開發人員指南

Amazon Route 53

API 版本 2013-04-01

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Route 53: 開發人員指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，或由 Amazon 贊助。

Table of Contents

什麼是 Amazon Route 53？ 1
網域註冊的運作方式 2
如何將網際網路流量路由到您的網站或 Web 應用程式 3
如何設定 Amazon Route 53 為網域路由網際網路流量的概觀 3
Amazon Route 53 如何為您的網域路由流量 4
Amazon Route 53 檢查資源的運作狀態 6
Amazon Route 53 概念 7
網域註冊概念 8
網域名稱系統 (DNS) 概念 9
控制和資料平面概念 13
運作狀態檢查概念 14
如何開始使用 Amazon Route 53 15
相關服務 15
存取 Amazon Route 53 15
AWS Identity and Access Management 16
Amazon Route 53 定價和計費 16
使用 AWS SDK 17
設定 18
註冊 AWS 帳戶 18
建立管理使用者 18
下載工具 19
開始使用 21
將您的網域用於靜態網站 21
必要條件 22
步驟 1：註冊網域 22
步驟 2：為根網域建立 S3 儲存貯體 23
步驟 3 (選用)：為根網域建立另一個 S3 儲存貯體 23
步驟 4：設定網站託管的根網域儲存貯體 24
步驟 5：(選用)：設定用於網站重新引導的子網域儲存貯體 25
步驟 6：上傳索引以建立網站內容 25
步驟 7：編輯 S3 封鎖公有存取設定 26
步驟 8：連接儲存貯體政策 27
步驟 9：測試您的網域端點 28
步驟 10：將您網域的 DNS 流量路由到您的網站儲存貯體 28

步驟 11：測試您的網站 30
步驟 12（可選）：使用 Amazon CloudFront 加快內容的分發 31
使用 Amazon CloudFront 分發服務靜態網站 31
必要條件 32
步驟 1：註冊網域 32
步驟 2：請求公有憑證 32
步驟 3：建立 S3 儲存貯體以託管您的子網域 33
步驟 4：為您的根網域建立另一個 S3 儲存貯體 34
步驟 5：將網站檔案上傳到您的子網域儲存貯體 34
步驟 6：設定用於網站重新引導的根網域儲存貯體 35
步驟 7：為您的子域創建 Amazon CloudFront 分發 36
步驟 8：為您的根網域建立 Amazon CloudFront 分發 37
步驟 9：將您網域的 DNS 流量路由到您的 CloudFront 分佈 38
步驟 10：測試您的網站 39
與其他服務整合 41
記錄、監控和標記 41
將流量路由到其他 AWS 資源 41
DNS 網域名稱格式 44
為網域名稱註冊設定網域名稱的格式 44
為託管區域和記錄設定網域名稱的格式 44
在託管區域和記錄的名稱中使用星號 (*) 45
設定國際化網域名稱的格式 46
註冊和管理網域 48
註冊新網域 49
註冊新網域 49
註冊或轉移網域時所指定的值 61
Amazon Route 53 在您註冊網域時傳回的值 66
檢視網域註冊的狀態 67
更新網域設定 69
更新網域的聯絡資訊和所有權 69
為網域的聯絡資訊啟用或停用隱私權保護 79
啟用或停用網域自動續約 81
鎖定網域以防止未經授權轉移到另一個註冊商 83
延長網域的註冊期間 84
更新名稱伺服器以使用其他註冊商 87
新增或變更網域的名稱伺服器和黏附記錄 89

續約網域的註冊 94
還原已過期或已刪除的網域 96
更換網域的託管區域 98
轉移網域 99
將網域註冊轉移到 Route 53 99
檢視網域轉移的狀態 122
將網域轉移到 Route 53 對過期日期有何影響 125
將網域轉移到其他 AWS 帳戶 126
從 Route 53 轉移網域 129
重新傳送授權和確認電子郵件 138
更新您的電子郵件地址 139
重新傳送電子郵件 139
設定網域的 DNSSEC 143
DNSSEC 如何保護網域的概觀 144
為網域設定 DNSSEC 的先決條件和上限 145
為網域新增公開金鑰 145
刪除網域的公開金鑰 148
尋找註冊商 150
檢視網域的相關資訊 150
刪除網域名稱註冊 151
就網域註冊問題聯絡 S AWS upport 155
如果您可以登入您的 AWS 帳戶，請聯絡 AWS Support 部門 156
如果您無法登入 AWS 帳戶，請聯絡 AWS Support 部門 157
下載網域帳單報告 157
可向 Amazon Route 53 註冊的網域 159
支援的頂層網域的索引 159
一般頂層網域 163
地理頂層網域 416
將 Amazon Route 53 設定為 DNS 服務 473
將 Route 53 設定為現有網域的 DNS 服務 473
將 Route 53 做為使用中網域的 DNS 服務 474
將 Route 53 設定為非作用中網域的 DNS 服務 481
設定新網域的 DNS 路由 485
將流量路由至您的資源 486
路由傳送子網域的流量 486
使用託管區域 492

使用公有託管區域 492
使用私有託管區域 515
將託管區域遷移到其他 AWS 帳戶 525
處理記錄 535
選擇路由政策 536
選擇別名或非別名記錄 555
支援的 DNS 記錄類型 558
使用 Amazon Route 53 主控台來建立記錄 571
資源記錄集許可 574
您指定的值 574
透過匯入區域檔案建立記錄 657
編輯記錄 659
刪除記錄 659
列出記錄 660
使用流量流程來路由 DNS 流量 662
建立和管理流量政策 664
建立和管理政策記錄 677
設定 DNSSEC 簽署 682
啟用 DNSSEC 簽署並建立信任鏈 683
停用 DNSSEC 簽署 692
使用客戶受管金鑰 696
使用金鑰簽署金鑰 (KSK) 696
Route 53 中的 KMS 金鑰和 ZSK 管理 699
DNSSEC 不存在於 Route 53 中的證明 700
DNSSEC 簽署故障診斷 701
使用 AWS Cloud Map 建立記錄和運作狀態檢查 702
DNS 限制和行為 702
最大回應大小 702
授權區段處理 702
其他區段處理 702
什麼是 Route 53 Resolver？ 703
在 VPC 和您網路之間解析 DNS 查詢 705
您網路上的 DNS 解析程式如何將 DNS 查詢轉送至 Route 53 Resolver 端點 708
Route 53 Resolver 端點如何從您的 VPC 轉送 DNS 查詢到您的網路 708
建立傳入和傳出端點時的注意事項 715
Route 53 解析器可用性和擴展 718

開始使用 Route 53 Resolver 720
將傳入 DNS 查詢轉送到您的 VPC 722
設定傳入轉送 722
當您建立或編輯傳入端點時所指定的值 722
將傳出 DNS 查詢轉送到您的網路 725
設定傳出轉送 726
當您建立或編輯傳出端點時所指定的值 727
當您建立或編輯規則時所指定的值 730
管理傳入端點 731
檢視和編輯傳入端點 731
檢視傳入端點的狀態 732
刪除傳入端點 733
管理傳出端點 733
檢視和編輯傳出端點 734
檢視輸出端點的狀態 734
刪除傳出端點 735
管理轉送規則 736
檢視和編輯轉送規則 736
建立轉送規則 737
新增反向查詢的規則 737
建立轉送規則與 VPC 的關聯 738
取消轉送規則與 VPC 的關聯 738
與其他 AWS 帳戶共享解析器規則並使用共享規則 739
刪除轉送規則 741
Resolver 中反向 DNS 查詢的轉送規則 742
啟用 DNSSEC 驗證 743
將網際網路流量路由到您的 AWS 資源 744
Amazon API Gateway API 744
必要條件 745
設定 Route 53 將流量路由到 API Gateway 端點 745
Amazon CloudFront 分佈 747
必要條件 748
設定 Amazon 路由 53 以將流量路由到分 CloudFront 發 748
Amazon EC2 執行個體 750
必要條件 751
設定 Amazon Route 53 將流量路由到 Amazon EC2 執行個體 751

App Runner 服務 753
必要條件 753
設定 Amazon Route 53 將流量路由到 App Runner 服務 754
AWS Elastic Beanstalk 環境 755
將應用程式部署至 Elastic Beanstalk 環境 755
取得 Elastic Beanstalk 環境的網域名稱 755
建立 Route 53 記錄 756
ELB 負載平衡器 759
必要條件 759
設定 Amazon Route 53 將流量路由到 ELB 負載平衡器 759
Amazon S3 儲存貯體 761
必要條件 762
設定 Amazon Route 53 將流量路由到 S3 儲存貯體 762
Amazon Virtual Private Cloud 介面端點 764
必要條件 764
Amazon VPC 介面端點 765
Amazon WorkMail 766
其他 AWS 資源 769
建立運作狀態檢查和設定 DNS 備援 770
運作狀態檢查的類型 771
Route 53 決定運作狀態檢查是否良好的方式 772
Route 53 如何判斷監控端點的運作狀態檢查的狀態 772
Route 53 如何判斷監控其他運作狀態檢查的檢查狀態 774
Route 53 如何判斷監控 CloudWatch 警示的健康狀態檢查狀態 774
建立、更新和刪除運作狀態檢查 775
建立和更新運作狀態檢查 775
您在建立或更新運作狀態檢查時指定的值 776
當您建立運作狀態檢查時 Route 53 顯示的值 788
變更 CloudWatch 鬧鐘設定時更新健康狀態檢查 788
刪除運作狀態檢查 789
當已設定 DNS 備援時，更新或刪除運作狀態檢查 790
為運作狀態檢查設定路由器和防火牆規則 791
監控運作狀態檢查狀態和取得通知 791
檢視運作狀態檢查狀態和運作狀態檢查失敗的原因 792
監控運作狀態檢查程式和端點之間的延遲 793
使用 CloudWatch 監控運作狀態檢查 795

設定 DNS 備援 801
設定 DNS 備援的任務清單 802
簡單組態中運作狀態檢查的運作方式 803
複雜組態中運作狀態檢查的運作方式 806
當您已設定運作狀態檢查時，Route 53 會如何選擇記錄 813
主動-主動和主動-被動容錯移轉 815
在私有託管區域中設定容錯移轉 818
Route 53 如何避免容錯移轉問題 818
命名和標記運作狀態檢查 819
標籤限制 820
新增、編輯和刪除運作狀態檢查的標籤 820
使用 2012-12-12 之前的 API 版本 822
Route 53 Resolver DNS 防火牆 823
Route 53 Resolver DNS 防火牆的運作方式 824
DNS 防火牆元件和設定 824
Route 53 Resolver DNS 防火牆如何篩選 DNS 查詢 825
使用 DNS 防火牆的高階步驟 826
在多個區域中使用 DNS 防火牆規則群組 827
開始使用 Route 53 Resolver DNS 防火牆 827
Route 53 Resolver DNS 防火牆圍牆花園範例 827
Route 53 Resolver DNS 防火牆封鎖清單範例 829
DNS 防火牆規則群組與規則 831
DNS 防火牆中的規則群組設定 832
DNS 防火牆中的規則設定 832
DNS 防火牆中的規則動作 834
管理 DNS 防火牆中的規則群組和規則 835
Route 53 Resolver DNS 防火牆網域清單 837
受管網域清單 837
管理您自己的網域清單 842
為 DNS 防火牆設定查詢日誌記錄 844
在多個 帳戶之間共用 規則群組 845
為 VPC 啟用 DNS 防火牆保護 848
管理 VPC 與防火牆規則群組之間的關聯 848
DNS 防火牆 VPC 組態 849
什麼是 Amazon Route 53 on Outposts？ 851
Route 53 on Outposts 功能 851

將 AWS Outposts 與 VPC 中斷連線時的 Route 53 Resolver 行為 852
開始在 AWS Outposts 上使用 Route 53 Resolver 852
建立傳入端點 853
當您在 Outpost 上建立或編輯傳入端點時所指定的值 854
建立傳出端點 855
當您在 AWS Outposts 中建立或編輯傳出端點時所指定的值 856
建立傳出端點的轉送規則 857
管理 Outpost 上的解析程式 858
編輯 Outpost 上的解析程式 858
檢視 Outpost 上的解析程式狀態 858
刪除 Outpost 上的解析程式 859
在 Outpost 上管理解析程式上的傳入端點 860
檢視和編輯傳入端點 860
檢視傳入端點的狀態 861
刪除傳入端點 862
在 Outpost 上管理解析程式上的傳出端點 862
檢視和編輯傳出端點 863
檢視輸出端點的狀態 863
刪除傳出端點 864
建立 AWS CloudFormation 資源。 866
Route 53、Route 53 Resolver 和 AWS CloudFormation 範本 866
進一步了解 AWS CloudFormation 867
程式碼範例 868
Route 53 868
動作 869
53 號路線域名註冊 871
動作 877
案例 907
安全性 940
資料保護 940
防止懸置委派記錄 941
身分識別和存取權管理 942
使用身分驗證 943
存取控制 946
管理存取概觀 946
針對 Route 53 使用 IAM 政策 951

使用服務連結角色 962
AWS 受管政策 966
使用 IAM 政策條件管理資源記錄集 974
Route 53 API 許可參考 980
記錄和監控 981
合規驗證 982
復原能力 983
基礎設施安全性 983
監控 984
公有 DNS 查詢日誌記錄 984
為 DNS 查詢設定日誌記錄 985
使用 Amazon CloudWatch 訪問 DNS 查詢日誌 986
變更日誌的保留期間並將日誌匯出到 Amazon S3 987
停止查詢日誌記錄 987
出現在 DNS 查詢日誌中的值 988
查詢日誌範例 989
解析程式查詢日誌記錄 989
您可以將 Resolver 查詢日誌傳送至其中的資源 991
管理組態 993
監控網域註冊 1000
使用 Amazon Route 53 健康檢查和 Amazon 監控您的資源 CloudWatch 1000
運作狀態檢查的指標與維度 1000
使用 Amazon 監控託管區域 CloudWatch 1003
CloudWatch Route 53 公共託管區域的度量 1003
CloudWatch Route 53 公共託管區域量度的維度 1005
使用 Amazon 監控 Route 53 解析器端點 CloudWatch 1005
Resolver 的指標與維度 1005
使用 Amazon 監控 Route 53 解析器 DNS 防火牆規則群組 CloudWatch 1008
DNS 防火牆的指標與維度 1008
使用管理 DNS 防火牆事件 EventBridge 1011
Route 53 解析程式 DNS 防火牆事件 1011
傳送 DNS 防火牆事件 1012
許可 1014
其他資源 1014
事件 DNS 防火牆詳細資料參 1015
使用日誌記錄 Amazon 路線 53 API 調用 AWS CloudTrail 1021

53 號路線資訊 CloudTrail 1022
檢視事件歷史記錄中的 Route 53 事件 1023
了解 Route 53 日誌檔案項目 1023
故障診斷 1031
我的網域在網際網路上不可用 1031
您註冊新的網域，但沒有按一下確認電子郵件中的連結 1031
您將網域註冊轉移到 Amazon Route 53，但未轉移 DNS 服務 1032
您轉移網域註冊並在網域設定中指定錯誤的名稱伺服器 1033
您先轉移 DNS 服務，但沒有等待足夠長時間就轉移網域註冊 1034
刪除 Route 53 用於路由網域網際網路流量的託管區域 1035
您的網域已暫停 1035
我的網域已暫停使用 (狀態為 ClientHold) 1036
您註冊新的網域，但沒有按一下確認電子郵件中的連結 1036
您已停用網域自動續約，而且網域已過期 1037
您已變更註冊申請人的聯絡人電子郵件地址，但您尚未驗證新的電子郵件地址是有效的 1037
我們無法處理您的自動網域續約付款，而且網域已過期 1037
使用者違反 AWS 可接受的使用政策，因此我們暫停網域 1038
由於法院判決而暫停網域 1038
我的網域轉移到 Amazon Route 53 失敗 1038
沒有按一下授權電子郵件中的連結 1038
您從目前註冊商取得的授權碼無效 1038
嘗試將 .es 網域轉移到 Amazon Route 53 時出現「請求中的參數無效」錯誤 1039
您要轉移到 Amazon Route 53 的國際化網域名稱是否列在 Punycode 中？ 1039
我變更 DNS 設定，但沒有生效 1039
您在過去 48 小時將 DNS 服務轉移到 Amazon Route 53，所以 DNS 仍在使用您之前的 DNS 服務 1039
您最近將 DNS 服務轉移到 Amazon Route 53，但沒有向網域註冊商更新名稱伺服器 1040
DNS 解析程式仍使用記錄的舊設定 1041
您有多個託管區域使用相同名稱，且您更新了未與網域關聯的託管區域 1042
我的瀏覽器顯示「找不到伺服器」錯誤 1043
您未建立網域或子網域名稱的記錄 1043
您建立記錄，但指定錯誤的值 1043
流量路由到的資源不可用 1043
我無法將流量路由到為網站託管而設定的 Amazon S3 儲存貯體 1044
同一個託管區域被收費兩次 1044
我的網域收取了多張發票費用 1044

我的 AWS 帳戶已關閉、暫停或終止，且我的網域已在 Route 53 註冊 1045
IP 地址範圍 1046
Route 53 名稱伺服器的 IP 地址範圍 1046
Route 53 運作狀態檢查的 IP 地址範圍 1046
參考字首清單 1047
Route 53 運作狀態檢查的內部 IP 地址範圍 1047
標記 資源 1048
教學課程 1049
將 Amazon Route 53 做為子網域的 DNS 服務，而不需遷移父系網域 1049
無需遷移父系網域，建立使用 Amazon Route 53 做為 DNS 服務的子網域 1049
無需遷移父系網域，將子網域的 DNS 服務遷移到 Amazon Route 53 1052
轉換到 Amazon Route 53 中的以延遲為基礎的路由 1055
在 Amazon Route 53 中將另一個區域新增到以延遲為基礎的路由 1057
使用 Amazon Route 53 中的延遲和加權記錄，將流量路由至區域中的多個 Amazon EC2 執行個體 1059
在 Amazon Route 53 中管理超過 100 個加權記錄 1060
在 Amazon Route 53 中對容錯多記錄回答進行加權 1061
最佳實務 1063
Amazon Route 53 DNS 的最佳實務 1063
Resolver 的最佳實務 1065
避免對 Resolver 端點使用迴圈組態 1065
Resolver 端點擴展 1065
Resolver 端點的高可用性 1066
DNS 區域遍歷 1067
Amazon Route 53 運作狀態檢查的最佳實務 1067
適用於運作狀態檢查的彈性 IP 地址的最佳實務 1067
配額 1068
使用 Service Quotas 來檢視和管理配額 1068
實體的配額 1068
網域的配額 1069
託管區域的配額 1069
記錄的配額 1070
Route 53 Resolver 的配額 1071
運作狀態檢查的配額 1077
查詢日誌組態的配額 1078
流量流程政策和政策記錄的配額 1078

可重複使用委派組的配額 1079
API 請求的上限 1079
ChangeResourceRecordSets 請求中元素和字元的數目 1079
Amazon Route 53 API 請求的頻率 1079
Route 53 Resolver API 請求的頻率 1080
相關資訊 1081
AWS 資源 1081
第三方工具和程式庫 1082
圖形使用者介面 1083
文件歷史記錄 1084
新聞稿 1084
2023 新聞稿 1085
2022 年發佈 1085
2021 版本 1086
2020 版本 1087
2018 年版本 1087
2017 年版本 1088
2016 年版本 1090
2015 年版本 1093
2014 年版本 1095
2013 年版本 1097
2012 年版本 1098
2011 年版本 1099
2010 年版本 1099
AWS 詞彙表 1100
..... mci

什麼是 Amazon Route 53？

Amazon Route 53 是一種可用性高、可擴展性強的網域名稱系統 (DNS) Web 服務。您可以使用 Route 53 執行三個主要功能的任意組合：網域註冊、DNS 路由和運作狀態檢查。

如果您選擇使用 Route 53 執行所有三個功能，請遵循以下步驟順序：

1. 註冊網域名稱

   您的網站需要名稱 (例如 example.com)。Route 53 可讓您為網站或 Web 應用程式註冊名稱 (稱為網域名稱)。

   - 如需概觀，請參閱 網域註冊的運作方式。
   - 相關程序請參閱註冊新網域。
   - 如需解說註冊網域和在 Amazon S3 儲存貯體中建立簡易網站之程序的教學，請參閱 Amazon Route 53 入門。

2. 將網際網路流量路由至您網域的資源

   當使用者開啟 Web 瀏覽器，並在網址列中輸入您的網域名稱 (example.com) 或子網域名稱 (acme.example.com)，Route 53 會協助將該瀏覽器與您的網站或 Web 應用程式連線。

   - 如需概觀，請參閱 如何將網際網路流量路由到您的網站或 Web 應用程式。
   - 如需程序，請參閱將 Amazon Route 53 設定為 DNS 服務。
   - 如需如何將電子郵件路由至 Amazon WorkMail 的程序，請參閱 將流量路由到 Amazon WorkMail。

3. 檢查資源的運作狀態

   Route 53 會透過網際網路傳送自動請求給資源 (例如 Web 伺服器)，以確認其可連線、可用並可運作。您也可以選擇在資源無法使用時接收通知，並選擇將網際網路流量從狀況不良的資源路由到他處。

   - 如需概觀，請參閱 Amazon Route 53 檢查資源的運作狀態。
   - 如需程序，請參閱建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。

主題

- 網域註冊的運作方式
- 如何將網際網路流量路由到您的網站或 Web 應用程式
- Amazon Route 53 檢查資源的運作狀態

- Amazon Route 53 概念
- 如何開始使用 Amazon Route 53
- 相關服務
- 存取 Amazon Route 53
- AWS Identity and Access Management
- Amazon Route 53 定價和計費
- 搭配 AWS SDK 使用 Route 53

網域註冊的運作方式

如果要建立網站或 Web 應用程式，請先註冊網站名稱 (稱為domain name)。您的網域名稱是使用者在瀏覽器中輸入以顯示您的網站的名稱 (例如 example.com)。

以下是如何向 Amazon Route 53 註冊網域名稱的概觀：

1. 選擇網域名稱，並確認其可用性，這表示沒有人已註冊您要的網域名稱。

   如果您要的網域名稱已有人使用，您可以嘗試使用其他名稱或嘗試只將「頂層網域」(如 .com) 變更為另一個頂層網域 (如 .ninja 或 .hockey)。如需 Route 53 支援的頂層網域的清單，請參閱 可向 Amazon Route 53 註冊的網域。
2. 向 Route 53 註冊網域名稱。當您註冊網域時，提供網域擁有者和其他聯絡人的姓名和聯絡資訊。

   當您向 Route 53 註冊網域時，服務會透過執行以下動作，自動將本身設為網域的 DNS 服務：

   - 建立與您的網域同名的hosted zone。
   - 將一組四個名稱伺服器指派給託管區域。當有人使用瀏覽器存取您的網站 (例如 www.example.com)，這些名稱伺服器會指示瀏覽器在哪裡尋找您的資源 (例如 Web 伺服器或 Amazon S3 儲存貯體)。(Amazon S3 是用來從 Web 上的任何位置存放和擷取任意資料量的物件儲存。儲存貯體是 S3 中用於存放物件的容器。)
   - 從託管區域取得名稱伺服器，並將其新增至網域。

   如需更多詳細資訊，請參閱 如何將網際網路流量路由到您的網站或 Web 應用程式。
3. 在註冊程序結束時，我們會將您的資訊傳送給網域註冊商。domain registrar是 Amazon Registrar, Inc. 或我們的註冊商合作夥伴 Gandi。若要找出您的網域註冊商是誰，請參閱尋找註冊商。
4. 註冊商會將您的資訊傳送給網域的「註冊機構」。註冊機構是銷售一或多個頂層網域 (如 .com) 的網域註冊的公司。

5. 註冊機構將您的網域相關資訊存放在其自己的資料庫中，並將其中一些資訊存放在公共 WHOIS 資料庫中。

如需有關如何註冊網域名稱的詳細資訊，請參閱註冊新網域。

如果您已經向另一個註冊商註冊網域名稱，可以選擇將網域註冊轉移到 Route 53。使用其他 Route 53 功能不需要此操作。如需更多詳細資訊，請參閱 將網域註冊轉移到 Amazon Route 53。

如何將網際網路流量路由到您的網站或 Web 應用程式

網際網路上的所有電腦 (從智慧手機或筆記型電腦，到為大量零售網站提供內容的伺服器)，都是透過使用數字相互通訊。這些數字 (稱為「IP 地址」) 採用下列其中一個格式：

- 網際網路通訊協定第 4 版 (IPv4) 格式，例如 192.0.2.44
- 網際網路通訊協定第 6 版 (IPv6) 格式，例如 2001:0db8:85a3:0000:0000:abcd:0001:2345

當您開啟瀏覽器並移至網站時，不需要記住並輸入這麼長的字元字串。相反地，您可以輸入網域名稱 (例如 example.com)，仍然可移至預期的網站。DNS 服務 (例如 Amazon Route 53) 有助於在網域名稱和 IP 地址之間建立連線。

主題

- 如何設定 Amazon Route 53 為網域路由網際網路流量的概觀
- Amazon Route 53 如何為您的網域路由流量

如何設定 Amazon Route 53 為網域路由網際網路流量的概觀

以下概述如何使用 Amazon Route 53 主控台註冊網域名稱，並設定 將網際網路流量路由到您的網站或 Web 應用程式。

1. 您註冊希望使用者用於存取您的內容的網域名稱。如需概觀，請參閱 網域註冊的運作方式。
2. 在註冊網域名稱之後，Route 53 會自動建立一個與該網域同名的公有託管區域。如需更多詳細資訊，請參閱 使用公有託管區域。
3. 若要將流量路由到您的資源，您可以在託管區域中建立「記錄」，也稱為「資源記錄集」。每個記錄包含有關您希望如何路由網域流量的資訊，例如：

Name

記錄名稱對應於您希望 Route 53 為其路由流量的網域名稱 (example.com) 或子網域名稱 (www.example.com、retail.example.com)。

託管區域中每個記錄的名稱必須以託管區域名稱結尾。例如，如果託管區域的名稱是 example.com，所有記錄名稱都必須以 example.com 結尾。Route 53 主控台會為您自動執行此操作。

類型

記錄類型通常決定您希望流量路由到的資源類型。例如，若要將流量路由到電子郵件伺服器，請將 Type (類型) 指定為 MX。若要將流量路由到具有 IPv4 IP 地址的 Web 伺服器時，請將「Type」(類型) 指定為 A。

值

「Value」(值) 與「Type」(類型) 密切相關。如果您將「Type」(類型) 指定為 MX，則對「Value」(值) 指定一或多個電子郵件伺服器的名稱。如果將「Type」(類型) 指定為 A，則指定 IPv4 格式的 IP 地址，例如 192.0.2.136。

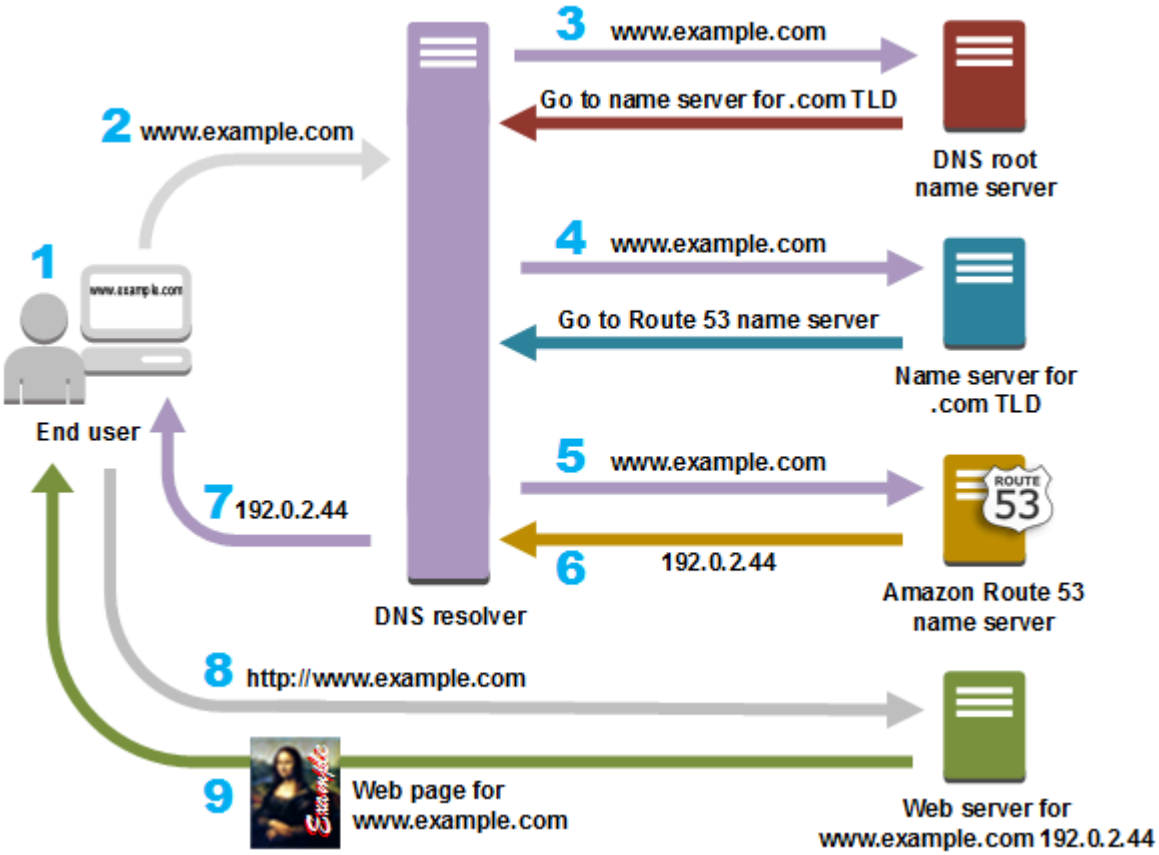
如需記錄的詳細資訊，請參閱 處理記錄。

您也可以建立特殊 Route 53 記錄，稱為別名記錄，它們會將流量路由到 Amazon S3 儲存貯體、Amazon CloudFront 分佈和其他 AWS 資源。如需更多詳細資訊，請參閱 選擇別名或非別名記錄 及 將網際網路流量路由到您的 AWS 資源。

如需將網際網路流量路由至資源的資訊，請參閱將 Amazon Route 53 設定為 DNS 服務。

Amazon Route 53 如何為您的網域路由流量

在您設定 Amazon Route 53 將網際網路流量路由到您的資源 (例如 Web 伺服器或 Amazon S3 儲存貯體) 後，若有人請求 www.example.com 的內容，將在短短幾毫秒內發生以下情況：



1. 使用者開啟 Web 瀏覽器並在網址列中輸入 www.example.com，然後按 Enter。
2. 對 www.example.com 的請求路由到 DNS 解析程式，該解析程式通常由使用者的網際網路服務提供者 (ISP) (例如有線網際網路服務提供者、DSL 寬頻提供者或公司網路) 進行管理。
3. ISP 的 DNS 解析程式將對 www.example.com 的請求轉送到 DNS 根名稱伺服器。
4. DNS 解析程式再次轉送對 www.example.com 的請求，這次轉送到 .com 網域的其中一個 TLD 名稱伺服器。.com 網域的名稱伺服器使用與 example.com 網域關聯的四個 Route 53 名稱伺服器的名稱來回應該請求。

   DNS 解析程式快取 (存放) 四個 Route 53 名稱伺服器。下次有人瀏覽 example.com，解析程式會略過步驟 3 和 4，因為它已有 example.com 的名稱伺服器。名稱伺服器通常會快取兩天。
5. DNS 解析程式選擇 Route 53 名稱伺服器，並將對 www.example.com 的請求轉送至該名稱伺服器。
6. Route 53 名稱伺服器在 example.com 託管區域中尋找 www.example.com 記錄、取得關聯值 (例如 Web 伺服器的 IP 地址 192.0.2.44)，並將該 IP 地址傳回至 DNS 解析程式。
7. DNS 解析程式最終取得使用者所需的 IP 地址。解析程式將該值傳回給 Web 瀏覽器。

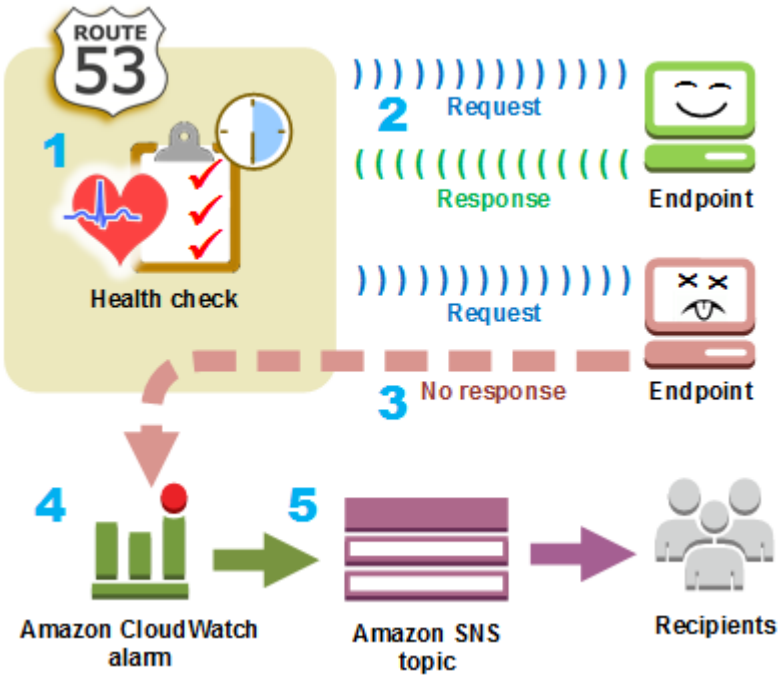
> **Note**
>
> DNS 解析程式還會將 example.com 的 IP 地址快取指定的一段時間，以便在下次有人瀏覽到 example.com 時，它可以更快地回應。如需更多詳細資訊，請參閱 time to live (TTL)。

8. Web 瀏覽器將對 www.example.com 的請求，傳送至它從 DNS 解析程式取得的 IP 地址。這是您的內容所在的位置，例如，在 Amazon EC2 執行個體上執行的 Web 伺服器，或設定為網站端點的 Amazon S3 儲存貯體。
9. 192.0.2.44 上的 Web 伺服器或其他資源將 www.example.com 的網頁傳回到 Web 瀏覽器，而 Web 瀏覽器會顯示該頁面。

