Alibaba Cloud Anti-Bot Service

快速入門

檔案版本：20180929

目錄

1 步驟1：添加網域名稱

購買並開通雲盾爬蟲風險管理產品後，您需要將您的網站網域名稱接入Anti-Bot執行個體實現惡意Bot流量防護。

> 说明：
> 由於Anit-Bot與Web Application Firewall（WAF）採用同樣的轉寄配置，因此如果您已經購買開通阿里雲WAF產品，您無需為已經接入WAF防護的網站網域名稱重新設定Anti-Bot接入，已接入WAF的網站網域名稱將直接顯示在防爬蟲風險管理控制台中，且網域名稱來源為雲端同步。

準備工作

在將您的網站網域名稱接入Anti-Bot執行個體前，您需要完成以下準備工作：

- 需要防護惡意Bot流量的網站網域名稱。

  > 说明：
  > 對於中國大陸地區的Anti-Bot執行個體，所添加的網站網域名稱必須已經通過工信部備案（無需通過阿里雲備案）；對于海外地區的Anti-Bot執行個體，對於網站網域名稱沒有備案要求。

- 該網站網域名稱的來源站點伺服器IP。

  > 说明：
  > 對於一個網站網域名稱，Anti-Bot支援配置多達20個來源站點IP。

- 對於支援HTTPS業務的網站，您還需要準備該網域名稱綁定的認證和私密金鑰資訊。
- 該網站網域名稱的DNS解析記錄的編輯許可權。即確保您在該網域名稱所在的網域名稱解析服務商（如萬網、新網、DNSPod）提供的管理主控台中可以修改該網域名稱的DNS解析記錄。

操作步驟

1. 登入#########，選擇您的Anti-Bot執行個體所在的地區。
2. 定位到網域名稱接入頁面，單擊添加網域名稱。
3. 填寫網站網域名稱相關配置資訊，單擊下一步。

參數	描述	說明
網域名稱	您想要防護的網站網域名稱	支援填寫泛網域名稱（如*.aliyundemo.cn），Anti-Bot將自動匹配該泛網域名稱的次層網域。

參數	描述	說明
		说明： 如果您同時配置泛網域名稱和精確網域名稱（如*.aliyundemo.cn和abc.aliyundemo.cn），Anti-Bot將優先使用精確網域名稱所配置的轉寄規則和防護策略。
協議類型	該網站支援的協議類型。如果您的網站支援HTTPS加密認證，請勾選HTTPS協議，並在添加網站後#########。	如果勾選HTTPS協議類型，可使用進階設定實現HTTP強制跳轉和HTTP回源等功能，保證訪問平滑。
伺服器位址	該網站網域名稱的來源站點伺服器位址。	網站接入Anti-Bot執行個體進行防護後，Anti-Bot會將過濾後的訪問請求轉寄至該伺服器位址。
	（推薦）勾選**IP**，填寫來源站點伺服器的IP（如Elastic Compute Service執行個體的IP、Server Load Balancer執行個體的IP等），配置成功後Anti-Bot將請求轉寄至該來源站點IP。	最多支援配置20個來源站點IP。如果配置多個回源IP，Anti-Bot將自動進行健全狀態檢查和負載平衡。
	勾選其它地址，填寫伺服器回源網域名稱（如Object Storage Service的CNAME等），配置成功後Anti-Bot將請求轉寄至該網域名稱。	伺服器回源網域名稱不應和要防護的網站網域名稱相同。
伺服器連接埠	該網站網域名稱的來源站點連接埠。網站接入Anti-Bot執行個體進行防護後，Anti-Bot會將過濾後的訪問請求轉寄至該連接埠。	HTTP協議預設為80連接埠；HTTPS協議預設為443連接埠。如果您想要使用其它連接埠，可單擊自訂進行添加。
Anti-Bot前是否有七層代理（高防/CDN等）	根據該網站業務的實際情況勾選。	如果該網站在Anti-Bot前需要配置其它七層代理進行轉寄，請務必勾選是，否則Anti-Bot將無法擷取訪問該網站的用戶端真實IP資訊。

