攻擊。攻擊者通過各種方法偽造一個請求，模仿使用者提交表單的行為，從而達到修改使用者的資料或者執行特定任務的目的。為了假冒使用者的身份，CSRF攻擊和XSS攻擊通常會相互配合，但也可以通過其它手段，例如誘使使用者單擊一個包含攻擊的連結。
- Http Heads攻擊：使用瀏覽器查看任何Web網站，無論您的Web網站採用何種技術和架構，都用到了HTTP協議。HTTP協議在Response header和content之間有一個空行，即兩組CRLF（0x0D 0A）字元，這

個空行標誌著headers的結束和content的開始，攻擊者可以利用這一點。只要攻擊者有辦法將任一字元注入到Headers中，這種攻擊就可以發生。

- 重新導向攻擊：一種常用的攻擊手段是“釣魚”。釣魚攻擊者通常會發送給受害者一個合法連結，當您訪問連結時，會被導向一個非法網站，從而達到騙取使用者信任、竊取使用者資料的目的。為防止這種行為，我們必須對所有的重新導向操作進行審核，以避免重新導向到一個危險的地方。常見解決方案是白名單，將合法的要重新導向的URL添加到白名單中，非白名單上的網域名稱重新導向時拒絕。第二種解決方案是重新導向token，在合法的URL上加上token，重新導向時進行驗證。

9.存取控制設定

9.1. 存取控制概述

您可以通過設定Referer、IP、UserAgent黑名單和白名單，以及URL鑒權、遠程鑒權來實現對訪客身份的識別和過濾，從而限制訪問CDN資源的使用者，提升CDN的安全性。

您可以通過CDN的存取控制功能，對網域名稱執行如下操作。

功能	說明
防盜鏈	您可以通過配置訪問的Referer黑名單和白名單來實現對訪客身份的識別和過濾，限制訪問CDN資源的使用者。
鑒權配置	您可以通過配置URL鑒權功能保護使用者網站的資源不被非法網站下載盜用。URL鑒權比Referer防盜鏈安全性更高。
配置遠程鑒權	通過配置遠程鑒權功能，對發送到CDN邊緣節點上的使用者請求進行校正，避免CDN節點上的資源被非授權使用者訪問。
IP黑名單和白名單	您可以通過配置IP黑名單和白名單來實現對訪客身份的識別和過濾，限制訪問CDN資源的使用者。
配置UA黑白名單	您可以通過配置UserAgent黑名單和白名單來實現對訪客身份的識別和過濾，限制訪問CDN資源的使用者。

9.2. 防盜鏈

功能介紹

- 防盜鏈功能基於 HTTP 協議支援的 Referer 機制，通過 referer 跟蹤來源，對來源進行識別和判斷。使用者可以通過配置訪問的 Referer 黑白名單來對訪問者身份進行識別和過濾，從而限制 CDN 資源被訪問的情況。
- 目前防盜鏈功能支援黑名單或白名單機制，訪客對資源發起請求後，請求到達 CDN 節點，CDN節點會根據使用者預設的防盜鏈黑名單或白名單，對訪客的身份進行過濾。符合規則可以順利請求到資源；若不符合規則，則該訪客請求會，返回403響應碼。

操作步驟

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**存取控制 > Refer防盜鏈**，單擊**修改配置**。
3. 單擊**黑名單**或**白名單**，在下框內輸入想要添加的網段。
4. 單擊**確認**。

注意事項

- 防盜鏈是可選配置，預設不啟用。
- 黑白名單互斥，同一時間您只能選擇一種方式。
- 配置後會自動添加泛網域名稱支援。例如，如果您填寫a.com，則最終配置生效的是*.a.com，所有子級網

域名稱都會生效。

- 您可以設定是否允許空 Referer 欄位訪問CDN資源，即允許在瀏覽器地址欄輸入地址直接存取資源URL。

9.3. 業務類型

9.3.1. 鑒權配置

URL鑒權功能主要用於保護使用者網站的內容資源不被非法網站下載盜用。雖然，通過防盜鏈方法添加 Referer 黑、白名單的方式可以解決一部分盜鏈問題。但是，由於 Referer 內容可以偽造，所以Referer 防盜鏈方式無法徹底保護網站資源。因此，採用URL鑒權方式保護使用者來源站點資源更為安全有效。

工作原理

URL鑒權功能通過阿里雲CDN加速節點與客戶資來源站點點配合，實現了一種更為安全可靠的來源站點資源防盜方法。

1. CDN客戶網站提供加密 URL（包含許可權驗證資訊）。
2. 您使用加密後的 URL 向加速節點發起請求。
3. 加速節點對加密 URL 中的許可權資訊進行驗證以判斷請求的合法性。正常響應合法請求，拒絕非法請求。

鑒權方式

阿里雲CDN 相容並支援鑒權方式A、鑒權方式B、鑒權方式C三種鑒權方式。您可以根據自己的業務情況，選擇合適的鑒權方式，來實現對來源站點資源的有效保護。

鑒權程式碼範例

您可以查看 鑒權程式碼範例。

配置引導

1. 在CDN控制台頁面下的**網域名稱管理** 頁，選擇需要設定的網域名稱，單擊**配置**。
2. 在**存取控制 > 鑒權配置**欄，單擊**修改配置**。
3. 單擊**開啟**URL鑒權配置，選擇鑒權**類型**，並**主KEY**。

9.3.2. 鑒權方式A

工作原理

使用者訪問加密 URL 構成

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

鑒權欄位描述

- `PrivateKey` 欄位使用者可以自行設定
- 有效時間1800s指使用者訪問客戶原始伺服器時間超過自訂失效時間（timestamp欄位指定）的1800s後，該鑒權失效。例如使用者佈建訪問時間為2020-08-15 15:00:00，則連結的真正失效時間為2020-08-15 15:30:00。

欄位	描述
timestamp	失效時間，整形正數，固定長度為10，是1970年1月1日以來的秒數。 控制失效時間，10位整數，有效時間1800s。
rand	隨機數，建議使用UUID (不能包含中劃線”-“，如：477b3bbc253f467b8def6711128c7bec 格式)。
uid	暫未使用（設定成0即可）
md5hash	通過md5演算法計算出的驗證串，由數字和小寫英文字母混合組成0-9a-z，固定長度32。

CDN伺服器拿到請求後，會首先判斷請求中的 `timestamp` 是否小於目前時間。

- 如果小於目前時間，則認為到期失效並返回HTTP 403錯誤。
- 如果 `timestamp` 大於目前時間，則構造出一個同樣的字串(參考以下sstring構造方式)。然後使用MD5演算法算出 `HashValue` ，再和請求中帶來的 `md5hash` 進行比對。比對結果一致，則認為鑒權通過，返迴文件。否則鑒權失敗，返回HTTP 403錯誤。

- `HashValue` 是通過以下字串計算出來的：

```
sstring = "URI-Timestamp-rand-uid-PrivateKey"  (URI是使用者的請求對象相對位址，不包含參數，如 /Filename)
HashValue = md5sum(sstring)
```

鑒權執行個體

1. 通過 `req_auth` 請求對象：

   ```
   http:// cdn.example.com/video/standard/1K.html
   ```

2. 設定密鑰為：aliyuncdnexp1234（您可以自行配置）
3. 設定鑒權設定檔有效時間為：2015年10月10日00:00:00，計算出秒數為1444435200。
4. CDN伺服器會構造一個用於計算Hashvalue的簽名字串：

   ```
   /video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234"
   ```

5. 根據該簽名字串，CDN伺服器會計算HashValue：

   ```
   HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") = 80cd3862d699b7118eed99103f2a3a4f
   ```

6. 則請求時url為：

   ```
   http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-80cd3862d699b7118eed99103f2a3a4f
   ```

   如果計算出的HashValue與使用者請求中帶的 md5hash = 80cd3862d699b7118eed99103f2a3a4f 值一致，則鑒權通過。

9.3.3. 鑒權方式B

鑒權方式B

原理說明

使用者訪問加密 URL 格式

使用者訪問的 URL 如下:

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

加密URL的構造:網域名稱後跟產生URL的時間（精確到分鐘）(timestamp)再跟md5值(md5hash)，最後拼接回原始伺服器的真實路徑(FileName)，URL有效時間為1800s。

當鑒權通過時，實際回源的URL是:

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

鑒權欄位描述

- 注意： `PrivateKey` 由CDN客戶自行設定
- 有效時間1800s是指，使用者訪問客戶原始伺服器時間超過自訂失效時間(timestamp欄位指定)的1800s後，該鑒權失效；例如使用者佈建訪問時間2020-08-15 15:00:00，連結真正失效時間是2020-08-15 15:30:00

欄位	描述
DomainName	CDN客戶網站的網域名稱
timestamp	資源失效時間，作為URL的一部分，同時作為計算 `md5hash` 的一個因子，格式為: `YYYYMMDDHHMM` ,有效時間1800s
md5hash	以timestamp、FileName和預先設定好的 PrivateKey 共同做MD5獲得的字串，即 md5(`PrivateKey` + `timestamp` + `FileName`)
FileName	實際回源訪問的URL (注意，鑒權時候FileName要以/開頭)

樣本說明

1. 回源請求對象:

   ```
   http://cdn.example.com/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
   ```

2. 密鑰設為：aliyuncdnexp1234 (使用者自行設定)。
3. 使用者訪問客戶原始伺服器時間為 201508150800（格式為： YYYYMMDDHHMM）。
4. 則CDN伺服器會構造一個用於計算 md5hash 的簽名字串:

   ```
   aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
   ```

5. 伺服器會根據該簽名字串計算 md5hash:

```
md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3") = 9044548ef1527deadafa49a890a377f0
```

6. 請求CDN時url:

```
http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

計算出來的 md5hash 與使用者請求中帶的 md5hash = 9044548ef1527deadafa49a890a377f0 值一致，於是鑒權通過。

9.3.4. 鑒權方式C

原理說明

使用者訪問加密 URL 格式

格式1

```
http://DomainName/{/}/FileName
```

格式2

```
http://DomainName/FileName{&KEY1=<md5hash>&KEY2=<timestamp>}
```

- 花括弧中的內容表示在標準的URL基礎上添加的加密資訊。
- `<md5hash>` 是驗證資訊經過 MD5 加密後的字串;
- `<timestamp>` 是未加密的字串，以明文表示。固定長度10，1970年1月1日以來的秒數，表示為十六進位。
- 採用格式一進行URL加密，例如:

  ```
  http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/test.flv
  ```

  `<md5hash>` 為 a37fa50a5fb8f71214b1e7c95ec7a1bd `<timestamp>` 為 55CE8100。

鑒權欄位描述

- `<md5hash>` 部分欄位描述。

欄位	描述
PrivateKey	幹擾串，不同客戶採用不同的幹擾串
FileName	實際回源訪問的URL (注意，鑒權時候path要以/開頭)
time	使用者訪問原始伺服器時間，取 UNIX 時間，以十六進位數字字元表示。

- PrivateKey 取值 `aliyuncdnexp1234`
- FileName 取值 `/test.flv`
- time 取值 `55CE8100`
- 因此 md5hash 值為:

```
md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5fb8f71214b1e7c95ec7a1bd
```

- 明文: `timestamp = 55CE8100`

  這樣產生加密 URL:

  格式一:

  ```
  http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/test.flv
  ```

  格式二:

  ```
  http://cdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1e7c95ec7a1bd&KEY2=55CE8100
  ```

樣本說明

使用者使用加密的 URL 訪問加速節點,CDN伺服器會先把加密串 1 提取出來, 並得到原始的 URL 的 `<FileName>` 部分，使用者訪問時間，然後按照定義的商務邏輯進行驗證:

1. 使用原始的 URL 中的 `<FileName>` 部分,請求時間及 PrivateKey 進行 MD5 加密得到一個加密串2。
2. 比較加密串 2 與加密串 1 是否一致，如果不一致則拒絕。
3. 取加速節點伺服器目前時間，並與從存取 URL 中所帶的明文時間相減，判斷是否超過設定的時限 t(時間域值 t 預設為 1800s)。
4. 有效時間1800s是指，使用者訪問客戶原始伺服器時間超過自訂時間的1800s後，該鑒權失效；例如使用者佈建訪問時間2020-08-15 15:00:00，連結真正失效時間是2020-08-15 15:30:00。
5. 時間差小於設定時限的為合法請求，CDN加速節點才會給予正常的響應，否則拒絕該請求，返回 http 403錯誤。

9.3.5. 鑒權程式碼範例

URL鑒權規則請查閱 URL鑒權，通過這個 demo 您可以根據業務需要，方便的對URL進行鑒權處理。以下Python Demo包含三種鑒權方式：A鑒權方式、B鑒權方式、C鑒權方式，分別描述了三種不同鑒權方式的請求URL構成、雜湊字串構成等內容。

Python版本

```
import re
import time
import hashlib
import datetime
def md5sum(src):
    m = hashlib.md5()
    m.update(src)
    return m.hexdigest()
def a_auth(uri, key, exp):
    p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
    if not p:
        return None
    m = p.match(uri)
    scheme, host, path, args = m.groups()
    if not scheme: scheme = "http://"
    if not path: path = "/"
```