Amazon Route 53 檢查資源的運作狀態

Amazon Route 53 運作狀態檢查監控 Web 伺服器和電子郵件伺服器等資源的運作狀態。您可以選擇性地為運作狀態檢查設定 Amazon CloudWatch 警示，以便在資源變得不可用時收到通知。

如果您希望在資源變得不可用時收到通知，下面是運作狀態檢查運作方式的概觀：



1. 您建立運作狀態檢查，並指定用於定義所要運作狀態檢查運作方式的值，例如：
   - 您希望 Route 53 監控的端點 (如 Web 伺服器) 的 IP 地址或網域名稱。(您也可以監控其他運作狀態檢查的狀態，或 CloudWatch 警示的狀態。)

- 您需要 Amazon Route 53 用於執行檢查的通訊協定：HTTP、HTTPS 或 TCP。
- 您希望 Route 53 傳送請求給端點的頻率，這就是「請求間隔」。
- 在 Route 53 認為端點狀況不良之前，端點必須無法回應請求的連續次數，這就是「失敗閾值」。
- (選用) 當 Route 53 檢測到端點狀況不良時，您希望接收通知的方式。當您設定通知，Route 53 會自動設定 CloudWatch 警示。CloudWatch 使用 Amazon SNS 通知使用者，端點狀況不良。

2. Route 53 開始以您在運作狀態檢查中指定的間隔向端點傳送請求。

   如果端點回應請求，Route 53 會認為端點正常運作，因此不會採取任何動作。
3. 如果端點沒有回應請求，Route 53 會開始計算端點未回應的連續請求的次數：
   - 如果計數達到為失敗閾值指定的值，Route 53 會認為端點狀況不良。
   - 如果在計數達到失敗閾值前，端點再度開始回應，Route 53 會將計數重設為 0，而 CloudWatch 不會通知您。
4. 如果 Route 53 認為端點狀況不良，而且您設定運作狀態檢查通知，Route 53 會通知 CloudWatch。

   如果您未設定通知，仍可在 Route 53 主控台中查看 Route 53 運作狀態檢查的狀態。如需更多詳細資訊，請參閱 監控運作狀態檢查狀態和取得通知。
5. 如果您設定了運作狀態檢查通知，CloudWatch 會觸發警示，並使用 Amazon SNS 傳送通知給指定收件人。

除了檢查指定端點的運作狀態之外，您還可以將運作狀態檢查設定為檢查一或多個其他運作狀態檢查的運作狀態，以便在指定數量的資源 (如五個 Web 伺服器中的兩個) 不可用時收到通知。您也可以設定運作狀態檢查來檢查 CloudWatch 警示的狀態，以便您可以根據廣泛的條件收到通知，而不僅僅限於資源是否回應請求。

如果您有多個執行相同功能的資源 (例如，Web 伺服器或資料庫伺服器)，而且您希望 Route 53 僅將流量路由到正常運作的資源，則可以透過將運作狀態檢查與資源的每個記錄相關聯，來設定 DNS 備援。如果運作狀態檢查判斷基本資源狀況不良，Route 53 會將流量從相關記錄路由到他處。

如需使用 Route 53 監控資源運作狀態的詳細資訊，請參閱 建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。

Amazon Route 53 概念

以下概述整個 Amazon Route 53 開發人員指南中所討論的概念。

主題

- 網域註冊概念
- 網域名稱系統 (DNS) 概念
- 控制和資料平面概念
- 運作狀態檢查概念

網域註冊概念

以下概述與網域註冊相關的概念。

- domain name
- domain registrar
- domain registry
- domain reseller
- top-level domain (TLD)

網域名稱

使用者在 Web 瀏覽器的網址欄中輸入的名稱 (例如 example.com)，用於存取網站或 Web 應用程式。為了讓您的網站或 Web 應用程式可在網際網路使用，請先註冊網域名稱。如需更多詳細資訊，請參閱 網域註冊的運作方式。

網域註冊商

ICANN (網際網路名稱和數字指派公司) 認可的公司，旨在處理特定頂層網域 (TLD) 的網域註冊。若要找出您的網域註冊商是誰，請參閱尋找註冊商。

網域註冊機構

有權銷售具有特定頂層網域之網域的公司。例如，VeriSign 是有權販售具有 .com TLD 之網域的註冊機構。網域註冊機構定義註冊網域的規則，例如地理 TLD 的居留權要求。網域註冊機構還會維護具有相同 TLD 的所有網域名稱的授權資料庫。註冊機構的資料庫包含每個網域的聯絡資訊和名稱伺服器等資訊。

網域經銷商

為註冊商 (例如 Amazon Registrar) 銷售網域名稱的公司。Amazon Route 53 是 Amazon Registrar 和我們的註冊商合作夥伴 Gandi 的網域經銷商。

頂層網域 (TLD)

網域名稱的最後一部分，例如 .com、.org 或 .ninja。有兩種類型的頂層網域：

一般頂層網域

這些 TLD 通常會讓使用者知道他們能夠在網站上找到什麼內容。例如，具有 TLD .bike 的網域名稱通常與摩托車或自行車企業或組織的網站有關。除了少數例外情況外，您可以使用任何您想要的一般 TLD，因此自行車俱樂部可將 .hockey TLD 用於其網域名稱。

地理頂層網域

這些 TLD 與地理區域 (如國家/地區或城市) 相關聯。有些地理 TLD 註冊機構具有居留權要求，而有些 (比如 the section called ".io (英屬印度洋領地)") 則允許甚至鼓勵將其做為一般 TLD。

如需向 Route 53 註冊網域名稱時可用的 TLD 清單，請參閱 可向 Amazon Route 53 註冊的網域。

網域名稱系統 (DNS) 概念

以下概述與網域名稱系統 (DNS) 相關的概念。

- alias record
- authoritative name server
- CIDR block
- DNS query
- DNS resolver
- Domain Name System (DNS)
- hosted zone
- IP address
- name servers
- private DNS
- recursive name server
- record (DNS record)
- reusable delegation set
- routing policy

- subdomain
- time to live (TTL)

別名記錄

您可以使用 Amazon Route 53 建立的一種記錄類型，其用於將流量路由到 AWS 資源，例如 Amazon CloudFront 分佈和 Amazon S3 存儲桶。如需更多詳細資訊，請參閱 選擇別名或非別名記錄。

授權名稱伺服器

名稱伺服器，具有關於網域名稱系統 (DNS) 的一部分的明確資訊，並透過傳回適用資訊回應來自 DNS 解析程式的請求。例如，.com 頂層網域 (TLD) 的授權名稱伺服器知道每個已註冊 .com 網域的名稱伺服器註冊的名稱。當 .com 授權名稱伺服器收到來自 example.com 的 DNS 解析程式的請求時，它會使用 example.com 網域的 DNS 服務的名稱伺服器的名稱進行回應。

Route 53 名稱伺服器是將 Route 53 做為 DNS 服務之每個網域的權威名稱伺服器。這些名稱伺服器知道，您希望如何根據您在網域託管區域中建立的記錄來路由網域和子網域的流量。(Route 53 名稱伺服器存儲將 Route 53 做為 DNS 服務的網域的託管區域。)

例如，如果 Route 53 名稱伺服器收到對 www.example.com 的請求，它會找到該記錄並傳回記錄中指定的 IP 地址 (如 192.0.2.33)。

CIDR 區塊

CIDR 區塊是與以 IP 為基礎的路由一起使用的 IP 範圍。在 Route 53 中，您可以為 IPv4 指定從 /0 到 /24 之間的 CIDR 區塊，為 IPv6 指定 0 到 /48 之間的 CIDR 區塊。例如，/24 IPv4 CIDR 區塊包含 256 個連續 IP 地址。您可以將 CIDR 區塊 (或 IP 範圍) 集組合成 CIDR 位置，然後將這些位置組合成可重複使用的 CIDR 集合。

DNS 查詢

通常為由裝置 (例如電腦或智慧型手機) 向與網域名稱關聯的資源的網域名稱系統 (DNS) 提交的請求。最常見的 DNS 查詢範例是當使用者開啟瀏覽器並在網址列中輸入網域名稱。對 DNS 查詢的回應通常是與資源 (如 Web 伺服器) 相關聯的 IP 地址。發出請求的裝置使用該 IP 地址與資源進行通訊。例如，瀏覽器可以使用 IP 地址從 Web 伺服器取得網頁。

DNS 解析程式

通常由網際網路服務提供者 (ISP) 管理的 DNS 伺服器，做為使用者請求和 DNS 名稱伺服器之間的媒介。當您開啟瀏覽器並在網址列中輸入網域名稱時，您的查詢會先傳送到 DNS 解析器。解析程

式與 DNS 名稱伺服器通訊，以取得對應資源 (例如 Web 伺服器) 的 IP 地址。DNS 解析程式也稱為遞迴名稱伺服器，因為它會將請求發傳送到一系列 DNS 授權名稱伺服器，直到它取得傳回到使用者裝置 (例如，筆記型電腦上的 Web 瀏覽器) 的回應 (通常為 IP 地址)。

網域名稱系統 (DNS)

全球伺服器網路，可協助電腦、智慧型手機、平板電腦和其他啟用 IP 的裝置相互通訊。網域名稱系統名稱會將容易了解的名稱 (例如 example.com) 轉換為數字 (稱為「IP 地址」)，讓電腦可在網際網路相互找到對方。

另請參閱 IP address。

託管區域

記錄容器，其中包含有關您希望如何路由某個網域 (如 example.com) 及其所有子網域 (如 www.example.com、retail.example.com 和 seattle.accounting.example.com) 的流量的資訊。託管區域和對應的網域名稱同名。

例如，example.com 的託管區域可能包含如下兩個記錄：一個記錄具有關於將 www.example.com 的流量路由到 IP 地址為 192.0.2.243 的 Web 伺服器的資訊；另一個記錄具有關於將 example.com 的電子郵件路由到兩個電子郵件伺服器 (mail1.example.com 和 mail2.example.com) 的資訊。每個電子郵件伺服器還需要自己的記錄。

另請參閱 record (DNS record)。

IP 地址

指派給網際網路上裝置—例如筆記型電腦、智慧型手機或 Web 伺服器—的數字，允許裝置與網際網路上的其他裝置通訊。IP 地址採用以下格式之一：

- 網際網路通訊協定第 4 版 (IPv4) 格式，例如 192.0.2.44
- 網際網路通訊協定第 6 版 (IPv6) 格式，例如 2001:0db8:85a3:0000:0000:abcd:0001:2345

Route 53 支援 IPv4 和 IPv6 地址，用於以下目的：

- 您可以建立類型為 A (適用於 IPv4 地址) 或類型為 AAAA (適用於 IPv6 地址) 的記錄。
- 您可以建立將請求傳送到 IPv4 或 IPv6 地址的運作狀態檢查。
- 如果 DNS 解析程式在 IPv6 網路上，它可以使用 IPv4 或 IPv6 向 Route 53 提交請求。

名稱伺服器

網域名稱系統 (DNS) 中的伺服器，可將網域名稱轉譯為 IP 地址，供電腦用於互相通訊。名稱伺服器是遞迴名稱伺服器 (亦稱為 DNS resolver) 或 authoritative name server。

如需 DNS 如何將流量路由到您資源 (包括 Route 53 在程序中的角色) 的概觀，請參閱 Amazon Route 53 如何為您的網域路由流量。

私有 DNS

本機版本的網域名稱系統 (DNS)，可讓您將網域及其子網域的流量路由到一或多個 Amazon Virtual Private Cloud (VPC) 中的 Amazon EC2 執行個體。如需更多詳細資訊，請參閱 使用私有託管區域。

記錄 (DNS 記錄)

託管區域中的物件，用來定義要如何路由網域或子網域的流量。例如，您可以為 example.com 與 www.example.com 建立記錄，將流量路由到 IP 地址為 192.0.2.234 的 Web 伺服器。

如需有關記錄的詳細資訊，包括有關 Route 53 特定記錄提供的功能的資訊，請參閱 將 Amazon Route 53 設定為 DNS 服務。

遞迴名稱伺服器

請參閱 DNS resolver。

可重複使用的委派組

一組可用於多個託管區域的四個授權名稱伺服器。在預設情況下，Route 53 會為每個新的託管區域指派隨機選取的名稱伺服器。為了更輕鬆地將大量網域的 DNS 服務遷移到 Route 53，您可以建立可重複使用的委派組，然後將可重複使用的委派組與新的託管區域關聯。(您不能變更與現有託管區域關聯的名稱伺服器。)

建立可重複使用的委派組，並以程式設計方式將其與託管區域關聯；不支援使用 Route 53 主控台。如需詳細資訊，請參閱 Amazon Route 53 API 參考中的 CreateHostedZone 和 CreateReusableDelegationSet。AWS 開發套件、AWS Command Line Interface 和 AWS Tools for Windows PowerShell 也可使用相同的功能。

路由政策

決定 Route 53 如何回應 DNS 查詢的記錄設定。Route 53 支援以下路由政策：

- 簡易路由政策 – 用於將網際網路流量路由到為網域執行指定功能的單一資源，例如，為 example.com 網站提供內容的 Web 伺服器。
- 容錯移轉路由政策 – 如果要設定主動-被動容錯移轉時使用。
- 地理位置路由政策 – 用於根據使用者位置將網際網路流量路由到您的資源。
- 地理位置鄰近性路由政策 – 用於根據資源位置路由流量，以及 (選用) 將流量從某個位置中的資源，轉移到另一個位置中的資源。

- 延遲路由政策 – 如果您的資源位於多個位置，並且您想要將流量路由到提供最佳延遲的資源，則可以使用該政策。
- 以 IP 為基礎的路由政策 - 用於在能夠取得流量來源 IP 地址的情況下根據使用者位置路由流量。
- 多值回答路由政策 – 如果您希望 Route 53 用隨機選取的正常記錄 (最多八個) 回應 DNS 查詢，可以使用該政策。
- 加權路由政策 – 用於按照您指定的比例將流量路由到多個資源。

如需更多詳細資訊，請參閱 選擇路由政策。

子網域

網域名稱，有一或多個標籤加到已註冊的網域名稱前面。例如，如果您註冊網域名稱 example.com，www.example.com 就是子網域。如果您為 example.com 網域建立託管區域 accounting.example.com，seattle.accounting.example.com 就是子網域。

若要為子網域路由流量，請建立一個具有所需名稱的記錄 (如 www.example.com)，並指定適用的值 (例如 Web 伺服器的 IP 地址)。

存留時間 (TTL)

在向 Route 53 提交另一個請求以取得記錄的目前值之前，您希望 DNS 解析程式快取 (存放) 該記錄值的時間 (秒)。如果 DNS 解析程式在 TTL 到期之前收到對同一個網域的另一個請求，該解析程式會傳回快取的值。

較長的 TTL 會降低您的 Route 53 費用，這有部分取決於 Route 53 回應的 DNS 查詢數目。在變更記錄中的值 (例如透過變更 www.example.com 的 Web 伺服器的 IP 地址) 之後，較短的 TTL 會縮短 DNS 解析程式將流量路由到較舊資源的時間。

控制和資料平面概念

以下為 Amazon Route 53 如何將其功能劃分為控制和資料平面相關概念的概觀。如同大多數的 AWS 服務，Route 53 服務包含一個讓您能執行建立、更新和刪除資源等管理操作的控制平面，以及一個提供服務核心功能的資料平面。雖然建置的這兩種功能都很可靠，但就資料一致性對控制平面進行最佳化，並就可用性對資料平面進行最佳化。資料平面的彈性設計允許其即使在控制平面可能變得不可用的罕見中斷事件期間，仍能維持可用性。因此，我們建議在可用性非常重要之處使用資料平面功能。

對於 Route 53 公有和私有 DNS 以及運作狀態檢查，控制平面位於 us-east-1 AWS 區域，資料平面為全域分佈。

Amazon Route 53 分為控制平面和資料平面，如下所示：

- 對於 Route 53 公有和私有 DNS，控制平面是 Route 53 主控台和 API，允許您管理 DNS 條目，包括 Route 53 和流量 API。資料平面是權威 DNS 服務，橫跨 200 多個連接點 (POP) 位置執行，根據託管區域和運作狀態檢查資料回答 DNS 查詢。
- 對於 Route 53 運作狀態檢查，控制平面是 Route 53 主控台和 Route 53 API，讓您能用來建立、更新和刪除運作狀態檢查。資料平面為全域分佈的服務，執行運作狀態檢查、彙整結果並將其傳遞到 Route 53 公有和私有 DNS 以及 AWS Global Accelerator 的資料平面。
- 對於 Amazon Route 53 Resolver，控制平面由解析程式主控台和 API 組成，允許您管理 Amazon VPC 設定、解析程式規則、查詢日誌記錄政策和 DNS 防火牆政策。資料平面是 DNS 解析程式服務，會回答 VPC 中的 DNS 查詢，端點將查詢轉發到其他解析程式，而 DNS 防火牆資料平面會套用政策以篩選 DNS 查詢。解析程式是一種區域性服務，其控制平面和資料平面在每個 AWS 區域 中獨立執行。
- 僅在 us-east-1 AWS 區域 的控制平面上管理 Route 53 網域註冊。

如需關於資料平面、控制平面以及 AWS 如何建置服務以滿足高可用性目標的資訊，請參閱 Amazon Builders' Library 中的使用可用區域的靜態穩定性報告。

運作狀態檢查概念

以下概述與 Amazon Route 53 運作狀態檢查相關的概念。

- DNS failover
- endpoint
- health check

DNS 備援

將流量從狀況不良的資源路由到正常運作的資源的一種方法。當您有多個資源—例如，多個 Web 伺服器或郵件伺服器—執行相同功能時，可以將 Route 53 運作狀態檢查設為檢查資源的運作狀態，並在您的託管區域中設定記錄，以將流量僅路由到正常的資源。

如需更多詳細資訊，請參閱 設定 DNS 備援。

endpoint

您將運作狀態檢查設為監控其運作狀態的資源 (例如 Web 伺服器或電子郵件伺服器)。您可以透過 IPv4 地址 (192.0.2.243)、IPv6 地址 (2001:0db8:85a3:0000:0000:abcd:0001:2345) 或網域名稱 (example.com) 指定端點。

> **Note**
>
> 您也可以建立運作狀態檢查，以監控其他運作狀態檢查的狀態或監控 CloudWatch 警示的警示狀態。

運作狀態檢查

Route 53 元件，可讓您執行以下操作：

- 監控指定的端點 (例如 Web 伺服器) 是否正常運作
- (選用) 當某個端點狀況不良時收到通知
- (選用) 設定 DNS 備援，以便將網際網路流量從狀況不良的資源路由到正常的資源

如需建立和使用運作狀態檢查的詳細資訊，請參閱建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。

如何開始使用 Amazon Route 53

如需 Amazon Route 53 入門資訊，請參閱本指南的下列主題：

- 設定 Amazon Route 53：說明如何註冊 AWS、如何安全存取 AWS 帳戶，以及如何設定透過編寫程式的方式存取 Route 53。
- Amazon Route 53 入門，說明如何註冊網域名稱，如何建立 Amazon S3 儲存貯體並設定託管靜態網站，以及如何將網際網路流量路由到該網站

相關服務

如需有關 Amazon Route 53 整合的 AWS 服務的資訊，請參閱 與其他服務整合。

存取 Amazon Route 53

您可以通過以下方式存取 Amazon Route 53：

- AWS Management Console – 本指南中的程序說明如何使用 AWS Management Console 執行任務。

- AWS 開發套件 – 如果您使用的是 AWS 有提供開發套件的程式設計語言，即可使用開發套件存取 Route 53。開發套件 (SDK) 可簡化身分驗證、與您的開發環境輕鬆整合，並且讓您易於存取 Route 53 命令。如需詳細資訊，請參閱 Amazon Web Services 適用工具。
- Route 53 API – 如果您使用沒有適用開發套件的程式設計語言，請參閱 Amazon Route 53 API 參考，以取得 API 動作以及如何提出 API 請求的相關資訊。
- AWS Command Line Interface – 如需詳細資訊，請參閱《AWS Command Line Interface 使用者指南》中的設定 AWS Command Line Interface。
- AWS Tools for Windows PowerShell – 如需詳細資訊，請參閱《AWS Tools for Windows PowerShell 使用者指南》中的設定 AWS Tools for Windows PowerShell。

AWS Identity and Access Management

Amazon Route 53 會與 AWS Identity and Access Management (IAM) 整合，而後者是可讓您的組織執行以下操作的服務：

- 使用您組織的 AWS 帳戶來建立使用者和群組
- 輕鬆地在帳戶中的使用者之間分享您的 AWS 帳戶資源
- 將唯一安全登入資料指派給每位使用者
- 細微控制每位使用者對服務與資源的存取

例如，您可以將 IAM 與 Route 53 搭配使用，控制您的 AWS 帳戶中的哪些使用者可以建立新的託管區域或變更記錄。

如需 IAM 的一般資訊，請參閱下列各項：

- Amazon Route 53 中的身分和存取管理
- Identity and Access Management (IAM)
- IAM 使用者指南

Amazon Route 53 定價和計費

如同其他 AWS 產品，對於使用 Amazon Route 53，並沒有合約或最低承諾。您只需為您設定的託管區域以及 Route 53 回應的 DNS 查詢數量付費。如需詳細資訊，請參閱 Amazon Route 53 定價。

有關 AWS 服務計費的詳細資訊 (包含如何檢視帳單和管理帳戶和付款)，請參閱 AWS Billing 使用者指南。

搭配 AWS SDK 使用 Route 53

AWS 軟體開發套件 (SDK) 適用於許多常用的程式設計語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

SDK 文件	程式碼範例
AWS SDK for C++	AWS SDK for C++ 程式碼範例
AWS SDK for Go	AWS SDK for Go 程式碼範例
AWS SDK for Java	AWS SDK for Java 程式碼範例
AWS SDK for JavaScript	AWS SDK for JavaScript 程式碼範例
適用於 Kotlin 的 AWS SDK	適用於 Kotlin 的 AWS SDK 程式碼範例
AWS SDK for .NET	AWS SDK for .NET 程式碼範例
AWS SDK for PHP	AWS SDK for PHP 程式碼範例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 程式碼範例
AWS SDK for Ruby	AWS SDK for Ruby 程式碼範例
適用於 Rust 的 AWS SDK	適用於 Rust 的 AWS SDK 程式碼範例
適用於 SAP ABAP 的 AWS SDK	適用於 SAP ABAP 的 AWS SDK 程式碼範例
適用於 Swift 的 AWS SDK	適用於 Swift 的 AWS SDK 程式碼範例

如需 Route 53 專屬範例，請參閱 適用於使AWS用 SDK 的 Route 53 程式碼範例。

> **可用性範例**
>
> 找不到所需的內容嗎？ 請使用本頁面底部的提供意見回饋連結申請程式碼範例。

設定 Amazon Route 53

本節中的概觀和程序可協助您開始使用 AWS。

主題

- 註冊 AWS 帳戶
- 建立管理使用者
- 下載工具

註冊 AWS 帳戶

如果您還沒有 AWS 帳戶，請完成以下步驟建立新帳戶。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為最佳安全實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

註冊程序完成後，AWS 會傳送一封確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇 我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立管理使用者

當您註冊 AWS 帳戶 之後，請保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立管理使用者，讓您可以不使用根使用者處理日常作業。

保護您的 AWS 帳戶根使用者

1. 選擇 根使用者 並輸入您的 AWS 帳戶電子郵件地址，以帳戶擁有者身分登入 AWS Management Console。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶根使用者啟用虛擬 MFA 裝置 (主控台)。

建立管理使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的教學課程，請參閱《使用 AWS IAM Identity Center 使用者指南中的以預設 IAM Identity Center 目錄 設定使用者存取權限。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 URL。

  如需有關如何使用 IAM Identity Center 使用者登入的說明，請參閱《AWS 登入 使用者指南》中的登入 AWS存取入口網站。

下載工具

AWS Management Console 包含 Amazon Route 53 的主控台，但如果您想要以程式設計方式存取服務，請參閱下列內容：

- API 指南記錄了服務支援的操作，並提供指向相關軟體開發套件和 CLI 文件的連結：
  - Amazon Route 53 API 參考
- 若要呼叫 API 而無需處理低層級詳細資訊，例如組合原始 HTTP 請求，您可以使用 AWS 軟體開發套件。AWS 開發套件提供可封裝 AWS 服務功能的功能與資料類型。若要下載 AWS 軟體開發套件並存取安裝說明，請參閱適用的頁面：
  - Java
  - JavaScript
  - .NET

- Node.js
- PHP
- Python
- Ruby

如需取得 AWS 軟體開發套件的完整清單，請參閱 Amazon Web Services 工具。

- 您可以使用 AWS Command Line Interface (AWS CLI) 從命令列控制多項 AWS 服務。您也可以使用指令碼自動執行命令。如需詳細資訊，請參閱 AWS Command Line Interface。
- AWS Tools for Windows PowerShell 支援這些 AWS 服務。如需詳細資訊，請參閱 AWS Tools for PowerShell Cmdlet 參考。

Amazon Route 53 入門

向 Amazon Route 53 註冊網域，並設定 Route 53 回應解析到靜態網站的 DNS 查詢，開始使用基本步驟。第一個教學會在開放的 Amazon S3 儲存貯體中託管一個靜態網站，第二個教學則使用 Amazon CloudFront 分發透過 SSL/TLS 為網站提供服務。

估計費用

- 註冊網域需要年費，金額從 $9 美元到數百美元不等，具體金額取決於頂層網域，例如 .com。如需詳細資訊，請參閱 Route 53 網域註冊的定價。此費用不可退款。
- 當您註冊網域，我們會自動建立一個與該網域同名的託管區域。可使用該託管區域指定希望 Route 53 將網域流量路由到哪裡。
- 在本教學課程中，您要建立 Amazon S3 儲存貯體以及上傳範例 Web 頁面。如果您是 AWS 新客戶，可免費開始使用 Amazon S3。如果您是現有 AWS 客戶，將根據您存放的資料量、對資料的請求量和轉移的資料量收費。如需詳細資訊，請參閱 Amazon S3 定價。
- CloudFront 費用取決於您的資料請求數量、您使用的節點數量，以及傳輸的資料量。如需詳細資訊，請參閱CloudFront 定價。

主題

- 將您的網域用於 Amazon S3 儲存貯體中的靜態網站
- 使用 Amazon CloudFront 分發服務靜態網站

將您的網域用於 Amazon S3 儲存貯體中的靜態網站

此入門教學課程說明如何執行以下任務：

- 註冊網域名稱，例如 example.com。
- 建立 Amazon S3 儲存貯體，並設定它來託管網站
- 建立範例網站，並將檔案儲存在 S3 儲存貯體
- 設定 Amazon Route 53 將流量路由到您的新網站

完成後，您將能夠開啟瀏覽器，輸入網域名稱，並檢視您的網站。

> **Note**
>
> 您也可以將現有網域轉移到 Route 53，但比起註冊新的網域，此程序更複雜且耗時。如需詳細資訊，請參閱 將網域註冊轉移到 Amazon Route 53。

主題

- 必要條件
- 步驟 1：註冊網域
- 步驟 2：為根網域建立 S3 儲存貯體
- 步驟 3 (選用)：為根網域建立另一個 S3 儲存貯體
- 步驟 4：設定網站託管的根網域儲存貯體
- 步驟 5：(選用)：設定用於網站重新引導的子網域儲存貯體
- 步驟 6：上傳索引以建立網站內容
- 步驟 7：編輯 S3 封鎖公有存取設定
- 步驟 8：連接儲存貯體政策
- 步驟 9：測試您的網域端點
- 步驟 10：將您網域的 DNS 流量路由到您的網站儲存貯體
- 步驟 11：測試您的網站
- 步驟 12（可選）：使用 Amazon CloudFront 加快內容的分發

必要條件

開始之前，請務必先完成 設定 Amazon Route 53 中的步驟。

步驟 1：註冊網域

若要使用網域名稱 (例如 example.com)，您必須找到一個未被使用的網域名稱並註冊該網域。當您註冊網域名稱，即表示您要保留它以供您在網際網路上的任何位置獨佔使用，通常為期一年。在預設情況下，我們會在每年年底自動續約您的網域，但您可以關閉自動續約。如需詳細資訊，請參閱 註冊新網域。

步驟 2：為根網域建立 S3 儲存貯體

Amazon S3 可讓您從網際網路上的任何位置儲存和擷取您的資料。若要組織您的資料，可以使用 AWS Management Console 建立儲存貯體並將資料上傳到儲存貯體。可以使用 Amazon S3 在儲存貯體中託管靜態網站。下列程序說明如何建立儲存貯體。

若要為根網域建立一個 S3 儲存貯體

1. 前往 https://console.aws.amazon.com/s3/ 開啟 Amazon S3 主控台。
2. 選擇建立儲存貯體。
3. 輸入下列值：

   儲存貯體名稱

   輸入您的網域名稱，例如 example.com。

   區域

   選擇最接近大多數使用者的區域。

   記下所選擇的區域，在稍後的程序中您需要此資訊。
4. 若要接受預設設定並建立儲存貯體，請選擇 Create bucket (建立儲存貯體)。

步驟 3 (選用)：為根網域建立另一個 S3 儲存貯體

在之前程序中，您為網域名稱 (例如 example.com) 建立儲存貯體。這樣您的使用者就可以使用您的網域名稱 (例如 example.com) 存取您的網站。

如果您還希望您的用戶能夠使用 www。 *your-domain-name*如要存取您的範例網站，請建立第二個 S3 儲存貯體，例如 www.example.com。設定第二個儲存貯體，將流量路由到第一個儲存貯體。

為 www 創建一個 S3 存儲桶。 your-domain-name

1. 選擇建立儲存貯體。
2. 輸入下列值：

   儲存貯體名稱

   輸入萬維網。 ***your-domain-name***。例如，如已註冊網域名稱 example.com，請輸入 www.example.com。

區域

選擇建立第一個儲存貯體的區域。

3. 若要接受預設設定並建立儲存貯體，請選擇 Create (建立)。

步驟 4：設定網站託管的根網域儲存貯體

現在您已有一個 S3 儲存貯體，可以為網站託管設定該儲存貯體。

若要允許在您的 S3 儲存貯體上託管網站

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在儲存貯體名稱清單中，選擇希望為靜態網站託管啟用的儲存貯體名稱。
3. 選擇 Properties (屬性)。
4. 在 Static website hosting (靜態網站託管)下，選擇 Enable (啟用)。
5. 選擇 Use this bucket to host a website (使用此儲存貯體來託管網站)。
6. 在 Static website hosting (靜態網站託管) 下，選擇Enable (啟用)。
7. 在索引文件中，輸入索引文件的名稱，通常是 `index.html`。

   索引文件名稱區分大小寫，而且必須完全符合您計畫上傳至 S3 儲存貯體的 HTML 索引文件檔案名稱。當您為網站託管設定儲存貯體時，必須指定索引文件。在對根網域或任何子資料夾提出請求時，Amazon S3 會傳回此索引文件。
8. (選用) 若要為 4XX 類別錯誤提供自己的自訂錯誤文件，請在 Error document (錯誤文件)中輸入自訂錯誤文件檔案名稱。

   如果您未指定自訂錯誤文件且發生錯誤，則 Amazon S3 會傳回預設的 HTML 錯誤文件。
9. (選用) 如果您要指定進階重新引導規則，請在 Redirection rules (重新引導規則) 中輸入 XML 來描述規則。

   如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的設定進階條件式重新引導。
10. 選擇儲存變更。
11. 在 Static website hosting 下，請記下 Endpoint (端點)。

Endpoint (端點) 是儲存貯體的 Amazon S3 網站端點。將儲存貯體設為靜態網站之後，您可以使用此端點來測試您的網站，如 步驟 9：測試您的網域端點 中所示。

使用如下步驟編輯公有存取設定並新增允許公有讀取存取權的設定之後，您可以使用網站端點存取您的網站。

步驟 5：(選用)：設定用於網站重新引導的子網域儲存貯體

設定用於網站託管的根網域儲存貯體之後，您可以選擇設定子網域儲存貯體，以將所有請求重新引導至根網域。例如，您可以設定 `www.example.com` 的所有要求以重新引導至 `example.com`。

若要設定重新引導

1. 在 Amazon S3 主控台中，於儲存貯體清單中選擇子網域儲存貯體名稱 (例如 `www.example.com`)。
2. 選擇 Properties (屬性)。
3. 在 Static website hosting (靜態網站託管) 下，選擇 Edit (編輯)。
4. 選擇 Redirect requests for an object (重新引導物件請求)。
5. 在 Target bucket (目標儲存貯體) 方塊中，輸入您的根網域，例如 **`example.com`**。
6. 在 Protocol (通訊協定)中，選擇 http。
7. 選擇 Save changes (儲存變更)。

步驟 6：上傳索引以建立網站內容

當您為儲存貯體允許靜態網站託管時，請輸入索引文件的名稱 (例如，**`index.html`**)。為儲存貯體允許靜態網站託管後，您可以將含有索引文件名稱的 HTML 檔案上傳到儲存貯體。

若要上傳索引檔案

1. 複製可將其作為本教學課程的簡單單頁網站的下列範例文字，將其貼到文字編輯器中，然後將其儲存為 index.html：

```
<html>
<head>
<title>Amazon Route 53 Getting Started</title>
</head>
```

```
<body>

<h1>Routing Internet Traffic to an Amazon S3 Bucket for Your Website</h1>

<p>For more information, see
<a href="https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-
started.html">Getting Started with Amazon Route 53</a>
in the <emphasis>Amazon Route 53 Developer Guide</emphasis>.</p>

</body>

</html>
```

2. 在 Buckets (儲存貯體名稱) 清單中，選擇希望為其啟用靜態網站託管的儲存貯體名稱。
3. 在 Amazon S3 主控台，選擇您在 若要允許在您的 S3 儲存貯體上託管網站 程序中建立的儲存貯體名稱 (按一下連結的儲存貯體名稱)。
4. 選擇 Upload (上傳)、Add Files (新增檔案)，從您儲存的位置選取 index.html，然後選取 Upload (上傳)。
5. 如果您建立並新增文件，例如 **`404.html`**，請依照步驟 3 至 5 來上傳。