參數	描述	說明
負載平衡演算法	如果配置多個來源站點IP，勾選**IP hash**或輪詢，Anti-Bot將根據所選擇的方式分發訪問請求，實現負載平衡。	-

4. 選擇修改該網域名稱DNS解析的方式（手動修改、CDN修改），單擊下一步，完成添加網域名稱資訊。

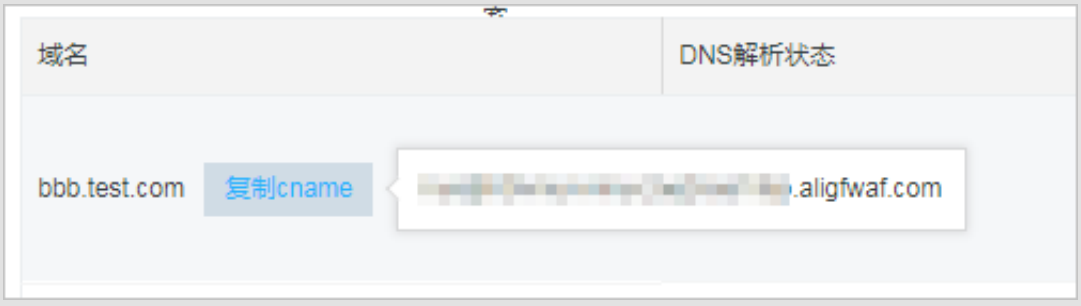
> 说明：
> 在*#######DNS##*前，建議您先*##################Anti-Bot##IP#*並*#####################*，確保該網站的訪問請求可以正常轉寄回來源站點伺服器。

網站網域名稱資訊添加成功後，Anti-Bot將自動為該網域名稱分配一個CNAME。通過將該網站網域名稱的訪問解析到該CNAME，所有訪問請求即可先經過該Anti-Bot執行個體後被轉寄至來源站點伺服器，實現安全防護。

> 说明：
> 如果想要擷取該網域名稱所分配到的Anti-Bot執行個體的IP，您通過Ping該網域名稱所分配到CNAME解析得到的IP即是所分配的Anti-Bot執行個體的IP。一般情況下，所分配的Anti-Bot執行個體IP不會頻繁變更。

登入##########，在網域名稱接入頁面，選擇已添加的網站網域名稱，將滑鼠移至複製**CName**按鈕上即可查看Anti-Bot為該網站網域名稱分配的CNAME。

> 说明：
> 單擊複製**CName**可將該CNAME複製到剪貼簿中。



上傳**HTTPS**認證和私密金鑰（僅適用於**HTTPS**網站）

如果您添加的網站支援HTTPS加密認證，且已勾選HTTPS協議類型，在添加網域名稱後，您還需要在##########上傳相應的認證和私密金鑰，否則將無法通過HTTPS協議訪問該網站。

網域名稱資訊添加成功後，在網域名稱接入頁面中，該網站網域名稱的HTTPS協議狀態將顯示為異常，提示您當前認證配置有誤。

參考以下步驟，為該網站網域名稱上傳認證和私密金鑰：

1. 登入#########，在網域名稱接入頁面，選擇該網站網域名稱。
2. 單擊HTTPS協議狀態右側的上傳認證按鈕。
3. 在更新認證對話方塊中，選擇上傳方式。
   - 勾選手動上傳，填寫認證名稱，將該網站網域名稱所綁定的認證檔案和私密金鑰檔案中的常值內容分別複製粘貼到認證檔案和私密金鑰檔案文字框中。

     说明：
     對於一般格式的認證（如.pem、.cer、.crt等格式的認證），您可用文字編輯器直接開啟認證檔案複製其中的常值內容；對於其他格式的認證（如.pfx、.p7b等格式的認證）的認證，則需要將認證檔案轉換成.pem格式後再用文字編輯器開啟來複製其中的常值內容。關於認證格式的轉換方式，請查看*HTTPS#####PEM##*。