```
    if not args: args = ""
    rand = "0"      # "0" by default, other value is ok
    uid = "0"       # "0" by default, other value is ok
    sstring = "%s-%s-%s-%s-%s" %(path, exp, rand, uid, key)
    hashvalue = md5sum(sstring)
    auth_key = "%s-%s-%s-%s" %(exp, rand, uid, hashvalue)
    if args:
        return "%s%s%s%s&auth_key=%s" %(scheme, host, path, args, auth_key)
    else:
        return "%s%s%s%s?auth_key=%s" %(scheme, host, path, args, auth_key)
def b_auth(uri, key, exp):
    p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
    if not p:
        return None
    m = p.match(uri)
    scheme, host, path, args = m.groups()
    if not scheme: scheme = "http://"
    if not path: path = "/"
    if not args: args = ""
    # convert unix timestamp to "YYmmDDHHMM" format
    nexp = datetime.datetime.fromtimestamp(exp).strftime('%Y%m%d%H%M')
    sstring = key + nexp + path
    hashvalue = md5sum(sstring)
    return "%s%s/%s/%s%s%s" %(scheme, host, nexp, hashvalue, path, args)
def c_auth(uri, key, exp):
    p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
    if not p:
        return None
    m = p.match(uri)
    scheme, host, path, args = m.groups()
    if not scheme: scheme = "http://"
    if not path: path = "/"
    if not args: args = ""
    hexexp = "%x" %exp
    sstring = key + path + hexexp
    hashvalue = md5sum(sstring)
    return "%s%s/%s/%s%s%s" %(scheme, host, hashvalue, hexexp, path, args)
def main():
    uri = "http://xc.cdnpe.com/ping?foo=bar"            # original uri
    key = "<input private key>"                         # private key of authorization
    exp = int(time.time()) + 1 * 3600                   # expiration time: 1 hour after cur
rent itme
    authuri = a_auth(uri, key, exp)                     # auth type: a_auth / b_auth / c_au
th
    print("URL : %s\nAUTH: %s" %(uri, authuri))
if __name__ == "__main__":
    main()
```

9.4. 配置遠程鑒權

通過配置遠程鑒權功能，CDN可以按照您指定的方式將使用者請求轉寄給鑒權伺服器，由鑒權伺服器對使用者請求進行校正。校正通過即允許訪問，校正失敗會拒絕訪問或進行相應的限制，可有效避免CDN節點上的資源被非授權使用者訪問。

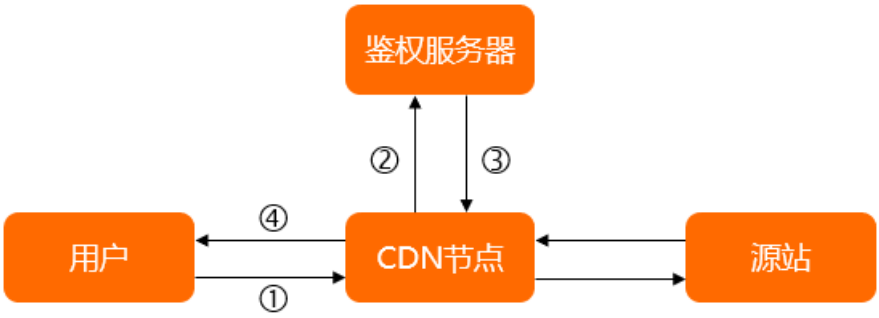
功能介紹

遠程鑒權功能是一種存取控制功能，用於對發送到CDN邊緣節點上的使用者請求進行校正，並根據鑒權伺服器返回的校正結果來判斷如何處理使用者的請求。

遠程鑒權和URL鑒權的作用一樣，都用於保護資源，讓資源只被授權成功的使用者訪問，非授權使用者將無法訪問。這兩個功能在技術實現方案上有如下差異：

- URL鑒權：使用者把網域名稱的鑒權規則下發給CDN節點，由CDN節點完成鑒權的整個資料互動流程。
- 遠程鑒權：使用者有自己單獨設定的鑒權伺服器，CDN節點收到使用者請求後，需要把使用者請求轉寄給鑒權伺服器完成鑒權，鑒權伺服器由使用者自主管理。

遠程鑒權功能的資料互動流程如下：



序號	互動說明
①	使用者發起的資源訪問請求到達CDN節點，請求中攜帶了鑒權參數。
②	CDN節點收到使用者請求，將使用者請求轉寄給鑒權伺服器。
③	鑒權伺服器根據使用者請求中攜帶的鑒權參數給出鑒權結果，並返回給CDN節點。
④	CDN節點根據鑒權伺服器返回的鑒權結果執行對應的動作，並返回對應的資料給使用者。 鑒權結果舉例說明如下： • 舉例1：鑒權成功，CDN節點與使用者開始正常的快取資料訪問互動。 • 舉例2：鑒權失敗，CDN節點返回404狀態代碼給使用者。 • 舉例3：鑒權失敗，CDN節點對使用者訪問進行限速。 • 舉例4：鑒權逾時，CDN節點執行鑒權逾時的預設動作，即允許存取使用者請求。

操作步驟

1.
2.
3.
4.
5. 單擊 **遠程鑒權** 頁簽。
6. 開啟 **遠程鑒權** 開關，根據介面提示，配置遠程鑒權資訊。

> **說明** 開啟遠程鑒權功能後，使用者的每次請求都要鑒權，當請求訪問量大時，需考慮鑒權伺服器的壓力和效能。

參數	說明
鑒權伺服器位址	鑒權伺服器對外可以訪問的地址。系統會對您輸入的鑒權伺服器位址進行校正，包括格式校正和值校正。 ○ 格式要求 格式必須為以下幾種類型之一： ■ http://example.com/auth ■ https://example.com/auth ■ http://192.0.2.1/auth ■ https://192.0.2.1/auth ○ 值要求 值不能包含127.0.0.1和localhost，因為這類本地地址屬於無效地址。
要求方法	鑒權伺服器支援的要求方法。支援GET、HEAD和POST這三種要求方法，預設使用GET方法請求。
鑒權檔案類型	○ **所有檔案類型**：所有的檔案類型都參與鑒權。 ○ **指定檔案類型**：僅指定的檔案類型參與鑒權。 ■ 指定檔案類型時，如果您輸入多個檔案類型，多個檔案類型用豎線（|）分隔，例如：mp4|flv。 ■ 檔案類型區分大小寫，即jpg和JPG是兩種不同的檔案類型。
保留參數設定	用於控制使用者請求URL中需要參與鑒權的參數。可以選擇保留所有參數、保留指定參數和刪除所有URL參數。 ○ 保留指定參數時，多個參數用豎線（|）分隔，例如：user|token。 ○ 參數區分大小寫，即key和KEY是兩種不同的參數。
添加自訂參數	為CDN節點轉寄給鑒權伺服器的請求URL添加自訂參數。您可以自訂設定參數和取值，也可以直接使用CDN控制台上預設的變數。 ○ 自訂設定參數和取值時，要求如下： ■ 多個參數用豎線（|）分隔，例如：token=$arg_token\|vendor=ali_cdn。 ■ 參數值區分大小寫，即key和KEY是兩種不同的參數值。 ○ 使用預設變數時，您可以提取變數的值添加到CDN轉寄給鑒權伺服器的請求上。 例如，選擇提取變數$http_host，則使用者請求的URL地址會加上host=$http_host，此處的host表示使用者要求標頭中的host值。變數名稱與變數含義的介紹，請參見 變數名稱。

參數	說明
保留要求標頭設定	用於控制使用者要求標頭中需要參與鑒權的參數。可以選擇保留所有參數、保留指定參數和刪除所有要求標頭參數。 ○ 保留指定參數時，多個要求標頭用豎線（|）分隔，例如：user_agent|reffer|cookies。 ○ 參數不區分大小寫，即http_remote_addr和HTTP_Remote_Addr一樣。 **說明** 選擇“保留所有參數”時，CDN節點預設會刪除HOST頭，如果您需要保留HOST頭，可通過“保留指定參數”或者“添加自訂參數”來保留。CDN節點預設刪除HOST頭的原因是CDN節點轉寄給鑒權伺服器的鑒權請求中攜帶的HOST頭是加速網域名稱，這可能會導致鑒權伺服器無法識別鑒權請求，從而導致訪問404、鑒權失敗。
添加自訂參數	為CDN節點轉寄給鑒權伺服器的要求標頭添加自訂參數。您可以自訂設定參數和取值，也可以直接使用CDN控制台上預設的變數。 ○ 自訂設定參數和取值時，要求如下： ■ 多個要求標頭用豎線（|）分隔，例如：User-Agent=$http_user_agent\|vendor=ali_cdn。 ■ 參數不區分大小寫，即http_remote_addr和HTTP_Remote_Addr一樣。 ○ 使用預設變數時，您可以提取變數的值添加到CDN轉寄給鑒權伺服器的請求上。 例如，選擇提取變數$http_host，則使用者請求的URL地址會加上host=$http_host，此處的host表示使用者要求標頭中的host值。變數名稱與變數含義的介紹，請參見 變數名稱。
鑒權成功狀態代碼	鑒權伺服器在鑒權成功時返回的HTTP狀態代碼，即鑒權結果。 例如，將鑒權成功狀態代碼設定為200，當鑒權伺服器返回200時，表示鑒權成功。 如果鑒權伺服器返回的狀態代碼不是成功狀態代碼，也不是失敗狀態代碼，結果即為鑒權逾時。
鑒權失敗狀態代碼	鑒權伺服器在鑒權失敗時返回的HTTP狀態代碼，即鑒權結果。 例如，將鑒權失敗狀態代碼設定為403，當鑒權伺服器返回403時，表示鑒權失敗。 如果鑒權伺服器返回的狀態代碼不是成功狀態代碼，也不是失敗狀態代碼，結果即為鑒權逾時。
響應自訂狀態代碼	鑒權伺服器返回鑒權失敗狀態代碼給CDN，即使用者請求鑒權失敗時，CDN節點返回給使用者的狀態代碼。 例如，將響應自訂狀態代碼設定為403，當使用者請求鑒權失敗時，CDN節點會返回403給使用者。
鑒權逾時時間長度	統計的是從CDN節點發起鑒權請求開始，到CDN節點收到鑒權伺服器返回的結果為止的時間。單位為毫秒，鑒權逾時時間長度最長可以設定為3000。

參數	說明
鑒權逾時之後的動作	CDN與鑒權伺服器之間的資料互動逾時後，CDN對使用者請求的處理。支援 **通過** 和 **拒絕** 這兩種動作，區別如下： ○ **通過** ：鑒權逾時，CDN將直接允許存取使用者的請求。 ○ **拒絕** ：鑒權逾時，CDN將返回上面配置的 **響應自訂狀態代碼** 給使用者。

7. 單擊 **確定**，完成配置。

   成功配置遠程鑒權功能後，您可以在 **遠程鑒權** 頁簽下，對當前的配置進行修改或關閉遠程鑒權功能。

變數名稱

添加自訂參數時，您可以選擇直接使用CDN控制台上預設的變數。變數名稱與變數含義見下表。

變數名稱	變數含義
$http_host	要求標頭中的host值。
$http_user_agent	要求標頭中的user_agent值。
$http_referer	要求標頭中的referer值。
$http_content_type	要求標頭中的content_type值。
$http_x_forward_for	要求標頭中的x_forward_for值。
$remote_addr	請求的client ip資訊。
$scheme	請求的協議類型。
$server_protocol	請求的協議版本。
$uri	請求的原始uri。
$args	請求的Query String，不包含問號（？）。
$request_method	要求方法。
$request_uri	uri+'?'+args的內容。

相關API

BatchSetCdnDomainConfig

9.5. IP黑名單和白名單

功能介紹

通過IP黑名單功能，您可以添加IP到黑名單，從而使該IP無法訪問當前加速網域名稱。通過IP白名單功能，您可以添加IP到白名單，則只有該IP訪問當前加速網域名稱。

當前，IP黑/白名單支援IP網段添加，例如127.0.0.1/24。

說明 127.0.0.1/24 24表示採用子網路遮罩中的前24位為有效位，即用32-24=8bit來表示主機號，該子網可以容納2^8 - 2 = 254 台主機。故127.0.0.1/24 表示IP網段範圍是：127.0.0.1~127.0.0.255。

操作步驟

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**存取控制 > IP黑/白名單**，單擊**修改配置**。
3. 單擊**黑名單**或**白名單**，在下框內輸入想要添加的網段。
4. 單擊**確認**。

9.6. 配置UA黑白名單

您可以配置UserAgent黑名單和白名單實現對訪客身份的識別和過濾，從而限制訪問CDN資源的使用者，提升CDN的安全性。本文為您介紹UserAgent黑白名單的配置方法。

背景信息

當您需要根據HTTP要求標頭中的UserAgent欄位進行存取控制時，請配置UserAgent黑白名單功能，實現對請求的過濾。

- UserAgent黑名單：黑名單內的UserAgent欄位均無法訪問當前資源。

  如果您的UserAgent欄位被加入黑名單，該帶有UserAgent欄位的請求仍可訪問到CDN節點，但是會被CDN節點拒絕並返回403，CDN日誌中仍會記錄這些黑名單中的UserAgent欄位請求記錄。
- UserAgent白名單：只有白名單內的UserAgent欄位才能訪問當前資源，白名單以外的UserAgent欄位均無法訪問當前資源。

操作步驟

1.
2.
3.
4.
5. 單擊 **UA黑/白名單**頁簽。
6. 在 **UA黑/白名單**頁簽下，單擊 **修改配置**。
7. 根據介面提示，配置UserAgent的 **黑名單**或 **白名單**。

參數	說明