步驟 7：編輯 S3 封鎖公有存取設定

根據預設，Amazon S3 會封鎖對帳戶和儲存貯體的公開存取。如想要使用儲存貯體託管靜態網站，請使用這些步驟編輯公有存取設定：

> **Warning**
>
> 在完成此步驟之前，請檢閱封鎖對 Amazon S3 儲存的公開存取，以確保您了解並接受允許公開存取所涉及的風險。當您關閉封鎖公開存取設定以公開儲存貯體時，網際網路上的任何人都可以存取您的儲存貯體。我們建議您封鎖對儲存貯體的所有公用存取權。

若要將流量路由到您的網站

1. 開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
2. 選擇已設定為靜態網站的儲存貯體名稱。
3. 選擇 Permissions (許可)。

4. 在 Block public access (bucket settings) (封鎖公開存取 (儲存貯體設定)) (封鎖公開存取 (儲存貯體設定)) 下，選擇 Edit (編輯)。
5. 清除 Block all public access (封鎖所有公開存取)，然後選擇 Save changes (儲存變更)。

Amazon S3 會關閉儲存貯體的封鎖公開存取設定。若要建立公開的靜態網站，在新增儲存貯體原則之前，可能還需要針對您的帳戶編輯封鎖公開存取設定。如果帳戶的封鎖公開存取設定目前已開啟，您在封鎖公開存取 (儲存貯體設定) 下會看到附註。

步驟 8：連接儲存貯體政策

編輯 Amazon S3 封鎖公開存取設定之後，您可以新增儲存貯體政策，以授予儲存貯體物件的公用讀取權限。當您授予公有讀取權限時，網際網路上的任何人都可以存取您的儲存貯體。

> **Warning**
>
> 在完成此步驟之前，請檢閱封鎖對 Amazon S3 儲存的公開存取，以確保您了解並接受允許公開存取所涉及的風險。當您關閉封鎖公開存取設定以公開儲存貯體時，網際網路上的任何人都可以存取您的儲存貯體。我們建議您封鎖對儲存貯體的所有公用存取權。

若要將流量路由到您的網站

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在 Buckets(儲存貯體) 下方，選擇儲存貯體的名稱。
3. 選擇 Permissions (許可)。
4. 在 Bucket Policy (儲存貯體政策) 下，選擇 Edit (編輯)。
5. 複製下列儲存貯體政策並貼至文字編輯器。此政策授與網際網路上的每個人許可權 (`"Principal":"*"`)，以取得與您的網域名稱相關聯的 S3 儲存貯體 (`"Action": ["s3:GetObject"]`) 中的檔案 (`"arn:aws:s3:::`*`your-domain-name`*`/*"`)：

```
{
   "Version":"2012-10-17",
   "Statement":[{
      "Sid":"AddPerm",
      "Effect":"Allow",
      "Principal":"*",
      "Action":[
```

```
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::your-domain-name/*"
         ]
      }]
}
```

6. 例如 *your-domain-name*，Resource將的值更新為**example.com**。
7. 選擇儲存變更。

步驟 9：測試您的網域端點

將網域儲存貯體設定為託管公有網站後，您就可以測試自己的端點。您只能測試網域儲存貯體的端點，因為子網域儲存貯體已設置為網站重新引導，且不是靜態網站託管。

> **Note**
>
> Amazon S3 不支援使用 HTTPS 存取網站。如果您想使用 HTTPS，則可以使用 Amazon CloudFront 為 Amazon S3 上託管的靜態網站提供服務。
> 如需詳細資訊，請參閱 < 在檢視者之間需要 HTTPS 進行通訊 > 和CloudFront。

1. 在 Buckets (儲存貯體) 下方，選擇儲存貯體的名稱。
2. 選擇 Properties (屬性)。
3. 在頁面底部的 Static website hosting (靜態網站託管) 下，選擇您的 Bucket website endpoint (儲存貯體網站端點)。

   您的索引文件會在不同的瀏覽器視窗中開啟。

步驟 10：將您網域的 DNS 流量路由到您的網站儲存貯體

您的 S3 儲存貯體中現在有單頁網站。若要開始將網域的網際網路流量路由到您的 S3 儲存貯體，請執行以下程序。

若要將流量路由到您的網站

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。

2. 在導覽窗格中，選擇 Hosted zones (託管區域)。

> **Note**
>
> 當您註冊網域時，Amazon Route 53 自動建立同名的託管區域。託管區域包含有關您希望 Route 53 如何路由網域流量的資訊。

3. 在託管區域清單，請選擇您的網域名稱。
4. 選擇 Create record (建立記錄)。

> **Note**
>
> 每個記錄包含有關您希望如何路由某個網域 (如 example.com) 或一個子網域 (例如 www.example.com 或 test.example.com) 流量的資訊。記錄儲存在網域的託管區域中。

5. 選擇 Switch to wizard (切換至精靈)。
6. 選擇 Simple routing (簡易路由)，然後選擇 Next (下一步)。
7. 選擇 Define simple record (定義簡易記錄)。
8. 在 Record name (記錄名稱) 中，接受預設值，這是您的託管區域與網域的名稱。
9. 在 Record type (記錄類型) 中，選擇 A – 將流量路由至 IPv4 位址和某些 AWS 資源。
10. 在 Value/Route traffic to (值/路由傳送流量至) 中，選擇 Alias to S3 website endpoint (連至 S3 網站端點的別名)。
11. 選擇 區域。
12. 選擇 S3 儲存貯體。

    儲存貯體名稱應與 Name (名稱) 方塊中顯示的名稱相符。在 Choose S3 bucket (選擇 S3 儲存貯體) 清單中，儲存貯體名稱會與建立儲存貯體之區域的 Amazon S3 網站端點一起顯示，例如 `s3-website-us-west-1.amazonaws.com (example.com)`。

    如果以下條件之一為真，則 Choose S3 bucket (選擇 S3 儲存貯體) 會列出儲存貯體：

    - 您將儲存貯體設定為靜態網站。
    - 儲存貯體與您要建立的記錄同名。
    - 目前 AWS 帳戶已建立儲存貯體。

如果您的儲存貯體未出現在 Choose S3 bucket (選擇 S3 儲存貯體) 清單中，請輸入建立儲存貯體之區域的 Amazon S3 網站端點，例如 **s3-website-us-west-2.amazonaws.com**。如需 Amazon S3 網站端點的完整清單，請參閱 Amazon S3 網站端點。如需別名目標的詳細資訊，請參閱 簡單別名記錄的專用值 中的「值/路由傳送流量至」。

13. 在 Evaluate target health (評估目標運作狀態) 中，選擇 No (否)。
14. 選擇 Define simple record (定義簡易記錄)。

(選用) 若要新增子網域 (**www.example.com**) 的別名記錄

如果您為子網域建立儲存貯體，請同時為其新增別名記錄。

1. 在 Configure records (設定記錄) 下，選擇 Define simple record (定義簡易記錄)。
2. 在子網域的 Record name (記錄名稱) 中，輸入 www。
3. 在 Record type (記錄類型) 中，選擇 A – 將流量路由至 IPv4 位址和某些 AWS 資源。
4. 在 Value/Route traffic to (值/路由傳送流量至) 中，選擇 Alias to S3 website endpoint (連至 S3 網站端點的別名)。
5. 選擇區域。
6. 選擇 S3 儲存貯體，例如 `s3-website-us-west-2.amazonaws.com (example.com)`。

   如果您的儲存貯體未出現在 Choose S3 bucket (選擇 S3 儲存貯體) 清單中，請輸入建立儲存貯體之區域的 Amazon S3 網站端點，例如 **s3-website-us-west-2.amazonaws.com**。
7. 在 Evaluate target health (評估目標運作狀態) 中，選擇 No (否)。
8. 選擇 Define simple record (定義簡易記錄)。
9. 在 Configure records (設定記錄) 頁面上，選擇 Create records (建立記錄)。

步驟 11：測試您的網站

若要確認網站正常運作，請開啟 Web 瀏覽器並瀏覽到下列 URL：

- 例如 *your-domain-name*，http://example.com— 顯示*your-domain-name*值區中的索引文件
- http://www. *your-domain-name*例如，www.example.com— 將您的請求重定向到*your-domain-name*存儲桶

在某些情況下，您可能需要清除快取，才能看到預期的行為。

如需路由網際網路流量的進階資訊，請參閱將 Amazon Route 53 設定為 DNS 服務。如需將網際網路流量路由至 AWS 資源的資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

步驟 12（可選）：使用 Amazon CloudFront 加快內容的分發

CloudFront 是一種 Web 服務，可以加快向用戶分發靜態和動態 Web 內容（例如 .html，.css，.js 和圖像文件）的速度。 CloudFront 透過稱為節點位置的全球資料中心網路傳遞您的內容。當使用者要求您提供服務的內容時 CloudFront，會將使用者路由至提供最低延遲 (時間延遲) 的節點，以便以最佳效能傳遞內容。

- 如果內容已經位於延遲最低的節點位置，請立即 CloudFront 傳送。
- 如果內容不在該節點，請從 Amazon S3 儲存貯體或 HTTP 伺服器 (例如 Web 伺服器) CloudFront 擷取該內容，該伺服器是您已識別為內容最終版本的來源。

如需使用將內容分發 CloudFront 到 Amazon S3 儲存貯體的相關資訊，請參閱 Amazon CloudFront 開發人員指南中的從 Amazon S3 分發內容 CloudFront 時新增。

使用 Amazon CloudFront 分發服務靜態網站

此入門教學課程說明如何執行以下任務：

- 註冊網域名稱，例如 example.com。
- 為您的網域建立憑證。
- 建立兩個 Amazon S3 儲存貯體，並設定一個儲存貯體用於託管網站，另一個用於重新引導至子網域。
- 建立範例網站，並將檔案儲存在 S3 儲存貯體
- 為兩個 S3 儲存貯體建立 CloudFront 分發。
- 設定 Amazon 路線 53 以將流量路由到 CloudFront 分發。

完成後，您將能夠開啟瀏覽器，輸入網域名稱，並安全地檢視您的網站。

主題

- 必要條件
- 步驟 1：註冊網域

- 步驟 2：請求公有憑證
- 步驟 3：建立 S3 儲存貯體以託管您的子網域
- 步驟 4：為您的根網域建立另一個 S3 儲存貯體
- 步驟 5：將網站檔案上傳到您的子網域儲存貯體
- 步驟 6：設定用於網站重新引導的根網域儲存貯體
- 步驟 7：為您的子域創建 Amazon CloudFront 分發
- 步驟 8：為您的根網域建立 Amazon CloudFront 分發
- 步驟 9：將您網域的 DNS 流量路由到您的 CloudFront 分佈
- 步驟 10：測試您的網站

必要條件

開始之前，請務必先完成 設定 Amazon Route 53 中的步驟。

步驟 1：註冊網域

若要使用網域名稱 (例如 example.com)，您必須找到一個未被使用的網域名稱並註冊該網域。當您註冊網域名稱，即表示您要保留它以供您在網際網路上的任何位置獨佔使用，通常為期一年。依預設，我們會在每年年底自動續約網域名稱，但您可以關閉自動續約。如需詳細資訊，請參閱 註冊新網域。

步驟 2：請求公有憑證

Amazon CloudFront 分發需要公有憑證才能進行設定，以 CloudFront 要求檢視者使用 HTTPS，以便在與檢視者 CloudFront 通訊時加密連線。

若要請求 AWS Certificate Manager(ACM) 公有憑證 (主控台)

1. 前往 https://console.aws.amazon.com/acm/home 登入 AWS 管理主控台並開啟 ACM 主控台。

   > **Note**
   >
   > 確定您是在美國東部 (維吉尼亞北部) 區域建立憑證。這是 Amazon 所必需的 CloudFront。

   在左側導覽區中選擇請求憑證，然後在請求憑證頁面上依次選擇請求公有憑證和下一步。

2. 在網域名稱區段中，輸入 **example.com** 之類的網域。

   選擇將其他名稱新增至此憑證，在網域名稱前輸入星號，以請求所有子網域的萬用字元憑證，例如 ***.example.com**。

3. 在驗證方法區段中，選擇 DNS 驗證。
4. 在金鑰演算法區段中，選擇 RSA 2048。
5. 在新增標籤區段中，您可以選擇標記憑證。標籤是做為中繼資料的鍵/值對，可用來識別和整理 AWS 資源。

   選擇請求以進入憑證頁面。

6. 當新憑證的狀態顯示為擱置中時，請選擇憑證 ID，然後在憑證詳細資訊頁面上選擇在 Route 53 中建立記錄，以自動新增網域的 CNAME 記錄，然後選擇建立記錄。

   所以此 Certificate status（憑證狀態）頁面應該開啟並顯示狀態橫幅報告 Successfully created DNS records（成功建立 DNS 記錄）。

   您的新憑證可能會繼續顯示 Pending validation（待定驗證）狀態最多 30 分鐘。

步驟 3：建立 S3 儲存貯體以託管您的子網域

為 www 創建一個 S3 存儲桶。 your-domain-name

Amazon S3 可讓您從網際網路上的任何位置儲存和擷取您的資料。在此步驟中，您將建立一個 S3 儲存貯體來儲存網站的所有檔案。

1. 前往 https://console.aws.amazon.com/s3/ 開啟 Amazon S3 主控台。
2. 選擇建立儲存貯體。
3. 輸入下列值：

   儲存貯體名稱

   輸入萬維網。 ***your-domain-name***。例如，如已註冊網域名稱 example.com，請輸入 www.example.com。

   區域

   為您的儲存貯體選擇一個區域。

4. 若要接受預設設定並建立儲存貯體，請選擇 Create bucket (建立儲存貯體)。

如需 S3 儲存貯體設定的詳細資訊，請參閱 Amazon S3 使用者指南中的檢視儲存貯體屬性。

步驟 4：為您的根網域建立另一個 S3 儲存貯體

如果您還希望您的用戶能夠使用根域，請. *your-domain-name*(例如 example.com) 若要存取您的範例網站，請建立第二個 S3 儲存貯體。在本教學課程中，您需設定第二個儲存貯體 (根網域)，以將流量路由到第一個儲存貯體。

若要為其建立 S3 儲存貯體 your-domain-name

1. 前往 https://console.aws.amazon.com/s3/ 開啟 Amazon S3 主控台。
2. 選擇建立儲存貯體。
3. 輸入下列值：

   儲存貯體名稱

   輸入 ***your-domain-name***。例如，如已註冊網域名稱 example.com，請輸入 example.com。

   區域

   選擇建立第一個儲存貯體的區域。
4. 若要接受預設設定並建立儲存貯體，請選擇 Create bucket (建立儲存貯體)。

步驟 5：將網站檔案上傳到您的子網域儲存貯體

現在您有了一個 S3 儲存貯體，可以上傳您的網站檔案。在本教學課程中，您只需上傳一個在頁面上顯示文字的簡單 index.html 檔案。

若要為網站託管啟用 S3 儲存貯體

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在 Buckets (儲存貯體) 清單中，選擇您要上傳網站檔案的目標儲存貯體名稱，例如 **`www.example.com`**。
3. 複製建立一個簡單的單頁網頁的示例文字，將其貼到文字編輯器中，並將其儲存為 index.html：

```
<html>
```

```
<head>
<title>Amazon Route 53 Getting Started</title>
</head>

<body>

<h1>Routing Internet traffic to Cloudfront distributions for your website stored in
 an S3 bucket</h1>

<p>For more information, see
<a href="https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-
started.html">Getting Started with Amazon Route 53</a>
in the <emphasis>Amazon Route 53 Developer Guide</emphasis>.</p>

</body>

</html>
```

4. 在 Objects (物件) 標籤上，選擇 Upload (上傳)。
5. 在 Files and folders (檔案和資料夾) 下方，選擇 Add files (新增檔案) 並上傳您的網站檔案。在本教學課程中，請上傳您在步驟 3 中儲存的 index.html 檔案。

步驟 6：設定用於網站重新引導的根網域儲存貯體

設定用於網站託管的根網域儲存貯體之後，您可以選擇設定根網域儲存貯體，以將所有請求重新引導至子網域。例如，您可以設定 `example.com` 的所有要求以重新引導至 `www.example.com`。

若要設定重新引導

1. 在 Amazon S3 主控台中，於 Buckets (儲存貯體) 清單中選擇子網域儲存貯體 (例如 `example.com`)。
2. 選擇 Properties (屬性)。
3. 在 Static website hosting (靜態網站託管) 下，選擇 Edit (編輯)。
4. 在 Static website hosting (靜態網站託管) 下，選擇 Enable (啟用)。
5. 選擇 Redirect requests for an object (重新引導物件請求)。
6. 在 Host name (主機名稱) 方塊中，輸入您的子網域，例如 **`www.example.com`**。
7. 請在 Protocol (通訊協定) 中選擇 HTTPS。
8. 選擇儲存變更。

9. 在 Static website hosting 下，請記下 Endpoint (端點)。

   Endpoint (端點) 是儲存貯體的 Amazon S3 網站端點。您將使用此端點來設定 Amazon CloudFront 分發。

步驟 7：為您的子域創建 Amazon CloudFront 分發

在此步驟中，您會為子網域建立 CloudFront 分佈，例如 www.example.com，讓您的網站能夠使用 HTTPS，以便使用者可以安全地檢視它。

建立 CloudFront 分佈

1. 在開啟 CloudFront 主控台https://console.aws.amazon.com/cloudfront/v4/home。
2. 選擇 Create Distribution (建立分佈)。
3. 在來源下，對於來源網域，選擇您先前建立的 Amazon S3 儲存貯體。

   對於原始存取，選取舊版存取身分。對於 Origin access identity (原始存取身分)，您可以從清單選擇，或選擇 Create new OAI (建立新的 OAI) (兩者都可以發揮作用)。

   對於 Bucket policy (儲存貯體政策)，選擇 Yes, update the bucket policy (是，更新儲存貯體政策)。
4. 對於 Default Cache Behavior Settings (預設快取行為設定) 下的設定，在 Viewer (檢視器) 下將 Viewer protocol policy (檢視器通訊協定政策) 設定為 Redirect HTTP to HTTPS (重新導向 HTTP 到 HTTPS)，並接受其餘的預設值。

   如需快取行為選項的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的快取行為設定。
5. 在 Web 應用程式防火牆 (WAF) 區段中，您可以選擇啟用或停用 AWS WAF 安全保護。
6. 對於 Settings (設定) 下的欄位，執行下列動作：

   - 為 Alternate domain name (CNAME) - optional (備用網域名稱 (CNAME) - 選y用) 選擇 Add item (新增項目)，然後輸入您的子網域，例如 **`www.example.com`**。
   - 對於 Custom SSL Certificate (自訂 SSL 憑證)，選擇您先前建立的憑證。
   - 在 Default root object (預設根物件) 文字方塊中，輸入 **`index.html`**。
   - 接受剩餘欄位的預設值，然後選擇建立分佈。

     如需分佈選項的詳細資訊，請參閱分佈設定。

7. 在頁面底部，選擇 Create Distribution (建立分佈)。
8. CloudFront 建立發行版之後，發佈的 [狀態] 欄的值會從 [進行中] 變更為 [已部署]。通常這需要幾分鐘的時間。

   記錄指 CloudFront 派給您的發行版的網域名稱，該網域名稱會出現在發行版清單中。您可以使用此網域名稱來測試分佈。

步驟 8：為您的根網域建立 Amazon CloudFront 分發

在此步驟中，您可以為根網域建立一個 CloudFront 分發，以便在其 URL 重新導向至子網域時使用 HTTPS。

建立 CloudFront 分佈

1. 在開啟 CloudFront 主控台https://console.aws.amazon.com/cloudfront/v4/home。
2. 選擇 Create Distribution (建立分佈)。
3. 在 Origin Settings (原始設定) 下方，對於 Origin Domain Name (原始網域名稱)，請輸入儲存貯體網站端點。對於您先前建立的 Amazon S3 儲存貯體，您從 Properties (屬性) 的 Static website hosting (靜態網站託管) 部分取得此資訊。

   對於其餘的欄位，請接受預設值。
4. 對於 Default Cache Behavior Settings (預設快取行為設定) 下的欄位，執行下列動作：

   - 在 Viewer (檢視器) 下方，設定 Viewer protocol policy (檢視器通訊協定政策) 為 Redirect HTTP to HTTPS (重新引導 HTTP 到 HTTPS)。
   - 將 「快取」設定設定為CachingDisabled。
   - 接受其餘欄位的預設值。

   如需快取行為選項的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的快取行為設定。
5. 對於 Settings (設定) 下的欄位，執行下列動作：

   - 為 Alternate domain name (CNAME) - optional (備用網域名稱 (CNAME) - 選用) 選擇 Add item (新增項目)，然後輸入您的根網域，例如 **`example.com`**。
   - 對於 Custom SSL Certificate (自訂 SSL 憑證)，選擇您先前建立的憑證。
   - 對於其餘的欄位，請接受預設值。

如需分佈選項的詳細資訊，請參閱分佈設定。

6. 在頁面底部，選擇 Create Distribution (建立分佈)。
7. CloudFront 建立發行版之後，發佈的 [狀態] 欄的值會從 [進行中] 變更為 [已部署]。通常這需要幾分鐘的時間。

   記錄指 CloudFront 派給您的發行版的網域名稱，該網域名稱會出現在發行版清單中。您可以使用此網域名稱來測試分佈

步驟 9：將您網域的 DNS 流量路由到您的 CloudFront 分佈

您現在在 S3 儲存貯體中有一個使用 CloudFront 分發的單頁網站。若要開始將您網域的網際網路流量路由至 CloudFront 發佈，請執行下列程序。

如需將流量路由至 CloudFront 分發的詳細資訊，請參閱使用您的網域名稱將流量路由到 Amazon CloudFront 分發。

若要將流量路由到您的網站

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。

   > **Note**
   >
   > 當您註冊網域時，Amazon Route 53 自動建立同名的託管區域。託管區域包含有關您希望 Route 53 如何路由網域流量的資訊。

3. 在託管區域清單，請選擇您的網域名稱。
4. 選擇 Create record (建立記錄)。

   如果您位於 Quick create record (快速建立記錄) 檢視，選擇 Switch to wizard (切換至精靈)。

   > **Note**
   >
   > 每個記錄包含有關您希望如何路由某個網域 (如 example.com) 或子網域 (例如 www.example.com 或 test.example.com) 流量的資訊。記錄儲存在網域的託管區域中。

5. 選擇 Simple routing (簡易路由)，然後選擇 Next (下一步)。

6. 選擇 Define simple record (定義簡易記錄)。
7. 在 Record name (記錄名稱) 中，在預設值的前方輸入 **www**，這是您的託管區域與網域的名稱。
8. 在 Record type (記錄類型) 中，選擇 A – 將流量路由至 IPv4 位址和某些 AWS 資源。
9. 在流量值/路由到中，選擇要分配的別名。 CloudFront
10. 選擇分佈。

    分佈名稱應與 Distributions (分佈) 清單的 Domain name (網域名稱) 方塊中出現的名稱相符，例如 `dddjjjkkk.cloudfront.net`。
11. 在 Evaluate target health (評估目標運作狀態) 中，選擇 No (否)。
12. 選擇 Define simple record (定義簡易記錄)。

新增根網域 (**`example.com`**) 的別名記錄

同時新增根網域的別名記錄，以便它指向將流量重新引導到 `www.example.com` 的 S3 儲存貯體。如需將流量路由至 CloudFront 分發的詳細資訊，請參閱使用您的網域名稱將流量路由到 Amazon CloudFront 分發。

1. 在 Configure records (設定記錄) 下，選擇 Define simple record (定義簡易記錄)。
2. 在 Record name (記錄名稱) 中，接受預設值。
3. 在 Record type (記錄類型) 中，選擇 A – 將流量路由至 IPv4 位址和某些 AWS 資源。
4. 在值/將流量路由至下，選擇 CloudFront 分佈的別名。
5. 選擇分佈。

    分佈名稱應與 Distributions (分佈) 清單的 Domain name (網域名稱) 方塊中出現的名稱相符，例如 `dddjjjkkk.cloudfront.net`。
6. 在 Evaluate target health (評估目標運作狀態) 中，選擇 No (否)。
7. 選擇 Define simple record (定義簡易記錄)。
8. 在 Configure records (設定記錄) 頁面上，選擇 Create records (建立記錄)。

步驟 10：測試您的網站

若要確認網站正常運作，請開啟 Web 瀏覽器並瀏覽到下列 URL：

- https://www. *`your-domain-name`* 例如 `www.example.com` — 在 *`www ######## your-domain-name`* 桶

- *your-domain-name*例如，example.com-將您的請求重定向到 *www# your-domain-name*桶

在某些情況下，您可能需要清除快取，才能看到預期的行為。

如需路由網際網路流量的進階資訊，請參閱將 Amazon Route 53 設定為 DNS 服務。如需將網際網路流量路由至 AWS 資源的資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

與其他服務整合

您可以整合 Amazon Route 53 與其他 AWS 服務，記錄傳送到 Route 53 API 的請求、監控資源的狀態，以及將標籤指派給資源。此外，可以使用 Route 53 將網際網路流量路由到您的 AWS 資源。

主題

- 記錄、監控和標記
- 將流量路由到其他 AWS 資源

記錄、監控和標記

AWS CloudTrail

Amazon Route 53 與 AWS CloudTrail 整合，此服務可擷取由 AWS 帳戶傳送到 Route 53 API 之每個請求的相關資訊。您可使用 CloudTrail 日誌檔案中的資訊來判定對 Route 53 提出的請求、每個請求的來源 IP 地址、提出請求的人員、提出時間等等。

如需更多詳細資訊，請參閱 使用日誌記錄 Amazon 路線 53 API 調用 AWS CloudTrail。

Amazon CloudWatch

您可以使用 Amazon CloudWatch 來監控 Route 53 運作狀態檢查的狀態 (狀態良好或狀態不佳)。運作狀態檢查監控 Web 應用程式、Web 伺服器和其他資源的運作狀態與效能。Route 53 會以您指定的定期間隔，透過網際網路向您的應用程式、伺服器或其他資源提交自動請求，以驗證其連線能力、可用性和功能。

如需更多詳細資訊，請參閱 使用 CloudWatch 監控運作狀態檢查。

標籤編輯器

標籤是您指派給 AWS 資源 (包括 Route 53 網域、託管區域及運作狀態檢查) 的標籤。每個標籤皆包含由您定義的索引鍵和值。例如，您可以將標籤指派給鍵為 "Customer"、值為 "Example Corp" 的註冊網域。標籤具有多種用途；一個常見的用途是對 AWS 成本進行分類和追蹤。

如需更多詳細資訊，請參閱 標記 Amazon Route 53 資源。

將流量路由到其他 AWS 資源

您可以使用 Amazon Route 53 將流量路由到各種 AWS 資源。

Amazon API Gateway

Amazon API Gateway 可讓您建立、發佈、維護、監控任何規模的 API，並保護其安全。您可以建立可存取 AWS 或其他 Web 服務的 API，以及 AWS 雲端中所存放的資料。

您可使用 Route 53 將流量路由到 API Gateway API。如需更多詳細資訊，請參閱 使用網域名稱將流量路由到 Amazon API Gateway API。

Amazon CloudFront

若要加速交付 Web 內容，您可以使用 Amazon CloudFront，即 AWS 內容交付網路 (CDN)。CloudFront 可使用全球節點網路來發佈您的整個網站—包括動態、靜態、串流和互動式內容。CloudFront 將對於內容的請求路由到可為使用者提供最低延遲的節點。您可以使用 Route 53 將網域流量路由到您的 CloudFront 分發。如需更多詳細資訊，請參閱 使用您的網域名稱將流量路由到 Amazon CloudFront 分發。

Amazon EC2

Amazon EC2 在 AWS 雲端中提供可擴展的運算容量。您可以使用預先設定的範本 (Amazon Machine Image，即 AMI) 啟動 EC2 虛擬運算環境 (執行個體)。當您啟動 EC2 執行個體時，EC2 會自動安裝作業系統 (Linux 或 Microsoft Windows) 和包含在 AMI 中的其他軟體，例如 Web 伺服器或資料庫軟體。

如果您在 EC2 執行個體上託管網站或執行 Web 應用程式，可以使用 Route 53 將網域 (例如 example.com) 的流量路由到您的伺服器。如需更多詳細資訊，請參閱 將流量路由到 Amazon EC2 執行個體。

AWS Elastic Beanstalk

如果您使用 AWS Elastic Beanstalk 在 AWS 雲端中部署和管理應用程式，你可使用 Route 53 將網域 (例如 example.com) 的 DNS 流量路由到 Elastic Beanstalk 環境。如需更多詳細資訊，請參閱 將流量路由到 AWS Elastic Beanstalk 環境。

Elastic Load Balancing

如果您在多個 Amazon EC2 執行個體上託管網站，可以使用 Elastic Load Balancing (ELB) 負載平衡器在執行個體之間分配網站流量。當網站的流量隨時間發生變化時，ELB 服務會自動擴展負載平衡器。負載平衡器還會監控其註冊執行個體的運作狀況，而且只將網域流量路由到正常運作的執行個體。

您可以使用 Route 53 將網域流量路由到 Classic Load Balancer、Application Load Balancer 或 Network Load Balancer。如需更多詳細資訊，請參閱 將流量路由到 ELB 負載平衡器。

Amazon Lightsail

Amazon Lightsail 提供以低廉、可預測的每月價格，在雲端部署及管理網站、Web 應用程式和資料庫所需的運算、儲存及聯網容量與功能。

如果您使用 Lightsail，則可以使用 Route 53 將流量路由傳送到 Lightsail 執行個體。如需詳細資訊，請參閱使用 Route 53 將網域指向 Amazon Lightsail 執行個體。

Amazon S3

Amazon Simple Storage Service (Amazon S3) 提供安全、耐用、高擴展性的雲端儲存。您可以設定 S3 儲存貯體來託管包括網頁和用戶端指令碼的靜態網站。(S3 不支援伺服器端指令碼。) 您可以使用 Route 53 將流量路由到 Amazon S3 儲存貯體。如需詳細資訊，請參閱下列主題：

- 如需有關路由流量到儲存貯體的詳細資訊，請參閱將流量路由到 Amazon S3 儲存貯體中託管的網站。
- 如需如何在 S3 儲存貯體中託管靜態網站的更詳細說明，請參閱 Amazon Route 53 入門。

Amazon Virtual Private Cloud (Amazon VPC)

界面端點可讓您連接至採用 AWS PrivateLink 技術的服務。這些服務包含一些 AWS 服務、其他 AWS 客戶和合作夥伴在其專屬 VPC 中託管的服務 (稱為「端點服務」)，以及支援的 AWS Marketplace 合作夥伴服務。

您可以使用 Route 53 將流量路由到界面端點。如需更多詳細資訊，請參閱 使用網域名稱將流量路由到 Amazon Virtual Private Cloud 介面端點。

Amazon WorkMail

如果您要使用 Amazon WorkMail 處理商業電子郵件，用 Route 53 做為 DNS 服務，您可以使用 Route 53 將流量路由到您的 Amazon WorkMail 電子郵件網域。如需更多詳細資訊，請參閱 將流量路由到 Amazon WorkMail。

如需詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

DNS 網域名稱格式

網域名稱 (包括網域、託管區域和記錄的名稱) 是由一系列以點分隔的標籤所組成。每個標籤長度最多可達 63 個位元組。網域名稱的總長度不能超過 255 個位元組 (包括點)。Amazon Route 53 支援任何有效的網域名稱。

命名需求取決於您是註冊網域名稱還是指定託管區域或記錄的名稱。請參閱適用的主題。

主題

- 為網域名稱註冊設定網域名稱的格式
- 為託管區域和記錄設定網域名稱的格式
- 在託管區域和記錄的名稱中使用星號 (*)
- 設定國際化網域名稱的格式

為網域名稱註冊設定網域名稱的格式

對於網域名稱註冊，網域名稱只能包含 a-z、0-9 和 – (連字號)。不能在標籤開頭或結尾指定連字號。

如需有關如何註冊國際化網域名稱 (IDN) 的詳細資訊，請參閱設定國際化網域名稱的格式。

為託管區域和記錄設定網域名稱的格式

對於託管區域和記錄，網域名稱可以包含下列任何可列印的 ASCII 字元 (不含空格)：

- a-z
- 0-9
- - (連字號)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

Amazon Route 53 會將字母字元儲存為小寫字母 (a-z)，不論儲存時指定為大寫、小寫字母或逸出碼中的對應字母。

如果您的網域名稱包含下列任何字元，則必須使用 \###### 格式的逸出碼來指定字元：

- 八進位字元 000 到 040 (0 至 32 十進位，0x00 到 0x20 十六進位)
- 八進位字元 177 到 377 (127 至 255 十進位，0x7F 到 0xFF 十六進位)

- . (句號)，八進位字元 056 (十進位 46、十六進位 0x2E)，當在網域名稱中用做字元時。使用 . 做為標籤之間的分隔符號時，則不需要使用逸出碼。

如果網域名稱包含 z、0-9、- (連字號) 或 _ (底線) 以外的任何字元，Route 53 API 動作會將這些字元當做逸出碼傳回。無論您在建立實體時將字元指定為字元或逸出碼，都是如此。Route 53 主控台會將字元顯示為字元，而不顯示為逸出碼。

如需對應八進位碼的 ASCII 字元清單，請在網際網路上搜尋「ascii 表格」。

若要指定國際化網域名稱 (IDN)，請將名稱轉換為 Punycode。如需更多詳細資訊，請參閱 設定國際化網域名稱的格式。

在託管區域和記錄的名稱中使用星號 (*)

您可以建立名稱中包含 * 的託管區域和記錄。

託管區域

- 網域名稱最左邊的標籤中不可包含 *。例如，不允許 *. example.com。
- 如果您在其他位置包含 *，DNS 會將它視為 * 字元 (ASCII 42)，而不是萬用字元。

記錄

DNS 會根據 * 字元出現在名稱中的位置，將其視為萬用字元或 * 字元 (ASCII 42)。請注意下列在記錄名稱中使用 * 做為萬用字元的限制：

- * 必須取代網域名稱最左邊的標籤，例如 *. example.com 或 *.acme.example.com。如果您在任何其他位置包含 * (例如 prod.*.example.com)，則 DNS 會將其視為 * 字元 (ASCII 42)，而不是萬用字元。
- * 必須取代整個標籤。例如，您無法指定 *prod.example.com 或 prod*.example.com。
- 特定網域名稱具有高優先順序。例如，如果您建立 *. example.com 和 acme.example.com 的記錄，Route 53 一律會使用 acme.example.com 記錄中的值，回應 acme.example.com 的 DNS 查詢。
- * 適用於包含星號之子網域層級的 DNS 查詢，以及該子網域的所有子網域。例如，如果您建立名為 *.example.com 的記錄，Route 53 會使用該記錄中的值，以回應 zenith.example.com、acme.zenith.example.com 和 pinnacle.acme.zenith.example.com 的 DNS 查詢 (如果該託管區域沒有任何類型的記錄)。