     说明：
     如果該HTTPS認證有多個認證檔案（如憑證鏈結），需要將認證檔案中的常值內容拼接合并後粘貼至認證檔案文字框中。

     認證檔案常值內容範例

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx8ixZJ4krc+1M+
j2kcubVpsE2
cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOk
jgvhlqt9vc
65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9
nIrHsPl8YKk
vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

     私密金鑰檔案常值內容範例

```
-----BEGIN RSA PRIVATE KEY-----
DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQ
```

```
Cr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJ
aiygoIYo
aMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDz
FdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

- 如果該網站網域名稱所綁定的HTTPS認證已添加至該雲帳號的雲盾認證服務進行管理，勾選選擇已有認證，直接選擇該認證即可。

4. 單擊儲存，該網域名稱所綁定的認證和私密金鑰即上傳成功，HTTPS協議狀態更新為正常。

2 步驟2：配置允許存取Anti-Bot回源IP段

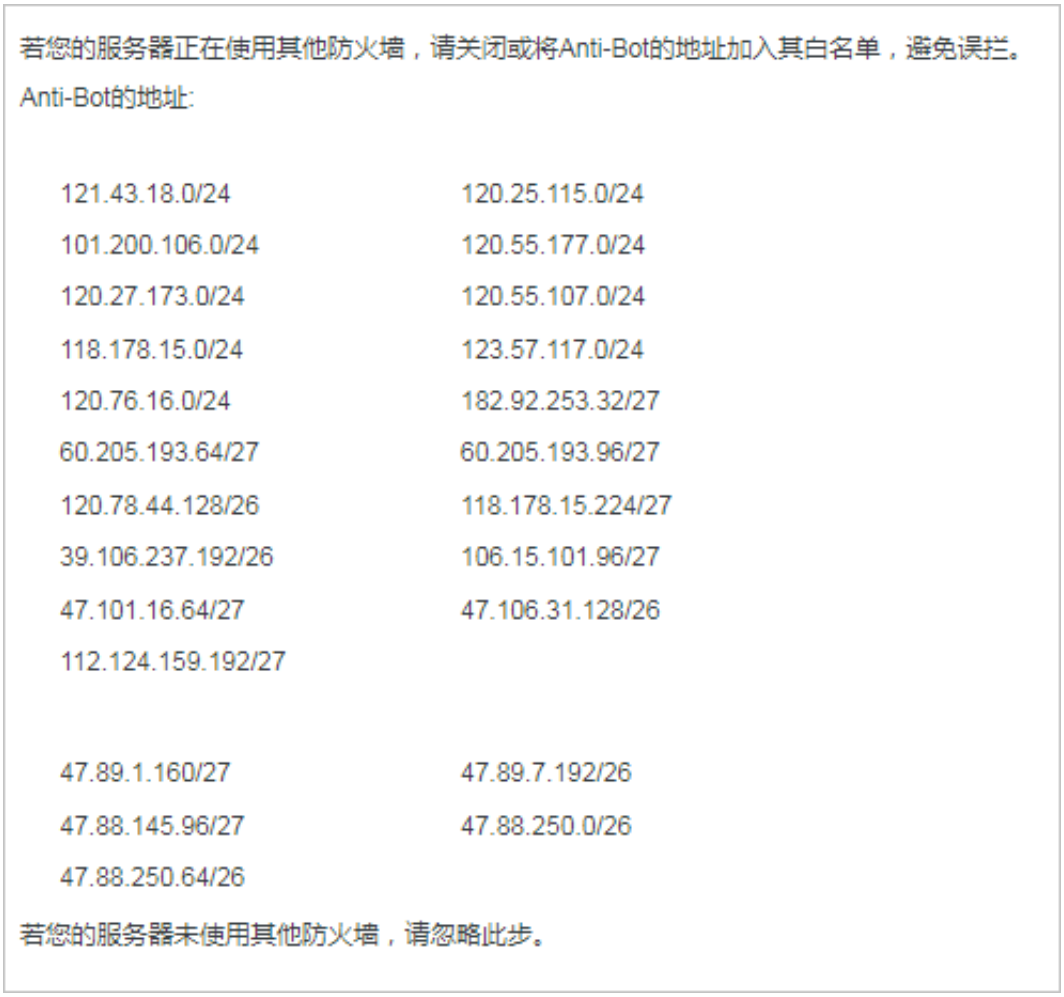
您的網站網域名稱成功接入Anti-Bot防護後，訪問您網站的所有請求將先流轉到Anti-Bot執行個體，經Anti-Bot執行個體過濾惡意Bot流量後再返回到來源站點伺服器。其中，流量經Anti-Bot執行個體返回來源站點的操作稱為回源。

由於Anti-Bot執行個體的IP數量有限，來源站點伺服器收到的所有請求都將來自這些IP，在來源站點伺服器上的安全軟體（如安全狗、雲鎖）看來，這種情況是很可疑的，且可能會屏蔽Anti-Bot執行個體的回源IP。因此，在接入Anti-Bot防護後，您需要在來源站點伺服器的其它防火牆、安全軟體上設定允許存取所有Anti-Bot回源IP。

操作步驟

防爬風險管理控制台提供了最新的回源IP段列表，您可以參照以下步驟進行操作：