參數	說明
名单类型	UserAgent名單類型如下： ○ 黑名單 黑名單內的UserAgent欄位均無法訪問當前資源。 ○ 白名單 只有白名單內的UserAgent欄位能訪問當前資源，白名單以外的UserAgent欄位均無法訪問當前資源。 **說明** 黑名單和白名單互斥，同一時間只支援其中一種方式生效。
规则	配置UserAgent欄位時，用豎線（|）分割多個值，支援萬用字元號（*）。例如：*curl*|*IE*|*chrome*|*firefox*。 **說明** 如果UA要求標頭為空白，則可以使用 `^$` 表示。

8. 單擊 **確定**，完成配置。

9.7. CDN的安全防護功能

通過本文您可以瞭解CDN提供的基本安全防護功能。

CDN基本防護配置如下：

- Referer防盜鏈功能

  該功能是根據HTTP請求的Referer欄位來對請求來源的網域名稱進行篩選和連結。CDN支援三種防盜鏈設定：白名單、黑名單以及是否允許空refer。防盜鏈功能主要通過URL過濾的方法對來源Host的地址進行過濾，您可指定請求來源的網域名稱，其中黑名單和白名單只能有一種生效，通過該功能可以對請求來源進行限制。具體設定方法，請參見 防盜鏈。

- IP黑名單

  可以設定相應的IP黑名單針對來源IP進行限制。具體設定方法，請參見 IP黑名單和白名單。

- URL鑒權

  該功能是CDN為保護使用者安全係數較高的URL的安全功能，需要使用者按照指定的簽名方式對於特定的URL增加鑒權認證。該功能適合於安全密級較高的檔案，不建議一般的檔案使用，因為每次簽名都需要通過用戶端臨時產生。相比於正常的訪問會增加其訪問時間。具體設定方法，請參見 鑒權配置。

10.效能最佳化設定

10.1. 效能最佳化概述

您可以閱讀本文，設定加速網域名稱的效能最佳化功能，縮小訪問檔案的體積，提升加速業務的效率和頁面可讀性。

您可以通過效能最佳化功能，對網域名稱執行如下操作。

功能	說明
頁面最佳化	開啟頁面最佳化功能，CDN會自動刪除頁面的冗餘內容，例如HTML頁面、內嵌JavaScript和CSS中的注釋以及重複的空白符，可以有效去除頁面的冗餘資訊，縮小檔案體積，提高加速分發效率，同時也可以提升頁面的可閱讀性。
智能壓縮	開啟智能壓縮功能，CDN節點向您返回請求的資源時，會對文字檔進行Gzip壓縮，可以有效縮小傳輸檔案的大小，提升檔案傳輸效率，減少頻寬消耗。
Brotli壓縮	開啟Brotli壓縮功能，CDN節點向您返回請求的資源時，會對文字檔進行Brotli壓縮，可以有效縮小傳輸檔案的大小，提升檔案傳輸效率，減少頻寬消耗。
影像處理	通過影像處理功能，CDN可直接在回源節點對圖片行處理和分發，可減輕來源站點壓力，減少回源鏈路，節省回源流量。
過濾參數	開啟過濾參數，用戶端回源擷取資源時會去除URL請求中 `?` 之後的參數，有效提高檔案快取命中率，減少回源次數，節省回源流量，同時提升分發效率。開啟過濾參數後，如果需要保留部分參數，您可以配置需要保留的指定參數。
開啟過濾參數及配置刪除參數	開啟過濾參數，用戶端回源擷取資源時會去除URL請求中 `?` 之後的參數，有效提高檔案快取命中率，減少回源次數，節省回源流量，同時提升分發效率。開啟過濾參數後，如果需要保留多數參數，僅刪除部分參數，您可以配置需要忽略的參數，忽略參數將被刪除。

10.2. 頁面最佳化

功能介紹

開啟頁面最佳化功能，您可以刪除 html中的注釋以及重複的空白符；這樣可以有效地去除頁面的冗餘內容，減小檔案體積，提高加速分發效率。

操作步驟

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**效能最佳化** > **智能壓縮**開啟功能。

10.3. 智能壓縮

功能介紹

開啟智能壓縮功能後，您可以對大多數靜態檔案進行壓縮，有效減少使用者傳輸內容大小，加速分發效果。

當前支援的壓縮內容格式包括：text/xml 、text/plain 、text/css 、application/javascript 、application/x-javascript 、application/rss+xml、 text/javascript 、image/tiff、 image/svg+xml、application/json。

適用業務類型：所有。

操作步驟

1. 進入**網域名稱管理**頁面，選擇需要設定的網域名稱，單擊**管理**。
2. 在**效能最佳化** > **智能壓縮**開啟功能。

10.4. Brotli壓縮

Brotli是開源的一種新型壓縮演算法，開啟Brotli壓縮功能，CDN節點向您返回請求的資源時，會對文字檔進行Brotli壓縮，可以有效縮小傳輸檔案的大小，提升檔案傳輸效率，減少頻寬消耗。

背景信息

- Brotli壓縮支援的檔案類型有
- 用戶端請求攜帶要求標頭 `Accept-Encoding: br` ：用戶端希望擷取對應資源時進行Brotli壓縮。
- 服務端響應攜帶回應標頭 `Content-Encoding: br` ：服務端響應的內容是經過Brotli壓縮後的資源。

注意事項

操作步驟

1.
2.
3.
4.
5. 在 **Brotli压缩**地區框中，開啟 **Brotli压缩**開關，完成配置。

   成功開啟Brotli壓縮功能後，您可以對比原始檔案大小和壓縮後的檔案大小，壓縮後的檔案大小變小了，說明檔案已經被壓縮了。

相關API

BatchSetCdnDomainConfig

10.5. 影像處理

10.5.1. 影像處理概述

通過影像處理功能，CDN可直接在回源節點對圖片行處理和分發，可減輕來源站點壓力，減少回源鏈路，節省回源流量。使用影像處理功能，您可以對CDN上的原圖進行縮放、裁剪、添加浮水印等操作，滿足多種業務情境下的圖片需求。阿里雲CDN的影像處理和阿里雲OSS的圖片處理是兩個獨立的功能，不能相互混用。

> **說明** 影像處理為付費服務，當前免費使用，收費時間另行通知。

適用情境

使用影像處理功能前，您需要先在CDN上添加加速網域名稱，添加成功後才能開通影像處理功能。通過CDN進行圖片處理，所有的圖片處理和緩衝都通過CDN節點完成，來源站點無感知。

下表為您列出了影像處理常見的適用情境，適用情境較多，不僅限於以下情境。

適用情境	說明
電商平台	• 多種樣式處理滿足多終端圖片顯示情境，圖片編輯更加高效便捷。 • 可對商品圖、圖片評論等進行壓縮，縮小圖片品質，達到省流的目的。 • 支援添加浮水印，用於著作權保護，具有品牌識別、宣傳推廣作用。
社交軟體	• 簡單、靈活的圖片編輯方式滿足社交圖片標準處理的需求。 • 支援添加浮水印，保護個人資訊不被盜用。
線上教育	• 簡單、靈活的圖片編輯方式滿足線上教育課件圖等標準處理的需求。 • 您可以根據不同情境需求使用不同壓縮功能，平衡壓縮收益與視覺體驗。
素材網站	• 多種樣式處理滿足多終端圖片顯示情境，圖片編輯更加高效便捷。 • 針對需要使用高清大圖的素材網站及平台，您可以使用圖片自動瘦身進行視覺無損壓縮，在不損失視覺觀感的情況下最大化壓縮比，增益圖片載入速度。

功能優勢

影像處理功能的優勢如下：

- **更快分發**

  原圖在回源節點被緩衝後，邊緣觸發的多尺寸圖片訪問需求直接在回源節點進行處理和分發，減少回源鏈路，更快到達邊緣。

- **減輕來源站點壓力**

  處理後的靶心圖表大量消耗來源站點的儲存和計算能力，增加了來源站點的維護成本。通過CDN進行圖片處理，所有的圖片處理和緩衝都通過CDN節點完成，來源站點無感知。

- **提升重新整理預熱效率**

  當原圖失效後，處理後的靶心圖表也會全部失效且無法訪問，對圖片進行處理可降低提交重新整理預熱的次數和回源的頻寬，加速新圖片的更新，避免原圖和靶心圖表訪問失效問題。

- **邊緣需求定製**

  通過圖片處理參數對圖片處理進行控制，可以根據不同的瀏覽器和用戶端版本定製不同的圖片處理需求，滿足不同的業務能力。

使用限制

使用影像處理功能時有如下限制：

- 原圖限制
  - 圖片格式只支援JPEG、PNG、WebP、BMP、GIF、TIFF、JPEG 2000。
  - 原圖大小不能超過10 MB。
  - 原圖的寬×高不能超過16777216 px。

- 處理後的圖片限制
  - 圖片的寬×高不能超過16777216 px。
  - 轉WebP格式時，圖片的寬×高不能超過16777216 px，且寬和高單邊均不能超過16,384 px。

影像處理開通與操作方法

- 開通影像處理功能，具體操作，請參見 影像處理開通流程。
- 影像處理操作方式，具體操作，請參見 影像處理操作方法。

10.5.2. 開通影像處理

影像處理功能對涉及到圖片的所有App和網站都開放，開通後即可使用影像處理功能。您可以根據本文介紹的影像處理操作方法傳入縮放、裁剪、旋轉等指定參數處理圖片，以滿足多種業務情境下的圖片需求。

影像處理開通流程

> **說明** 影像處理為付費服務，當前免費使用，收費時間另行通知。

1.
2.
3.
4.
5. 在 **影像處理** 地區框中，開啟 **影像處理** 開關。
6. 根據介面提示，配置影像處理資訊。

參數	說明
支援轉換的圖片類型	選擇支援轉換的圖片類型，影像處理支援的圖片類型有JPEG、PNG、WebP、BMP、GIF、TIFF、JPEG 2000。
自適應WEBP	選擇是否開啟 **自適應WEBP** 。開啟 **自適應WEBP** ，可將其他格式圖片自動轉換為WEBP格式。 **注意** 開啟該功能後，短時間內會導致命中率下降，過後會自動回復正常，請勿在業務高峰期開啟。
圖片自動旋轉	選擇是否開啟 **圖片自動旋轉** 。圖片自動旋轉只對帶有旋轉參數的圖片生效，開啟 **圖片自動旋轉** ，可自動調正圖片。 **說明** 開啟該功能後，短時間內會導致命中率下降，過後會自動回復正常，請勿在業務高峰期開啟。

參數	說明
圖片自動瘦身	圖片自動瘦身僅支援JPEG和WEBP格式，開啟圖片自動瘦身可以在不改變原圖的寬×高和格式的前提下對圖片進行壓縮，節省訪問流量。 您可以選擇是否開啟 **圖片自動瘦身** ，預設為開啟狀態，90%指保留原圖的90%。 ○ 100%：表示不開啟。 ○ 非100%：表示開啟。

7. 單擊 **確定** ，完成開通。

   成功開通影像處理功能後，您需要根據下方的影像處理操作方法傳入指定參數對圖片進行處理。

影像處理操作方法

影像處理操作方法說明

CDN支援邊緣圖片處理，處理的類型以參數形式傳入。圖片處理的請求參數為 `image_process` ，支援攜帶多個轉換參數，例如 `crop` 、 `rotate` 等，多個轉換參數用正斜線（/）分隔，CDN將按影像處理轉換參數的順序處理圖片。例如 `image_process=resize,w_200/rotate,90` 表示將圖片先按比例縮放至寬200 px，再將圖片旋轉90°。

- 處理方法： `image_process=action1,param_value1/action2,param_value2` 。
- 操作樣本： `image_process=resize,l_200/quality,q_90/format,webp` 。

通過圖片的訪問URL處理圖片

您可以在圖片的訪問URL後添加相應的圖片處理參數處理圖片，具體如下：

- 格式： `http://example.com/example.jpg?image_process=action,param_value`
  - `example.com` ：您的CDN加速網域名稱。
  - `example.jpg` ：圖片名稱。
  - `image_process` ：固定參數，標明使用圖片處理參數對圖片檔案進行處理。
  - `action,param_value` ：影像處理的操作（action）即轉換參數、參數（param）和值（value），用於定義圖片處理的方式。影像處理支援的轉換參數，請參見 影像處理轉換參數。
- 樣本： `http://example.com/example.jpg?image_process=resize,w_200/rotate,90`

影像處理轉換參數

CDN支援攜帶一個或多個轉換參數處理圖片，下表為您匯總了圖片處理的轉換參數，您可以根據實際需求，對CDN上的原圖進行處理。

圖片處理功能	轉換參數	說明
格式轉換	format	轉換圖片格式。
品質轉換	quality	調整圖片品質。
圖片裁剪	crop	裁剪指定大小的圖片。
圖片縮放	resize	將圖片縮放至指定大小。

圖片處理功能	轉換參數	說明
圖片旋轉	• 圖片自動旋轉：auto-orient • 指定旋轉方向：rotate	將攜帶旋轉參數的圖片進行自適應旋轉或按指定角度以順時針方向旋轉圖片。
圖片色彩	• 圖片亮度：bright • 圖片對比：contrast • 圖片銳利化：sharpen	調整圖片的亮度、對比和清晰度。
浮水印管理	watermark	為圖片添加圖片浮水印或文字浮水印。
擷取資訊	info	擷取圖片資訊，包括圖片的長、寬、高、圖片格式和圖片品質等資訊。

10.5.3. 格式轉換

圖片格式轉換包含自適應WEBP和普通圖片格式轉換，您可以通過轉換參數將CDN上的圖片轉換為指定的圖片格式。本文介紹圖片格式轉換所用到的參數及樣本。

> **說明** 影像處理為付費服務，當前免費使用，收費時間另行通知。

自適應WEBP

WEBP是一種支援有損壓縮和無損壓縮的圖片檔案格式。CDN支援自適應WEBP功能，開啟自適應WEBP，通過對要求標頭Accept進行判斷，如果要求標頭Accept包含 `image/webp` ，則CDN會將其他格式圖片自動轉換為WEBP格式進行訪問。開啟自適應WEBP，請參見 影像處理開通流程。

> **說明**

操作樣本

下方的Accept內容僅作為樣本，實際的Accept內容以真實情況為準。樣本中Accept裡包含了 `image/webp` ，表示支援自適應WEBP功能。

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

圖片格式轉換

參數說明

操作名稱： `format`

下表列出了支援轉換的圖片格式。

支援轉換的圖片格式	說明

支援轉換的圖片格式	說明
JPEG	將原圖儲存為JPG或JPEG格式。
PNG	將原圖儲存為PNG格式。
WEBP	將原圖儲存為WEBP格式。
BMP	將原圖儲存為BMP格式。
GIF	將原圖儲存為GIF格式。 說明 GIF有動圖效果，若轉換為其他圖片格式，則只保留靜圖效果。
TIFF	將原圖儲存為TIFF格式。
JPEG 2000	將原圖儲存為JPEG 2000格式，圖片尾碼為JP2。

操作樣本