如果您建立名為 *.example.com 的記錄，且 example.com 記錄不存在，Route 53 會以 NXDOMAIN (不存在的網域) 回應 example.com 的 DNS 查詢。

- 針對同一層級所有子網域和網域名稱，您可以將 Route 53 設定為對 DNS 查詢傳回相同的回應。例如，您可以使用 example.com 記錄，將 Route 53 設定為回應 acme.example.com 和 zenith.example.com 等 DNS 查詢。執行以下步驟：

  1. 建立網域的記錄，例如 example.com。
  2. 建立子網域的別名記錄，例如 *.example.com。指定您在步驟 1 建立的記錄，做為別名記錄的目標。

- * 不可用做 NS 類型之記錄的萬用字元。

設定國際化網域名稱的格式

當您註冊新的網域名稱或建立託管區域和記錄，您可以指定 a-z 之外的字母 (例如法語中的 ç)、其他字母 (例如斯拉夫字母或阿拉伯字母) 中的字元，以及中文、日文或韓文等語言中的字元。Amazon Route 53 會用 Punycode 儲存這些國際化網域名稱 (IDN) (將 Unicode 字元轉換為 ASCII 字串表示)。

如果您要註冊網域名稱，請注意下列事項：

- 只有在頂層網域 (TLD) 支援 IDN 並支援您要使用的語言時，才能使用 a-z、0-9 和 - (連字號) 以外的字元。若要判斷 TLD 支援哪些語言，請參閱可向 Amazon Route 53 註冊的網域。
- 如果名稱址包含字母 a-z，您可以指定不支援語言的名稱。例如，如果 TLD 不支援法文，但您要使用的名稱只包含 a-z 的字母 (而沒有變音符號)，您仍可使用該名稱。在此範例中，可允許包含 "c" 的名稱，不允許包含 "ç" 的名稱。
- 如果 TLD 不支援 IDN 或不支援您要用於網域名稱的語言，您也無法以 Punycode 指定名稱，即使 Punycode 只包含 a-z、0-9 和 - 亦然。

以下範例顯示國際化網域名稱「中国.asia」的 Punycode 表示：

```
xn--fiqs8s.asia
```

當您在現代瀏覽器的網址列中輸入 IDN，瀏覽器會先將它轉換為 Punycode，然後提交 DNS 查詢或提出 HTTP 請求。

如何輸入 IDN 取決於您要建立的內容 (網域名稱、託管區域或記錄)，以及建立方式 (API、開發套件或 Route 53 主控台)：

- 如果您使用 Route 53 API 或其中一個 AWS 開發套件，可以透過程式設計方式將 Unicode 值轉換為 Punycode。例如，如果您使用 Java，可以透過使用 java.net.IDN 程式庫的 toASCII 方法，將 Unicode 值轉換為 Punycode。
- 如果您使用 Route 53 主控台註冊網域名稱，可以將名稱 (包括 Unicode 字元) 貼至名稱欄位，然後主控台會先將值轉換為 Punycode，再進行儲存。
- 如果您使用 Route 53 主控台來建立託管區域或記錄，需要先將網域名稱轉換為 Punycode，然後在適用的 Name (名稱) 欄位中輸入名稱。如需線上轉換器的詳細資訊，請在網際網路上搜尋「punycode 轉換器」。

如果您要註冊網域名稱，請注意並非所有頂層網域 (TLD) 都支援 IDN。如需 Route 53 支援的 TLD 清單，請參閱 可向 Amazon Route 53 註冊的網域。已記錄不支援 IDN 的 TLD。

使用 Amazon Route 53 註冊和管理網域

當您想要取得新的網域名稱時 (例如 URL http://example.com 的 example.com 部分)，可以向 Amazon Route 53 註冊該網域名稱。也可以將現有網域的註冊從其他註冊商轉移到 Route 53，或將向 Route 53 註冊的網域轉移到其他註冊商。

本章中的程序說明如何使用 Route 53 主控台註冊和轉移網域，以及如何編輯網域設定和檢視網域狀態。如果您只想註冊和管理幾個網域，使用主控台是最簡單的方法。

如果您需要註冊和管理許多網域，您可能更喜歡以程式設計方式進行變更。如需詳細資訊，請參閱 設定 Amazon Route 53。

> **Note**
>
> 如果您使用的是 AWS SDK 存在的語言，請使用 SDK，而不是嘗試通過 API 工作。開發套件可簡化身分驗證、與您的開發環境輕鬆整合，並可輕鬆存取 Route 53 命令。

我們提供的網域名稱註冊服務遵循我們的網域名稱註冊合約。

主題

- 註冊新網域
- 更新網域設定
- 續約網域的註冊
- 還原已過期或已刪除的網域
- 更換已向 Route 53 註冊的網域託管區域
- 轉移網域
- 重新傳送授權和確認電子郵件
- 設定網域的 DNSSEC
- 尋找您的註冊商和有關您網域的其他資訊
- 刪除網域名稱註冊
- 就網域註冊問題聯絡 S AWS upport
- 下載網域帳單報告

- 可向 Amazon Route 53 註冊的網域

註冊新網域

如需有關註冊新網域、轉移網域以及檢視網域註冊狀態的資訊，請參閱適用的主題。

主題

- 註冊新網域
- 註冊或轉移網域時所指定的值
- Amazon Route 53 在您註冊網域時傳回的值
- 檢視網域註冊的狀態

註冊新網域

為現有網域註冊新網域或更新名稱伺服器

您可以將 Amazon Route 53 與您向 Route 53 註冊的網域搭配使用，也可以將其與向其他 DNS 提供者註冊的網域搭配使用。視您的 DNS 提供者而定，選擇下列其中一個程序來向 Route 53 註冊並使用新網域：

- 若要註冊新網域，請參閱 若要使用 Route 53 註冊網域。
- 對於現有網域，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。
- 如需將網域移至其他註冊商，請參閱在您想要使用其他 DNS 服務時更新名稱伺服器。

網域註冊的考量事項

開始之前，請注意下列事項：

聯絡 S AWS upport

如果您在註冊網域時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

網域註冊定價

如需有關註冊網域的費用資訊，請參閱 Amazon Route 53 網域註冊定價。

支援的網域

如需支援的 TLD 清單，請參閱可向 Amazon Route 53 註冊的網域。

您將無法在註冊網域名稱之後予以變更

如果您不慎註冊了錯誤的網域名稱，將無法變更。反之，您需要註冊另一個網域名稱，並指定正確的名稱。您也無法取得錯誤註冊的網域名稱的退款。

AWS 學分

您無法使用 AWS 積分支付在 Route 53 註冊新網域的費用。

特殊或高級的價格

TLD 註冊機構向一些網域名稱指派特殊或優惠的價格。您無法使用 Route 53 註冊具有特殊或高級價格的網域。

託管區域的費用

當您向 Route 53 註冊網域時，我們會為該網域自動建立託管區域，而且除了網域註冊的年費外，還會對該託管區域收取小額的月費。您可以在此託管區域存放有關如何將網域流量路由到 Amazon EC2 執行個體或 CloudFront 分發的資訊。如果您不想立即使用網域，則可刪除該託管區域；如果在註冊網域後的 12 小時內刪除託管區域，您的 AWS 帳單中將不會包含有關託管區域的任何費用。我們還會針對所收到對網域的 DNS 查詢收取小額費用。如需詳細資訊，請參閱 Amazon Route 53 定價。

更換網域的託管區域

如果您為網域建立新的託管區域，則還必須更新網域的名稱伺服器，以將這些名稱伺服器用於新的託管區域。如需詳細資訊，請參閱 更換已向 Route 53 註冊的網域託管區域

若要使用 Route 53 註冊網域

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台

- 舊主控台

New console

若要使用 Route 53 註冊網域

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇網域，然後選擇已註冊的網域。
3. 在已註冊的網域頁面上，選擇註冊網域。

   a. 在搜尋網域區段中，輸入要註冊的網域名稱，然後選擇搜尋，了解該網域名稱是否可用。

      如果您想要註冊的網域名稱包含非 a-z、A-Z、0-9 和 – (連字號) 的字元，請注意下列事項：

      - 您可以使用適用的字元來輸入名稱。您不需要將名稱轉換為 Punycode。
      - 隨即顯示語言清單。選擇指定名稱的語言。例如，如果您輸入 příklad (捷克文的「範例」)，請選擇捷克文 (CES) 或捷克文 (CZE)。

      > **Note**
      >
      > 對於具有多個程式碼的語言，您可能需要嘗試兩種程式碼。即使 CES 和 CZE 是同義詞，某些 TLD 註冊機構只支援其中一個。

      如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。

      如果您輸入的網域可用，則會顯示該網域；如果沒有顯示該網域，類似的網域會顯示為建議。

      您最多可以選擇五個網域進行註冊。您選取的網域會出現在選取的網域清單中。

   b. 若要註冊多個網域，請重複步驟 3a 到 3b。
4. 選擇前往結帳。
5. 在定價頁面上，選擇您要註冊之網域的年數，以及是否希望我們在到期日期前自動續約網域註冊。

> **Note**
>
> 網域名稱註冊和續約不接受退款。如果您啟用自動網域續約，而且在我們為您續約註冊之後，您決定不需要該網域名稱，您無法取得續約成本的退款。

選擇下一步。

6. 在 [連絡人資訊] 頁面上，輸入網域註冊人、管理員、技術人員和帳單聯絡人的聯絡資訊。您在此處輸入的值將套用至要註冊的所有網域。如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

   請注意下列注意事項：

   姓名

   針對 First Name (名字) 和 Last Name (姓氏)，建議您指定官方 ID 上的姓名。對於網域設定的某些變更，有些網域註冊機構要求您提供身分證明。您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。

   不同的聯絡人

   在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果您想要為一個或多個聯絡人輸入不同資訊，請將與註冊聯絡人相同切換開關的值變更至關閉位置。

   > **Note**
   >
   > 對於 .it 網域，註冊人和管理聯絡人必須相同。

   > **Note**
   >
   > 對於 .jp 網域，技術與管理連絡人必須相同。

   多個網域

   如果您註冊多個網域，所有網域都會使用相同的聯絡資訊。

其他必要資訊

對於某些頂層網域 (TLD)，我們需要收集更多資訊。對於這些 TLD，請在 Postal/Zip Code (郵遞區號) 欄位後輸入適用的值。

隱私權保護

選擇是否要向 WHOIS 查詢隱藏您的聯絡資訊。

> **Note**
>
> 您必須為管理員、註冊人、技術人員和帳單聯絡人指定相同的隱私權設定。

如需詳細資訊，請參閱下列主題：

- 為網域的聯絡資訊啟用或停用隱私權保護
- 可向 Amazon Route 53 註冊的網域

> **Note**
>
> 若要針對 .uk、.co.uk、.me.uk 和 .org.uk 網域啟用隱私權保護，您必須開立一個支援案例並請求隱私權保護。

選擇下一步。

7. 在檢閱頁面上，檢閱您輸入的資訊，選擇性地加以更正，閱讀服務條款，並選取確認您已閱讀服務條款的核取方塊。

   選擇提交。

8. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要向 Route 53 註冊網域，請執行下列步驟以支付註冊網域的費用。

   a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。

   b. 在 Payments Due (付款到期) 區段中，找到適用的發票。

   c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

   在您的發票付款後，我們會完成網域註冊並發送適用的電子郵件。

> **Important**
>
> 如果您在五天內未支付發票，則會取消發票。若要在取消商業發票後註冊網域，請重新提交請求。

如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

9. 在導覽窗格中，依次選擇網域和請求。

   在此頁面上，您可以檢視網域的狀態，以及確認您是否需要回應註冊聯絡人驗證電子郵件。您也可以選擇重新傳送驗證電子郵件。

   如果您為註冊聯絡人指定了從未用來向 Route 53 註冊網域的電子郵件地址，某些 TLD 註冊機構會要求您驗證該地址是否有效。

   我們會從下列其中一個電子郵件地址傳送驗證電子郵件：

   - noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD。
   - noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD。若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

   > **Important**
   >
   > 註冊聯絡人必須按照電子郵件中的指示來驗證已收到電子郵件，否則我們必須按照 ICANN 的要求暫停該網域。當網域已暫停，無法在網際網路上存取該網域。

   a. 當您收到驗證電子郵件，選擇電子郵件中用於確認電子郵件地址是否有效的連結。如果您沒有立即收到電子郵件，請檢查您的垃圾電子郵件資料夾。

   b. 返回請求頁面。如果狀態未自動更新指出電子郵件地址已驗證，請重新整理瀏覽器。

10. 當網域註冊完成，下一步取決於您要使用 Route 53 還是其他 DNS 服務做為網域的 DNS 服務：

    - Route 53 – 在您註冊網域時 Route 53 建立的託管區域中，建立記錄以告知 Route 53 您希望如何為網域和子網域路由流量。

例如，當有人在瀏覽器中輸入您的網域名稱，且該查詢被轉送到 Route 53 時，您希望 Route 53 用您資料中心 Web 伺服器的 IP 地址回應查詢，還是用 ELB 負載平衡器的名稱回應查詢？

如需詳細資訊，請參閱 處理記錄。

> **Important**
>
> 如果您在 Route 53 自動建立的託管區域之外的託管區域中建立記錄，則必須更新網域的名稱伺服器，以將這些名稱伺服器用於新的託管區域。

- 其他 DNS 服務 – 設定您的新網域，將 DNS 查詢路由到其他 DNS 服務。請執行更新名稱伺服器以使用其他註冊商程序。

Old console

若要使用 Route 53 註冊網域

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 若您是初次使用 Route 53，請選擇 Get Started (開始使用)。

   如果您已經在使用 Route 53，請在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 選擇 Register Domain (註冊網域)，並指定您想註冊的網域：

   a. 輸入要註冊的網域名稱，然後選擇 Check (檢查)，了解該網域名稱是否可用。

      如果您想要註冊的網域名稱包含非 a-z、A-Z、0-9 和 – (連字號) 的字元，請注意下列事項：

      - 您可以使用適用的字元來輸入名稱。您不需要將名稱轉換為 Punycode。
      - 隨即顯示語言清單。選擇指定名稱的語言。例如，如果您輸入 příklad (捷克文的「範例」)，請選擇捷克文 (CES) 或捷克文 (CZE)。

> **Note**
>
> 對於具有多個程式碼的語言，您可能需要嘗試兩種程式碼。即使 CES 和 CZE 是同義詞，某些 TLD 註冊機構只支援其中一個。

b. 如果網域可用，請選擇 Add to cart (加入購物車)。網域名稱會出現在您的購物車中。

   Related domain suggestions (相關網域建議) 清單顯示您可能希望註冊的其他網域，以在您的首選域不可用時取代首選域，或者在首選域之外註冊其他網域。對於您希望註冊的每個額外網域，選擇 Add to cart (加入購物車)，最多可選擇五個網域。

   選擇下一步。

c. 在購物車，選擇網域要註冊的年數。

d. 若要註冊多個網域，請重複步驟 3a 到 3c。

4. 選擇 繼續。

5. 在 [n 網域的聯絡詳細資料] 頁面上，輸入網域註冊人、管理員、技術和帳單聯絡人的聯絡資訊。您在此處輸入的值將套用至要註冊的所有網域。如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

   請注意下列注意事項：

   姓名

   針對 First Name (名字) 和 Last Name (姓氏)，建議您指定官方 ID 上的姓名。對於網域設定的某些變更，有些網域註冊機構要求您提供身分證明。您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。

   不同的聯絡人

   在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果要輸入一或多個聯絡人的不同資訊，請將 My Registrant, Administrative, and Technical Contacts are all the same (我的網域註冊者、管理員和技術聯絡人是同一人) 的值變更為 No (否)。

   > **Note**
   >
   > 對於 .it 網域，註冊人和管理聯絡人必須相同。

> **Note**
>
> 對於 .jp 網域，技術與管理連絡人必須相同。

多個網域

如果您註冊多個網域，所有網域都會使用相同的聯絡資訊。

其他必要資訊

對於某些頂層網域 (TLD)，我們需要收集更多資訊。對於這些 TLD，請在 Postal/Zip Code (郵遞區號) 欄位後輸入適用的值。

隱私權保護

選擇是否要向 WHOIS 查詢隱藏您的聯絡資訊。

> **Note**
>
> 您必須為管理員、註冊人、技術人員和帳單聯絡人指定相同的隱私權設定。

如需詳細資訊，請參閱下列主題：

- 為網域的聯絡資訊啟用或停用隱私權保護
- 可向 Amazon Route 53 註冊的網域

> **Note**
>
> 若要針對 .uk、.co.uk、.me.uk 和 .org.uk 網域啟用隱私權保護，您必須開立一個支援案例並請求隱私權保護。

6. 選擇 繼續。
7. 僅限部分 TLD – 如果您為註冊人聯絡人指定了從未用來向 Route 53 註冊網域的電子郵件地址，某些 TLD 註冊會要求您驗證該地址是否有效。

   如果註冊機構要求驗證，而且您可以在網域註冊程序中驗證地址，主控台會顯示驗證註冊聯絡人的電子郵件地址區段：

- 如果此區段未顯示，請跳到步驟 8。
- 如果此區段顯示而且狀態為 email-address is verified (電子郵件地址已驗證)，請跳到步驟 8。
- 如果此區段顯示而且值為 Registrant email not verified (註冊人電子郵件未驗證)，請繼續進行此步驟。

執行以下步驟：

a. 選擇 Send verification email (傳送驗證電子郵件)。我們會從下列其中一個電子郵件地址傳送驗證電子郵件：

   - noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD。
   - noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD。若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

   > **Important**
   >
   > 註冊聯絡人必須按照電子郵件中的指示來驗證已收到電子郵件，否則我們必須按照 ICANN 的要求暫停該網域。當網域已暫停，無法在網際網路上存取該網域。

b. 當您收到驗證電子郵件，選擇電子郵件中用於確認電子郵件地址是否有效的連結。如果您沒有立即收到電子郵件，請檢查您的垃圾電子郵件資料夾。

c. 返回 Route 53 主控台。如果狀態未自動更新指出 email-address is verified (電子郵件地址已驗證)，請選擇 Refresh status (重新整理狀態)。

8. 選擇您是否希望我們在到期之前自動續約您的網域註冊。

   > **Note**
   >
   > 網域名稱註冊和續約不接受退款。如果您啟用自動網域續約，而且在我們為您續約註冊之後，您決定不需要該網域名稱，您無法取得續約成本的退款。

9. 檢閱您輸入的資訊，閱讀服務條款，並選取確認您已閱讀服務條款的核取方塊。
10. 選擇 Complete Purchase (完成購買)。

11. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要向 Route 53 註冊網域，請執行下列步驟以支付註冊網域的費用。

    a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。

    b. 在 Payments Due (付款到期) 區段中，找到適用的發票。

    c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

    在您的發票付款後，我們會完成網域註冊並發送適用的電子郵件。

    > **Important**
    >
    > 如果您在五天內未支付發票，則會取消發票。若要在取消商業發票後註冊網域，請重新提交請求。

    如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

12. 僅限一般 TLD – 驗證註冊聯絡人電子郵件地址是有效的。

    > **Note**
    >
    > 如已在步驟 7 驗證了電子郵件地址，請跳到步驟 13。

    如果註冊機構要求我們驗證註冊聯絡人的電子郵件地址，但不允許我們在此程序的早期進行驗證，那麼我們會從下列其中一個電子郵件地址傳送驗證電子郵件：

    - noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD。
    - noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD。

    若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

    當您收到驗證電子郵件，選擇電子郵件中用於確認電子郵件地址是否有效的連結。如果您沒有立即收到該電子郵件：

    - 檢查網域的設定以確認為註冊聯絡人指定正確的電子郵件地址。
    - 檢查您的垃圾電子郵件資料夾。

> **Important**
>
> 註冊聯絡人必須按照電子郵件中的指示來確認已收到電子郵件，否則我們必須按照 ICANN 的要求暫停該網域。當網域已暫停，無法在網際網路上存取該網域。

13. 對於所有 TLD，當您的網域註冊獲得核准，您會收到一封電子郵件。

    若要確定請求的最新狀態，請參閱 檢視網域註冊的狀態。

14. (選用) 所有一般 TLD 和許多地理 TLD 的網域註冊商都允許您鎖定網域，以防止有人在未經您許可的情況下將網域轉移到其他註冊商。若要判斷您網域的註冊商是否能讓您鎖定網域，請參閱 可向 Amazon Route 53 註冊的網域。如果註冊商支援鎖定，而且您希望鎖定您的網域，請參閱 鎖定網域以防止未經授權轉移到另一個註冊商。

15. 當網域註冊完成，下一步取決於您要使用 Route 53 還是其他 DNS 服務做為網域的 DNS 服務：

    - Route 53 – 在您註冊網域時 Route 53 建立的託管區域中，建立記錄以告知 Route 53 您希望如何為網域和子網域路由流量。

      例如，當有人在瀏覽器中輸入您的網域名稱，且該查詢被轉送到 Route 53 時，您希望 Route 53 用您資料中心 Web 伺服器的 IP 地址回應查詢，還是用 Elastic Load Balancing 負載平衡器的名稱回應查詢？

      如需詳細資訊，請參閱 處理記錄。

      > **Important**
      >
      > 如果您在 Route 53 自動建立的託管區域之外的託管區域中建立記錄，則必須更新網域的名稱伺服器，以將這些名稱伺服器用於新的託管區域。

    - 其他 DNS 服務 – 設定您的新網域，將 DNS 查詢路由到其他 DNS 服務。請執行更新名稱伺服器以使用其他註冊商程序。

註冊或轉移網域時所指定的值

> **Note**
>
> 我們已經更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台，也可以使用新的主控台。Route 53 傳回的大部分資訊在兩個主控台上皆相同。以下清單中註明了差異。

當您註冊網域或將網域註冊轉移到 Amazon Route 53 時，需指定本主題中描述的值。

> **Note**
>
> 如果您註冊多個網域，Route 53 會使用您為購物車中的所有網域指定的值。

也可以變更目前已向 Route 53 註冊的網域的值。注意下列事項：

- 如果您變更網域的聯絡資訊，我們會向註冊聯絡人傳送有關此變更的電子郵件通知。這封電子郵件來自 route53-dev-admin@amazon.com。對於大多數變更，註冊聯絡人不需要回應。
- 如果聯絡資訊變更還構成所有權變更，我們會向註冊聯絡人另外傳送一封電子郵件。ICANN 要求註冊聯絡人確認已收到電子郵件。如需詳細資訊，請參閱本節後面的 First Name, Last Name (姓名) 和 Organization (組織)。

如需變更現有網域的設定的詳細資訊，請參閱更新網域設定 。

您指定的值

- My Registrant, Administrative, and Technical contacts are all the same
- Contact Type
- First Name, Last Name
- Organization
- Email
- Phone
- Address 1
- Address 2

- Country
- State
- City
- Postal/Zip Code
- Fields for selected top-level domains
- Privacy Protection
- Auto-renew

新主控台：與註冊聯絡人相同 - 舊主控台：我的註冊者、管理員和技術聯絡人都相同

指定是否要對網域註冊者、管理聯絡人和技術聯絡人使用相同的聯絡資訊。

聯絡人類型

此聯絡人的類別。注意下列事項：

- 如果您選擇 Person (個人) 以外的選項，您必須輸入組織名稱。
- 對於某些 TLD，可用的隱私權保護取決於您為 Contact Type (聯絡人類型) 選擇的值。對於 TLD 隱私權保護設定的詳細資訊，請參閱可向 Amazon Route 53 註冊的網域。
- 對於 .es 網域，所有三個聯絡人的 Contact Type (聯絡類型) 必須是 Person (人員)。

名字、姓氏

聯絡人的姓氏和名字。

> **Important**
>
> 針對 First Name (名字) 和 Last Name (姓氏)，建議您指定官方 ID 上的姓名。若要對網域設定進行一些變更，您必須提供身分證明，而且您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。

如果您要將網域移轉到 Route 53 而下列項目為 true，您就要變更網域的擁有者：

- 聯絡人類型是 Person (個人)。
- 您要變更現有設定之註冊聯絡人的 First Name (名字) 及/或 Last Name (姓氏) 欄位。

在此情況下，ICANN 會要求我們向註冊聯絡人傳送電子郵件以獲得核准。我們會從下列其中一個電子郵件地址傳送電子郵件：

TLD	發出核准電子郵件的電子郵件地址
Amazon Registrar 註冊的 TLD	noreply@registrar.amazon.com
.fr	nic@nic.fr (電子郵件會同時傳送到目前的註冊聯絡人和新的註冊聯絡人。)
所有其他	noreply@domainnameverification.net

若要確定您的 TLD 註冊商是誰，請參閱 可向 Amazon Route 53 註冊的網域。

> **Important**
>
> 註冊聯絡人必須按照電子郵件中的指示來確認已收到電子郵件，否則我們必須按照 ICANN 的要求暫停該網域。當網域已暫停，無法在網際網路上存取該網域。

如果您變更註冊聯絡人的電子郵件地址，我們會同時向註冊聯絡人的新舊電子郵件地址傳送此電子郵件。

有些 TLD 註冊商會對變更網域擁有者收取費用。當您變更其中一個值，Route 53 主控台會顯示訊息，告訴您是否會有費用。

組織

與聯絡人相關聯的組織 (如果有)。對於申請人和管理聯絡人，此組織通常為註冊網域的組織。對於技術連絡人，這可能是管理網域的組織。

當聯絡人類型是 Person (個人) 以外的任何值，而且您變更註冊聯絡人的 Organization (組織) 欄位時，您會變更網域的擁有者。ICANN 要求我們向註冊聯絡人傳送電子郵件以獲得核准。我們會從下列其中一個電子郵件地址傳送電子郵件：

TLD	發出核准電子郵件的電子郵件地址
Amazon Registrar 註冊的 TLD	noreply@registrar.amazon.com

TLD	發出核准電子郵件的電子郵件地址
.fr	nic@nic.fr (電子郵件會同時傳送到目前的註冊聯絡人和新的註冊聯絡人。)
所有其他	noreply@domainnameverification.net

若要確定您的 TLD 註冊商是誰，請參閱可向 Amazon Route 53 註冊的網域。

如果您變更註冊聯絡人的電子郵件地址，我們會同時向註冊聯絡人的新舊電子郵件地址傳送此電子郵件。

有些 TLD 註冊商會對變更網域擁有者收取費用。當您變更 Organization (組織) 的值時，Route 53 主控台會顯示訊息，告訴您是否會產生費用。

電子郵件

聯絡人的電子郵件地址。

如果您變更註冊聯絡人的電子郵件地址，我們會同時向新舊電子郵件地址傳送通知電子郵件。這封電子郵件來自 route53-dev-admin@amazon.com。

電話

聯絡人的電話號碼：

- 如果您輸入美國或加拿大境內位置的電話號碼，請在第一個欄位中輸入 1，並在第二個欄位中輸入 10 位數的區碼和電話號碼。
- 如果要輸入其他任何位置的電話號碼，請在第一個欄位中輸入國家代碼，然後在第二個欄位中輸入電話號碼的其餘部分。如需電話國家/地區代碼的清單，請參閱 Wikipedia 文章國際電話區號清單。

地址 1

聯絡人的街道地址。

地址 2

聯絡人的其他地址資訊，例如，公寓號碼或郵寄地址。

國家

聯絡人的國家/地區。

州

聯絡人的州或省 (如果有)。

城市

聯絡人的城市。

Postal/Zip code

聯絡人的郵遞區號。

選取的頂層網域的欄位

下列頂層網域 (TLD) 要求您指定其他值：

- .com.au 和 .net.au
- .ca
- .es
- .fi
- .fr
- .it
- .ru
- .se
- .sg
- .co.uk、.me.uk、.org.uk 和 uk

此外，許多 TLD 需要增值稅識別碼。

如需有效值的相關資訊，請參閱 Amazon 路線 53 API 參考ExtraParam中的。

隱私權保護

是否要向 WHOIS 查詢隱藏您的聯絡資訊。如果您選擇開啟隱私權保護 (新主控台) 或隱藏聯絡資訊 (舊主控台)，WHOIS (「誰是」) 查詢會傳回註冊商的聯絡資訊或「受政策保護」的值。

> **Note**
>
> 您必須為管理員、註冊人、技術人員和帳單聯絡人指定相同的隱私權設定。

如果您選取 Don't hide contact information (不要隱藏聯絡資訊)，您將在指定的電子郵件地址收到更多垃圾電子郵件。

任何人都可以傳送針對某個網域的 WHOIS 查詢，並取得該網域的所有聯絡資訊。WHOIS 命令在許多作業系統中都可用，在許多網站上也會以 Web 應用程式的形式提供。

> **Important**
>
> 雖然有合法使用者希望取得與您的網域關聯的聯絡資訊，但最常見的使用者是垃圾郵件傳送者，他們的目標是向網域聯絡人傳送不需要的電子郵件和偽造優惠。一般而言，建議您為 Privacy Protection (隱私權保護) 選擇 Hide contact information (隱藏聯絡資訊)。

若要針對某些網域啟用或停用隱私權保護，您必須建立支援案例並請求隱私權保護。

如需隱私權保護的詳細資訊，請參閱下列主題：

- 為網域的聯絡資訊啟用或停用隱私權保護
- 可向 Amazon Route 53 註冊的網域

自動續約 (僅在編輯網域設定時可用)

您是否希望 Route 53 在網域到期之前自動續約網域。註冊費將從您的 AWS 帳戶中收取。在舊主控台上，只有在編輯網域設定時，才能使用此設定。如需詳細資訊，請參閱 續約網域的註冊。

> **Important**
>
> 如果您停用自動續約，則過期日期過後將不續約網域註冊，您可能失去對網域名稱的控制。

您可以續約網域名稱的期間因頂層網域 (TLD) 而異。如需續約網域的概觀，請參閱續約網域的註冊。如需有關將網域註冊延長指定年數的資訊，請參閱延長網域的註冊期間。

Amazon Route 53 在您註冊網域時傳回的值

當您向 Amazon Route 53 註冊網域，Route 53 還會傳回以下值。

註冊於

最初向 Route 53 註冊網域的日期。

到期日為

目前註冊期間到期的日期和時間，採用格林威治標準時間 (GMT)。

註冊期間通常為一年，但某些頂層網域 (TLD) 的註冊商提供更長的註冊期間。如需 TLD 註冊和續約期間，請參閱可向 Amazon Route 53 註冊的網域。

對於大多數 TLD，您最多可將註冊期間延長十年。如需詳細資訊，請參閱 延長網域的註冊期間。

網域名稱狀態碼

網域目前的狀態。

ICANN 是維護網域名稱的中央資料庫的組織，它開發了一組網域名稱狀態碼 (也稱為 EPP 狀態碼)，這些狀態碼可以告訴您針對網域名稱的各種操作的狀態。例如，註冊網域名稱、將網域名稱轉移到其他註冊商、續約網域名稱註冊等等。所有註冊商都使用這組相同的狀態碼。

如需網域名稱狀態碼的目前清單和每個狀態碼意義的說明，請前往 ICANN 網站並搜尋 epp status codes。(在 ICANN 網站上搜尋；Web 搜尋有時會傳回舊版文件。)

轉移鎖定

是否鎖定網域以降低有人未經您許可而將您的網域轉移至其他註冊商的可能性。如果網域已鎖定，轉移鎖定的值為開啟。如果網域未鎖定，值為關閉。

自動續約

Route 53 是否在過期日期前自動續約此網域的註冊。

授權碼

將此網域的註冊轉移到其他註冊商時需要的代碼。授權代碼只根據請求產生。如需將網域轉移到其他註冊商的詳細資訊，請參閱將網域從 Amazon Route 53 轉移到其他註冊商。

名稱伺服器

回應此網域的 DNS 查詢的 Route 53 伺服器。我們建議您不要刪除 Route 53 名稱伺服器。

如需新增、變更或刪除名稱伺服器的詳細資訊，請參閱新增或變更網域的名稱伺服器和黏附記錄。

檢視網域註冊的狀態

ICANN 是維護網域名稱的中央資料庫的組織，它開發了一組網域名稱狀態碼 (也稱為 EPP 狀態碼)，這些狀態碼可指明各種操作 (例如，註冊網域名稱、將網域名稱轉移到其他註冊商、續約網域名稱註冊等) 的狀態。所有註冊商都使用這組相同的狀態碼。

若要檢視您的網域的狀態碼，請執行下列程序。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

檢視網域的 ICANN 狀態碼

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，展開網域，然後選擇已註冊的網域。
3. 請選取網域的連結名稱。
4. 如果您需要採取動作，例如將驗證電子郵件重新傳送給註冊聯絡人，頁面頂端的橫幅會指出您需要採取的動作。
5. 如需網域目前的狀態，請參閱網域狀態碼欄位的值。

   如需網域名稱狀態碼的目前清單和每個狀態碼意義的說明，請前往 ICANN 網站並搜尋 epp status codes。(在 ICANN 網站上搜尋；Web 搜尋有時會傳回舊版文件。)

您也可以在請求頁面上檢視註冊狀態。

檢視註冊狀態

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，展開網域，然後選擇請求。
3. 在請求頁面上，您可以檢視註冊狀態以及任何其他動作的狀態，例如刪除網域、鎖定網域轉移、新增或刪除 DNSSEC 金鑰、您已對網域進行的操作，

   此外還會列出您可能必須採取的用來完成程序 (例如驗證電子郵件) 的任何動作。

- 若要回應動作請求，請選取網域名稱旁邊的選項按鈕，然後從動作下拉式選單中選取動作。

Old console

檢視網域的 ICANN 狀態碼

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 請選取網域的連結名稱。
4. 如需網域目前的狀態，請參閱 Domain name status (網域名稱狀態) 欄位的值。

   如需網域名稱狀態碼的目前清單和每個狀態碼意義的說明，請前往 ICANN 網站並搜尋 epp status codes。(在 ICANN 網站上搜尋；Web 搜尋有時會傳回舊版文件。)

更新網域設定

如需有關更新網域設定的詳細資訊，請參閱適用的主題。

主題

- 更新網域的聯絡資訊和所有權
- 為網域的聯絡資訊啟用或停用隱私權保護
- 啟用或停用網域自動續約
- 鎖定網域以防止未經授權轉移到另一個註冊商
- 延長網域的註冊期間
- 更新名稱伺服器以使用其他註冊商
- 新增或變更網域的名稱伺服器和黏附記錄