1. 在您將網域名稱資訊添加至Anti-Bot執行個體時，您會看到Anti-Bot執行個體的回源IP端。



2. 在來源站點伺服器的防火牆、安全軟體上，將步驟1中的IP段添加到白名單中。

常見問題

什麼是回源**IP**？

回源IP是Anti-Bot用來代理用戶端請求伺服器時用的源IP，在伺服器看來，接入Anti-Bot防護後所有源IP都會變成Anti-Bot執行個體的回源IP，而真實的用戶端地址會被加在HTTP頭部的XFF欄位中。

在接入Anti-Bot執行個體後，您應確保來源站點已將Anti-Bot的全部回源IP允許存取（加入白名單），不然可能會出現網站打不開或開啟極其緩慢等情況。

為何要允許存取回源**IP**段？

接入Anti-Bot執行個體後，Anti-Bot作為一個反向 Proxy存在於用戶端和伺服器之間，伺服器的真實IP被隱藏起來，用戶端只能看到Anti-Bot執行個體，而看不到來源站點伺服器。

因此，在來源站點（真實伺服器）看來，所有的請求源IP都會變成Anti-Bot執行個體的回源IP段。

由於來源的IP變得更加集中，頻率會變得更快，來源站點伺服器上的防火牆或安全軟體很容易認為這些IP在發起攻擊，從而限制來自這些IP的訪問。一旦Anti-Bot執行個體的回源IP被封鎖，由Anti-Bot執行個體轉寄的請求將無法得到來源站點的正常響應，故務必確保Anti-Bot的回源IP在來源站點上不會被攔截。

3 步驟3：本地驗證轉寄配置生效

在把業務流量切到Anti-Bot上之前，建議您先通過本地驗證確保一切配置正常，Anti-Bot轉寄正常。本地驗證需要在本地類比接入Anti-Bot，然後訪問被防護網站，驗證Anti-Bot執行個體正常轉寄訪問請求。

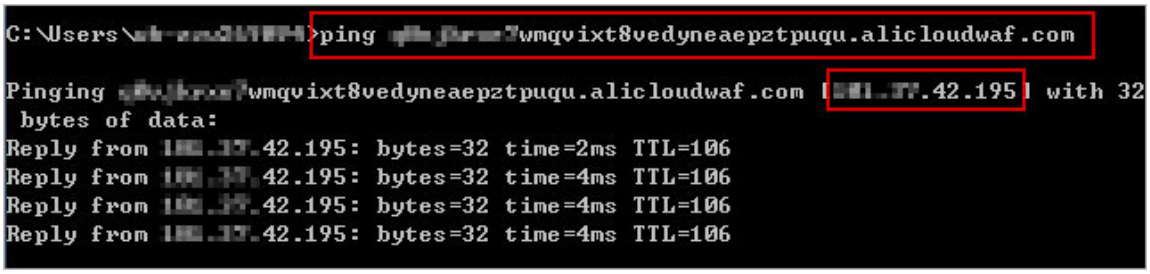
本地接入**Anti-Bot**

通過修改本地hosts檔案（*###hosts##*）類比接入Anti-Bot，將從本地訪問被防護網站的請求導向Anti-Bot執行個體。以Windows作業系統為例：

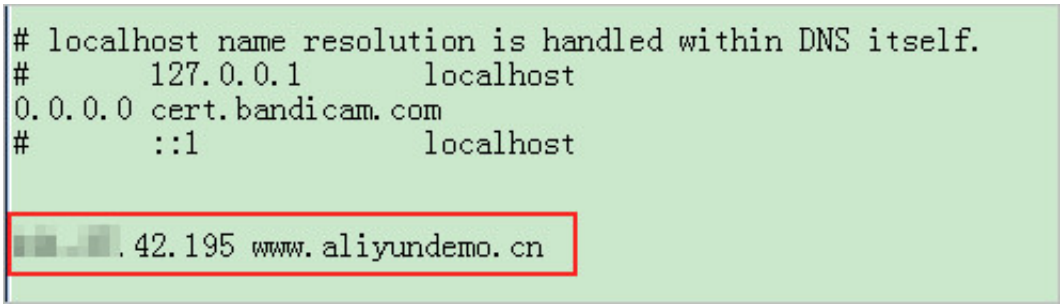
1. 用記事本或notepad++等文字編輯器開啟hosts檔案，hosts檔案一般位於`C:\Windows\System32\drivers\etc\hosts`路徑。
2. 在最後一行添加如下內容：`Anti-Bot`執行個體的`IP` 被防護的網域名稱。

   以網域名稱`www.aliyundemo.cn`為例，該網域名稱已按照*##1#######*添加到Anti-Bot執行個體中，且Anti-Bot為其分配了以下CNAME值：`xxxxxxxxxxxxxxx.alicloudwaf.com`