```
image_process=format,bmp
```

10.5.4. 品質轉換

圖片品質轉換包含圖片自動瘦身、絕對品質轉換和相對品質轉換。品質轉換是使用原圖本身的格式對圖片進行壓縮，您可以通過品質轉換參數，修改CDN上原圖的品質。

說明 影像處理為付費服務，當前免費使用，收費時間另行通知。

圖片自動瘦身

圖片自動瘦身僅支援JPG和WebP格式，開啟圖片自動瘦身可以在不改變原圖的寬×高和格式的前提下對圖片進行壓縮，縮小圖片品質，節省訪問流量。開啟圖片自動瘦身，請參見 影像處理開通流程。

圖片品質轉換

參數說明

操作名稱： `quality`

參數說明見下表。

參數	說明	取值範圍

參數	說明	取值範圍
Q	圖片的絕對品質。按絕對品質進行轉換，轉換成指定大小的品質，如果當前品質小於待轉換的品質，則不轉換。	0<Q<100，且Q必須是5的倍數，不在品質值範圍內的其他值均不支援。 **說明** 品質值越大圖片品質越高，圖片越清晰；品質值越小圖片品質越低，圖片越不清晰，推薦設定為95。
q	圖片的相對品質。按相對品質進行轉換，根據當前圖片的品質乘以待轉換係數，得到最終要轉換的圖片品質。	0<q<100，且q必須是5的倍數，不在品質值範圍內的其他值均不支援。 **說明** 品質值越大圖片品質越高，圖片越清晰；品質值越小圖片品質越低，圖片越不清晰，推薦設定為95。

操作樣本

- 絕對品質轉換：`image_process=quality,Q_90`，如果當前品質是80，轉換後品質仍為80。
- 相對品質轉換：`image_process=quality,q_90`，如果當前品質是80，轉換後品質為72。

10.5.5. 圖片裁剪

您可以通過圖片裁剪參數，在原圖上裁剪指定大小的圖片。本文介紹圖片裁剪所用到的參數及樣本。

說明 影像處理為付費服務，當前免費使用，收費時間另行通知。

參數說明

操作名稱：`crop`

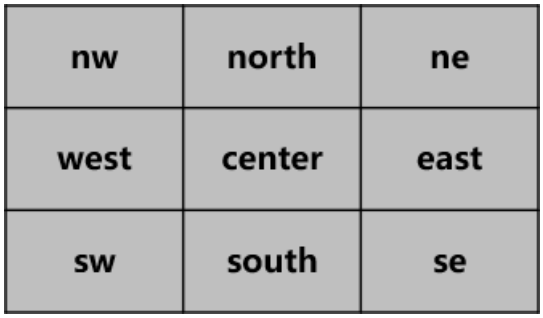
參數說明見下表。

說明 當任意參數值為負數時，將不對圖片進行任何處理直接返回原圖。

參數	描述	取值範圍
w	指定裁剪寬度。	預設值為0，寬×高不能超過16777216 px。
h	指定裁剪高度。	
x	指定裁剪起點橫座標（預設左上方為原點）。	
y	指定裁剪起點縱座標（預設左上方為原點）。	

參數	描述	取值範圍
g	設定裁剪的原點位置。原點按照九宮格的形式分布，一共有九個位置可以設定，為每個九宮格的左上方頂點。	• nw：左上 • north：中上 • ne：右上 • west：左中 • center：中部 • east：右中 • sw：左下 • south：中下 • se：右下 詳情請參見下方裁剪原點位置示意圖。

裁剪原點位置示意圖。



操作樣本

下表列出了圖片裁剪方式和樣本。

圖片裁剪方式	說明	樣本
圓切	指定圓半徑進行剪下，半徑不超過原圖的一半。	`image_process=circle,200`
九宮格切	設定原點位置，原點按九宮格分布。	`image_process=crop,w_200,h_200,g_se`
指定X、Y軸剪下	按指定x、y、寬和高裁剪，以x和y為起點，裁剪寬x高大小的圖片內容。	`image_process=crop,x_10,y_10,w_400,h_200`

圖片裁剪方式	說明	樣本
圖片置中剪下	從圖片置中部分裁剪指定寬和高的圖片內容。	`image_process=crop,mid,w_400,h_200`

10.5.6. 圖片縮放

您可以通過圖片縮放參數，調整原圖的圖片大小。本文介紹圖片縮放所用到的參數及樣本。

> **說明** 影像處理為付費服務，當前免費使用，收費時間另行通知。

參數說明

操作名稱：`resize`

參數說明見下表。

> **說明** 當任意參數值為負數時，將不對圖片進行任何處理直接返回原圖。

參數	說明	取值範圍
w	指定目標縮放圖的寬度。	預設值為0，寬×高不能超過16777216 px。
h	指定目標縮放圖的高度。	
l	指定目標縮放圖的最長邊。	
s	指定目標縮放圖的最短邊。	
fw、fh	指定目標縮放圖的寬高。	
p	按原圖長寬比例進行縮放。	[0,100]

操作樣本

下表列出了圖片縮放方式和樣本。

圖片縮放方式	說明	樣本
原圖比例縮放	按原圖長寬比例進行縮放。	`image_process=resize,p_80`

圖片縮放方式	說明	樣本
按條件縮放	當圖片大於等於1024000位元組時，進行縮放，單位為Byte。 **說明** 這裡的1024000為舉例所用的樣本值，實際取值需根據您的實際情況設定。	`image_process=resize,l_200/threshold,1024000`
按長邊固定自適應等比縮放	長邊固定長度，短邊自適應縮放。	`image_process=resize,l_200`
按短邊固定自適應等比縮放	短邊固定長度，長邊自適應縮放。	`image_process=resize,s_200`
按寬固定自適應等比縮放	固定寬度，長度自適應。	`image_process=resize,w_200`
按高固定自適應等比縮放	固定高度，寬邊自適應。	`image_process=resize,h_200`
指定寬高縮放	指定縮放的寬高。	`image_process=resize,fw_200,fh_200`

10.5.7. 圖片旋轉

圖片旋轉包含圖片自動旋轉和按指定方向旋轉。您可以通過圖片旋轉參數，將CDN上的原圖進行自動旋轉或按指定方向旋轉。本文介紹圖片旋轉所用到的參數及樣本。

說明 影像處理為付費服務，當前免費使用，收費時間另行通知。

圖片自動旋轉

某些手機拍攝出來的照片可能帶有旋轉參數，圖片自動旋轉只對帶有旋轉參數的圖片生效。開啟圖片自動旋轉，可自動調正圖片，方便使用者查看。通過控制台開啟圖片自動旋轉，請參見 影像處理開通流程。

> 說明

操作名稱： `auto-orient`

操作樣本