更新網域的聯絡資訊和所有權

對於網域的管理員和技術聯絡人，您可以變更所有聯絡資訊，而無需授權變更。如需詳細資訊，請參閱更新網域的聯絡人資訊。

用於註冊聯絡人時，您可以變更大多數值，而無需授權變更。但用於某些 TLD 時，變更網域擁有者就需要授權。如需詳細資訊，請參閱適用的主題。

主題

- 網域擁有者是誰？
- 需要特殊處理才能變更擁有者的 TLD
- 更新網域的聯絡人資訊
- 當註冊機構要求網域所有權變更表單時變更網域擁有者

網域擁有者是誰？

當聯絡人類型是 Person (個人)，而您變更註冊聯絡人的 First Name (名字) 或 Last Name (姓氏) 欄位時，您會變更網域的擁有者。

當聯絡人類型是 Person (個人) 以外的任何值，而您變更 Organization (組織) 時，您會變更網域的擁有者。

變更網域擁有者時，請注意以下各項：

- 對於某些 TLD，變更網域擁有者需要付費。若要判斷您的網域的 TLD 是否要付費，請參閱 Amazon Route 53 網域註冊的定價中的「變更擁有權價格」欄。

  > **Note**
  >
  > 您無法使用 AWS 點數支付費用 (如果有的話) 來變更網域的擁有者。

- 對於某些 TLD，當您變更網域擁有者，我們會傳送授權電子郵件到註冊聯絡人的電子郵件地址。註冊聯絡人必須依照電子郵件中的指示授權變更。
- 對於某些 TLD，您需要填寫「網域所有權變更表單」，並提供身分證明，以便 Amazon Route 53 支援工程師可以為您更新值。如果網域的 TLD 要求「網域所有權變更表單」，主控台會顯示連結至表單的訊息，以開啟支援案例。如需詳細資訊，請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

需要特殊處理才能變更擁有者的 TLD

當您變更網域的擁有者時，有些 TLD 的註冊會需要特殊處理。如果您要變更下列任一網域的擁有者，請執行適用的程序。如果您要變更任何其他網域的擁有者，您可以透過程式或使用 Route 53 主控台自行變更擁有者。請參閱 更新網域的聯絡人資訊。

下列 TLD 需要特殊處理才能變更網域擁有者：

.be, .cl, .com.br, .es, .fi, .ru, .se, .sh

.be

您必須從 .be 網域的登錄取得轉移代碼，然後向 Sup AWS port 人員開啟案例。

- 要獲取轉移代碼，請參閱 https://www.dnsbelgium.be/en/ manage-your-domain-name /變更持有者 #transfer，然後按照提示進行操作。
- 若要開啟案例，請參閱 就網域註冊問題聯絡 S AWS upport。

.cl

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

.com.ar

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

.com.br

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

.es

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

.fi

在 Route 53 主控台啟動所有者更改。啟動變更後，您將收到來自 fi-domain-tech@traficom .fi 電子郵件地址的持有人轉移金鑰。收到金鑰後，請向支援人員開啟 Support AWS 援案例，並與我們分享金鑰代碼。請參閱 就網域註冊問題聯絡 S AWS upport。

.qa

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

.ru

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

.se

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

.sh

您必須填寫並提交表單給 Sup AWS port 部門。請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者。

更新網域的聯絡人資訊

若要更新網域的聯絡資訊，請執行以下程序。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

更新網域的聯絡資訊

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。

3. 選擇要為其更新聯絡資訊之網域的名稱。
4. 在聯絡資訊索引標籤中，選擇編輯。
5. 如果您變更註冊申請人的聯絡人電子郵件地址，請執行以下步驟。如果您未變更註冊申請人的聯絡人電子郵件地址，請跳到步驟 6。

   a. 僅變更註冊申請人的聯絡人電子郵件地址。不變更該網域的任何聯絡人的任何其他值。如果您還要變更其他值，請稍後在此程序中變更。

      選擇儲存變更。

      為了驗證新的電子郵件地址，我們將向新地址傳送驗證電子郵件 (如 TLD 需要)。您必須選擇電子郵件中的連結，以確認新的電子郵件地址是否有效。如果需要進行驗證，但您未驗證新的電子郵件地址，Route 53 會根據 ICANN 的要求暫停網域。

      如果您需要重新傳送驗證電子郵件，請導覽至已註冊的網域頁面，選擇您更新的網域名稱旁邊的選項按鈕，然後選擇您正在更新的網域名稱。在驗證您的電子郵件以避免網域暫停提醒上，選擇再次傳送電子郵件。

   b. 如果您想要變更網域的註冊人、管理員、技術人員或帳單聯絡人的其他值，請返回步驟 1 並重複上述程序。
6. 更新適用的值。您也可以選擇複製註冊聯絡人，以自動填入您為註冊聯絡人輸入的相同資訊。如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

   根據網域的 TLD 以及要變更的值，主控台可能會顯示以下訊息：

   "To change the registrant name or organization, open a case." (若要變更申請者名稱或組織，請開啟案例。)

   如果您看到該訊息，請跳過此程序的其餘部分，並請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者 以取得更多資訊。
7. 選擇儲存。
8. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要在 TLD 註冊商收取變更擁有者的費用時變更網域擁有者，請執行以下步驟支付延伸的費用。

   a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。

   b. 在 Payments Due (付款到期) 區段中，找到適用的發票。

   c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

在您付款發票後，我們會變更註冊聯絡人的適用設定。

> **Important**
>
> 如果您在五天內未支付發票，則會取消發票。若要在取消發票後變更註冊的聯絡人的設定，請重新提交申請。

如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

9. 當您已依照 網域擁有者是誰？ 所述變更網域擁有者後，我們就會向網域的註冊聯絡人傳送一封電子郵件。這封電子郵件會要求變更擁有者的授權。

   如果我們未在 3 到 15 天內收到變更授權 (取決於頂層網域)，我們必須根據 ICANN 要求取消變更請求。

   電子郵件來自下列其中一個電子郵件地址。

TLD	發出授權電子郵件的電子郵件地址
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
所有其他	下列其中一個電子郵件地址： • noreply@registrar.amazon.com • noreply@domainnameverification.net

10. 如果您在更新聯絡資訊時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Old console

更新網域的聯絡資訊

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要為其更新聯絡資訊之網域的名稱。
4. 選擇 Edit Contacts (編輯聯絡人)。
5. 如果您變更註冊申請人的聯絡人電子郵件地址，請執行以下步驟。如果您未變更註冊申請人的聯絡人電子郵件地址，請跳到步驟 6。

   a. 僅變更註冊申請人的聯絡人電子郵件地址。不變更該網域的任何聯絡人的任何其他值。如果您還要變更其他值，請稍後在此程序中變更。

      選擇儲存。

      為了驗證新的電子郵件地址是否可寄達，我們將向新地址發送驗證電子郵件 (如 TLD 需要)。您必須選擇電子郵件中的連結，以確認新的電子郵件地址是否有效。如果需要進行驗證，但您未驗證新的電子郵件地址，Route 53 會根據 ICANN 的要求暫停網域。

   b. 如果您想要變更網域註冊人、系統管理或技術連絡人的其他值，請回到步驟 1 並重複此程序。
6. 更新適用的值。如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

   根據網域的 TLD 以及要變更的值，主控台可能會顯示以下訊息：

   "To change the registrant name or organization, open a case." (若要變更申請者名稱或組織，請開啟案例。)

   如果您看到該訊息，請跳過此程序的其餘部分，並請參閱 當註冊機構要求網域所有權變更表單時變更網域擁有者 以取得更多資訊。
7. 選擇儲存。
8. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要在 TLD 註冊商收取變更擁有者的費用時變更網域擁有者，請執行以下步驟支付延伸的費用。

   a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。

   b. 在 Payments Due (付款到期) 區段中，找到適用的發票。

c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

在您付款發票後，我們會變更註冊聯絡人的適用設定。

> **Important**
>
> 如果您在五天內未支付發票，則會取消發票。若要在取消發票後變更註冊的聯絡人的設定，請重新提交申請。

如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

9. 當您已依照 網域擁有者是誰？ 所述變更網域擁有者後，我們就會向網域的註冊聯絡人傳送一封電子郵件。這封電子郵件會要求變更擁有者的授權。

如果我們未在 3 到 15 天內收到變更授權 (取決於頂層網域)，我們必須根據 ICANN 要求取消變更請求。

電子郵件來自下列其中一個電子郵件地址。

TLD	發出授權電子郵件的電子郵件地址
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
所有其他	下列其中一個電子郵件地址： • noreply@registrar.amazon.com • noreply@domainnameverification.net

10. 如果您在更新聯絡資訊時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

如需可用來更新連絡人資訊之 API 的相關資訊，請參閱UpdateDomainContact。

當註冊機構要求網域所有權變更表單時變更網域擁有者

如果您的網域註冊局要求您完成變更網域擁有權，並將表單提交給 Sup AWS port 部門，請執行下列程序。若要判斷是否需要執行此程序，請參閱下列主題：

- 若要判斷您變更的值是否算是變更擁有者，請參閱 網域擁有者是誰？。
- 若要判斷您的網域是否需要「變更網域擁有者」表單，請參閱 需要特殊處理才能變更擁有者的 TLD。

在註冊機構要求網域所有權變更表單時變更網域擁有者

1. 請參閱此主題的簡介，以判斷您網域的登錄商是否需要特殊處理以變更網域的擁有者。如果是，而且需要變更網域擁有權表單，請繼續此程序。

   如果不需要變更網域擁有權表單，請執行適用的主題中的程序。
2. 下載網域所有權變更表單。檔案會壓縮成 .zip 檔案。
3. 填寫表單。
4. 針對網域前所有人及新擁有者的註冊聯絡人，取得身分證明的簽章影本 (身分證、駕照、護照或其他身分法律證明文件)。

   此外，如果法人實體列為註冊組織，請收集網域前所有人及新擁有者的下列資訊：

   - 證明網域的註冊組織存在。
   - 前所有人及新擁有者代表組織行使權力的授權證明。此文件必須是經過認證，包含組織名稱和官方代表姓名 (例如 CEO、總裁或執行總監) 的法律文件。
5. 掃描「網域所有權變更」表單和所需的證明。將掃描文件儲存為常見的格式，例如 .pdf 檔案或 .png 檔案。
6. 使用網域目前註冊的 AWS 帳戶登入 Sup AWS port 中心。

> **Important**
>
> 您必須使用根帳戶登入，或使用以下列一或多種方式授予 IAM 許可的使用者登入：

- 系統會為使用者指派受AdministratorAccess管理的策略。
- 系統會為使用者指派 AmazonRoute53 個DomainsFullAccess受管理的策略。
- 系統會為使用者指派 AmazonRoute53 個FullAccess受管理的策略。

如果您不使用根帳戶或具有所需許可的使用者登入，我們無法更新網域擁有者。此要求可防止未經授權的使用者變更網域的擁有者。

7. 指定下列值：

Regarding

接受預設值 Account and Billing Support (帳戶與帳單支援)。

服務

接受 Billing (帳單) 預設值。

類別

接受 Domain name registration issue (網域名稱註冊問題) 預設值。

主旨

指定 Change the owner of a domain (變更網域擁有者)。

描述

請提供下列資訊：

- 要變更其擁有者的網域。
- 註冊網域之AWS 帳戶的 12 位數帳號 ID

新增附件

上傳您在步驟 5 中掃描的文件。

聯絡方式

指定聯絡方式，並輸入適用的值。

8. 選擇提交。

Sup AWS port 工程師會檢閱您提供的資訊，並更新設定。工程師會在更新完成時與您聯絡，或者隨時聯絡您以了解更多資訊。

為網域的聯絡資訊啟用或停用隱私權保護

當您向 Amazon Route 53 註冊網域或將網域轉移到 Route 53 時，預設會針對網域的所有聯絡人啟用隱私權保護。這通常會在 WHOIS (即「誰是」) 查詢中隱藏大聯絡資訊，並減少收到的垃圾郵件數量。啟用隱私權保護時，您的聯絡人資訊會更換為註冊商的聯絡資訊，或是以「為保設隱私權而編輯」或「代表 <網域名稱> 擁有者」字樣取代。

如果您選擇停用隱私權保護，則必須針對網域的所有聯絡人停用此保護。如果您停用隱私權保護，任何人都可以對網域傳送 WHOIS 查詢，而且對於大多數頂層網域 (TLD) 而言，可以取得您在註冊或轉移網域時提供的所有聯絡資訊，包括姓名、地址、電話號碼和電子郵件地址。WHOIS 命令是廣泛可用；它包含在許多作業系統中，也在許多網站上以 Web 應用程式的形式提供。

如果您要將網域轉移到其他註冊商，且網域聯絡人已啟用隱私權保護，則驗證轉移的電子郵件將從已向 Amazon Registrar 註冊的 TLD 的 identity-protect.org 地址傳送。若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

WHOIS 查詢中隱藏的資訊，取決於兩個主要因素：

頂層網域的註冊機構

大部分 TLD 註冊機構會自動隱藏所有聯絡資訊，有些則允許選擇隱藏所有聯絡資訊，另外一些僅允許隱藏某些資訊，還有一些不允許隱藏任何資訊。

啟用網域的隱私權保護時，您的聯絡人資訊會更換為隱私權保護服務的聯絡人資訊，或是以「已隱藏以保護隱私」字樣取代。隱私權保護服務將套用垃圾郵件防護功能 (地址輪換和 SPF/DKIM/垃圾郵件分析)，並且在大多數情況下會自動轉發通過這些篩選條件的電子郵件。但是，建議不要將重要電子郵件傳送到受隱私權保護的電子郵件地址，因為垃圾郵件機制可能會阻止它們轉發。

此外，網域所使用的隱私權保護機制將無法設定，且將由系統會自動選取。我們的隱私權保護服務的聯繫方式將無法手動更新。

> **Note**
>
> 若要針對某些網域啟用或停用隱私權保護，您必須建立支援案例並請求隱私權保護。如需詳細資訊，請參閱 可向 Amazon Route 53 註冊的網域中的適用章節。
>
> - .co.uk (英國)
> - .me.uk (英國)
> - .org.uk (英國)
> - .link

註冊商

當您向 Route 53 註冊網域或將網域轉移至 Route 53 時，網域的註冊商是 Amazon Registrar 或我們的註冊商合作夥伴 Gandi。根據預設，Amazon Registrar 和 Gandi 隱藏不同的資訊：

- Amazon Registrar – 根據預設，隱藏所有聯絡資訊。不過，TLD 註冊機構的規定優先。
- Gandi – 根據預設，隱藏組織名稱以外的所有聯絡資訊 (如有)。不過，TLD 註冊機構的規定優先。

  針對不允許隱私保護的地理 TLD，Gandi 網站的 Whois 目錄搜尋頁面會將您的個人資訊標示為 "redacted" (受保護)。不過，網域註冊機構或第三方 WHOIS 網站可能會使用您的個人資訊。

若要了解網域的 TLD 隱藏哪些資訊，請參閱 可向 Amazon Route 53 註冊的網域。

當您想要為使用 Route 53 註冊的網域啟用或停用隱私權保護，請執行下列程序。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

啟用或停用網域聯絡資訊的隱私權保護

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 選擇要為其啟用或停用隱私權保護的網域名稱。
4. 在聯絡資訊區段中，選擇編輯。
5. 在隱私權保護區段中，選擇是否要隱藏聯絡資訊。您必須為所有四個聯絡人指定相同的隱私權設定：管理員、註冊人、技術人員和帳單。

> **Note**
>
> 如果您的 TLD 不支援隱私權保護，則不會顯示隱私權保護區段。

6. 選擇儲存變更。
7. 如果您在啟用或停用隱私權保護時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Old console

啟用或停用網域聯絡資訊的隱私權保護

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要為其啟用或停用隱私權保護的網域名稱。
4. 選擇 Edit Contacts (編輯聯絡人)。
5. 選擇是否要隱藏聯絡人資訊。您必須為全部三個聯絡人指定相同的隱私權設定：管理員、註冊者和技術聯絡人。
6. 選擇儲存。
7. 如果您在啟用或停用隱私權保護時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

啟用或停用網域自動續約

當您想要變更 Amazon Route 53 是否在網域註冊過期日期之前自動為網域續約註冊，或者想查看目前自動續約設定，請執行下列程序。

請注意，您無法使用 AWS 點數支付網域註冊續約費用。

> **Note**
>
> 如果您想要取消 AWS 帳戶，請務必關閉自動續訂功能。否則，您將繼續收到來自的續訂通知 AWS。但是，除非您重新啟用帳戶，否則您的網域不會續約。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

若要啟用或停用網域自動續約

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 選擇要更新的網域名稱。
4. 在詳細資訊區段的動作下拉式選單中，選擇開啟自動續約

   在為 <網域名稱> 開啟自動續約？中，同意支付年費，然後選擇開啟。

   > **Note**
   >
   > 列出的價格是當前註冊期間的價格，並且可以更改。如需詳細資訊，請參閱 Amazon Route 53 網域註冊的定價。
5. 若要關閉自動續約，請在動作下拉式選單中選取關閉自動續約。
6. 如果您在啟用或停用自動續約時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Old console

若要啟用或停用網域自動續約

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要更新的網域名稱。
4. 在詳細資訊區段的動作下拉式選單中，選擇開啟轉移鎖定。

   您可以導覽至請求頁面，以查看請求的進度。

   > **Note**
   >
   > 列出的價格是當前註冊期間的價格，並且可以更改。如需詳細資訊，請參閱 Amazon Route 53 網域註冊的定價。

5. 如果您在啟用或停用自動續約時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

鎖定網域以防止未經授權轉移到另一個註冊商

所有一般 TLD 和許多地理 TLD 的網域註冊商都允許您鎖定網域，以防止有人在未經您許可的情況下將網域轉移到其他註冊商。若要判斷您網域的註冊商是否能讓您鎖定網域，請參閱 可向 Amazon Route 53 註冊的網域。如果有支援鎖定，而且您希望鎖定網域，請執行下列程序。如果希望將網域轉移到另一個註冊商，也可以使用此程序來停用鎖定。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

若要鎖定網域以防止未經授權轉移到另一個註冊商

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要更新的網域名稱。
4. 在詳細資訊區段的動作下拉式選單中，選擇開啟轉移鎖定或關閉轉移鎖定，具體視您是要開啟還是關閉轉移鎖定而定。

   您可以導覽至請求頁面，以查看請求的進度。
5. 如果您在鎖定網域時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Old console

若要鎖定網域以防止未經授權轉移到另一個註冊商

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要更新的網域名稱。
4. 選擇 Enable (啟用) (鎖定網域) 或 Disable (停用) (解鎖網域)。
5. 選擇儲存。
6. 如果您在鎖定網域時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

在 WHOIS 搜索中，此狀態顯示為：`clientTransferProhibited`。另外，某些 TLD 可能還具有以下狀態：

- `clientUpdateProhibited`
- `clientDeleteProhibited`

延長網域的註冊期間

當您向 Amazon Route 53 註冊網域或將網域註冊轉移到 Route 53 時，我們會將網域設定為自動續約。自動續約期間通常為一年，但某些頂層網域 (TLD) 的註冊商提供更長的續約期間。

注意下列事項：

最長續約期間

所有一般 TLD 和許多國家/地區代碼 TLD 都允許將網域註冊延長為更長的期間，通常可長達 10 年 (以一年為增量)。若要判斷是否可以延長網域註冊期間，請參閱可向 Amazon Route 53 註冊的網域。如果允許更長的註冊期間，請執行以下程序。

您何時可續約或延長網域註冊的限制

有些 TLD 註冊機構對於何時可以續約或延長網域註冊有所限制，例如網域過期前兩個月。即使註冊機構允許延長網域的註冊期間，他們也可能不允許在網域過期之前的目前天數延期。

AWS 學分

您無法使用 AWS 點數支付延長網域註冊期限的費用。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

延長網域的註冊期間

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要為其延長註冊期間的網域名稱。
4. 在詳細資訊區段的動作下拉式選單中選擇續約網域註冊。
5. 在續約網域註冊對話方塊的續約期間下拉式選單中，選擇您要延長註冊的年數。

   此清單根據目前過期日期以及此網域的註冊機構允許的最長註冊期間，顯示所有目前的選項。套用該年數的到期日期會列在持續時間下方。
6. 選擇續約網域註冊。

當我們收到註冊機構已更新您的過期日期的確認通知，我們會傳送一封電子郵件給您，確認我們已變更過期日期。

7. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要延長網域的註冊，請執行下列步驟支付延伸費用。

   a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。

   b. 在 Payments Due (付款到期) 區段中，找到適用的發票。

   c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

   在您付款發票後，我們會完成延期並傳送適用的電子郵件。

   > **Important**
   >
   > 如果您在五天內未支付發票，則會取消發票。若要在取消發票後延長網域註冊，請重新提交要求。

   如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

8. 如果您在延長網域註冊期間時遇到問題，可以免費聯絡 Sup AWS port。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Old console

延長網域的註冊期間

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要為其延長註冊期間的網域名稱。

   在 Expires on (過期日期) 欄位會列出網域目前的過期日期。如果 TLD 的註冊機構允許延長註冊期間，過期日期右側會顯示 extend (延長) 連結。

4. 選擇 extend (延長)。
5. 在 Extend registration for (延長註冊期間) 清單中，請選擇您希望延長註冊的年數。

此清單根據目前過期日期以及此網域的註冊機構允許的最長註冊期間，顯示所有目前的選項。New expiration date (新過期日期) 欄位會顯示已套用該年數的過期日期。

6. 選擇 Extend domain registration (延長網域註冊)。

   當我們收到註冊機構已更新您的過期日期的確認通知，我們會傳送一封電子郵件給您，確認我們已變更過期日期。

7. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要延長網域的註冊，請執行下列步驟支付延伸費用。

   a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。
   b. 在 Payments Due (付款到期) 區段中，找到適用的發票。
   c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

      在您付款發票後，我們會完成延期並傳送適用的電子郵件。

   > **Important**
   >
   > 如果您在五天內未支付發票，則會取消發票。若要在取消發票後延長網域註冊，請重新提交要求。

   如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

8. 如果您在延長網域註冊期間時遇到問題，可以免費聯絡 Sup AWS port。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

更新名稱伺服器以使用其他註冊商

如果您想要將 DNS 管理移至其他註冊商，則需要更新名稱伺服器，以指向

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

若要在您要使用其他 DNS 服務時更新網域的名稱伺服器

1. 使用由 DNS 服務提供的程序，取得網域的名稱伺服器。
2. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
3. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
4. 選擇您要設定為使用其他 DNS 服務的網域的名稱。
5. 在詳細資訊區段的動作下拉式選單中，選擇編輯名稱伺服器。
6. 刪除現有的名稱伺服器，然後將名稱伺服器的名稱新增至您在步驟 1 中從 DNS 服務取得的名稱伺服器。
7. 選擇儲存變更。
8. (選用) 刪除 Route 53 在您註冊網域時自動建立的託管區域。這可以防止您因為未使用的託管區域被收取費用。

    a. 在導覽窗格中，選擇 Hosted Zones (託管區域)。

    b. 選擇與您的網域名稱同名的託管區域的選項按鈕。

    c. 選擇 Delete Hosted Zone (刪除託管區域)。

    d. 選擇 Confirm (確認)，確認要刪除託管區域。

Old console

若要在您要使用其他 DNS 服務時更新網域的名稱伺服器

1. 使用由 DNS 服務提供的程序，取得網域的名稱伺服器。
2. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
3. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
4. 選擇您要設定為使用其他 DNS 服務的網域的名稱。
5. 選擇 Add/Edit Name Servers (新增/編輯名稱伺服器)。

6. 將名稱伺服器的名稱變更為您在步驟 1 中從 DNS 服務取得的名稱伺服器。
7. 選擇更新。
8. (選用) 刪除 Route 53 在您註冊網域時自動建立的託管區域。這可以防止您因為未使用的託管區域被收取費用。

   a. 在導覽窗格中，選擇 Hosted Zones (託管區域)。
   b. 選擇與您的網域名稱同名的託管區域的選項按鈕。
   c. 選擇 Delete Hosted Zone (刪除託管區域)。
   d. 選擇 Confirm (確認)，確認要刪除託管區域。

新增或變更網域的名稱伺服器和黏附記錄

當您向 Route 53 註冊網域時，我們會自動建立網域的託管區域、為託管區域指派四個名稱伺服器，然後更新網域註冊以使用這些名稱伺服器。除非您想要使用其他 DNS 服務或您想要使用白標籤名稱伺服器，否則一般不需要變更這些設定。

Route 53 中每個網域的名稱伺服器數目上限為 6 個。

> **Warning**
>
> 如果您將名稱伺服器變更為錯誤的值，在黏附記錄中指定錯誤的 IP 地址，或者刪除一或多個名稱伺服器而未指定新的名稱伺服器，您的網站或應用程式可能在網際網路上變得無法使用，時間可長達兩天。

主題

- 變更名稱伺服器和黏附記錄的考量事項
- 新增或變更名稱伺服器或黏附記錄

變更名稱伺服器和黏附記錄的考量事項

在變更組態之前，請考慮以下問題。

主題

- You want to make Route 53 the DNS service for your domain
- You want to use another DNS service

- You want to use white-label name servers
- You're changing name servers for a .it domain

您希望將 Route 53 設定為網域的 DNS 服務

如果您目前正在使用其他 DNS 服務，而您希望將 Route 53 做為網域的 DNS 服務，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務，以取得如何將 DNS 服務遷移到 Route 53 的詳細說明。

> **Important**
>
> 如果您未嚴格遵守遷移程序，您的網域可能會無法在網際網路上使用，時間可長達兩天。

您希望使用其他 DNS 服務

如果您的網域想要使用 Route 53 以外的 DNS 服務，請使用下列程序將網域註冊的名稱伺服器變更為其他 DNS 服務提供的名稱伺服器。

> **Note**
>
> 如果您變更名稱伺服器而 Route 53 傳回以下錯誤訊息，則 TLD 註冊機構無法辨識您指定為有效的名稱伺服器：
> `"We're sorry to report that the operation failed after we forwarded your request to our registrar associate. This is because: One or more of the specified name servers are not known to the domain registry."`
> TLD 註冊機構普遍支援公有 DNS 服務提供的名稱伺服器，但不支援私有 DNS 伺服器，例如您在 Amazon EC2 執行個體上設定的 DNS 伺服器，除非註冊機構有這些名稱伺服器的 IP 地址。Route 53 不支援使用 TLD 註冊機構無法識別的名稱伺服器。如果發生此錯誤，您必須變更為 Route 53 的名稱伺服器或其他公有 DNS 服務。

您希望使用白標籤名稱伺服器

如果您希望名稱伺服器的名稱成為您網域名稱的子網域，您可以建立白標籤名稱伺服器。(白標籤名稱伺服器也稱為虛名伺服器或私有名稱伺服器。) 例如，您可以透過網域 example.com 的 ns4.example.com 建立名稱伺服器 ns1.example.com。若要使用白標籤名稱伺服器，請使用下列程序指定名稱伺服器的 IP 地址，而非名稱。這些 IP 地址稱為黏附記錄。

如需設定白標籤名稱伺服器的詳細資訊，請參閱設定白標籤名稱伺服器。

您要變更 .it 網域的名稱伺服器

如果變更 .it 網域的名稱伺服器，則 .it 網域的註冊機構會執行檢查，確認名稱伺服器有效。如果您指定錯誤的名稱伺服器且檢查失敗，註冊機構會持續檢查 22 天。在這段期間，您無法更新名稱伺服器的名稱以更正錯誤，因為 EPP 狀態碼為 `pendingUpdate`。註冊機構會繼續使用變更前的名稱伺服器回應 DNS 查詢。如果之前的名稱伺服器不再提供使用，您的網域就無法在網際網路上使用。

> **Important**
>
> 每當變更網域的名稱伺服器時，請先確認 DNS 會使用新的名稱伺服器回應查詢，再取消舊的 DNS 服務或刪除使用舊名稱伺服器的 Route 53 託管區域。

如需取得協助， AWS 以使用 ..it 網域的登錄更正您的名稱伺服器名稱的相關資訊，請參閱就網域註冊問題聯絡 S AWS upport。

新增或變更名稱伺服器或黏附記錄

若要新增或變更名稱伺服器或黏附記錄，請執行下列程序。

> **Note**
>
> 根據預設，DNS 解析器通常會快取伺服器的名稱兩天。因此，您的變更可能需要兩天的時間才會生效。如需詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

若要新增或變更網域的名稱伺服器或黏附記錄

1. 檢閱 變更名稱伺服器和黏附記錄的考量事項，並解決適用的問題 (如有)。
2. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
3. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
4. 選擇要為其編輯設定的網域名稱。
5. 在詳細資訊區段的動作下拉式選單中，選擇編輯名稱伺服器。
6. 在編輯名稱伺服器對話方塊中，您可以執行以下操作：

   - 執行以下作業之一，變更您網域的 DNS 服務：
     - 將其他 DNS 服務的名稱伺服器替換為 Route 53 託管區域的名稱伺服器
     - 將 Route 53 託管區域的名稱伺服器替換為其他 DNS 服務的名稱伺服器
     - 將一個 Route 53 託管區域的名稱伺服器替換為其他 Route 53 託管區域的名稱伺服器

     如需變更網域 DNS 服務的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。如需取得網域所用 DNS 服務之 Route 53 託管區域的名稱伺服器相關資訊，請參閱 取得公有託管區域的名稱伺服器。
   - 新增一或多個名稱伺服器。
   - 取代現有名稱伺服器的名稱。
   - 如果指定白標籤名稱伺服器，請在黏附記錄中新增或變更 IP 地址。您可以輸入 IPv4 或 IPv6 格式的地址。如果名稱伺服器有多個 IP 地址，請在不同的行中輸入每個地址。

     白標籤名稱伺服器的名稱 (例如 ns1.example.com) 中包含您的網域名稱 (例如 example.com)。當您指定白標籤名稱伺服器時，Route 53 會提示您為名稱伺服器指定一或多個 IP 地址。IP 地址又稱為黏附記錄。如需詳細資訊，請參閱 設定白標籤名稱伺服器。
   - 刪除名稱伺服器。選擇該名稱伺服器欄位右側的 x 圖示。

> **Warning**
>
> 如果您將名稱伺服器變更為錯誤的值，在黏附記錄中指定錯誤的 IP 地址，或者刪除一或多個名稱伺服器而未指定新的名稱伺服器，您的網站或應用程式可能在網際網路上變得無法使用，時間可長達兩天。

7. 選擇更新。
8. 如果您在新增或變更名稱伺服器或膠合記錄時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Old console

若要新增或變更網域的名稱伺服器或黏附記錄

1. 檢閱 變更名稱伺服器和黏附記錄的考量事項，並解決適用的問題 (如有)。
2. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
3. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
4. 選擇要為其編輯設定的網域名稱。
5. 選擇 Add/Edit Name Servers (新增/編輯名稱伺服器)。
6. 在 Edit Name Servers (編輯名稱伺服器) 對話方塊中，您可以執行以下操作：
   - 執行以下作業之一，變更您網域的 DNS 服務：
     - 將其他 DNS 服務的名稱伺服器替換為 Route 53 託管區域的名稱伺服器
     - 將 Route 53 託管區域的名稱伺服器替換為其他 DNS 服務的名稱伺服器
     - 將一個 Route 53 託管區域的名稱伺服器替換為其他 Route 53 託管區域的名稱伺服器

     如需變更網域 DNS 服務的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。如需取得網域所用 DNS 服務之 Route 53 託管區域的名稱伺服器相關資訊，請參閱 取得公有託管區域的名稱伺服器。
   - 新增一或多個名稱伺服器。
   - 取代現有名稱伺服器的名稱。
   - 如果指定白標籤名稱伺服器，請在黏附記錄中新增或變更 IP 地址。您可以輸入 IPv4 或 IPv6 格式的地址。如果名稱伺服器有多個 IP 地址，請在不同的行中輸入每個地址。

     白標籤名稱伺服器的名稱 (例如 ns1.example.com) 中包含您的網域名稱 (例如 example.com)。當您指定白標籤名稱伺服器時，Route 53 會提示您為名稱伺服器指定一或多個 IP 地址。IP 地址又稱為黏附記錄。如需詳細資訊，請參閱 設定白標籤名稱伺服器。
   - 刪除名稱伺服器。選擇該名稱伺服器欄位右側的 x 圖示。

> **Warning**
>
> 如果您將名稱伺服器變更為錯誤的值，在黏附記錄中指定錯誤的 IP 地址，或者刪除一或多個名稱伺服器而未指定新的名稱伺服器，您的網站或應用程式可能在網際網路上變得無法使用，時間可長達兩天。

7. 選擇更新。
8. 如果您在新增或變更名稱伺服器或膠合記錄時遇到問題，可以免費聯絡 Sup AWS port 部門。如需更多詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

續約網域的註冊

當您向 Amazon Route 53 註冊網域或將網域註冊轉移到 Route 53 時，我們會將網域設定為自動續約。自動續約期間通常為一年，但某些頂層網域 (TLD) 的註冊商提供更長的續約期間。如需 TLD 註冊和續約期間，請參閱可向 Amazon Route 53 註冊的網域。

> **Note**
>
> 您無法使用 AWS 點數支付網域註冊續約費用。

對於大多數頂層網域 (TLD)，您可以變更網域的過期日期。如需詳細資訊，請參閱 延長網域的註冊期間。

> **Important**
>
> 如果您關閉自動續約，請注意對網域的以下影響：
>
> - 如果您續約得不夠早，有些 TLD 註冊機構會在過期日期之前刪除網域。如果您要保留某個網域名稱，強烈建議您將自動續約保持啟用狀態。
> - 此外，我們還強烈建議您不要計劃在網域到期後重新註冊網域。有些註冊商在網域到期後立即允許其他人註冊這些網域，因此您可能無法在其他人取得網域之前重新註冊該網域。
> - 有些註冊機構會對還原已過期的網域收取高額費用。
> - 在過期日期當天或接近的日期，網域在網際網路上會變得無法使用。

若要判斷網域是否啟用自動續約的詳細資訊，請參閱啟用或停用網域自動續約。

如果自動續約已啟用，發生的情況如下：

過期前 45 天

我們會向註冊聯絡人傳送電子郵件，告知您目前已啟用自動續約功能並說明如何停用該功能。將註冊聯絡人的電子郵件地址保持最新，以免錯過此電子郵件。

過期前 35 或 30 天

對於除 .com.ar、.com.br 和 .jp 網域之外的所有網域，都在過期日期之前 35 天續約網域註冊，這樣在網域名稱到期之前，我們便有足夠的時間來解決與續約有關的任何問題。