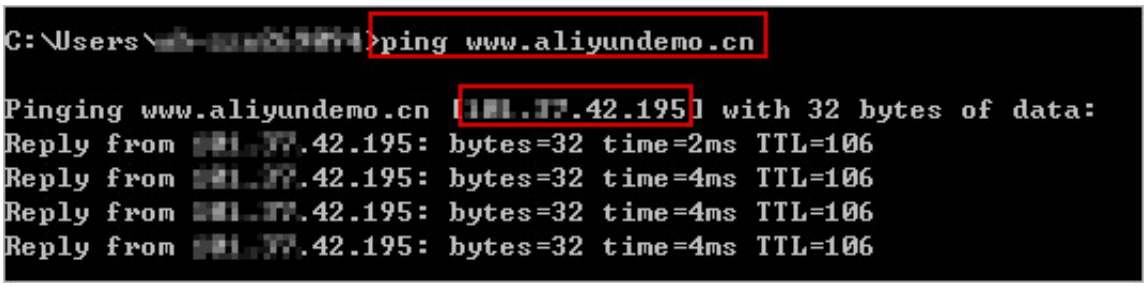
   a. 在Windows中開啟cmd命令列工具，運行`ping xxxxxxxxxxxxxxx.alicloudwaf.com`命令擷取Anti-Bot執行個體的IP。如下圖所示，在響應結果中可以看到用來防護您的網域名稱的Anti-Bot執行個體的IP。

   b. 在hosts檔案添加如下內容，前面的IP地址即上一步擷取的Anti-Bot執行個體的IP地址，後面的網域名稱即被防護的網域名稱。

3. 修改hosts檔案後儲存，然後本地對被防護的網域名稱執行`ping`命令。



預期此時解析到的IP地址應該是剛才綁定的Anti-Bot執行個體的IP地址。如果依然是來源站點地址，可嘗試重新整理本地的DNS緩衝（Windows的cmd下可以使用`ipconfig /flushdns`命令）。

驗證Anti-Bot轉寄正常

確認hosts綁定已經生效（網域名稱已經本地解析為Anti-Bot執行個體的IP）後，開啟瀏覽器，輸入該網域名稱進行訪問，如果Anti-Bot的網域名稱接入配置正確，預期網站能夠正常開啟。

上述驗證通過後，您可以參照*##4###DNS##*，把業務流量正式切換至Anti-Bot上。

4 步驟4：修改DNS解析

通過修改網域名稱的DNS解析記錄將網站網域名稱解析到Anti-Bot，完成業務正式接入。

建議您使用CNAME方式接入Anti-Bot，成功添加網域名稱到防爬風險管理控制台後，Anti-Bot會為網域名稱分配一個CNAME值，您只需添加/修改網域名稱的CNAME解析記錄為分配的CNAME值，即可完成接入。

说明：

參考*##1#######*中的方法查看並記錄Anti-Bot為該網站網域名稱分配的CNAME值，如`xxxxxxxxxxxx.alicloudwaf.com`。

CNAME接入說明

Anti-Bot通常採用CNAME解析的方式將網站接入進行防護，也支援A記錄解析的方式接入。

说明：

強烈建議您採用CNAME解析的方式。因為在某些極端情況下（如節點故障、機房故障等），通過CNAME解析方式接入Anti-Bot，可以實現自動切換節點IP甚至將直接解析切回來源站點，從而最大程度保證業務的穩定運行，提供高可用性和災備能力。

如果必須使用A記錄解析的方式接入（例如，@記錄與MX記錄衝突等情況），您可以通過Ping Anti-Bot分配的CNAME值擷取所分配的Anti-Bot執行個體的IP（該IP地址一般不會頻繁變更），然後將網站網域名稱通過A記錄解析的方式接入Anti-Bot進行防護。