```
image_process=auto-orient
```

指定旋轉方向

指定旋轉方向是指將圖片按順時針和指定的角度進行旋轉，只支援90°、180°和270°三個旋轉角度。

操作名稱： `rotate`

操作樣本

```
image_process=rotate,180
```

10.5.8. 圖片色彩

圖片色彩包含圖片的亮度、對比和圖片銳利化。您可以通過亮度參數、對比參數和銳利化參數來調節CDN上原圖的亮度、對比和清晰度。本文介紹圖片色彩所用到的參數及樣本。

> **說明** 影像處理為付費服務，當前免費使用，收費時間另行通知。

參數說明

圖片亮度、對比和圖片銳利化對應的操作名稱如下：

- 圖片亮度： `bright`
- 圖片對比： `contrast`
- 圖片銳利化： `sharpen`

操作樣本

下表列出了圖片色彩包含的操作方式和樣本。

操作方式	說明	樣本
圖片亮度	設定圖片的亮度，亮度值範圍為[-100,100]。	`image_process=bright,50`

操作方式	說明	樣本
圖片對比	設定圖片的對比，對比值範圍為[-100,100]。	`image_process=contrast,50`
圖片銳利化	設定圖片銳利化，銳利化值範圍為[50,399]，推薦您使用50、100、150、200、250和300這六個銳利化值。	`image_process=sharpen,100`

10.5.9. 浮水印管理

CDN支援圖片浮水印和文字浮水印。您可以通過浮水印參數為圖片添加圖片浮水印和浮水印文字。本文介紹為圖片添加浮水印所用到的參數及樣本。

> **說明** 影像處理為付費服務，當前免費使用，收費時間另行通知。

圖片浮水印

參數說明

操作名稱：`watermark`

下表列出了圖片浮水印支援的功能及功能對應的參數。

> **說明**
> - 圖片浮水印暫不支援縮放，浮水印圖片原圖不能超過1 MB。
> - 支援同時添加多個浮水印，且支援同時添加圖片浮水印和文字浮水印，最多支援添加5個。

支援的功能	功能描述	參數	取值範圍
浮水印地址	指定可以訪問的圖片浮水印地址，浮水印地址可以公開訪問，若有鑒權或使用權限設定，可能導致擷取浮水印地址失敗。 浮水印地址需進行Base64編碼。詳細資料，請參見 浮水印編碼。	image	Base64編碼後的字串。

操作樣本

- 圖片浮水印

```
image_process=watermark,image_Base64編碼後的圖片請求,x_20,y_20,g_se,t_70
```

- 文字和圖片浮水印

```
image_process=watermark,text_Base64編碼後的文字內容,x_10,y_10,g_nw,size_24,color_FF0000,t_70/watermark,image_Base64編碼後的圖片請求,x_20,y_20,g_se,t_70
```

文字浮水印

參數說明

操作名稱： `watermark`

下表列出了文字浮水印支援的功能及功能對應的參數。

> **說明** 支援同時添加多個浮水印，且支援同時添加圖片浮水印和文字浮水印，最多支援添加5個。

支援的功能	功能描述	參數	取值範圍
文字內容	指定文字浮水印的文字內容，文字內容需進行Base64編碼。詳細資料，請參見 浮水印編碼。	text	Base64編碼後的字串，最大長度不能超過60個字元。
文字字型	指定文字浮水印的字型，字型名稱需進行Base64編碼。詳細資料，請參見 浮水印編碼。	type	共支援10種文字字型，字型及字型編碼請參見 文字字型 。 **說明** 如果您使用的是10種文字字型之外的其他字型，系統會識別出您使用的是預設字型alihyaihei。
文字顏色	指定文字浮水印的文字顏色，參數值為RGB顏色值。	color	RGB顏色值，例如：000000表示黑色，FFFFFF表示白色。 預設值：000000（黑色）。
文字旋轉	指定文字順時針旋轉角度。	rotate	支援按順時針旋轉90°、180°和270°。
文字鋪滿	指定是否將文字浮水印鋪滿原圖。	fill	取值範圍[0,1]，預設值為0。 • 0：表示不將文字浮水印鋪滿原圖。 • 1：表示將文字浮水印鋪滿原圖。

操作樣本

- 文字浮水印

```
image_process=watermark,text_Base64編碼後的文字內容,type_YWxpaHlhaWhlaQ,x_10,y_10,g_se,size_24,color_FF0000,t_70,rotate_45,fill_0
```

- 文字和圖片浮水印

```
image_process=watermark,text_Base64編碼後的文字內容,x_10,y_10,g_nw,size_24,color_FF0000,t_70/watermark,image_Base64編碼後的圖片請求,x_20,y_20,g_se,t_70
```

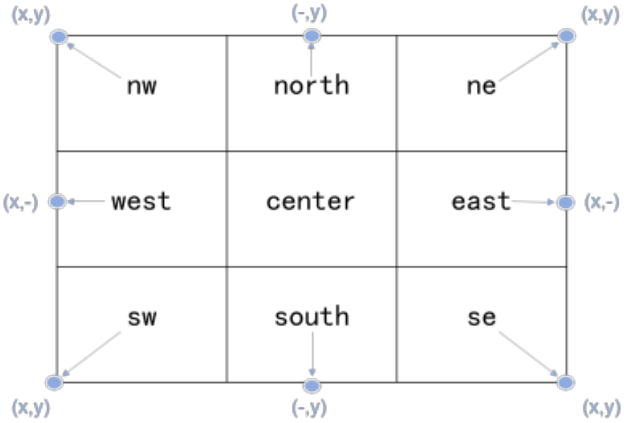
下表列出了文字浮水印支援的10種文字字型。

文字字型

文字字型	中文含義	編碼值
alihyaihei	阿里漢儀智能黑體，預設字型	YWxpaHlhaWhlaQ
hysong	漢儀宋體	aHlzb25n
hyhei	漢儀黑體	aHloZWk
hyshuangxian	漢儀雙線體	aHlzaHVhbmd4aWFu
fzltzhk	方正蘭亭中黑	ZnpsdHpoaw
fzshengsks	方正盛世楷書	ZnpzaGVuZ3Nrcw
fzqusongjian	方正趣宋簡體	ZnpxdXNvbmdqaWFu
zzgfxingyan	造字工房星岩	enpnZnhpbmd5YW4
comfortaa	Comfortaa	Y29tZm9ydGFh
notosans	NotoSans	bm90b3NhbnM

浮水印位置

圖片浮水印和文字浮水印均可以按照九宮格定位、浮水印垂直邊距和浮水印水平邊距來設定浮水印的位置。九宮格定位、垂直邊距和水平邊距不僅可以調節浮水印在圖片中的位置，當圖片存在多重浮水印時，還可以調節浮水印在圖中的布局。地區數值以及每個地區對應的基準點如下圖所示。



參數	說明	取值範圍
t	指定浮水印圖片或浮水印文字的透明度。	[0,100] 預設值為100， 表示透明度100%（即不透明）。

參數	說明	取值範圍
g	指定浮水印在圖片中的位置。	• nw：左上 • north：中上 • ne：右上 • west：左中 • center：中部 • east：右中 • sw：左下 • south：中下 • se：右下 詳情請參見上方基準點圖片。
x	指定浮水印的水平邊距， 即距離圖片邊緣的水平距離。這個參數只有當浮水印位置是左上、左中、左下、右上、右中、右下才有意義。	[0,4096] 預設值為10 ，單位：px（像素）。
y	指定浮水印的垂直邊距，即距離圖片邊緣的垂直距離。 這個參數只有當浮水印位置是左上、中上、右上、左下、中下、右下才有意義。	[0,4096] 預設值為10， 單位：px（像素）。

浮水印編碼

添加浮水印時，文字浮水印的文字內容、文字字型和圖片浮水印的浮水印地址需進行URL安全的Base64編碼。編碼方式如下：

1. 將內容編碼成Base64。

   推薦使用 URL-safe Baes64編碼工具 對文字浮水印的文字內容、文字字型和圖片浮水印的浮水印地址進行編碼。浮水印編碼後的內容僅適合應用在浮水印操作的特定參數中，請勿將其用在簽名字串（Signature）的內容裡。

2. 替換編碼結果中的部分編碼。
   - 將結果中的加號（+）替換成短劃線（-）。
   - 將結果中的正斜線（/）替換成底線（_）。
   - 將結果中尾部的等號（=）省略。

10.5.10. 擷取資訊

本文介紹如何擷取處理後的圖片資訊，以及擷取圖片資訊所用到的參數及樣本。

參數說明

操作名稱： `info`

返回的圖片資訊為JSON格式，返回的參數包括圖片的長、寬、高、圖片格式、圖片品質和圖片方向。