.com.ar、.com.br 和 .jp 網域的註冊機構，要求在網域過期前 30 天內續約網域。您將在過期前 30 天收到來自註冊商合作夥伴 Gandi 的續約電子郵件 (如果已啟用自動續約，這是續約網域的同一天)。

> **Note**
>
> 當我們續約您的網域時，會向您傳送一封電子郵件，告知您我們已續約網域。如果續約失敗，我們會傳送一封電子郵件給您，說明失敗原因。

如果自動續約已停用，則在網域名稱的過期日期接近時，將出現以下情況：

過期前 45 天

我們會向網域的註冊聯絡人傳送電子郵件，告知您目前已停用自動續約功能並說明如何啟用該功能。將註冊聯絡人的電子郵件地址保持最新，以免錯過此電子郵件。

過期前 30 天和 7 天

如果網域自動續約已停用，網域註冊管理機構 ICANN 是會要求註冊商傳送一封電子郵件給您。電子郵件來自下列其中一個電子郵件地址：

- noreply@registrar.amazon.com – 適用於註冊商為 Amazon Registrar 的網域。
- noreply@domainnameverification.net – 適用於註冊商是註冊商合作夥伴 Gandi 的網域。

若要確定您的 TLD 註冊商是誰，請參閱 可向 Amazon Route 53 註冊的網域。

如果您在過期前 30 天啟用自動續約，而且續約期間未過，我們會在 24 小時內續約網域。

> **Important**
>
> 有些 TLD 註冊機構在過期日期前 25 天不再允許續約，許多註冊機構都在過期日期後不允許續約。此外，處理續約最多需要一天時間。如果您在啟用自動續約前拖延太久，網域可能未及時處理續約就已經到期，您可能會因此失去該網域。如果過期日期將近，我們建議您手動延長網域的過期日期。如需詳細資訊，請參閱 延長網域的註冊期間。

如需有關續約期間的詳細資訊，請參閱 可向 Amazon Route 53 註冊的網域 中 TLD 的「續約及還原網域的截止日期」區段。

在過期日期之後

註冊商會在網域到期之後的短時間內保留大多數網域，這樣您便可以在到期日期之後續約已到期的網域；但如果您要保留網域，我們強烈建議您將自動續約功能保持啟用狀態。如需有關過期日期後嘗試續約網域的詳細資訊，請參閱還原已過期或已刪除的網域。

如果您的網域過期，但允許延遲續約，您可以按標準續約價格續約網域。若要判斷網域是否仍在延遲續約期間內，請執行延長網域的註冊期間一節中的程序。如果仍列出網域，表示它仍在延遲續約期間內。

如需有關續約期間的詳細資訊，請參閱 可向 Amazon Route 53 註冊的網域 中 TLD 的「續約及還原網域的截止日期」區段。

還原已過期或已刪除的網域

如果您沒有在延遲續約期間結束之前續約網域，或者您不小心刪除該網域，對於某些頂層網域 (TLD) 註冊機構，您可以在該網域可供其他人註冊之前還原該網域。

當網域已刪除，或其延遲續約期間已過，它不會再出現在 Amazon Route 53 主控台中。

> **Important**
>
> 還原網域通常較高一些，有時遠遠超過註冊或續約網域的價格。如需有關還原網域的目前價格，請參閱 Amazon Route 53 網域註冊定價中的「還原價格」欄。

您無法使用 AWS 點數支付還原過期網域的費用。

在網域已刪除或延遲續約期間已過時嘗試還原網域註冊

1. 判斷網域的 TLD 註冊機構是否支援還原網域，如果有的話，確定允許還原的期間。

   a. 前往 可向 Amazon Route 53 註冊的網域。

   b. 尋找您網域的 TLD，並檢閱「續約及還原網域的截止日期」區段中的值。

   > **Important**
   >
   > 我們會將還原請求轉寄給 Gandi，Gandi 將在星期一到星期五的工作時間處理這些請求。Gandi 位於巴黎，其時間為 UTC/GMT +1 小時。因此，在極少數情況下，可能需要一週甚至更長時間才能完成請求處理，而實際上會依您提交請求的時間而定。

2. 審閱還原網域的定價，通常這個價格會較高，且有時遠遠超過註冊或續約網域的價格。在 Amazon Route 53 網域註冊定價中，尋找適合您網域使用的 TLD (例如 .com)，然後在「註冊價格」欄中核取定價。如果您仍要還原此網域，請記下該定價，因稍後步驟將會用到。
3. 使用註冊網域的 AWS 帳戶登入 Sup AWS port 中心。
4. 指定下列值：

   Regarding

   接受預設值 Account and Billing Support (帳戶與帳單支援)。

   服務

   接受 Billing (帳單) 預設值。

   類別

   接受 Domain name registration issue (網域名稱註冊問題) 預設值。

   主旨

   輸入 Restore an expired domain (還原過期的網域) 或 Restore a deleted domain (還原已刪除的網域)。

   描述

   請提供下列資訊：

   - 要還原的網域
   - 註冊網域之帳 AWS 戶的 12 位數帳號 ID

- 確認，即表示您同意還原網域的定價。使用以下文字：

  「I agree to the price of $____ for restoring my domain. (我同意以 $____ 的定價來還原我的網域)」

  將空白處填入您在步驟 2 中找到的定價。

聯絡方式

指定聯絡方式，如果選擇 Phone (電話)，請輸入適用的值。

5. 選擇提交。
6. 當我們瞭解我們是否能夠還原您的網域時，Sup AWS port 代表會與您聯絡。此外，如果我們能夠還原您的網域時，主控台將重新顯示網域。過期日期取決於網域是過期還是被意外刪除：

   網域過期

   新的過期日期通常是在舊的過期日期之後一至兩年 (取決於 TLD)。

   > **Note**
   >
   > 新的過期日期並非自網域的還原日期開始起算。

   網域被意外刪除

   過期日期通常不會變更。

更換已向 Route 53 註冊的網域託管區域

如果您刪除網域的託管區域，當您準備在網際網路上提供網域時，需要建立另一個託管區域。請執行以下程序。

更換網域的託管區域

1. 建立公有的託管區域。如需詳細資訊，請參閱 建立公有託管區域。
2. 在託管區域中建立記錄。記錄會定義您希望如何路由網域 (example.com) 和子網域 (acme.example.com、zenith.example.com) 的流量。如需詳細資訊，請參閱 處理記錄。
3. 更新網域組態以使用新託管區域的名稱伺服器。如需詳細資訊，請參閱 新增或變更網域的名稱伺服器和黏附記錄。

> **Important**
>
> 當您建立託管區域時，Route 53 會將一組四個名稱伺服器指派給託管的區域。如果您刪除託管區域又建立一個區域，Route 53 會指派另一組四個名稱伺服器。一般而言，新託管區域的名稱伺服器沒有一個會符合前一個託管區域的名稱伺服器。如果您不更新網域組態以使用新託管區域的名稱伺服器，即無法在網際網路上使用該網域。

4. 如果您在取代網域的託管區域時遇到問題，可以免費聯絡 Sup AWS port。如需詳細資訊，請參閱就網域註冊問題聯絡 S AWS upport。

轉移網域

您可以將在另一個註冊機構註冊的網域轉移到 Amazon Route 53、從一個 帳戶轉移到另一個 AWS 帳戶，或從 Route 53 轉移到其他註冊機構。將域名從一個 AWS 帳戶轉移到另一個帳戶無需支付任何費用。

主題

- 將網域註冊轉移到 Amazon Route 53
- 檢視網域轉移的狀態
- 將網域轉移到 Amazon Route 53 對網域註冊的過期日期有何影響
- 將網域轉移到其他 AWS 帳戶
- 將網域從 Amazon Route 53 轉移到其他註冊商

將網域註冊轉移到 Amazon Route 53

> **Important**
>
> 在將任何國碼頂層網域 (ccTLD) 傳輸至 Route 53 的期間 (.cc 和 .tv 除外)，系統會忽略擁有者聯絡資訊的更新，並使用登錄檔中的擁有者聯絡資訊。您可以在傳輸完成後更新聯絡資訊。如需詳細資訊，請參閱 更新網域的聯絡資訊和所有權。

若要將網域註冊轉移到 Amazon Route 53，請遵循此主題中的程序。

> **Important**
>
> 如果您跳過步驟，網域可能在網際網路上無法使用。

注意下列事項：

聯絡 S AWS upport

如果您在轉移網域時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

過期日期

如需有關轉移網域如何影響目前過期日期的詳細資訊，請參閱將網域轉移到 Amazon Route 53 對網域註冊的過期日期有何影響。

轉移費用

當您將網域轉移到 Route 53 時，我們向您的 AWS 帳戶收取的轉移費用取決於頂層網域，例如 .com 或 .org。如需詳細資訊，請參閱 Route 53 定價。

您無法使用 AWS 點數支付轉移網域至 Route 53 的費用 (如果有的話)。

> **Note**
>
> Route 53 會先向您收取轉移網域的費用，再開始進行轉移程序。如果因某些原因導致轉移失敗，我們會立即取消收取您的轉移費用。

特殊和高級網域名稱

TLD 註冊機構向一些網域名稱指派特殊或優惠的價格。如果網域具有特殊或高級網域價格，您無法將網域轉移至 Route 53。

網域配額

每個帳戶的預設網域數 AWS 目上限為 20。您可以申請更高的配額。如需詳細資訊，請參閱 網域的配額。

名稱伺服器限制

Route 53 中每個網域的名稱伺服器數目上限為 6 個。

主題

- 頂層網域的轉移需求
- 步驟 1：確認 Amazon Route 53 支援頂層網域
- 步驟 2 (選用)：將 DNS 服務轉移到 Amazon Route 53 或其他 DNS 服務提供者
- 步驟 3：透過目前註冊商變更設定
- 步驟 4：取得名稱伺服器的名稱
- 步驟 5：請求轉移
- 步驟 6：僅限印度 AISPL 客戶：支付轉移費用
- 步驟 7：按一下確認和授權電子郵件中的連結
- 步驟 8：更新網域組態

頂層網域的轉移需求

大多數的網域註冊商強制要求將網域轉移到其他註冊商。這些要求的主要目的是防止詐騙網域擁有者不斷地將網域轉移至不同的註冊商。要求各有不同，但以下為典型要求：

- 您必須在至少 60 天前已向目前的註冊商註冊網域，或已將網域的註冊轉移到目前的註冊商。
- 如果網域名稱的註冊已過期，並且必須還原，則必須已在至少 60 天前還原。
- 網域不能有任何以下網域名稱狀態碼：
  - clientTransferProhibited
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - serverTransferProhibited
- 部分頂層網域的註冊機構不允許在完成變更 (例如對網域擁有者的變更) 之前轉移。

如需網域名稱狀態碼的目前清單和每個狀態碼意義的說明，請前往 ICANN 網站並搜尋 EPP 狀態碼。(在 ICANN 網站上搜尋；Web 搜尋有時會傳回舊版文件。)

> **Note**
>
> ICANN 這個組織制定用於管理網域名稱註冊和轉移的政策。

您也可以在 Whois 網站中搜尋網域名稱，以瞭解您網域的狀態碼和其他資訊。

步驟 1：確認 Amazon Route 53 支援頂層網域

請參閱 可向 Amazon Route 53 註冊的網域。如果要轉移的網域的頂層網域在清單中，則可將該網域轉移到 Amazon Route 53。

如果 TLD 不在清單中，則無法將網域註冊轉移到 Route 53。我們偶爾會在清單中新增更多的 TLD，因此請返回查看對您的網域是否新增支援。

步驟 2 (選用)：將 DNS 服務轉移到 Amazon Route 53 或其他 DNS 服務提供者

為什麼先轉移 DNS？

某些註冊機構提供免費的 DNS 服務，一旦他們收到 Route 53 轉移網域註冊的要求，就會停用這項服務。如果您希望 Route 53 為您的網域提供 DNS 服務，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

步驟 3：透過目前註冊商變更設定

使用目前註冊商提供的方法，對要轉移的每個網域執行每個以下任務。

- Confirm that the email for the registrant contact for your domain is up to date
- Unlock the domain so it can be transferred
- Confirm that the domain status allows you to transfer the domain
- Disable DNSSEC for the domain
- Get an authorization code
- Renew your domain registration before you transfer the domain (selected geographic TLDs)

確認網域的註冊聯絡人的電子郵件是最新的

我們會傳送電子郵件到該電子郵件地址，以請求轉移授權。您必須按一下電子郵件中的連結，授權轉移。如果不按一下連結，我們必須取消轉移。

解鎖網域以便轉移

ICANN (網域註冊管理機構) 要求您在轉移網域之前先解鎖網域。

確認網域狀態可讓您轉移網域

如需詳細資訊，請參閱 頂層網域的轉移需求。

停用網域的 DNSSEC

如果您將 DNSSEC 與網域搭配使用，並將網域註冊轉移到 Route 53，您必須先在之前的註冊商中停用 DNSSEC。然後，在您轉移網域註冊之後，請執行步驟以在 Route 53 中為網域設定 DNSSEC。Route 53 支援 DNSSEC 進行網域註冊和 DNSSEC 簽署。如需詳細資訊，請參閱 在 Amazon Route 53 中設定 DNSSEC 簽署。

> **Important**
>
> 如果您在 DNSSEC 設定時將網域註冊轉移至 Route 53，DNSSEC 公有金鑰也會轉移。如果您將 DNS 服務轉移到另一個不支援 DNSSEC 的提供者，DNS 解析會間歇性地失敗，直到您從網域刪除 DNSSEC 金鑰。如需詳細資訊，請參閱 刪除網域的公開金鑰。

取得授權碼

來自目前註冊商的授權碼會授權我們請求將網域註冊轉移到 Route 53。您在稍後的程序中於 Route 53 主控台輸入此代碼。

有些頂層網域有額外要求：

.co.za 網域

您不需要取得授權碼就能將 .co.za 網域轉移至 Route 53。

.es 網域

如果要轉移 .es 網域至 Route 53，不需要取得授權碼。

.uk、.co.uk、.me.uk 和 .org.uk 網域

如果要轉移 .uk、.co.uk、.me.uk 或 .org.uk 網域至 Route 53，不需要取得授權碼。相反地，請使用目前網域註冊機構提供的方法，將網域 IPS 標籤的值更新為全部大寫的 GANDI。(.uk 網域名稱的註冊機構 Nominet 需要 IPS 標籤。) 如果您的註冊機構未提供變更 IPS 標籤值的方法，請聯絡 Nominet。

變更 IPS 標籤時，請注意以下各項：

您必須在五天內請求轉移

若您未在變更 IPS 標籤後五天內請求轉移，標籤即會回復為先前的值。您必須再次變更 IPS 標籤的值，否則轉移要求會失敗。

在 WHOIS 查詢中檢視 IPS 標籤

轉移至 Route 53 的作業完成後，WHOIS 查詢中才會顯示對 IPS 標籤進行的變更。

Gandi 寄來的電子郵件

您可能會從我們的註冊機構合作夥伴 Gandi 收到關於轉移程序的電子郵件。如果您收到 Gandi (transfer-auth@gandi.net) 關於轉移網域的電子郵件，請忽略電子郵件中的指示，因為它們與 Route 53 無關。請改為遵循本主題中的指示。

在轉移網域 (選取的地理 TLD) 之前，請先續約您的網域註冊

對於大多數 TLD 而言，當您轉移網域時，註冊會自動延長一年。但是，對某些地理 TLD 而言，當您轉移網域時，註冊不會延長。如果您將網域轉移至有這些 TLD 之一的 Route 53，建議您在轉移網域前續約網域註冊，特別是接近過期日的情況。

> **Important**
>
> 如果您未在轉移網域之前續約網域，註冊有可能在完成轉移之前過期。如果發生這種情況，該網域將無法在網際網路上使用，而且其他人將可以購買該網域名稱。

當您將以下網域轉移到其他註冊商時，註冊不會自動延長：

- .ch (瑞士)
- .cl (智利)
- .co.uk (英國)
- .co.za (南非)
- .com.au (澳洲)
- .cz (捷克共和國)
- .es (西班牙)
- .fi (芬蘭)
- .im (曼島)
- .jp (日本)
- .me.uk (英國)
- .net.au (澳洲)
- .org.uk (英國)
- .se (瑞典)

- .uk (英國)

步驟 4：取得名稱伺服器的名稱

如果您使用 Amazon Route 53 做為您的 DNS 服務，或者您要繼續使用現有的 DNS 服務，我們將在稍後的程序中自動為您取得名稱伺服器的名稱。跳至 步驟 5：請求轉移。

如果要在將網域轉移到 Route 53 的同時，將 DNS 服務變更為 Route 53 以外的提供者，請使用由 DNS 服務提供者提供的步驟，針對要轉移的每個網域取得名稱伺服器的名稱。

> **Important**
>
> 如果網域的註冊商也是網域的 DNS 服務提供者，請在繼續進行網域註冊轉移過程之前，先將 DNS 服務轉移到 Route 53 或其他 DNS 服務提供者。
> 如果在轉移網域註冊的同時也轉移 DNS 服務，則您的網站、電子郵件以及與該網域相關聯的 Web 應用程式可能變得無法使用。如需詳細資訊，請參閱 步驟 2 (選用)：將 DNS 服務轉移到 Amazon Route 53 或其他 DNS 服務提供者。

步驟 5：請求轉移

若要將網域註冊從目前註冊商轉移到 Amazon Route 53，請使用 Route 53 主控台請求轉移。Route 53 會處理與網域的目前註冊商的通訊。

您可以使用主控台轉移最多五個網域。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

使用的程序取決於要轉移單一網域還是多達五個網域：

- 將單一網域的網域註冊轉移至 Route 53
- 若要將最多五個網域的網域註冊轉移到 Route 53

使用將網域轉移至您的帳戶程序，將單一網域轉移至帳戶。

將單一網域的網域註冊轉移至 Route 53

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 在已註冊的網域頁面上，從轉入下拉式選單中，選擇單一網域。
4. 在將網域轉移至您的帳戶頁面的檢查網域可轉移性區段中，輸入要將註冊轉移至 Route 53 之網域的名稱，然後選擇檢查。
5. 如果網域註冊可供轉移，請確認您已完成頂層網域的轉移要求，然後選擇下一步。

   如果網域註冊不可以轉移，Route 53 主控台會列出原因。請聯絡您的註冊商，了解如何解決防止您轉移註冊的問題。
6. 在 DNS 服務頁面上，檢閱名稱伺服器的相關資訊，然後選擇下一步。
7. 如果收到提示，請輸入您在 步驟 3：透過目前註冊商變更設定 中從目前註冊商處取得的授權碼或 IPS 標籤。

   > **Note**
   >
   > 您不需要輸入授權碼就能將 .co.za、.es、.uk、.co.uk、.me.uk 或 .org.uk 網域轉移至 Route 53。

   選擇下一步。
8. 在網域定價選項頁面上，選擇要註冊之網域的轉移年數，以及是否希望我們在到期日期前自動續約網域註冊。

   > **Note**
   >
   > 網域名稱註冊和續約不接受退款。如果您啟用自動網域續約，而且在我們為您續約註冊之後，您決定不需要該網域名稱，您無法取得續約成本的退款。

選擇下一步。

9. 在 [連絡人資訊] 頁面上，輸入網域註冊人、管理員、技術人員和帳單聯絡人的聯絡資訊。您在此處輸入的值將套用至要註冊的所有網域。如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

   請注意下列注意事項：

   姓名

   針對 First Name (名字) 和 Last Name (姓氏)，建議您指定官方 ID 上的姓名。對於網域設定的某些變更，有些網域註冊機構要求您提供身分證明。您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。

   不同的聯絡人

   在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果您想要為一個或多個聯絡人輸入不同資訊，請將與註冊聯絡人相同切換開關的值變更至關閉位置。

   > **Note**
   >
   > 對於 .it 網域，註冊者和管理聯絡人必須相同。

   其他必要資訊

   對於某些頂層網域 (TLD)，我們需要收集更多資訊。對於這些 TLD，請在 Postal/Zip Code (郵遞區號) 欄位後輸入適用的值。

   隱私權保護

   選擇是否要向 WHOIS 查詢隱藏您的聯絡資訊。

   > **Note**
   >
   > 您必須為管理員、註冊者和技術聯絡人指定相同的隱私權設定。

   如需詳細資訊，請參閱下列主題：

   - 為網域的聯絡資訊啟用或停用隱私權保護

- 可向 Amazon Route 53 註冊的網域

> **Note**
>
> 若要針對 .uk、.co.uk、.me.uk 和 .org.uk 網域啟用隱私權保護，您必須開立一個支援案例並請求隱私權保護。

選擇下一步。

10. 在檢閱頁面上檢閱您輸入的資訊，並選擇性地加以更正。閱讀服務條款，並選取核取方塊以確認您已閱讀服務條款。

    選擇 Submit request (提交請求)。

11. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要向 Route 53 註冊網域，請執行下列步驟以支付註冊網域的費用。

    a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。

    b. 在 Payments Due (付款到期) 區段中，找到適用的發票。

    c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

    在您的發票付款後，我們會完成網域註冊並發送適用的電子郵件。

> **Important**
>
> 如果您在五天內未支付發票，則會取消發票。若要在取消商業發票後註冊網域，請重新提交請求。

如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

12. 在導覽窗格中，依次選擇網域和請求。

    在此頁面上，您可以檢視網域的狀態，以及確認您是否需要回應註冊聯絡人驗證電子郵件。您也可以選擇重新傳送驗證電子郵件。

    如果您為註冊聯絡人指定了從未用來向 Route 53 註冊網域的電子郵件地址，某些 TLD 註冊機構會要求您驗證該地址是否有效。

我們會從下列其中一個電子郵件地址傳送驗證電子郵件：

- noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD。
- noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD。若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

> **Important**
>
> 註冊聯絡人必須按照電子郵件中的指示來驗證已收到電子郵件，否則我們必須按照 ICANN 的要求暫停該網域。當網域已暫停，無法在網際網路上存取該網域。

a. 當您收到驗證電子郵件，選擇電子郵件中用於確認電子郵件地址是否有效的連結。如果您沒有立即收到電子郵件，請檢查您的垃圾電子郵件資料夾。

b. 返回請求頁面。如果狀態未自動更新指出 email-address is verified (電子郵件地址已驗證)，請選擇 Refresh status (重新整理狀態)。

13. 當網域轉移完成時，下一步取決於您要使用 Route 53 還是其他 DNS 服務作為網域的 DNS 服務：

- Route 53 – 在您註冊網域時 Route 53 建立的託管區域中，建立記錄以告知 Route 53 您希望如何為網域和子網域路由流量。

  例如，當有人在瀏覽器中輸入您的網域名稱，且該查詢被轉送到 Route 53 時，您希望 Route 53 用您資料中心 Web 伺服器的 IP 地址回應查詢，還是用 Elastic Load Balancing 負載平衡器的名稱回應查詢？

  如需詳細資訊，請參閱 處理記錄。

  > **Important**
  >
  > 如果您在 Route 53 自動建立的託管區域之外的託管區域中建立記錄，則必須更新網域的名稱伺服器，以將這些名稱伺服器用於新的託管區域。

- 其他 DNS 服務 – 設定您的新網域，將 DNS 查詢路由到其他 DNS 服務。請執行更新名稱伺服器以使用其他註冊商程序。

使用下列程序將最多五個網域轉移至帳戶。

若要將最多五個網域的網域註冊轉移到 Route 53

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 在已註冊的網域頁面上，從轉入下拉式選單中選擇多個網域。
4. 在將多個網域轉移至您的帳戶頁面上，每行輸入最多五個您要轉移的網域及其授權碼 (如有需要)，然後選擇檢查。
5. 如果網域註冊可供轉移，則其在網域可用性清單中會列為可用。選取要轉移註冊之每個網域的核取方塊，確認您已完成頂層網域的轉移要求，然後選擇下一步。

   如果網域註冊不可以轉移，Route 53 主控台會列出原因。請聯絡您的註冊商，了解如何解決防止您轉移註冊的問題。
6. 在 DNS 服務頁面上，檢閱名稱伺服器的相關資訊，然後選擇下一步。
7. 在網域定價選項頁面上，選擇要註冊之網域的轉移年數，以及是否希望我們在到期日期前自動續約網域註冊。

   > **Note**
   >
   > 網域名稱註冊和續約不接受退款。如果您啟用自動網域續約，而且在我們為您續約註冊之後，您決定不需要該網域名稱，您無法取得續約成本的退款。

   選擇下一步。
8. 在聯絡資訊頁面上，輸入網域註冊者、管理員和技術聯絡人的聯絡資訊。您在此處輸入的值將套用至要轉移的所有網域。

   > **Important**
   >
   > 我們建議您為註冊聯絡人 (網域擁有者) 指定下列值：
   >
   > - First and last name (名字和姓氏)：建議您指定官方 ID 上的姓名。對於網域設定的某些變更，有些網域註冊機構要求您提供身分證明。您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。
   > - Contact details (聯絡詳細資料)：在網域轉移期間，建議您指定與目前註冊商所指定的相同值。當您變更註冊聯絡人的聯絡詳細資料時，您會變更網域擁有者，且某些

TLD 註冊機構不允許您在網域轉移期間變更網域擁有者。如果您變更註冊聯絡人的聯絡詳細資料，轉移可能會失敗。您可以在轉移網域後變更註冊聯絡人的聯絡詳細資料。

在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果您想要為一個或多個聯絡人輸入不同資訊，請將與註冊聯絡人相同的值設為關閉位置。

> **Note**
>
> 對於 .it 網域，註冊者和管理聯絡人必須相同。

如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

9. 對於某些 TLD，我們需要收集更多資訊。對於這些 TLD，請在 Postal/Zip Code (郵遞區號) 欄位後輸入適用的值。
10. 如果 Contact Type (聯絡人類型) 的值是 Person (個人)，請選擇是否要在 WHOIS 查詢中隱藏您的聯絡資訊。如需詳細資訊，請參閱 為網域的聯絡資訊啟用或停用隱私權保護。
11. 選擇提交。
12. 檢閱您輸入的資訊，閱讀服務條款，並選取確認您已閱讀服務條款的核取方塊。
13. 選擇 Submit request (提交請求)。

    我們確認網域符合轉移條件，並向網域的註冊聯絡人傳送一封電子郵件，以請求轉移網域的授權。
14. 僅限 AISPL（印度）客戶：如果您的聯繫地址位於印度，則您的用戶協議是與印度當地賣家 Amazon 互聯網服務列兵有限公司（AISPL）簽訂的用戶協議。 AWS 若要向 Route 53 註冊網域，請執行下列步驟以支付註冊網域的費用。

    a. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。
    b. 在 Payments Due (付款到期) 區段中，找到適用的發票。
    c. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

    在您的發票付款後，我們會完成網域註冊並發送適用的電子郵件。

> **Important**
>
> 如果您在五天內未支付發票，則會取消發票。若要在取消商業發票後註冊網域，請重新提交請求。

如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

15. 在導覽窗格中，依次選擇網域和請求。

    在此頁面上，您可以檢視網域的狀態，以及確認您是否需要回應註冊聯絡人驗證電子郵件。您也可以選擇重新傳送驗證電子郵件。

    如果您為註冊聯絡人指定了從未用來向 Route 53 註冊網域的電子郵件地址，某些 TLD 註冊機構會要求您驗證該地址是否有效。

    我們會從下列其中一個電子郵件地址傳送驗證電子郵件：

    - noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD。
    - noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD。若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

    > **Important**
    >
    > 註冊聯絡人必須按照電子郵件中的指示來驗證已收到電子郵件，否則我們必須按照 ICANN 的要求暫停該網域。當網域已暫停，無法在網際網路上存取該網域。

    a. 當您收到驗證電子郵件，選擇電子郵件中用於確認電子郵件地址是否有效的連結。如果您沒有立即收到電子郵件，請檢查您的垃圾電子郵件資料夾。

    b. 返回請求頁面。如果狀態未自動更新指出 email-address is verified (電子郵件地址已驗證)，請選擇 Refresh status (重新整理狀態)。

16. 當網域轉移完成時，下一步取決於您要使用 Route 53 還是其他 DNS 服務作為網域的 DNS 服務：

    - Route 53 – 在您註冊網域時 Route 53 建立的託管區域中，建立記錄以告知 Route 53 您希望如何為網域和子網域路由流量。

例如，當有人在瀏覽器中輸入您的網域名稱，且該查詢被轉送到 Route 53 時，您希望 Route 53 用您資料中心 Web 伺服器的 IP 地址回應查詢，還是用 ELB 負載平衡器的名稱回應查詢？

如需詳細資訊，請參閱 處理記錄。

> **Important**
>
> 如果您在 Route 53 自動建立的託管區域之外的託管區域中建立記錄，則必須更新網域的名稱伺服器，以將這些名稱伺服器用於新的託管區域。

- 其他 DNS 服務 – 設定您的新網域，將 DNS 查詢路由到其他 DNS 服務。請執行更新名稱伺服器以使用其他註冊商程序。

Old console

使用的程序取決於要轉移多達五個網域或超過五個網域：

- 將最多五個網域的網域註冊轉移到 Route 53
- 若要將超過五個網域的網域註冊轉移到 Route 53

> **Important**
>
> 如果您使用轉移超過五個網域的程序，Route 53 會自動設定轉移的網域，對要轉移的所有網域使用目前 DNS 服務。如果網域的註冊商也是網域的 DNS 服務提供者，而且您未將 DNS 服務轉移到另一個提供者，則您的網站、電子郵件以及與該網域相關聯的 Web 應用程式可能變得無法使用。如需詳細資訊，請參閱 步驟 2 (選用)：將 DNS 服務轉移到 Amazon Route 53 或其他 DNS 服務提供者。

將最多五個網域的網域註冊轉移到 Route 53

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇 Transfer Domain (轉移網域)。
4. 輸入要將註冊轉移到 Route 53 的網域名稱，然後選擇 Check (檢查)。

5. 如果網域註冊可供轉移，請選擇 Add to cart (加入購物車)。

   如果網域註冊不可以轉移，Route 53 主控台會列出原因。請聯絡您的註冊商，了解如何解決防止您轉移註冊的問題。

6. 如果要轉移其他網域註冊，請重複步驟 4 和 5。
7. 當您已新增要轉移的所有網域註冊，請選擇 Continue (繼續)。
8. 對於要轉移的每個網域名稱，請輸入適用的值：

   授權碼

   輸入您在步驟 3：透過目前註冊商變更設定中從目前註冊商取得的授權碼。

   > **Note**
   >
   > 您不需要輸入授權碼就能將 .co.za、.es、.uk、.co.uk、.me.uk 或 .org.uk 網域轉移至 Route 53。

   名稱伺服器選項

   請選擇適用的選項：

   - 繼續使用目前註冊商或 DNS 服務提供的名稱伺服器 – 如果網域的目前註冊商正在提供 DNS 服務，建議您在轉移網域之前，先將 DNS 服務轉移到其他 DNS 服務提供者。

     > **Important**
     >
     > 有些註冊商在您一旦請求轉移到另一個註冊商，即停止提供 DNS 服務。如果目前的註冊商停用 DNS 服務，網域在網際網路上就會變得無法使用。

   - 從與網域同名的 Route 53 託管區域匯入名稱伺服器 – 當您選取此選項，主控台就會顯示與網域同名的託管區域清單。選擇您要用於路由網域流量的託管區域。
   - 指定新的名稱伺服器以取代目前註冊機構的名稱伺服器 (不建議) – 如果此網域使用 Route 53 以外的 DNS 服務，請輸入您在 步驟 4：取得名稱伺服器的名稱 中取得的名稱伺服器名稱。

> **Important**
>
> 我們不建議選擇此選項，因為將 DNS 服務從一個 DNS 服務提供者轉移到另一個 DNS 服務提供者可能需要長達兩天的時間。目前註冊商在您一旦請求轉移到另一個註冊商，可能會立即停止提供 DNS 服務。如果目前的註冊商停用 DNS 服務，在對另一個 DNS 服務提供者的變更生效之前，您的網域在網際網路上將會無法使用。

名稱伺服器

如果您選擇 Specify new name servers to replace the current registrar's name servers (指定新的名稱伺服器以取代目前註冊機構的名稱伺服器)，請輸入您在步驟 4：取得名稱伺服器的名稱中從網域 DNS 服務取得的名稱伺服器名稱。根據預設，Name server (名稱伺服器) 欄位會顯示網域目前名稱伺服器的名稱。

黏附記錄

如果名稱伺服器的名稱是您要轉移的網域的子網域 (例如 example.com 網域中的 ns1.example.com)，請為每個名稱伺服器輸入一或多個 IP 地址。您可以輸入 IPv4 或 IPv6 格式的地址。如果名稱伺服器有多個 IP 地址，請在不同的行中輸入每個地址。

9. 在 Contact Details for Your n Domains (您的 n 個網域聯絡詳細資訊) 頁面上，輸入網域註冊者、管理員和技術聯絡人的聯絡資訊。您在此處輸入的值將套用至要轉移的所有網域。

> **Important**
>
> 我們建議您為註冊聯絡人 (網域擁有者) 指定下列值：
>
> - First and last name (名字和姓氏)：建議您指定官方 ID 上的姓名。對於網域設定的某些變更，有些網域註冊機構要求您提供身分證明。您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。
> - Contact details (聯絡詳細資料)：在網域轉移期間，建議您指定與目前註冊商所指定的相同值。當您變更註冊聯絡人的聯絡詳細資料時，您會變更網域擁有者，且某些 TLD 註冊機構不允許您在網域轉移期間變更網域擁有者。如果您變更註冊聯絡人的聯絡詳細資料，轉移可能會失敗。您可以在轉移網域後變更註冊聯絡人的聯絡詳細資料。

在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果要輸入一或多個聯絡人的不同資訊，請將 My Registrant, Administrative, and Technical contacts are all the same (我的網域註冊者、管理員和技術聯絡人是同一人) 的值變更為 No (否)。