網域名稱主機記錄說明

關於網域名稱的主機記錄，以網域名稱`abc.com`為例：

- www： 用於精確匹配www開頭的網域名稱，如`www.abc.com`，但無法匹配`abc.com`
- @： 用於匹配直接存取`abc.com`的情況
- *： 用於匹配泛網域名稱，即匹配任意網域名稱，如`blog.abc.com`、`www.abc.com`、`abc.com`等

修改**DNS**解析記錄的注意事項

- 對於同一個主機記錄，CNAME解析記錄值只能填寫一個，您可以將該記錄值修改為Anti-Bot的CNAME值，從而將網站網域名稱接入Anti-Bot進行防護。
- 由於不同DNS解析記錄類型存在衝突，對於同一個主機記錄，CNAME記錄與A記錄、MX記錄、TXT記錄等其他記錄互相衝突。您需要刪除原其它記錄後再添加CNAME記錄解析記錄，或者將原記錄類型修改為CNAME類型。

说明：
刪除其它解析記錄並新增CNAME解析記錄的過程應儘可能在短時間內完成。如果刪除A記錄後長時間沒有添加CNAME解析記錄，可能導致網域名稱無法正常解析。

- 如果必須保留MX記錄（郵件伺服器記錄），您可以使用A記錄解析的方式將網域名稱解析到Anti-Bot的IP。通過Ping CNAME擷取所分配的Anti-Bot執行個體的IP（該IP地址一般不會頻繁變更）後，將網站網域名稱A解析記錄類型的記錄值修改為該Anti-Bot執行個體的IP。

说明：
使用A記錄解析的方式進行接入，Anti-Bot將無法支援自動故障叢集調度和故障bypass操作。

操作步驟

本文以阿里雲Alibaba Cloud DNS和花生殼為例，介紹DNS配置方式，其它DNS供應商可以參考本文檔進行類似配置。

阿里雲雲解析配置樣本

说明：
如果您使用*###Alibaba Cloud DNS*進行網域名稱解析，並且在執行*##1#######*前已經為網域名稱設定並啟用了A記錄（且如果是中國大陸網域名稱，已完成備案），則您在添加網站配置時，可以一鍵添加網站並自動更新解析記錄。以下操作步驟適用於您的網域名稱已經添加到Anti-Bot網域名稱列表，但DNS解析狀態為異常的情況。

參照以下步驟，在阿里雲雲解析修改CNAME記錄來接入Anti-Bot：

1. 登入*#########*。
2. 選擇要操作的網域名稱，單擊其操作列的解析設定。
3. 選擇要操作的主機記錄，單擊其操作列下的修改。

说明：
您也可以刪除已有的A記錄，然後單擊添加記錄，添加一條新的CNAME記錄。刪除原解析記錄後，請儘快添加CNAME解析記錄，否則可能導致網站網域名稱解析失敗。

4. 將記錄類型修改為**CNAME**，記錄值修改為Anti-Bot所分配的CNAME值。