```
{ "Length":1055089, "Width":1920, "Height":1080, "Quality":100, "Format":"JPEG", "Orientation":"UNDEFINED"}
```

操作樣本

```
image_process=info
```

10.6. 過濾參數

功能介紹

過濾參數是指：URL請求中，如果攜帶“？”（半形）和參數，則請求到CDN節點時，CDN節點在收到該請求後是否將該帶參數的請求URL請求回來源站點。

- 如果開啟過濾參數，該請求到CDN節點後會截取到沒有參數的URL向來源站點請求，且CDN節點僅保留一份副本。
  - 由於http 請求中大多包含參數，但往往參數內容優先順序不高，可以忽略參數瀏覽檔案，適合開啟該功能；開啟後可以有效提高檔案快取命中率，提升分發效率。
  - 若參數有重要含義，例如包含檔案版本資訊等，推薦設定“保留參數”。您可以設定多個保留參數。如請求中包含任一“保留參數”，會攜保留參數回源。
- 如果關閉過濾參數，則每個不同的URL都緩衝不同的副本在CDN的節點上。

適用業務類型：所有。

樣本

例如：`http://www.abc.com/a.jpg?x=1` 請求URL到CDN節點

- 開啟“過濾參數”功能後，
  i. CDN節點向來源站點發起請求 `http://www.abc.com/a.jpg` （忽略參數x=1）。
  ii. 來源站點響應該請求內容後，響應到達CDN節點。
  iii. CDN節點會保留一份副本，然後繼續向終端響應 `http://www.abc.com/a.jpg` 的內容。
  iv. 所有類似的請求 `http://www.abc.com/a.jpg?參數` 均響應CDN副本 `http://www.abc.com/a.jpg` 的內容。
- 關閉“過濾參數”功能，`http://www.abc.com/a.jpg?x=1` 和 `http://www.abc.com/a.jpg?x=2` 會響應不同參數來源站點的響應內容。

> **說明** URL鑒權功能的優先順序高於過濾參數。由於A類型鑒權資訊包含在http請求的參數部分，所以系統會先進行鑒權判斷，鑒權通過後在CDN節點緩衝一份副本。

操作步驟

1. 進入**網域名稱管理**頁，選擇需要設定的網域名稱，單擊**配置**。
2. 在**效能最佳化** > **過濾參數**欄，點擊**修改配置**。

   您可以在此開啟或關閉**過濾參數**，並**設定保留參數**。

11.視頻相關配置

11.1. 概述

您可以通過視頻相關功能來滿足在音視頻內容分發情境下提升命中率、降低回源頻寬、音頻與視頻分離、音視頻試看、M3U8加密等相關需求。

您可以通過視頻相關功能，對網域名稱執行如下操作。

功能	說明
Range回源	開啟Range回源功能，可以提升快取命中率，減少回源流量消耗，並且提升資源響應速度。
拖拽播放	開啟拖拽播放功能後，當播放視音頻時，隨意拖拽播放進度，而不影響視音訊播放效果。
配置聽視頻	開啟聽視頻功能後，可以直接聽視頻的音頻並降低頻寬的使用。
配置音視頻試看	開啟音視頻試看功能後，可以實現非會員試看試聽體驗。
配置M3U8標準加密改寫	開啟M3U8標準加密改寫功能後，可以使用自訂參數進行HLS標準加密。

11.2. Range回源

功能介紹

Range回源是指用戶端通知來源站點伺服器只返回部分內容，以及部分內容的範圍。這對於較大檔案的分發加速有很大協助。開啟Range回源功能，可以減少回源流量消耗，並且提升資源回應時間。

需要來源站點支援range請求，即對於http要求標頭中包含 Range 欄位，來源站點能夠響應正確的206檔案分區。

Range回源	具體描述	樣本
開啟	該參數可以請求回來源站點。此時來源站點需要依據 Range 的參數，回應檔的位元組範圍。同時CDN節點也會向用戶端響應相應位元組範圍的內容。	用戶端向CDN請求中含有range:0-100，則來源站點端收到的請求中也會含有range:0-100這個參數。並且來源站點響應給CDN節點，然後CDN節點響應給用戶端的就是範圍是0-100的一共101個位元組內容。
關閉	CDN上層節點會向來源站點請求全部的檔案，並且由於用戶端會在收到Range定義的位元組後自動斷開http連結，請求的檔案沒有緩衝到CDN節點上。最終導致緩衝的命中率較低，並且回源流量較大。	用戶端向CDN請求中含有range：0-100，則server端收到的請求中沒有range這個參數。來源站點響應給CDN節點完整檔案，但是CDN節點響應給用戶端的就是101個位元組，但是由於串連斷開了，會導致該檔案沒有緩衝到CDN節點上。

說明 需要來源站點支援range請求，即對於http要求標頭中包含 Range 欄位,來源站點能夠響應正確的206檔案分區。

操作步驟

Range回源是可選配置項，預設不開啟。您可以變更配置，開啟Range回源。

1. 進入CDN**網域名稱管理**頁面，選擇網域名稱，單擊**管理**。
2. 在**視頻相關 > Range回源**，選擇**修改配置**。
3. 選擇 **開啟**、**關閉**或**強制**Range回源功能。

> **說明** 您指定range回源為強制後，任何分區請求都會強制分區回源。

您還可以參考Range回源的API文檔，使用該功能。

11.3. 拖拽播放

功能介紹

拖拽播放功能是指：在ApsaraVideo for VOD情境中，如果使用者拖拽播放進度時，用戶端會向伺服器端發送類似 `http://www.aliyun.com/test.flv?start=10` 的URL請求。此時，伺服器端會向用戶端響應從第10位元組的前一個主要畫面格（如果start=10不是主要畫面格所在位置）的資料內容。

開啟該功能，CDN節點可以支援此項配置，可以在響應請求時直接向client響應從第10位元組的前一個主要畫面格（如果start=10不是主要畫面格所在位置）（FLV格式）或第10s（MP4格式）開始的內容。

注意事項

- 需要來源站點支援range請求，即如果http要求標頭中包含 Range 欄位，來源站點需要能夠響應正確的206檔案分區。請參考Range回源。
- 目前支援檔案格式有：MP4和FLV。
- 目前FLV只支援音頻為aac，且視頻為avc的編碼格式。

檔案類型	meta資訊	start參數	舉例
MP4	來源站點視頻的meta資訊必須在檔案頭部，不支援meta資訊在尾部的視頻。	start參數表示的是時間，單位是s，支援小數以表示ms（如start=1.01，表示開始時間是1.01s），CDN會定位到start所表示時間的前一個主要畫面格（如果當前start不是主要畫面格）。	請求http://domain/video.mp4?start=10就是從第10秒開始播放視頻。
FLV	來源站點視頻必須帶有meta資訊。	start參數表示位元組，CDN會自動定位到start參數所表示的位元組的前一個主要畫面格（如果start當前不是主要畫面格）。	對於http://domain/video.flv,請求http://domain/video.flv?start=10就是從第10位元組的前一個主要畫面格（如果start=10不是主要畫面格所在位置）開始播放視頻。

操作步驟

1. 進入**網域名稱管理**頁，選擇需要設定的網域名稱，單擊**配置**。
2. 在**視頻相關** > **拖拽播放**欄，開啟該功能。

11.4. 配置聽視頻

開啟聽視頻功能後，CDN節點會將視頻檔案中的音頻分離，並返回給用戶端，實現聽視頻的同時降低頻寬的使用，有效節省流量。通過本文您可以瞭解開啟音視頻分離的操作方法。

背景信息

當用戶端請求訪問視頻檔案時，向伺服器端發送URL請求，例如：`http://www.aliyun.com/test.flv?ali_audio_only=1`，CDN伺服器端僅向用戶端發送純音頻資料。用戶端必須支援`Transfer-Encoding: chunked`傳輸方式。

> **說明**
>
> - 聽視頻功能不支援Range請求，但是播放視頻時許多用戶端都會發起Range請求（包括但不限於Safari、iOS裝置上的瀏覽器），建議您使用自研的用戶端對接該功能。
> - 聽視頻過程中如果需要拖動進度條播放，需同時配置拖拽功能。進行拖拽時，會先讀取原音視頻檔案的meta資訊擷取播放時間長度，將播放時間長度作為播放進度來實現播放進度的拖拽具體操作。更多資訊，請參見 拖拽播放。
> - 目前聽視頻功能不支援mp4 box header size等於16的情境（64位），僅支援mp4 box header size等於8的情境。

操作步驟

1.
2.
3.
4.
5. 在 **听视频**地區，開啟聽視頻開關。

   開啟聽視頻功能後，需要配合請求參數`ali_audio_only`使用。支援的檔案格式如下表所示。

檔案格式	meta資訊	ali_audio_only參數	舉例
MP4	來源站點視頻的meta資訊必須在檔案頭部，不支援meta資訊在尾部的視頻。	`ali_audio_only`參數表示該請求為音視頻分離請求，服務端只返回meta資訊和音頻資訊，視頻資訊會被過濾掉。如果不帶該參數或參數值非1，則該功能失效。	請求`http://domain/video.mp4?ali_audio_only=1`。
FLV	無要求。	`ali_audio_only`參數表示該請求為音視頻分離請求，服務端只返回meta資訊和音頻資訊，視頻資訊會被過濾掉。如果不帶該參數或參數值非1，則該功能失效。	請求`http://domain/video.flv?ali_audio_only=1`。

相關文檔

- 大量設定網域名稱

11.5. 配置音視頻試看

開啟阿里雲CDN的音視頻試看功能，您可以進行非會員試看試聽體驗，本文為您介紹了音視頻試看功能及控制台具體操作。

背景信息

音視頻試看功能可以使CDN節點只給用戶端返回指定時間長度的音視頻檔案。

音視頻試看支援TS和MP3格式檔案。FLV和MP4格式檔案試看可以通過拖拽播放的自訂參數 `end` 實現，拖拽播放操作請參見 拖拽播放。

操作步驟

1.
2.
3.
4.
5. 在 **音视频试看** 地區，開啟 **音视频试看** 開關。
6. 單擊 **自定义试看参数名** 對應的 **修改** 。
7. 設定自訂試看參數名。

   用戶端返回試看音視頻檔案的時間，單位為秒。例如：設定 **自定义试看参数名** 為free_time，用戶端的請求欄位為free_time=15，表示CDN節點只需返回15秒的音視頻檔案內容。

   > **說明** **自定义试看参数名** 的數值，沒有時間長度限制。但是如果超過了媒體檔案本身的播放時間長度，那超過部分時間長度則沒有效果。設定 **自定义试看参数名** 的數值需要精確，建議用戶端設定的值稍大點，更加穩妥。例如：使用者需要試看13秒的音視頻，建議在用戶端上設定15秒。

8. 單擊 **确定**。

相關文檔

- 大量設定網域名稱

11.6. 配置M3U8標準加密改寫

本文為您介紹M3U8標準加密改寫功能和操作流程。

功能介紹

HLS（HTTP Live Streaming）標準加密改寫是改寫HLS中M3U8檔案的 `#EXT-X-KEY` 標籤，改寫成功後會在 `#EXT-X-KEY` 標籤中的URI末尾追加一個參數，該參數的值由用戶端請求攜帶。

M3U8標準加密改寫 功能支援開啟HLS（M3U8）標準加密改寫，開啟加密後可自訂追加參數名稱，以配合您的用戶端使用個人化的加密參數名。如果不設定自訂參數名，則預設的參數名為 `MtsHlsUriToken` 。

操作步驟

1.

2.
3.
4.
5. 在 **M3U8标准加密改写**地區，開啟 **M3U8标准加密改写**開關。

   > **說明** 開啟 **M3U8標準加密改寫** 功能後，預設的參數名為 `MtsHlsUriToken` 。

6. （可選） 如果您需要配合您的用戶端修改參數名，請執行以下操作步驟。
   i. 單擊 **自訂參數名** 對應的 **修改** 。
   ii. 在 **自訂參數名** 對話方塊，設定 **參數名** 。

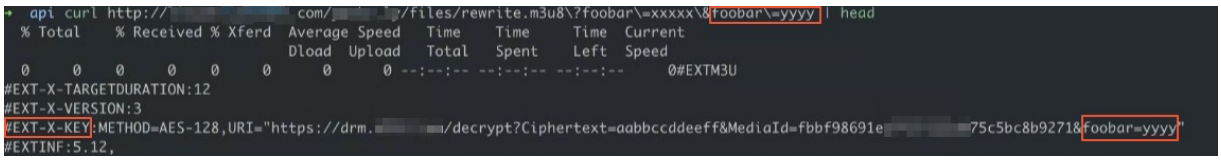
   > **說明** 參數名大小寫敏感，請確保設定的參數名和用戶端請求攜帶的參數名完全一致。例如用戶端請求攜帶 `foobar` 參數，如果在CDN控制台設定自訂參數名為 `FooBar` 將不生效。

   iii. 單擊 **確定**，完成配置。

樣本展示

在CDN控制台開啟 **M3U8標準加密改寫** ，並設定自訂參數名為 `foobar` ，如下圖所示。

用戶端請求中攜帶自訂的 `foobar` 參數，參數的值為 `yyyy` ，當CDN解密播放時，會將 `foobar=yyyy` 追加到M3U8檔案中 `#EXT-X-KEY` 標籤的URI末尾，如下圖所示。



相關文檔

- 大量設定網域名稱

12.安全配置

12.1. 配置CDN WAF

CDN結合邊緣Web Application FirewallWAF（Web Application Firewall）能力，將業務流量進行惡意特徵識別及防護，將正常、安全的流量回源到伺服器。避免網站伺服器被惡意入侵，保障業務的核心資料安全，解決因惡意攻擊導致的伺服器效能異常問題。 通過本文您可以瞭解WAF防護功能、使用情境、費用說明和設定方法。

前提條件

- 您已通過 開通CDN WAF進階版或者企業版。
- 開啟加速節點的WAF防護前請您確認網域名稱的加速地區選取項目符合您的業務需要（即選擇為 **全球** 或者 **全球（不包含中國內地）** ）。修改網域名稱加速地區的操作方法，請參見 切換加速地區。

增值服務

關於CDN WAF具體功能配置，請參見 Web Application Firewall，企業版的具體功能單擊下表中連結即可。

功能項	企業版
Web掃描防護	支援
帳號安全	支援
CC攻擊防護	支援
海量IP黑名單封鎖	支援
Rate Limit	支援
爬蟲情報庫	支援
驗證碼整合	支援
爬蟲智能演算法	支援
基礎Web攻擊防護	支援
0 DAY規則更新防護	支援
預警|阻斷模式	支援
解碼防混淆編碼繞過	支援
規則群組自訂	支援
HTTP欄位存取控制	支援
Log Service	支援 （3T）

背景資訊

阿里雲CDN的WAF功能，是指CDN融合了WAF能力，在CDN節點上，提供WAF防護功能。WAF防護具體功能，請參見 什麼是Web Application Firewall。

CDN的WAF服務主要適用於金融、電商、O2O、互連網+、遊戲、政府、保險等行業，保護您的網站在使用CDN加速的同時，免受因外部惡意攻擊而導致的意外損失。

使用CDN WAF功能後，可以協助您解決以下問題：

- 防資料泄密，避免因駭客的注入式攻擊導致網站核心資料被拖庫泄露。
- 阻止木馬上傳網頁篡改，保障網站的公信力。
- 提供虛擬補丁，針對網站被曝光的最新漏洞，最大可能地提供快速修複規則。

當您開啟WAF功能後，CDN WAF會對此網域名稱的所有請求進行檢測，並按照賬戶維度，對網域名稱開啟WAF功能的請求次數匯總，然後收費。CDN WAF計費價格，請參見 增值服務計費-CDN WAF計費 。

操作步驟

1.
2.
3.
4. 在指定網域名稱的左側導覽列，單擊 **安全配置**。
5. 在 **CDN WAF** 頁簽，開啟邊緣Web Application Firewall開關。
6. 單擊 **修改配置** 。