> **Note**
>
> 對於 .it 網域，註冊人和管理聯絡人必須相同。

如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

10. 對於某些 TLD，我們需要收集更多資訊。對於這些 TLD，請在 Postal/Zip Code (郵遞區號) 欄位後輸入適用的值。
11. 如果 Contact Type (聯絡人類型) 的值是 Person (個人)，請選擇是否要在 WHOIS 查詢中隱藏您的聯絡資訊。如需詳細資訊，請參閱 為網域的聯絡資訊啟用或停用隱私權保護。
12. 選擇 Continue (繼續)。
13. 選擇您是否希望我們在到期之前自動續約您的網域註冊。

> **Note**
>
> 網域名稱註冊和續約不接受退款。如果您啟用自動網域續約，而且在我們為您續約註冊之後，您決定不需要該網域名稱，您無法取得續約成本的退款。

14. 檢閱您輸入的資訊，閱讀服務條款，並選取確認您已閱讀服務條款的核取方塊。
15. 選擇 Complete Purchase (完成購買)。

我們確認網域符合轉移條件，並向網域的註冊聯絡人傳送一封電子郵件，以請求轉移網域的授權。

若要將超過五個網域的網域註冊轉移到 Route 53

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇 Transfer Domain (轉移網域)。
4. 在 Transfer domain to Route 53 (將網域轉移到 Route 53) 頁面上，選擇 Transfer multiple domains to Route 53 (將多個網域轉移到 Route 53)。

5. 為每個要轉移的網域，輸入下列格式的網域名稱和授權碼。請注意網域名稱和授權碼之間的逗號：

```
domain-name-1,authorization-code-1
domain-name-2,authorization-code-2
```

如果網域不需要授權碼，則省略逗號：

```
domain-name-3
```

> **Note**
>
> 您不需要輸入授權碼就能將 .co.za、.es、.uk、.co.uk、.me.uk 或 .org.uk 網域轉移至 Route 53。

6. 輸入要轉移的所有網域後，請選擇 Continue (繼續)。
7. Check domain transferability (檢查網域可轉移性) 頁面會列出您在上一頁中輸入的網域，以及每個網域是否可以轉移。您有下列選項：

   如果所有網域都是可轉移的

   選擇 Add transferable domains to cart (將可轉移的網域加入購物車)。

   如果一或多個網域是不可轉移的，而且您希望轉移它們

   請檢閱頂層網域的轉移需求，以確認每個不可轉移的網域是否符合轉移要求。如果您未發現任何明顯的問題，請聯絡目前的註冊商，以確定網域無法轉移到 Route 53 的原因。

   在您進行任何變更讓網域變成可轉移的之後 (例如，停用轉移鎖定)，請選擇 Check transferability (檢查可轉移性)，Route 53 就會重複可轉移性檢查。

   如果一或多個網域是不可轉移的，而且您不希望轉移它們

   選擇 Add transferable domains to cart (將可轉移的網域加入購物車)。
8. 選擇 繼續。
9. 在 Contact Details for Your n Domains (您的 n 個網域聯絡詳細資訊) 頁面上，輸入網域註冊者、管理員和技術聯絡人的聯絡資訊。您在此處輸入的值將套用至要轉移的所有網域。

> **Important**
>
> 我們建議您為註冊聯絡人 (網域擁有者) 指定下列值：
>
> - First and last name (名字和姓氏)：建議您指定官方 ID 上的姓名。對於網域設定的某些變更，有些網域註冊機構要求您提供身分證明。您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。
> - Contact details (聯絡詳細資料)：在網域轉移期間，建議您指定與目前註冊商所指定的相同值。當您變更註冊聯絡人的聯絡詳細資料時，您會變更網域擁有者，且某些 TLD 註冊機構不允許您在網域轉移期間變更網域擁有者。如果您變更註冊聯絡人的聯絡詳細資料，轉移可能會失敗。您可以在轉移網域後變更註冊聯絡人的聯絡詳細資料。

在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果要輸入一或多個聯絡人的不同資訊，請將 My Registrant, Administrative, and Technical contacts are all the same (我的網域註冊者、管理員和技術聯絡人是同一人) 的值變更為 No (否)。

如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

10. 對於某些 TLD，我們需要收集更多資訊。對於這些 TLD，請在 Postal/Zip Code (郵遞區號) 欄位後輸入適用的值。
11. 如果 Contact Type (聯絡人類型) 的值是 Person (個人)，請選擇是否要在 WHOIS 查詢中隱藏您的聯絡資訊。如需詳細資訊，請參閱 為網域的聯絡資訊啟用或停用隱私權保護。
12. 選擇 Continue (繼續)。
13. 選擇您是否希望我們在到期之前自動續約您的網域註冊。

> **Note**
>
> 網域名稱註冊和續約不接受退款。如果您啟用自動網域續約，而且在我們為您續約註冊之後，您決定不需要該網域名稱，您無法取得續約成本的退款。

14. 檢閱您輸入的資訊，閱讀服務條款，並選取確認您已閱讀服務條款的核取方塊。
15. 選擇 Complete Purchase (完成購買)。

我們確認網域符合轉移條件，並向網域的註冊聯絡人傳送一封電子郵件，以請求轉移網域的授權。

步驟 6：僅限印度 AISPL 客戶：支付轉移費用

如果您的聯絡地址位於印度，則您的使用者協議為印度當地 AWS 賣家 Amazon 網際網路服務列兵有限公司 (AISPL) 簽訂的使用者協議。若要轉移網域至 Route 53，請執行下列程序以支付轉移網域的費用。

若要支付轉移費用

1. 前往 AWS Management Console中的 Orders and Invoices (訂單和發票) 頁面。
2. 在 Payments Due (付款到期) 區段中，找到適用的發票。
3. 在 Actions (動作) 欄位中，選擇 Verify and Pay (驗證和付款)。

   在您的發票付款後，我們會完成網域轉移並發送適用的電子郵件。

> **Important**
>
> 如果您在五天內未支付發票，則會取消發票。若要在取消發票後轉移網域，請重新提交請求。

如需詳細資訊，請參閱 AWS Billing 使用者指南中的管理您在印度的付款。

步驟 7：按一下確認和授權電子郵件中的連結

您請求轉移後，我們可能會立即傳送一或多封電子郵件給網域的註冊聯絡人：

確認可聯絡到註冊申請人的電子郵件

如果您從未向 Route 53 註冊過網域或將網域轉移到 Route 53，我們會傳送一封電子郵件給您，要求您確認電子郵件地址是有效的。我們會保留此資訊，以便日後不必再傳送此確認電子郵件。

獲得網域轉移授權的電子郵件

對於某些 TLD，您需要回應電子郵件才能授權轉移網域。

一般 TLD (例如 .com、.net 和 .org)

有 .com、.net 或 .org 等一般 TLD 的網域不需要授權。

地理 TLD (例如 .co.uk 和 .jp)

針對有地理 TLD 的網域，我們需要取得您的授權才能轉移網域。如果您要傳輸 10 個網域，我們必須向您傳送 10 封電子郵件，而您需要按一下每封郵件中的授權連結。

所有的電子郵件都會傳送至網域註冊的聯絡人：

- 如果您是網域的註冊聯絡人，請依照電子郵件中的指示授權轉移。
- 如果其他人是網域的註冊聯絡人，請要求他依照電子郵件中的指示授權轉移。

> **Important**
>
> 如果您要轉移有地理 TLD 的網域，我們會等待註冊聯絡人授權轉移，最多五天。如果註冊聯絡人在五天內未回應，我們將取消轉移操作，並向註冊聯絡人傳送一封電子郵件，以告知取消事宜。

主題

- 新擁有者或電子郵件地址的授權電子郵件
- 發出授權電子郵件的電子郵件地址
- 目前註冊機構的核准
- 接下來會發生什麼狀況？

新擁有者或電子郵件地址的授權電子郵件

如果您變更了下列值，我們會另外寄給您一封電子郵件，要求您提供授權：

網域擁有者

如果您變更網域擁有者 (如網域擁有者是誰？中所述)，我們會向網域的註冊聯絡人傳送一封電子郵件。

註冊聯絡人的電子郵件地址 (僅適用於某些 TLD)

對於某些 TLD，如果您變更註冊聯絡人的電子郵件地址，我們會同時向註冊聯絡人的新舊電子郵件地址傳送電子郵件。這兩個電子郵件地址的收件者必須按照電子郵件中的指示授權變更。

對於網域擁有者或註冊聯絡人電子郵件地址的變更，如果我們未在 3-15 天內收到變更授權 (具體時間取決於頂層網域)，則我們必須按照 ICANN 的要求取消請求。

發出授權電子郵件的電子郵件地址

所有電子郵件都是來自下列其中一個電子郵件地址。

TLD	發出授權電子郵件的電子郵件地址
.com.au 和 .net.au	no-reply@ispapi.net 此電子郵件包含 http://transfers.ispapi.net 的連結。
.fr	nic@nic.fr (如果您在轉移網域的同時，也要變更 .fr 網域名稱的註冊聯絡人)。(電子郵件會同時傳送到目前的註冊聯絡人和新的註冊聯絡人。)
所有其他	下列其中一個電子郵件地址： • noreply@registrar.amazon.com • noreply@domainnameverification.net

若要確定您的 TLD 註冊商是誰，請參閱可向 Amazon Route 53 註冊的網域。

目前註冊機構的核准

如果註冊聯絡人授權轉移，我們將開始與您目前的註冊商合作轉移您的網域。此步驟最多可能需要 10 天，具體時間取決於 TLD 網域：

- 一般頂層網域 - 最多需要七天
- 地理頂層網域 (也稱為國家/地區代碼頂層網域) - 最多需要十天

如果您目前的註冊商沒有回覆我們的轉移請求 (此情況在註冊商中很常見)，將自動進行轉移。如果您目前的註冊商拒絕轉移請求，我們會傳送電子郵件通知給目前的註冊聯絡人。註冊者需要聯絡目前的註冊商並解決轉移問題。

接下來會發生什麼狀況？

當您的網域轉移已獲得核准，我們會傳送另一封電子郵件給註冊聯絡人。如需此程序的詳細資訊，請參閱檢視網域轉移的狀態。

我們會在轉移完成後立即向您的 AWS 帳戶收取網域轉移的費用。如需依 TLD 分類的收費清單，請參閱 Amazon Route 53 的網域註冊定價。

> **Note**
>
> 這是一次性費用，因此費用不會顯示在您的 CloudWatch 帳單指標中。如需有關指CloudWatch標的詳細資訊，請參閱 Amazon 使用者指南中的使 CloudWatch 用 Amazon 指 CloudWatch 標。

步驟 8：更新網域組態

轉移完成後，您可以選擇變更以下設定：

轉移鎖定

若要將網域轉移至 Route 53，您必須停用轉移鎖定。如果要重新啟用鎖定以防止未經授權的轉移，請參閱鎖定網域以防止未經授權轉移到另一個註冊商。

自動續約

我們將轉移的網域設定為在網域過期日期將近時自動續約。有關如何變更此設定的詳細資訊，請參閱啟用或停用網域自動續約。

延長註冊期間

在預設情況下，Route 53 每年都會續約網域。如果要讓網域註冊更長的時間，請參閱延長網域的註冊期間。

DNSSEC

如需設定網域的 DNSSEC 的詳細資訊，請參閱設定網域的 DNSSEC。

檢視網域轉移的狀態

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。您仍然可以在轉換期間，視需要選擇使用舊的主控台。

在您開始將網域從其他網域註冊商轉移到 Amazon Route 53 之後，可以在 Route 53 主控台的請求頁面 (新主控台) 或待處理的請求 (舊主控台) 頁面上追蹤狀態。Status (狀態) 欄包含目前步驟的簡要說明。以下清單包含主控台中的文字，以及每個步驟的詳細說明。

> **Note**
>
> 當您提交轉移請求，初始狀態是 Domain transfer request submitted (提交網域轉移請求)，表示我們已收到您的請求。

判斷網域是否符合轉移要求 (步驟 1/14)

我們正在確認您網域的狀態是否符合轉移資格。您必須解鎖網域，而且在提交轉移請求時，該網域不能包含以下任何狀態碼：

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

僅限地理 TLD - 驗證 WHOIS 資訊 (步驟 14 之 2)

如果您轉移的網域有地理 TLD，我們會針對您的網域傳送 WHOIS 查詢，判斷您是否已停用網域的隱私權保護。如果目前的註冊商仍然啟用隱私權保護，我們將無法存取轉移網域所需的資訊。

> **Note**
>
> 有 .com、.net 或 .org 等一般 TLD 的網域不需要授權。

僅限地理 TLD - 將電子郵件傳送給註冊聯絡人以取得轉移授權 (步驟 14 之 3)

如果您要轉移的網域有地理 TLD，我們已將電子郵件傳送給網域的註冊聯絡人。電子郵件旨在確認轉移請求是由授權的網域聯絡人提出。

> **Note**
>
> 有 .com、.net 或 .org 等一般 TLD 的網域不需要授權。

向目前的註冊商驗證轉移 (步驟 4/14)

我們已傳送請求給網域目前的註冊商，以啟動轉移。

僅限地理 TLD - 等待註冊聯絡人的授權 (步驟 14 之 5)

我們已傳送電子郵件給網域的註冊聯絡人 (請參閱步驟 3/14)，而且我們正在等待註冊聯絡人按一下電子郵件中的連結，以授權轉移。如果您要轉移的網域有地理 TLD，而您因某些原因未收到電子郵件，請參閱重新傳送授權和確認電子郵件。

已聯絡目前的註冊商以請求轉移 (步驟 6/14)

我們正在與網域目前的註冊商合作，以完成轉移。

等待目前的註冊商完成轉移 (步驟 7/14)

您目前的註冊商正在確認您的網域符合轉移要求。此步驟最多可能需要 10 天，具體時間取決於 TLD 網域：

- 一般頂層網域 - 最多需要七天
- 地理頂層網域 (也稱為國家/地區代碼頂層網域) - 最多需要十天

> **Note**
>
> 如果您在轉移 .JP 網域時已核准 Route 53 傳送的確認電子郵件，但在步驟 7 中已停止數日，請聯絡 AWS 支援中心尋求協助。

對於大多數註冊商，該程序是完全自動化的，無法加速。有些註冊商會傳送一封電子郵件給您，要求您核准轉移；如果您的註冊商傳送此確認電子郵件，則轉移程序可能會比七到十天快得多。

如需註冊商可能拒絕轉移的原因的詳細資訊，請參閱頂層網域的轉移需求。

向註冊聯絡人確認該聯絡人是否已啟動轉移 (步驟 8/14)

有些 TLD 註冊機構會傳送另一封電子郵件給註冊聯絡人，以確認授權使用者是否已請求網域轉移。

將名稱伺服器與註冊機構同步 (步驟 9/14)

只有在轉移請求中提供的名稱伺服器與目前註冊商列出的名稱伺服器不同時，才會執行此步驟。我們會嘗試將您的名稱伺服器更新為所提供的新名稱伺服器。

將設定與註冊機構同步 (步驟 10/14)

我們正在驗證轉移是否已成功完成，而且正在與我們的註冊商合作夥伴同步您的網域相關資料。

傳送更新的聯絡資訊到註冊機構 (步驟 11/14)

如果您在請求轉移時變更網域所有權，我們會嘗試進行此變更。不過，大多數註冊機構不允許在轉移網域的過程中轉移所有權。

完成轉移到 Route 53 (步驟 12/14)

我們正在確認轉移程序是否成功。

正在完成轉移 (步驟 13/14)

我們正在 Route 53 中設定您的網域。

轉移完成 (步驟 14/14)

您的轉移已成功完成。

將網域轉移到 Amazon Route 53 對網域註冊的過期日期有何影響

當您在註冊商之間轉移網域時，某些 TLD 註冊機構可讓網域的過期日期保持不變，某些註冊機構會將過期日期加一年，而某些註冊機構會將過期日期變更為轉移日期之後一年。

> **Note**
>
> 對於大多數 TLD，您可以在將網域轉移到 Amazon Route 53 之後將網域的註冊期間延長達十年之久。如需詳細資訊，請參閱 延長網域的註冊期間。

一般 TLD

當您將具有一般 TLD (例如 .com) 的網域轉移到 Route 53 時，網域的新過期日期為在先前註冊商規定的過期日期加一年。

地理 TLD

當您將具有地理 TLD (例如 .co.uk) 的網域轉移到 Route 53 時，網域的新過期日期取決於該 TLD。在下表中尋找您的 TLD，以判斷轉移網域對過期日期有何影響。

洲別	地理 TLD 和轉移網域對過期日期的影響
非洲	.co.za – 過期日期保持不變。
美洲	

洲別	地理 TLD 和轉移網域對過期日期的影響
	.cl、.com.ar、.com.br – 過期日期保持不變。 .ca、.co、.mx、.us – 舊的過期日期加一年。
亞洲/大洋洲	.co.nz、.com.au、.com.sg、.jp、.net.au、.net.nz、.org.nz、.sg – 過期日期保持不變。 .in – 舊的過期日期加一年。
歐洲	.ch、.co.uk、.es、.fi、.me.uk、.org.uk、.se – 過期日期保持不變。 .berlin、.eu、.io、.me、.ruhr、.wien – 舊的過期日期加一年。 .be、.de、.fr、.it、.nl – 新的過期日期是轉移日期後一年。

將網域轉移到其他 AWS 帳戶

如果您使用一個 AWS 帳戶註冊網域，而且想要將網域轉移到另一個 AWS 帳戶，則可以使用新的主控台或使用 AWS CLI 或其他程式設計方法輕鬆轉移網域。

主題

- 步驟 1：將網域轉移到其他 AWS 帳戶
- 步驟 2 (選擇性)：將託管區域移轉至其他 AWS 帳戶

步驟 1：將網域轉移到其他 AWS 帳戶

域名無法在註冊後的首個 14 天內轉移。

開始網域轉移時，您必須使用根帳戶登入，或使用以下列一種或多種方式取得 IAM 許可的使用者身分登入：

- 系統會為使用者指派受AdministratorAccess管理的策略。
- 系統會為使用者指派 AmazonRoute53 個DomainsFullAccess受管理的策略。
- 系統會為使用者指派 AmazonRoute53 個FullAccess受管理的策略。
- 系統會為使用者指派受PowerUserAccess管理的策略。

- 使用者具有執行下列所有動作的許可：TransferDomains、DisableDomainTransferLock 和 RetrieveDomainAuthCode。

如果您不使用根帳戶或具有所需許可的使用者登入，我們無法執行轉移。這項要求可防止未經授權的使用者將網域轉移到其 AWS 帳戶他

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。 AWS 帳戶 您可以在新主控台上完成下列轉移和接受網域轉移的程序。

轉移程序有兩個步驟。首先，原始帳戶擁有者開始在開始到另一個 AWS 帳戶的轉移程序中的轉移，然後目的地帳戶擁有者接受在接受來自另一個 AWS 帳戶的轉移程序中的轉移。

將網域轉移到其他 AWS 帳戶

1. 使 AWS 用目前註冊 AWS 帳戶 的網域登入。
2. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
3. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
4. 選擇要轉移到另一個 AWS 帳戶之網域的名稱。
5. 在詳細資訊區段上方的轉出下拉式選單中，選擇轉移至另一個 AWS 帳戶。
6. 在轉移至另一個 AWS 帳戶 對話方塊中，輸入目的地帳戶 ID。您可以從目的地 AWS 帳戶 擁有者處取得此 ID。
7. 選擇確認。
8. 在「產生密碼」對話方塊中，複製密碼，並將其轉寄給接收的 AWS 帳戶 擁有者。

   在請求頁面上，網域的狀態會顯示進行中，而類型則會顯示內部轉出。

接受來自不同 AWS 帳戶的網域轉移

1. 使用 AWS 接收網域的登入。 AWS 帳戶
2. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
3. 在導覽窗格中選擇請求。
4. 在「請求」頁面上，選取您要從其他網域轉移的網域名稱旁邊的選項按鈕 AWS 帳戶。如果網域已可供轉移，則狀態會是需要採取動作，且類型會是在其中的網域內部轉移。

您有三天的時間可以接受請求。如果未在三天內接受轉移，轉移請求將會取消。

5. 在動作下拉式選單中，選擇接受。

   您也可以選擇拒絕以取消轉移程序。

6. 如果您已接受，請在將網域轉移至您的帳戶頁面的密碼區段中，輸入您從原始帳戶擁有者收到的密碼。

   接受條款與條件，然後選擇下一步。

7. 導覽至請求頁面，以監控轉移狀態及其他要完成的步驟。
8. 轉移完成後，您可以更新聯絡資訊。如需詳細資訊，請參閱 更新網域的聯絡資訊和所有權。

以程式設計方式轉移網域

您也可以使用其中一個 AWS SDK 或 Route 53 API AWS CLI，以程式設計方式傳輸網域。如需詳細資訊，請參閱下列 文件：

- 如需轉移程序的概觀以及您使用 Route 53 網域註冊 API 轉移網域時所用 API 動作的文件，請參閱 Amazon Route 53 API 參考TransferDomainToAnotherAwsAccount中的。
- 如需有關以程式設計方式傳輸網域的其他選項的說明文件，請參閱「AWS 文件」頁面的「指南和 API 參考」一節中的「SDK 和工具組」。
- 接收帳戶有三天的時間，可以使用 transfer-domain-to-another-aws- account API 接受來自原始帳戶的轉移。如果未在三天內接受轉移，轉移請求將會取消。

> **Important**
>
> 當您以程式設計方式將網域轉移到其他 AWS 帳戶時，網域的託管區域不會轉移。如果您也想要轉移託管區域，請待網域完成轉移後，參閱步驟 2 (選擇性)：將託管區域移轉至其他 AWS 帳戶。

步驟 2 (選擇性)：將託管區域移轉至其他 AWS 帳戶

如果使用 Route 53 做為網域的 DNS 服務，當您將網域轉移至其他 AWS 帳戶時，Route 53 不會轉移託管區域。如果網域與一個帳戶相關聯，而對應的託管區域與另一個帳戶相關聯，則網域註冊和 DNS 功能都不受影響。唯一的影響是，您需要使用一個帳戶登入 Route 53 主控台查看網域，並使用另一個帳戶登入以查看託管區域。

如果您擁有網路轉移來源和目標的帳戶，您可以選擇是否將網域的託管區域遷移至不同的帳戶，但此非必要。Route 53 會繼續使用現有託管區域的記錄路由網域的流量。

> **Important**
>
> 如果您不同時擁有要轉移網域的來源帳戶和要轉移網域的帳戶，則必須將現有的託管區域遷移到要轉移網域的目標 AWS 帳戶，或者在您擁有的 AWS 帳戶中建立新的託管區域。如果建立路由網域流量之託管區域的帳戶非您所有，您即無法控制流量的路由方式。

若要將現有的託管區域遷移至新的帳戶，請參閱將託管區域遷移到其他 AWS 帳戶。

若要建立新的託管區域，請參閱將 Amazon Route 53 設定為現有網域的 DNS 服務。當您將網域從其他註冊商轉移到 Route 53 時，通常會使用此主題，但是當您將網域從一個 AWS 帳戶轉移到另一個帳戶時，程序相同。

將網域從 Amazon Route 53 轉移到其他註冊商

當您將網域從 Amazon Route 53 轉移到其他註冊機構時，您會從 Route 53 取得一些資訊，並將這些資訊提供給新的註冊機構。新註冊商會完成其餘的工作。

> **Important**
>
> 如果您目前使用 Route 53 做為您的 DNS 服務提供者，並且還要將 DNS 服務轉移到另一個提供者，請注意，以下 Route 53 功能與其他 DNS 服務提供者提供的功能並沒有直接平行關係。您將需要與新的 DNS 服務提供者一起合作，來決定如何實現類似的功能：
>
> - 別名記錄。如需詳細資訊，請參閱 選擇別名或非別名記錄。
> - 簡易路由政策以外的路由政策。如需詳細資訊，請參閱 選擇路由政策。
> - 與記錄相關聯的運作狀態檢查。如需詳細資訊，請參閱 設定 DNS 備援。

大多數的網域註冊商強制要求將網域轉移到其他註冊商。這些要求的主要目的是防止詐騙網域擁有者不斷地將網域轉移至不同的註冊商。要求各有不同，但以下為典型要求：

- 您必須在至少 60 天前已向目前的註冊商註冊網域，或已將網域的註冊轉移到目前的註冊商。
- 如果網域名稱的註冊已過期，並且必須還原，則必須已在至少 60 天前還原。
- 網域不能有任何以下網域名稱狀態碼：

- pendingDelete
- pendingTransfer
- redemptionPeriod
- clientTransferProhibited

如需網域名稱狀態碼的目前清單和每個狀態碼意義的說明，請前往 ICANN 網站並搜尋 epp status codes。(在 ICANN 網站上搜尋；Web 搜尋有時會傳回舊版文件。)

> **Note**
>
> 如果您想要將網域轉移到其他網域註冊機構，但該網域註冊的 AWS 帳戶已關閉、暫停或終止，您可以聯絡 Sup AWS port 人員尋求協助。域名無法在註冊後的首個 14 天內轉移。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

> **Note**
>
> 如果新註冊商需要 REG-ID 代碼，您可以聯絡 Support 人員尋求 AWS 協助。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

若要將網域從 Route 53 轉移到其他註冊商

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 選擇您要轉移到其他註冊商的網域的名稱。
4. 在網域名稱頁面上，檢查網域名稱狀態碼的值。如果它是下列其中一個值，則目前無法轉移網域：

   - pendingDelete
   - pendingTransfer
   - redemptionPeriod
   - clientTransferProhibited
   - serverTransferProhibited

   如需網域名稱狀態碼的目前清單和每個狀態碼意義的說明，請前往 ICANN 網站並搜尋 epp status codes。(在 ICANN 網站上搜尋；Web 搜尋有時會傳回舊版文件。)

   如果網域名稱狀態碼的值為 serverTransferProhibited，您可以免費聯絡 Sup AWS port 人員，瞭解您必須執行哪些動作，才能轉移網域。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。
5. 如果轉移鎖定的值為開啟，請從動作下拉式選單中選擇關閉轉移鎖定。

   > **Note**
   >
   > 請聯絡 S AWS upport 部門以解除鎖定 .jp 網域的註冊商轉移作業。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

6. 除了 .be、.co.za、.es、.ru、.uk、.co.uk、.me、.uk 和 .org.uk 網域以外的所有網域 — 在「網域名稱」頁面上，從「轉出」下拉式清單中選擇「轉移到其他註冊商」。

   在轉移到其他註冊商對話方塊中，選擇複製以複製網域轉移的授權碼。您將在此程序的後續步驟中向您的註冊商提供此值。

   .be、.co.za、.es、.ru、英國、.co.uk、.uk、.uk 網域和 .org.uk 網域 — 請執行下列操作：

   .be 網域名稱

   請從註冊處取得 .be 網域的授權碼，請到 DNS 澳門網站。

.co.za 網域

您不需要取得授權碼就能將 .co.za 網域轉移至另一個註冊商。

.es 網域

您不需要取得授權碼就能將 .es 網域轉移至另一個註冊商。

.ru 網域

從 .ru 網域的登錄檔中取得授權碼，網址為 https://www.nic.ru/en/auth/recovery/：

a. 選擇要以網域名稱復原登入資料的選項。

b. 輸入您的網域名稱，然後選擇 Continue (繼續)。

c. 按照螢幕上提示來存取 RU-CENTER 管理頁面。

d. 在 Manage your account (管理您的帳戶) 區段中，選擇 Domain transfer (網域轉移)。

e. 使用 REGRU-RU 確認移轉。

.uk、.co.uk、.me.uk 和 .org.uk 網域

將 IPS 標籤變更為新註冊機構的值：

a. 前往 Nominet 網站的 Find a Registrar (尋找註冊機構) 頁面，然後尋找新註冊機構的 IPS 標籤。(Nominet 是 .uk、.co.uk、.me.uk 和 .org.uk 網域的註冊商。)

b. 在 Registered Domains > domain name (已註冊網域 > 網域名稱) 頁面的 IPS Tag (IPS 標籤)，選擇 Change IPS Tag (變更 IPS 標籤)，並指定您在步驟 7a 中取得的值。

c. 選擇更新。

7. 如果您目前不是使用 Route 53 做為網域的 DNS 服務提供者，請跳至步驟 10。

如果您目前使用 Route 53 做為網域的 DNS 服務提供者，請執行以下步驟：

a. 選擇 Hosted Zones (託管區域)。

b. 選擇您網域的託管區域名稱。網域和託管區域有相同的名稱。

c. 如果您想要繼續使用 Route 53 作為網域 DNS 服務提供者：取得 Route 53 指派給託管區域的四個名稱伺服器的名稱。如需詳細資訊，請參閱 取得公有託管區域的名稱伺服器。

如果不要繼續使用 Route 53 做為網域的 DNS 服務提供者：請記下除 NS 和 SOA 記錄之外，所有記錄的設定。針對 Route 53 特定的功能 (例如別名記錄)，您需要與新的 DNS 服務提供者一起合作，決定如何實現類似的功能。

8. 如果您要將 DNS 服務轉移到另一個供應商，請使用新的 DNS 服務提供的方法執行以下任務：

- 建立託管區域
- 建立記錄來重現 Route 53 記錄的功能
- 取得新的 DNS 服務指派給託管區域的名稱伺服器

9. 使用由新註冊商提供的程序來請求轉移網域。

   除了 .co.za、.es、.uk、.co.uk、.me.uk 和 .org.uk 網域以外的所有網域 — 系統會提示您在本程序的步驟 7 中輸入從 Route 53 主控台取得的授權碼。

10. 如果您仍然希望使用 Route 53 做為 DNS 服務提供者，請使用由新註冊機構提供的程序，來指定您在步驟 8 中取得的 Route 53 名稱伺服器的名稱。如果要使用其他 DNS 服務提供者，請指定當您在步驟 9 中建立新的託管區域時新提供者所提供的名稱伺服器的名稱。

11. 回應確認電子郵件：

    .jp 網域以外的所有網域

    Route 53 會傳送確認電子郵件到網域的註冊聯絡人的電子郵件地址：

    - 如果您未回覆此電子郵件，則轉移會在指定日期自動執行。
    - 如果您希望盡快執行轉移或希望取消轉移，請選擇電子郵件中的連結來移至 Route 53 網站，然後選擇適用的選項。
    - 依據 TLD，確認電子郵件可能包含指向 https://approvemove.com 的連結，從中可以批准或拒絕轉移。當網域聯絡人啟用隱私權保護時，電子郵件將從已向 Amazon Registrar 註冊的 TLD 的 identity-protect.org 地址傳送。若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

    .jp 網域

    Route 53 會寄送一封確認電子郵件至網域註冊人聯絡人的電子郵件地址：noreply@domainnameverification.net，其中包含確認轉移的連結：

    - 如果您未回應此電子郵件，則轉移會在指定日期取消。
    - 如果您希望盡快執行轉移或希望取消轉移，請選擇電子郵件中的連結來移至 Route 53 網站，然後選擇適用的選項。您需要提供步驟 7 中獲得的網域授權代碼。

    此外，您可能會收到來自 Wixi.jp 的電子郵件。您可以忽略此電子郵件。

12. 如果您要將網域移轉到註冊機構，而該註冊機構回報轉移失敗，請與該註冊機構聯繫以取得詳細資訊。當您將網域移轉到其他註冊機構時，所有狀態更新會移至新的註冊機構，因此 Route 53 不會擁有轉移失敗原因的相關資訊。

如果新註冊商回報轉移失敗，因為您從 Route 53 取得的授權碼無效，請向 Sup AWS port 人員提出案例。(您無需簽署支援合約，亦無需付費)。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

13. 如果您將 DNS 服務轉移到另一個 DNS 服務提供者，則可以在 DNS 解析程式停止回應包含 Route 53 名稱伺服器的名稱的 DNS 查詢之後刪除託管區域中的記錄並刪除託管區域。此程序通常需要兩天時間，這是 DNS 解析程式快取網域的名稱伺服器的名稱通常所需的時間量。

    > **Important**
    >
    > 如果您在 DNS 解析程式仍回應包含 Route 53 名稱伺服器的名稱的 DNS 查詢時刪除託管區域，網域在網際網路上會變得無法使用。

    在您刪除託管區域之後，Route 53 會停止計算託管區域的月費。如需詳細資訊，請參閱下列文件：

    - 刪除記錄
    - 刪除公有託管區域
    - Route 53 定價

Old console

若要將網域從 Route 53 轉移到其他註冊商

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇您要轉移到其他註冊商的網域的名稱。
4. 在已註冊的網域 網域名稱頁面上，檢查網域名稱狀態碼的值。如果它是下列其中一個值，則目前無法轉移網域：

    - pendingDelete
    - pendingTransfer
    - redemptionPeriod
    - clientTransferProhibited

- serverTransferProhibited

如需網域名稱狀態碼的目前清單和每個狀態碼意義的說明，請前往 ICANN 網站並搜尋 epp status codes。(在 ICANN 網站上搜尋；Web 搜尋有時會傳回舊版文件。)

如果網域名稱狀態碼的值為 serverTransferProhibited，您可以免費聯絡 Sup AWS port 人員，瞭解您必須執行哪些動作，才能轉移網域。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

5. 如果 Transfer lock (轉移鎖定) 的值是 Enabled (已啟用)，請選擇 Disable (停用)。

> **Note**
>
> 請聯絡 S AWS upport 部門以解除鎖定 .jp 網域的註冊商轉移作業。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

6. 選擇 Save (儲存)。
7. 除了 .be、.co.za、.es、.ru、.uk、.co.uk、.me.uk 和 .org.uk 網域以外的所有網域 — 在 [註冊的網域] > [網域名稱] 頁面上，在 [授權碼] 上，選擇 [取得代碼] 並記下授權碼。您將在此程序的後續步驟中向您的註冊商提供此值。