说明：
TTL值一般建議設定為600秒（即10分鐘）。TTL值越大，則DNS記錄的同步和更新越慢。

花生殼配置樣本

部分網域名稱供應商（如花生殼）可能不支援直接修改已有解析記錄的記錄類型和主機記錄，您需要刪除原有的A記錄後，再添加新的CNAME解析記錄。


说明：
删除原解析記錄後，請儘快完成添加CNAME解析記錄，否則可能導致網站網域名稱解析失敗。

驗證DNS配置

將網站網域名稱的DNS解析切換至Anti-Bot後，您的網站網域名稱即接入Anti-Bot進行防護。解析記錄配置完成後，您可以通過Ping網站網域名稱的方式或*17ce*等其他工具驗證DNS解析生效情況。


说明：
由於DNS解析記錄生效需要一定時間，如果本地測試網域名稱無法訪問，您可以等待10分鐘後重新檢查。

5 DNS解析狀態異常說明

當網站網域名稱接入Anti-Bot後，您可以在#########的網域名稱接入頁面查看網站網域名稱的接入狀態，即DNS解析狀態。

如果網域名稱的DNS解析狀態顯示異常，則該網站網域名稱可能沒有正確接入Anti-Bot，請檢查網域名稱接入配置是否正確。

如果您確認已將該網站網域名稱解析到Anti-Bot執行個體分配的CNAME記錄，並且網站可以正常訪問，請諮詢阿里雲支援人員團隊。

DNS解析狀態判定條件說明

Anti-Bot根據以下條件判定已接入網域名稱的DNS解析狀態：

> 说明：
> 滿足其中一個條件即判定為DNS解析狀態正常，已接入Anti-Bot防護。

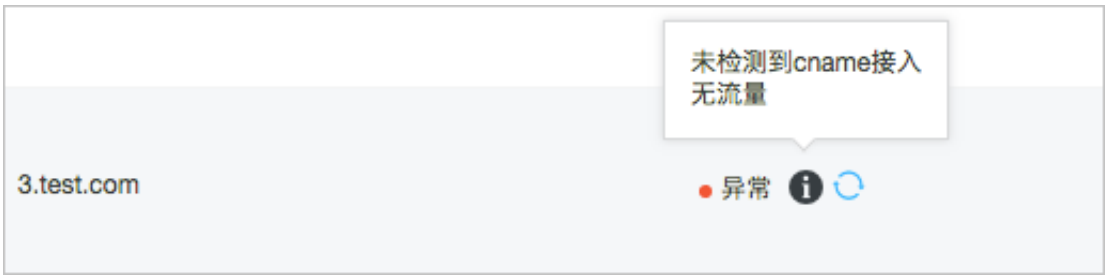
- 條件**1**：接入的網域名稱已通過CNAME記錄解析至Anti-Bot執行個體。
- 條件**2**：接入的網域名稱已有一定流量經過Anti-Bot執行個體。其中，在五秒內至少有大於10個請求才判定為有一定流量。如果每分鐘只有兩、三個請求，由於流量過低仍將判定為無流量。

  > 说明：
  > 您可以在資料報表 > 風險監控報表中查看網站網域名稱的歷史流量資訊。

常見DNS解析狀態異常說明

- 使用精確網域名稱（即不包含“*”的網域名稱，例如`3.test.com`）接入**Anti-Bot**

  如果即沒有通過CNAME記錄解析至Anti-Bot，又沒有一定流量經過Anti-Bot執行個體，則DNS解析狀態顯示以下異常說明：



- 使用泛網域名稱（例如`*.test.com`）接入**Anti-Bot**

  如果DNS解析狀態異常，僅可能顯示以下異常說明：

- **Anti-Bot**前部署其它七層代理（例如**CDN**）