7. 根據頁面提示，配置 **Web安全** 、 **Bot管理** 和 **存取控制/限流** 。

專案	參數	說明
Web安全	**狀態**	Web入侵防護開關。
	模式	Web入侵防護模式如下： ○ **攔截** ：發現入侵後直接攔截。 ○ **警示** ：發現入侵後只警示不攔截。
	防護規則群組	Web入侵防護規則如下： ○ **寬鬆規則** ：當您發現在 **中等規則** 下存在較多誤攔截時，建議您選擇 **寬鬆規則** 。寬鬆模式下對業務的誤判程度最低，但也容易漏過攻擊。 ○ **中等規則** ：預設使用中等規則。 ○ **嚴格規則** ：當您需要更嚴格地防護路徑穿越、SQL注入、命令執行時，建議您選擇 **嚴格規則** 。

專案		參數	說明
		解碼設定	設定需要正則防護引擎解碼分析的內容格式。 i. 單擊 ，開啟配置視窗。 ii. 選中或取消選中要解碼的格式。 ■ 不支援取消的格式： **URL解碼** 、 **JavaScript Unicode解碼** 、 **Hex解碼** 、 **注釋處理** 、 **空格壓縮** 。 ■ 支援取消的格式： **Multipart解析** 、 **JSON解析** 、 **XML解析** 、 **PHP序列化解碼** 、 **HTML實體解碼** 、 **UTF-7解碼** 、 **Base64解碼** 、 **Form解析** 。 iii. 單擊 **確定** 。 **說明** 為保證防護效果，正則防護引擎預設對請求中所有格式類型的內容進行解碼分析。如果您發現正則防護引擎經常對業務中包含指定格式內容的請求造成誤攔截，您可以取消解碼對應格式，針對性地降低誤殺率。
Bot管理（僅限企業版使用者）	**合法爬蟲**	**狀態**	合法爬蟲開關。 **說明** 合法爬蟲提供合法搜尋引擎白名單，可應用於全網域名稱下允許存取。您可以根據實際需求，單擊 **前去配置** ，啟用或者關閉合法爬蟲。
	典型爬蟲行為識別	**狀態**	典型爬蟲行為識別開關。 **說明** 典型爬蟲行為識別提供典型爬蟲行為識別的通用演算法執行個體，可配置基本業務參數和風險閾值進行機器學習，輸出智能防護結果以對抗進階爬蟲。您可以根據實際需求，單擊 **前去配置** ，添加演算法規則。

專案		參數	說明
	爬蟲威脅情報	**狀態**	爬蟲威脅情報開關。 **說明** 爬蟲威脅情報雲端式平台強大的計算能力，提供撥號池IP、IDC機房IP、惡意掃描工具IP以及雲端即時模型產生的惡意爬蟲庫等多種維度威脅情報，可應用於全網域名稱或指定路徑下進行阻斷。您可以根據實際需求，單擊 **前去配置** ，編輯情報。
存取控制/限流	**IP黑名單**	**狀態**	IP黑名單控制開關。 **說明** IP黑名單支援一鍵封鎖特定的IP地址和位址區段訪問，以及指定地區的IP地址的訪問限制能力。您可以根據實際需求，單擊 **前去配置** ，添加IP地址黑名單和IP地區黑名單。
	自訂防護策略	**狀態**	自訂防護策略開關。 **說明** 自訂防護策略支援自訂精準條件的存取控制規則，以及基於精準條件下的指定統計對象的訪問限制自訂規則。您可以根據實際需求，單擊 **前去配置** ，添加自訂防護策略。

角色授權

當您需要CDN邊緣Web Application Firewall自動角色授權時，可以使用CDN WAF功能，CDN將自動為您建立AliyunServiceRoleForCDNAccessingWAF角色，並授權CDN使用該角色，並授權CDN訪問WAF產品中的資源。

AliyunServiceRoleForCDNAccessingWAF角色中包含的許可權包括如下介面：

- DescribePayInfo
- CreatePostpaidInstance
- CreateOutputDomainConfig
- DeleteOutputDomainConfig
- DescribeDomainWebAttackTypePv
- ModifyLogServiceStatus
- DescribeProtectionModuleMode
- DescribeDomainRuleGroup
- DescribeRegions
- ModifyProtectionRuleStatus

- ModifyProtectionRuleCacheStatus
- DescribePeakValueStatisticsInfo
- DescribeDomainAccessStatus
- DescribeFlowStatisticsInfo
- DescribeDomainTotalCount
- DescribeResponseCodeStatisticsInfo
- DescribeDDosCreditThreshold
- ModifyDomainClusterType
- DescribeInstanceInfo
- DescribeOutputDomains
- CreateOutputDomain
- DeleteOutputDomain
- DeleteInstance
- DescribeInstanceSpecInfo
- DescribeDomainBasicConfigs

如果您希望刪除該AliyunServiceRoleForCDNAccessingWAF角色，您需要 刪除CDN WAF執行個體，關閉所有網域名稱的CDN WAF功能，然後才能在RAM中刪除該SLR。

12.2. 配置頻次控制

如果您的網站因遭受惡意CC攻擊導致響應緩慢，可通過頻次控制功能提供的預設策略或自訂策略來攔截惡意流量，秒級阻斷訪問該網站的所有請求，提升網站的安全性。

步驟一：申請開通頻次控制功能

目前CDN的頻次控制功能需要先申請開通，如需開通請加入以下DingTalk群：

- 一群：23184221（已滿）。
- 二群：33298914（已滿）。
- 三群：33137775。

步驟二：啟用頻次控制

1.
2.
3.
4. 在指定網域名稱的左側導覽列，單擊 **安全配置**。
5. 單擊 **頻次控制**頁簽。
6. 開啟 **頻次控制設定** 開關。
7. 單擊 **修改配置** 。
8. 在 **頻次控制**對話方塊，開啟 **參數檢測** 開關，並選擇 **控制模式** 。

參數	說明

參數	說明
參數檢測	開啟參數檢測，頻次控制規則中的URI會帶上完整的參數進行匹配。參數檢測僅與URI匹配相關，與自訂規則中的匹配規則無關。 **說明** **參數檢測** 僅適用於自訂規則。
控制模式	您可以選擇以下控制模式： ○ **正常** 預設頻次控制模式。當您的網站流量無明顯異常時，採用該模式，避免被誤殺。 ○ **緊急** 當您的網站響應緩慢，且流量、CPU、記憶體等指標異常時，採用該模式。 ○ **自訂** 您可以根據業務需求自訂防護規則，有效識別異常的高頻訪問，邊緣抵禦CC攻擊。配置自訂規則的方法，請參見下方的步驟9。

9. （可選）配置自訂規則。

說明

- 當 **控制模式** 選擇 **自訂** 時，需配置自訂規則，其他 **控制模式** 不需要配置自訂規則。
- 最多支援添加5條自訂規則。

i. 單擊 **自訂規則** 對應的 **添加規則** 。

ii. 根據介面提示和下表配置自訂規則。

參數	說明
規則名稱	■ 長度為4~30個字元，支援英文、數字。 ■ 同一個網域名稱的規則名稱不可重複。
URI	指定需要防護的具體地址，例如 `/register` 。如果地址中包含了參數，例如 `/user?action=login` ，需開啟參數檢測開關才會生效。

參數	說明
匹配方式	匹配方式預設按照完全符合、首碼匹配、模糊比對的順序排序並執行，您可以在同類規則中調整優先順序，優先順序按列表順序排序，執行規則時按照優先順序進行執行。 ■ **完全符合** 即精確匹配，請求地址必須與配置的URI完全一樣才會被統計。 ■ **首碼匹配** 即包含匹配，只要是請求的URI以此處配置的URI開頭就會被統計。例如，如果設定URI為 `/register` ，則 `/register.html` 會被統計。 ■ **模糊比對** 即根據運算式匹配，當請求的URI與此處的運算式匹配就會被統計。支援用英文句號（.）和星號（*）匹配： ■ 英文句號（.）：表示匹配任意單個字元。 ■ 星號（*）：表示匹配任意重複字元。
檢測及阻斷對象	頻次控制支援的檢測對象如下： ■ **源IP** ■ **請求Header中指定欄位** ■ **訪問網域名稱** ■ **請求URL中指定參數**
檢測時間長度	指定統計訪問次數的周期，需要和檢測對象配合。檢測時間長度為10s~600s（包含10s和600s）。
匹配規則	您可以單擊 **添加規則** ，配置規則的 **類型** 、 **參數** 、 **邏輯符** 和 **值** 。 **說明** 頻次控制命中匹配規則的請求次數是基於單節點進行統計，實際攔截策略生效會滯後，建議您增加訪問頻次，以便更快觸發攔截規則。

參數	說明
阻斷類型	指定觸發條件後的操作，可以是 **封鎖** 或 **人機識別** 。 ■ **封鎖** 觸發條件後直接中斷連線，所有請求返回403。 ■ **人機識別** 觸發條件後用重新導向的方式訪問用戶端（返回200狀態代碼），且系統會自動識別正常訪問和攻擊，對於攻擊行為進行封鎖，只有驗證通過後才允許存取。 例如，單個IP在20秒內訪問超過5次，則進行人機識別判斷，在10分鐘內該IP的訪問請求都需要通過人機識別，如果被識別為非法將會被攔截，只有被識別為合法才會允許存取。
阻斷時間長度	指定執行阻斷動作的時間，阻斷時間大於等於60秒。

iii. 單擊 **確定** 。

自訂規則配置樣本

自訂規則的配置樣本如下表所示。

> **說明** *N*表示可以取任意值，您可以根據實際業務需求設定。

情境	檢測對象	檢測時間長度	匹配規則	阻斷類型	阻斷時間長度
4xx/5xx異常	IP	10秒	`"status_ratio|404">60% && "count">50`	封鎖	10分鐘
QPS異常	網域名稱	10秒	`"count"> N`	人機識別	10分鐘

12.3. 配置CDN聯動DDoS高防

阿里雲CDN推出聯動DDoS高防功能，協助您的加速網域名稱更好地防禦DDoS攻擊。本文為您介紹在控制台配置CDN聯動DDoS高防功能的具體操作。

前提條件

CDN聯動功能正在邀測中，主要針對金融、零售、交通、傳媒及政府等企業級使用者開放，您可以加入DingTalk群（32615821）進行諮詢和開通該功能。在進行配置DDoS高防前，您需要購買DDoS高防執行個體，詳情請參見 DDoS高防控制台 。同時，DDoS高防產品的聯動調度器功能，也可以實現相同功能，建議您直接使用高防功能配置。

背景信息

如果您的業務使用CDN加速，並且需要防禦DDoS攻擊。當攻擊發生時，需要從CDN切換至DDoS高防，您可以使用該功能進行自動化調度。當DDoS攻擊結束後，可以自動將流量切換回CDN進行正常業務分發。

使用情境包括但不限於以下：

- 金融行業

  保障業務分發高可用，提升跨國訪問體驗，同時關注資訊、交易、資料資產的安全防護，避免網路攻擊給企業造成重大風險。

- 零售行業

  保障企業官網，電商平台，訂票平台，內部辦公協同軟體的網路分發品質，同時防護網路安全攻擊，保證業務的持續可用性。

- 傳媒行業

  保障公用媒體內容高效傳播，同時通過網路安全防護保障，避免業務突增和網路攻擊對業務穩定性的影響。

操作步驟

1.
2.
3.
4. 選擇 **安全配置 > CDN聯動DDoS** 。

   如果還未開通該功能，請單擊 **申請開通** 跳轉到DingTalk群進行諮詢和開通。

5. 開啟 **聯動DDoS防護** 開關。
6. 配置 **DDoS聯動產品** 、 **聯動目標類型** 及 **聯動目標** 。

   > **說明** 當前網域名稱沒有查詢到DDoS高防配置。
   >
   > - 未購買DDoS高防：您需要前往 DDoS高防控制台 購買高防執行個體。
   > - 已購買DDoS高防：您需要在 DDoS高防控制台 進行網域名稱配置。

7. 單擊 **確定** 完成配置。

執行結果

返回 **CDN聯動DDoS** 功能頁面，可查看是否配置成功。

您使用聯動DDoS功能，CDN將自動為您建立AliyunServiceRoleForCDNAccessingDDoS角色，並授權CDN使用該角色授權CDN訪問DDoS高防產品中的資源。AliyunServiceRoleForCDNAccessingDDoS角色中包含的許可權包括如下介面：

- DescribeDomainAttackEvents：查詢針對網站業務的攻擊事件。
- DescribeDomainDDoSAttackEvents：查詢DDoS的攻擊事件。
- DescribeDDoSEvents：查詢針對DDoS高防執行個體的攻擊事件。
- DescribeWebRules：查詢網站業務轉寄規則。
- DescribeDomainQPSList：查詢網站業務的QPS統計資訊。
- DescribeCdnLinkageRules：查詢聯動配置。

如果您希望刪除該AliyunServiceRoleForCDNAccessingDDoS角色，您需要關閉所有網域名稱的DDoS聯動功能，然後才能在RAM中刪除該SLR。

12.4. 地區封鎖

阿里雲CDN推出地區封鎖功能，協助您一鍵阻斷來自指定地區的訪問請求，解決部分地區高發的惡意請求問題。

背景信息

目前CDN地區封鎖功能需要您申請開通，如需開通請加入DingTalk群：31327650。

1. 登入 CDN控制台 。
2. 在左側導覽列，單擊 **域名管理**。
3. 在 **域名管理**頁面，單擊目標網域名稱對應的 **管理** 。
4. 在指定網域名稱的左側導覽列，單擊 **安全配置** 。
5. 在 **地區封鎖** 頁面，單擊 **修改配置**。
6. 在 **封鎖設定** 對話方塊，選擇 **封鎖類型** 和 **地區設定** 。

參數	說明
封鎖類型	○ 黑名單 黑名單內的地區均無法訪問當前資源。 ○ 白名單 只有白名單內的地區能訪問當前資源，白名單以外的地區均無法訪問當前資源。 黑名單和白名單互斥，同一時間只支援其中一種方式生效。
地區設定	設定黑白名單的地區。

7. 單擊 **確定**。
8. 當您需要刪除該配置時，單擊 **刪除配置** 。

13.頻寬封頂

功能介紹

頻寬封頂功能是指當統計周期（5分鐘）產生的平均頻寬超出所設定的頻寬最大值時，為了保護您的網域名稱安全，此時網域名稱會自動下線，所有的請求會回到來源站點。此時CDN將停止加速服務，避免異常流量帶來的非日常消費。網域名稱下線後，你可以在控制台重新啟動網域名稱。

> **說明** 頻寬封頂的功能，泛網域名稱暫不支援，設定後不會生效。

RAM子帳號需Cloud Monitor授權後使用，請授權**AliyunCloudMonitorFullAccess**策略組。

如何開啟頻寬封頂功能

1. 網域名稱列表單擊**配置**後，在選中網域名稱配置頁面找到**安全設定**，單擊**修改配置**。
2. 開啟頻寬封頂功能，頻寬單位支援Mbps, Gbps, Tbps。

   > **說明** 頻寬進位為1000。
3. 頻寬封頂功能成功開啟。
4. 您可以根據網域名稱的實際使用方式，選擇開啟或者關閉頻寬封頂功能。

注意事項

開啟頻寬封頂功能後，您的業務會受到頻寬封頂的限制而觸發下線，為了不影響您的網域名稱業務，建議您合理評估，謹慎設定頻寬峰值。

14.網域名稱管理FAQ

本文匯總了使用阿里雲CDN時，網域名稱相關問題及處理方法。