  假設部署的接入方式為CDN->Anti-Bot，網站網域名稱將被解析至CDN，因此Anti-Bot不會檢測到CNAME接入。同時，CDN轉寄至Anti-Bot的流量比較低，可能出現由於請求量太小無法達到DNS解析狀態檢測條件，導致DNS解析狀態顯示為異常。在這種情境中，DNS解析狀態異常不一定表明網域名稱未正確接入Anti-Bot，只要您確認網域名稱接入配置正確且網站能正常訪問即可。

6 App增強防護SDK

6.1 方案概述

Anti-Bot針對原生App端提供安全SDK解決方案。為您的App提供可信通訊、防機器指令碼濫刷等安全防護，有效識別高風險手機、貓池、牧場等特徵。

App端安全SDK方案整合了阿里巴巴集團多年來對抗黑灰產、羊毛黨的經驗和技術積累。將您的App整合Anti-Bot安全SDK後，您的App將獲得與天貓、淘寶、支付寶等App端相同的可信通訊技術能力，並可共用阿里巴巴集團多年對抗黑灰產、羊毛黨所積累的惡意裝置指紋庫，從根本上協助您解決App端的安全問題。

Anti-Bot提供的App端安全SDK方案協助您解決以下原生**App**端的安全問題：

- 惡意註冊、撞庫、暴力破解
- 針對App的大流量CC攻擊
- SMS/驗證碼介面被刷
- 薅羊毛、搶紅包
- 惡意秒殺限時限購商品
- 惡意查票、刷票（例如，機票、酒店等情境）
- 價值資訊爬取（例如，價格、徵信、融資、小說等內容）
- 機器批量投票
- 灌水、惡意評論

配置App端安全SDK方案

參考以下操作步驟，為您的App配置安全SDK解決方案：

> 说明：
> 配置App端安全SDK方案，您無需在伺服器端進行任何改動。配置完成後，Anti-Bot將自動過濾惡意請求，將合法的請求轉寄給來源站點伺服器。惡意請求產生的壓力將全部由Anti-Bot承擔，保障您的伺服器端穩定運行。

1. 登入##########，選擇您的Anti-Bot執行個體所在的地區。
2. 定位到網域名稱接入頁面，單擊添加網域名稱，為您App端使用的網域名稱添加網域名稱接入配置。具體操作步驟，參考########。
3. 在您App使用的網域名稱的DNS解析服務提供者處，添加Anti-Bot執行個體分配的CNAME記錄，將App的網域名稱解析指向Anti-Bot執行個體。具體操作步驟，參考*##DNS##*。

4. 在您的App中整合Anti-Bot提供的SDK組件。

    说明：
   整合SDK工作可能需要您投入1-2天時間的工作量。

   關於整合SDK的詳細操作說明，參考：

   - *iOS SDK####*
   - *Android SDK####*

5. 測試通過後，打包並發布已整合SDK的新App版本，即可享受App端安全SDK解決方案為您提供的安全防護。