   .be、.co.za、.es、.ru、英國、.co.uk、.uk、.uk 網域和 .org.uk 網域 — 請執行下列操作：

   .be 網域名稱

   請從註冊處取得 .be 網域的授權碼，請到 DNS 澳門網站。

   .co.za 網域

   您不需要取得授權碼就能將 .co.za 網域轉移至另一個註冊商。

   .es 網域

   您不需要取得授權碼就能將 .es 網域轉移至另一個註冊商。

   .ru 網域

   從 .ru 網域的登錄檔中取得授權碼，網址為 https://www.nic.ru/en/auth/recovery/：

   a. 選擇要以網域名稱復原登入資料的選項。

   b. 輸入您的網域名稱，然後選擇 Continue (繼續)。

   c. 按照螢幕上提示來存取 RU-CENTER 管理頁面。

d. 在 Manage your account (管理您的帳戶) 區段中，選擇 Domain transfer (網域轉移)。

e. 使用 REGRU-RU 確認移轉。

.uk、.co.uk、.me.uk 和 .org.uk 網域

將 IPS 標籤變更為新註冊機構的值：

a. 前往 Nominet 網站的 Find a Registrar (尋找註冊機構) 頁面，然後尋找新註冊機構的 IPS 標籤。(Nominet 是 .uk、.co.uk、.me.uk 和 .org.uk 網域的註冊商。)

b. 在 Registered Domains > domain name (已註冊網域 > 網域名稱) 頁面的 IPS Tag (IPS 標籤)，選擇 Change IPS Tag (變更 IPS 標籤)，並指定您在步驟 7a 中取得的值。

c. 選擇更新。

8. 如果您目前不是使用 Route 53 做為網域的 DNS 服務提供者，請跳至步驟 10。

如果您目前使用 Route 53 做為網域的 DNS 服務提供者，請執行以下步驟：

a. 選擇 Hosted Zones (託管區域)。

b. 選擇您網域的託管區域名稱。網域和託管區域有相同的名稱。

c. 如果您想要繼續使用 Route 53 作為網域 DNS 服務提供者：取得 Route 53 指派給託管區域的四個名稱伺服器的名稱。如需詳細資訊，請參閱 取得公有託管區域的名稱伺服器。

如果不要繼續使用 Route 53 做為網域的 DNS 服務提供者：請記下除 NS 和 SOA 記錄之外，所有記錄的設定。針對 Route 53 特定的功能 (例如別名記錄)，您需要與新的 DNS 服務提供者一起合作，決定如何實現類似的功能。

9. 如果您要將 DNS 服務轉移到另一個供應商，請使用新的 DNS 服務提供的方法執行以下任務：

- 建立託管區域
- 建立記錄來重現 Route 53 記錄的功能
- 取得新的 DNS 服務指派給託管區域的名稱伺服器

10. 使用由新註冊商提供的程序來請求轉移網域。

除了 .co.za、.es、.jp、.uk、.co.uk、.me.uk 和 .org.uk 網域以外的所有網域 – 系統會提示您輸入在此程序的步驟 7 中從 Route 53 主控台取得的授權碼。

11. 如果您仍然希望使用 Route 53 做為 DNS 服務提供者，請使用由新註冊機構提供的程序，來指定您在步驟 8 中取得的 Route 53 名稱伺服器的名稱。如果要使用其他 DNS 服務提供者，請指定當您在步驟 9 中建立新的託管區域時新提供者所提供的名稱伺服器的名稱。

12. 回應確認電子郵件：

.jp 網域以外的所有網域

Route 53 會傳送確認電子郵件到網域的註冊聯絡人的電子郵件地址：

- 如果您未回覆此電子郵件，則轉移會在指定日期自動執行。
- 如果您希望盡快執行轉移或希望取消轉移，請選擇電子郵件中的連結來移至 Route 53 網站，然後選擇適用的選項。
- 依據 TLD，確認電子郵件可能包含指向 https://approvemove.com 的連結，從中可以批准或拒絕轉移。當網域聯絡人啟用隱私權保護時，電子郵件將從已向 Amazon Registrar 註冊的 TLD 的 identity-protect.org 地址傳送。若要確定您的 TLD 註冊商是誰，請參閱 尋找註冊商。

.jp 網域

Route 53 會寄送一封確認電子郵件至網域註冊人聯絡人的電子郵件地址：noreply@domainnameverification.net，其中包含確認轉移的連結：

- 如果您未回應此電子郵件，則轉移會在指定日期取消。
- 如果您希望盡快執行轉移或希望取消轉移，請選擇電子郵件中的連結來移至 Route 53 網站，然後選擇適用的選項。您需要提供步驟 7 中獲得的網域授權代碼。

此外，您可能會收到來自 Wixi.jp 的電子郵件。您可以忽略此電子郵件。

13. 如果您要將網域移轉到註冊機構，而該註冊機構回報轉移失敗，請與該註冊機構聯繫以取得詳細資訊。當您將網域移轉到其他註冊機構時，所有狀態更新會移至新的註冊機構，因此 Route 53 不會擁有轉移失敗原因的相關資訊。

    如果新註冊商回報轉移失敗，因為您從 Route 53 取得的授權碼無效，請向 Sup AWS port 人員提出案例。(您無需簽署支援合約，亦無需付費)。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

14. 如果您將 DNS 服務轉移到另一個 DNS 服務提供者，則可以在 DNS 解析程式停止回應包含 Route 53 名稱伺服器的名稱的 DNS 查詢之後刪除託管區域中的記錄並刪除託管區域。此程序通常需要兩天時間，這是 DNS 解析程式快取網域的名稱伺服器的名稱通常所需的時間量。

    > **Important**
    >
    > 如果您在 DNS 解析程式仍回應包含 Route 53 名稱伺服器的名稱的 DNS 查詢時刪除託管區域，網域在網際網路上會變得無法使用。

在您刪除託管區域之後，Route 53 會停止計算託管區域的月費。如需詳細資訊，請參閱下列文件：

- 刪除記錄
- 刪除公有託管區域
- Route 53 定價

重新傳送授權和確認電子郵件

對於與網域註冊相關的幾個操作，ICANN 要求我們從網域的註冊聯絡人取得授權，或確認註冊聯絡人的電子郵件地址有效。為取得授權或確認，我們會向您傳送一封內含連結的電子郵件。您有 3 到 15 天的時間來按一下該連結，具體時間取決於操作和頂層網域。在這之後，該連結將失效。

如果您未在分配的時間內按一下電子郵件中的連結，ICANN 通常會要求我們暫停網域或取消操作，具體取決於您嘗試執行的操作：

註冊網域

我們暫停網域，因此無法在網際網路上存取它。若要重新傳送確認電子郵件，請參閱為網域註冊重新傳送確認電子郵件。

僅限地理 TLD – 將網域轉移到 Amazon Route 53

如果您要轉移的網域有地理 TLD，我們會取消轉移。若要重新傳送授權電子郵件，請參閱為網域轉移重新傳送授權電子郵件。

> **Note**
>
> 有 .com、.net 或 .org 等一般 TLD 的網域不需要授權。

變更網域註冊聯絡人 (擁有者) 的姓名或電子郵件地址

我們取消變更。若要重新傳送授權電子郵件，請參閱重新傳送授權電子郵件以更新註冊聯絡人或刪除網域。

刪除網域

我們取消刪除請求。若要重新傳送授權電子郵件，請參閱重新傳送授權電子郵件以更新註冊聯絡人或刪除網域。

僅限地理 TLD – 從 Route 53 將網域轉移到另一個註冊機構

如果您要轉移的網域有地理 TLD，新的註冊機構會取消轉移。

> **Note**
>
> 有 .com、.net 或 .org 等一般 TLD 的網域不需要授權。

主題

- 更新您的電子郵件地址
- 重新傳送電子郵件

更新您的電子郵件地址

我們一律向網域的註冊聯絡人的電子郵件地址傳送確認和授權電子郵件。對於某些 TLD，我們需要在以下情況下向註冊聯絡人的新舊電子郵件地址傳送電子郵件：

- 您要變更已向 Amazon Route 53 註冊的網域的電子郵件地址
- 您即將變更的電子郵件地址屬於要轉移至 Route 53 的網域

重新傳送電子郵件

請依循適用的程序重新傳送確認或授權電子郵件。

- 為網域註冊重新傳送確認電子郵件
- 為網域轉移重新傳送授權電子郵件
- 重新傳送授權電子郵件以更新註冊聯絡人或刪除網域

為網域註冊重新傳送確認電子郵件

1. 檢查註冊聯絡人的電子郵件地址，並在必要時更新。如需更多詳細資訊，請參閱 更新網域的聯絡資訊和所有權。
2. 在電子郵件應用程式的垃圾郵件程式中，檢查是否有來自下列其中一個電子郵件地址的電子郵件。

   如果時間太久，該連結會失效，但我們會再向您傳送一封確認電子郵件 (這時您知道在哪裡找到確認電子郵件)。

TLD	發出核准或確認電子郵件的電子郵件地址
.fr	nic@nic.fr
所有其他	下列其中一個電子郵件地址： • noreply@registrar.amazon.com • noreply@domainnameverification.net

> **Note**
>
> 這些電子郵件可能包含指向 www.verify-whois.com 的連結。您可以放心使用此連結。

3. 使用 Amazon Route 53 主控台重新傳送確認電子郵件：

   a. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。

   b. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。

   c. 選擇要為其重新傳送電子郵件的網域的名稱。

   d. 在標題為 "Your domain might be suspended" (您的網域可能已暫停) 的警告方塊中，選擇 Send email again (再次傳送電子郵件)。

   > **Note**
   >
   > 如果沒有警告方塊，則表示您已確認註冊聯絡人的電子郵件地址有效。

4. 如果重新傳送確認電子郵件時遇到問題，您可以免費聯絡 AWS Support。如需更多詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

為網域轉移重新傳送授權電子郵件

此方法不適用於 .jp 網域轉移要求。

1. 使用目前網域註冊商提供的方法，確認網域的隱私權保護是否已停用。如果沒有，請停用它。

   我們會向目前註冊商儲存在 WHOIS 資料庫中的電子郵件地址傳送授權電子郵件。啟用隱私權保護時，該電子郵件地址通常是混淆形式。目前註冊商可能不會將 Amazon Route 53 傳送到 WHOIS 資料庫中的電子郵件地址的電子郵件轉寄到您的實際電子郵件地址。

   > **Note**
   >
   > 如果目前的網域註冊機構不讓您關閉隱私保護，只要您指定 步驟 5：請求轉移 中的有效授權程式碼，我們仍然可以轉移網域。

2. 檢查註冊聯絡人的電子郵件地址，並在必要時更新。使用目前網域註冊商提供的方法。
3. 在電子郵件應用程式的垃圾郵件程式中，檢查是否有來自下列其中一個電子郵件地址的電子郵件。

   如果時間太久，該連結會失效，但我們會再向您傳送一封授權電子郵件 (這時您知道在哪裡找到授權電子郵件)。

TLD	發出核准或確認電子郵件的電子郵件地址
.com.au 和 .net.au	no-reply@ispapi.net 此電子郵件包含 https://approve.domainadmin.com 的連結。
.fr	nic@nic.fr
所有其他	下列其中一個電子郵件地址： • noreply@registrar.amazon.com • noreply@domainnameverification.net

> **Note**
>
> 這些電子郵件可能包含指向 www.verify-whois.com 的連結。您可以放心使用此連結。

4. 如果轉移已停止 (例如我們因為時間太長而取消轉移)，請再次請求轉移，我們會向您傳送另一封授權電子郵件。

   > **Note**
   >
   > 在您請求轉移後的前 15 天，您可以透過檢查 Route 53 主控台的 Dashboard (儀表板) 頁面上的 Notifications (通知) 表格，判斷轉移的狀態。在 15 天後，請使用 AWS CLI 以取得狀態。如需詳細資訊，請參閱 AWS CLI 命令參考中的 route53domains。

   如果轉移仍在進行，請執行以下步驟重新傳送授權電子郵件。

   a. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
   b. 在 Notifications (通知) 表格中，尋找您要轉移的網域。
   c. 在該網域的 Status (狀態) 欄中，選擇 Resend email (重新傳送電子郵件)。

5. 如果重新傳送網域轉移的授權電子郵件時遇到問題，您可以免費聯絡 AWS Support。如需更多詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

重新傳送授權電子郵件以更新註冊聯絡人或刪除網域

1. 檢查註冊聯絡人的電子郵件地址，並在必要時更新。如需更多詳細資訊，請參閱 更新網域的聯絡資訊和所有權。
2. 在電子郵件應用程式的垃圾郵件程式中，檢查是否有來自下列其中一個電子郵件地址的電子郵件。

   如果時間太久，該連結會失效，但我們會再向您傳送一封授權電子郵件 (這時您知道在哪裡找到授權電子郵件)。

TLD	發出授權電子郵件的電子郵件地址
.fr	nic@nic.fr
所有其他	下列其中一個電子郵件地址： • noreply@registrar.amazon.com • noreply@domainnameverification.net

TLD	發出授權電子郵件的電子郵件地址

> **Note**
>
> 這些電子郵件可能包含指向 www.verify-whois.com 的連結。您可以放心使用此連結。

3. 取消變更或刪除。您有兩種選擇：
   - 您可以等待 3 到 15 天，之後我們會自動取消請求的操作。
   - 或者，您可以聯絡 AWS Support，要求他們取消操作。
4. 取消變更或刪除後，您可以再次變更聯絡資訊或刪除網域，我們會向您傳送另一封授權電子郵件。
5. 如果重新傳送授權電子郵件時遇到問題，您可以免費聯絡 AWS Support。如需更多詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

設定網域的 DNSSEC

攻擊者有時會透過攔截 DNS 查詢並向 DNS 解析程式傳回自己的 IP 地址而不是網際網路端點的實際 IP 地址，來劫持通往這些端點的流量。然後系統會將使用者路由到攻擊者在詐騙回應中提供的 IP 地址，例如假網站。

可以透過設定用於確保 DNS 流量安全的通訊協定 – 網域名稱系統安全延伸 (DNSSEC)，來保護網域不受此類攻擊，稱為 DNS 詐騙或中間人攻擊。

> **Important**
>
> Amazon Route 53 支援 DNSSEC 簽署和 DNSSEC 以進行網域註冊。如果要為向 Route 53 註冊的網域設定 DNSSEC 簽署，請參閱 在 Amazon Route 53 中設定 DNSSEC 簽署。

主題

- DNSSEC 如何保護網域的概觀
- 為網域設定 DNSSEC 的先決條件和上限
- 為網域新增公開金鑰
- 刪除網域的公開金鑰

DNSSEC 如何保護網域的概觀

當您為網域設定 DNSSEC，DNS 解析程式會為來自中間解析程式的回應建立信任鏈。該信任鏈從網域 (您的網域的父區域) 的 TLD 註冊機構開始，至 DNS 服務提供者的授權名稱伺服器結束。並非所有 DNS 解析程式都支援 DNSSEC。只有支援 DNSSEC 的解析程式會執行所有簽章或真實性驗證。

為清晰起見，下面簡要說明如何為向 Amazon Route 53 註冊的網域設定 DNSSEC，以保護您的網際網路主機不受 DNS 詐騙：

1. 使用由 DNS 服務提供者提供的方法，透過非對稱金鑰對中的私有金鑰來簽署託管區域內的記錄。

   > **Important**
   >
   > Route 53 支援 DNSSEC 簽署和 DNSSEC 以進行網域註冊。如需進一步了解，請參閱在 Amazon Route 53 中設定 DNSSEC 簽署。

2. 將金鑰對中的公有金鑰提供給您的網域註冊商，並指定用於產生金鑰對的演算法。網域註冊商會將公開金鑰和演算法轉送給頂層網域 (TLD) 的註冊機構。

   如需如何為已向 Route 53 註冊的網域執行此步驟的資訊，請參閱 為網域新增公開金鑰。

在您設定 DNSSEC 之後，下面說明如何保護您的網域不受 DNS 詐騙：

1. 提交 DNS 查詢，例如透過瀏覽到網站或傳送電子郵件訊息。
2. 請求路由到 DNS 解析程式。解析程式負責根據請求向用戶端傳回適當的值，例如，執行 Web 伺服器或電子郵件伺服器的主機的 IP 地址。
3. 如果該 IP 地址已在 DNS 解析程式中快取 (因為其他人已提交過相同的 DNS 查詢，且解析程式已取得該值)，解析程式會將該 IP 地址傳回給提交請求的用戶端。然後用戶端使用該 IP 地址來存取主機。

   如果該 IP 地址未在 DNS 解析程式中快取，解析程式將向您的網域的父區域傳送請求，在 TLD 註冊機構該操作會傳回兩個值：

   - 委派簽署人 (DS) 記錄，這是與用來簽署記錄的私有金鑰對應的公開金鑰。
   - 網域的授權名稱伺服器的 IP 地址。
4. DNS 解析程式將原始請求傳送到另一個 DNS 解析程式。如果該解析程式沒有此 IP 地址，它會重複此程序，直到解析程式將請求傳送到位於您的 DNS 服務提供者的名稱伺服器。名稱伺服器會傳回兩個值：

- 網域的記錄，例如 example.com。這通常包含主機的 IP 地址。
- 您在設定 DNSSEC 時建立的記錄的簽章。

5. DNS 解析程式使用您向網域註冊商提供的公開金鑰 (註冊商再將其轉送給 TLD 註冊機構) 來執行下面的兩項操作：
   - 建立信任鏈。
   - 驗證來自 DNS 服務提供者的已簽署回應合法，並且未被攻擊者的錯誤回應取代。
6. 如果回應是真實的，解析程式會將該值傳回給提交請求的用戶端。

   如果回應無法驗證，解析程式會傳回錯誤給使用者。

   如果網域的 TLD 註冊機構沒有網域的公開金鑰，解析程式會使用它從 DNS 服務提供者取得的回應來回應 DNS 查詢。

為網域設定 DNSSEC 的先決條件和上限

若要為網域設定 DNSSEC，您的網域和 DNS 服務提供者必須符合以下先決條件：

- TLD 的註冊機構必須支援 DNSSEC。若要判斷您的 TLD 註冊機構是否支援 DNSSEC，請參閱可向 Amazon Route 53 註冊的網域。
- 網域的 DNS 服務提供者必須支援 DNSSEC。

> **Important**
>
> Route 53 支援 DNSSEC 簽署和 DNSSEC 以進行網域註冊。如需進一步了解，請參閱在 Amazon Route 53 中設定 DNSSEC 簽署。

- 您必須與 DNS 服務提供者設定 DNSSEC，然後才能將網域的公開金鑰新增到 Route 53。
- 可以新增到網域的公開金鑰數目取決於網域的 TLD：
  - .com 和 .net 網域 – 最多 13 個金鑰
  - 所有其他網域 – 最多 4 個金鑰

為網域新增公開金鑰

您在輪換金鑰或為網域啟用 DNSSEC 時，請在與網域的 DNS 服務提供者設定 DNSSEC 之後執行以下程序。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

若要為網域新增公開金鑰

1. 如果您尚未與您的 DNS 服務提供者設定 DNSSEC，請使用您的服務提供者提供的方法來設定 DNSSEC。
2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
4. 選擇要新增金鑰的網域的名稱。
5. 選擇 DNSSEC 金鑰索引標籤，然後選擇新增金鑰。
6. 指定下列值：

   Key type

   選擇您要上傳金鑰簽署金鑰 (KSK) 或區域簽署金鑰 (ZSK)。

   演算法

   選擇您用來簽署託管區域記錄的演算法。

   公有金鑰

   指定您與 DNS 服務提供者設定 DNSSEC 時所使用非對稱金鑰對中的公開金鑰。

   注意下列事項：

   - 請指定公開金鑰，而非摘要。
   - 您必須指定 base64 格式的金鑰。
7. 選擇 Add (新增)。

> **Note**
>
> 您一次只能新增一個公開金鑰。如果您需要新增更多金鑰，請等待，直到您從 Route 53 收到確認電子郵件。

8. 當 Route 53 收到來自註冊機構的回應時，我們會向網域的註冊聯絡人傳送電子郵件。電子郵件會確認已將公開金鑰新增到註冊機構的網域或解釋無法新增金鑰的原因。

Old console

若要為網域新增公開金鑰

1. 如果您尚未與您的 DNS 服務提供者設定 DNSSEC，請使用您的服務提供者提供的方法來設定 DNSSEC。
2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
4. 選擇要新增金鑰的網域的名稱。
5. 在 DNSSEC status (DNSSEC 狀態) 欄位，選擇 Manage keys (管理金鑰)。
6. 指定下列值：

   Key type

   選擇您要上傳金鑰簽署金鑰 (KSK) 或區域簽署金鑰 (ZSK)。

   演算法

   選擇您用來簽署託管區域記錄的演算法。

   公有金鑰

   指定您與 DNS 服務提供者設定 DNSSEC 時所使用非對稱金鑰對中的公開金鑰。

   注意下列事項：

   - 請指定公開金鑰，而非摘要。
   - 您必須指定 base64 格式的金鑰。
7. 選擇 Add (新增)。

> **Note**
>
> 您一次只能新增一個公開金鑰。如果您需要新增更多金鑰，請等待，直到您從 Route 53 收到確認電子郵件。

8. 當 Route 53 收到來自註冊機構的回應時，我們會向網域的註冊聯絡人傳送電子郵件。電子郵件會確認已將公開金鑰新增到註冊機構的網域或解釋無法新增金鑰的原因。

刪除網域的公開金鑰

您在輪換金鑰或為網域停用 DNSSEC 時，請執行以下程序刪除公開金鑰，然後與網域的 DNS 服務提供者停用 DNSSEC。注意下列事項：

- 如果您要輪換金鑰，我們建議您在新增新的公開金鑰之後最多等待 3 天，再刪除舊的公開金鑰。
- 如果您要停用 DNSSEC，請先刪除網域的公開金鑰。我們建議您最多等待 3 天，再與網域的 DNS 服務提供者停用 DNSSEC。

> **Important**
>
> 如果已為網域啟用 DNSSEC 並與 DNS 服務停用 DNSSEC，則支援 DNSSEC 的 DNS 解析程式將向用戶端傳回 `SERVFAIL` 錯誤，用戶端將無法存取與該網域關聯的端點。

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

若要刪除網域的公開金鑰

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 選擇要刪除金鑰的網域的名稱。
4. 在 DNSSEC 金鑰索引標籤中，選擇要刪除之金鑰旁邊的選項按鈕，然後選擇刪除金鑰。
5. 在刪除 DNSSEC 金鑰對話方塊中，在文字方塊內輸入刪除，以確認您要刪除此金鑰，然後選擇刪除。

> **Note**
>
> 您一次只能刪除一個公開金鑰。如果您需要刪除更多金鑰，請等待，直到您從 Amazon Route 53 收到確認電子郵件。

6. 當 Route 53 收到來自註冊機構的回應時，我們會向網域的註冊聯絡人傳送電子郵件。電子郵件會確認已從註冊機構的網域刪除公開金鑰或解釋無法刪除金鑰的原因。

Old console

若要刪除網域的公開金鑰

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 選擇要刪除金鑰的網域的名稱。
4. 在 DNSSEC status (DNSSEC 狀態) 欄位，選擇 Manage keys (管理金鑰)。
5. 找到您要刪除的金鑰，然後選擇 Delete (刪除)。

> **Note**
>
> 您一次只能刪除一個公開金鑰。如果您需要刪除更多金鑰，請等待，直到您從 Amazon Route 53 收到確認電子郵件。

6. 當 Route 53 收到來自註冊機構的回應時，我們會向網域的註冊聯絡人傳送電子郵件。電子郵件會確認已從註冊機構的網域刪除公開金鑰或解釋無法刪除金鑰的原因。

尋找您的註冊商和有關您網域的其他資訊

若要使用 GetDomainDetailAPI 檢視網域資訊，您可以使用任何 SDK 或 AWS CLI. 如需詳細資訊，請參閱get-domain-detail。

若要檢視包含 **get-domain-detail** CLI 的網域相關資訊

- 使用下列 CLI：

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> 這個命令只能在我們東 AWS 區域部 -1 中運行。

有關您網域的所有資訊都將列在輸出中，包括註冊商、註冊日期、隱私權設定等。

檢視已向 Route 53 註冊之網域的相關資訊

您可以檢視有關使用 Route 53 註冊的網域的資訊。這些資訊包括網域最初註冊的時間，以及網域擁有者以及技術、管理和帳單聯絡人的聯絡資訊。

WHOIS

WHOIS 是一個免費的公開目錄，其中包含有關網域註冊商和註冊機構贊助的網域的資訊。它既作為接受連接埠 43 上查詢的服務提供，又作為網站提供，服務和網站都可透過 IPv4 和 IPv6 存取。WHOIS 是一種分散式階層查詢。如需詳細資訊，請參閱關於 WHOIS。

向不同層級的階層發出的 WHOIS 請求可提供不同的資訊：

- 向根 WHOIS (whois.iana.org) 發出的請求可提供有關註冊機構的資訊。

- 向註冊機構 WHOIS 發出的請求可提供有關註冊商的資訊，以及有關網域的一些公開資訊。
- 向註冊商 WHOIS 發出的請求可提供有關網域的所有公開資訊。

WHOIS 有多個層級，包括 TLD 註冊機構和網域註冊商操作的 WHOIS 查詢，因此在 Route 53 主控台上關閉隱私權保護，只能在註冊商提供的 WHOIS 上關閉。無論您是否使用 Route 53 關閉，有些註冊機構都會故意為其 WHOIS 查詢服務維護隱私權保護或修訂服務。若要取得有關網域的完整資訊，我們建議您使用註冊商提供的 WHOIS。

注意下列事項：

啟用隱私權保護時，請傳送電子郵件給網域聯絡人

如果已為網域啟用隱私權保護，註冊者、技術和管理聯絡人的聯絡資訊會取代為 Amazon Registrar 隱私權服務的聯絡資訊。例如，若 example.com 網域已向 Amazon Registrar 註冊，且若已啟用隱私權保護，則 WHOIS 查詢回應中註冊者電子郵件的值會類似於 owner1234@example.com.identity-protect.org。

若要在啟用隱私權保護時聯絡一或多位網域聯絡人，請傳送電子郵件到適用的電子郵件地址。我們會自動將您的電子郵件轉寄給適用的聯絡人。

檢舉濫用情況

若要舉報任何非法活動或違反可接受之使用政策的行為，包括不適當的內容、網路釣魚、惡意軟體或垃圾郵件，請傳送電子郵件至 abuse@amazon.com。

檢視有關已向 Route 53 註冊之網域的資訊

1. 在 Web 瀏覽器中，前往下列其中一個網站：
   - Amazon Registrar WHOIS：https://registrar.amazon.com/whois
   - Amazon Registrar RDAP：https://registrar.amazon.com/rdap
   - Gandi WHOIS：https://whois.gandi.net
2. 請輸入您要檢視相關資訊的網域名稱，然後選擇 Search (搜尋)。

刪除網域名稱註冊

對於大多數頂層網域 (TLD)，可在不再需要網域時刪除註冊。如果註冊機構允許刪除註冊，請執行此主題中的程序。

注意下列事項：

無法退款註冊費

如果您在排定到期日之前刪除註冊的網域名稱， AWS 不會退還註冊費。

可讓您刪除網域註冊的 TLD

若要判斷您是否可以刪除網域註冊，請參閱可向 Amazon Route 53 註冊的網域。如果 TLD 區段不含「刪除網域註冊」小區段，則您可以刪除網域。刪除網域之前，請先確定您已停用網域鎖定。如需停用網域鎖定的詳細資訊，請參閱DisableDomainTransferLock。

如果無法刪除網域註冊怎麼辦？

如果網域的註機機構不允許您刪除網域名稱註冊，您必須等到網域過期。為了確保網域不會自動續約，請停用網域自動續約。當 Expires on (過期日期) 已過，Route 53 會自動刪除註冊的網域。有關如何變更自動續約設定的詳細資訊，請參閱啟用或停用網域自動續約。

在網域刪除且可供再次註冊之前的延遲

幾乎所有註冊機構會防止任何人立即註冊剛過期的網域。通常是延遲一到三個月，這取決於 TLD。如需詳細資訊，請參閱 可向 Amazon Route 53 註冊的網域 中的 TLD 的「續約及還原網域的截止日期」一節。

> **Important**
>
> 如果您只想在 AWS 帳戶之間轉移域名或將域名轉移到另一個註冊商，請勿刪除域名，並希望重新註冊該域名。請改以參閱適用的文件：
>
> - 將網域轉移到其他 AWS 帳戶
> - 將網域從 Amazon Route 53 轉移到其他註冊商

> **Note**
>
> 我們正在更新 Route 53 的網域主控台。在轉換期間，您可以繼續使用舊的主控台。

選擇您正在使用的主控台的索引標籤。

- 新主控台
- 舊主控台

New console

刪除網域名稱註冊

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered domains (已註冊的網域)。
3. 選擇網域名稱。

   如果您要刪除 .co.uk、.me.uk、.org.uk 或 .uk 網域，請參閱 若要刪除 .uk 網域名稱註冊，請執行下列步驟：。
4. 如果 TLD 註冊機構允許刪除網域名稱註冊，請選擇刪除網域。

   某些網域可能會要求我們傳送一封電子郵件給該網域註冊者，以驗證註冊者是否想要刪除該網域。如果您希望接收電子郵件，它將從下列其中一個電子郵件地址寄出：

   - noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD。
   - noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD。

   若要確定您的 TLD 註冊商是誰，請參閱 可向 Amazon Route 53 註冊的網域。
5. 如果您收到驗證電子郵件，請選擇電子郵件中的連結，核准或拒絕刪除網域的請求。

   > **Important**
   >
   > 註冊聯絡人必須按照電子郵件中的指示操作，否則我們必須根據 ICANN 的要求，在五天後取消刪除請求。

   當您的網域已刪除，您會收到另一封電子郵件。若要確定請求的最新狀態，請參閱 檢視網域註冊的狀態。
6. 在已刪除網域的託管區域中刪除記錄，然後刪除託管區域。在您刪除託管區域之後，Route 53 會停止計算託管區域的月費。如需詳細資訊，請參閱下列 文件：

   - 刪除記錄
   - 刪除公有託管區域
   - Route 53 定價

7. 如果您在刪除網域名稱註冊時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Old console

刪除網域名稱註冊

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇網域名稱。

   如果您要刪除 .co.uk、.me.uk、.org.uk 或 .uk 網域，請參閱 若要刪除 .uk 網域名稱註冊，請執行下列步驟：。
4. 選擇 Delete Domain (刪除網域)。
5. 如果 TLD 註冊機構允許刪除註冊的網域名稱，請選擇 Delete Domain (刪除網域)。

   我們會傳送一封電子郵件給網域註冊者，以驗證註冊者要刪除網域。(這是 ICANN 要求。) 電子郵件來自下列其中一個電子郵件地址：

   - noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD。
   - noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD。

   若要確定您的 TLD 註冊商是誰，請參閱 可向 Amazon Route 53 註冊的網域。
6. 當您收到驗證的電子郵件時，請選擇電子郵件中的連結，核准或拒絕刪除網域的請求。

   > **Important**
   >
   > 註冊聯絡人必須按照電子郵件中的指示操作，否則我們必須根據 ICANN 的要求，在五天後取消刪除請求。

   當您的網域已刪除，您會收到另一封電子郵件。若要確定請求的最新狀態，請參閱 檢視網域註冊的狀態。
7. 在已刪除網域的託管區域中刪除記錄，然後刪除託管區域。在您刪除託管區域之後，Route 53 會停止計算託管區域的月費。如需詳細資訊，請參閱下列 文件：

- 刪除記錄
- 刪除公有託管區域
- Route 53 定價

8. 如果您在刪除網域名稱註冊時遇到問題，可以免費聯絡 Sup AWS port 部門。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

若要刪除 .uk 網域名稱註冊，請執行下列步驟：

如果您想要刪除 .co.uk、.uk、.org.uk 或 .uk 網域，您可以使用名稱建立一個帳戶，也就是 .uk 網域的註冊處。如需詳細資訊，請參閱 Nominet 網站上的「取消您的網域名稱」，https://www.nominet.uk/domain-support/。

> **Important**
>
> 如果您刪除 (取消) .uk 網域，該網域將於當日結束時刪除，並成為可供任何人註冊。如果您只想轉移網域，請勿將其刪除。

下列為此程序的概觀：

1. 在 Nominet 網站上，按照指示來第一次登入。請參閱 https://secure.nominet.org.uk/auth/login.html。Nominet 向您發送一封包含建立密碼指示的電子郵件。
2. 按照您從 Nominet 收到的電子郵件中的指示操作。
3. 登入 Nominet 網站，並按照指示取消 (刪除) 網域。

就網域註冊問題聯絡 S AWS upport

AWS 為所有客戶提供免費的基本支援方 AWS 案。此計劃包含協助處理以下有關網域註冊的問題：

- 將網域轉移到 Amazon Route 53 或從中轉移網域
- 在 AWS 帳戶之間轉移網域
- 提高 Route 53 實體的配額，例如，可以註冊的網域數目 (請參閱 配額)。
- 變更網域擁有者
- 變更網域擁有者的聯絡資訊
- 重新傳送確認和授權電子郵件

- 續約網域
- 還原過期的網域
- 取得 Route 53 帳單資訊
- 提供 .uk 網域的身分證明
- 關閉 AWS 帳戶後刪除網域或停用自動續約

若要聯絡 Sup AWS port 部門以及其他與網域註冊相關的問題，請執行適用的程序。

主題

- 如果您可以登入您的 AWS 帳戶，請聯絡 AWS Support 部門
- 如果您無法登入 AWS 帳戶，請聯絡 AWS Support 部門

如果您可以登入您的 AWS 帳戶，請聯絡 AWS Support 部門

若要在您能夠登入 AWS 帳戶時聯絡 Sup AWS port 部門，請執行下列步驟：

1. 使用網域目前註冊的 AWS 帳戶登入 Sup AWS port 中心。

   > **Important**
   >
   > 您必須使用網域目前註冊到的根帳戶登入。此要求可防止未經授權的使用者攔截您的帳戶。

2. 指定下列值：

   Regarding

   接受預設值 Account and Billing Support (帳戶與帳單支援)。

   服務

   接受 Billing (帳單) 預設值。

   類別

   接受 Domain name registration issue (網域名稱註冊問題) 預設值。

   嚴重性

   選擇適用的嚴重性。

主旨

輸入問題的簡短摘要。

描述

詳細描述您發生的問題，並附上所有相關文件或螢幕擷取畫面。

聯絡方式

選擇聯絡方式 Web。我們會使用與您 AWS 帳戶相關聯的電子郵件地址與您聯絡。

3. 選擇提交。

如果您無法登入 AWS 帳戶，請聯絡 AWS Support 部門

若要在您無法登入 AWS 帳戶時聯絡 Sup AWS port 部門，請執行下列步驟：

1. 前往「我是 AWS 客戶，我正在尋找帳單或帳戶支援」頁面。
2. 填寫表單。
3. 選擇提交。

下載網域帳單報告

如果您的 AWS 帳單是以信用卡收取費用，每筆網域交易都會收到個別的發票。這些發票不含網域名稱。如果您管理多個網域，而且您想要依網域檢視特定期間的費用，您可以下載網域帳單報告。此報告包括適用於網域註冊的所有費用，包括下列項目：

- 註冊網域
- 續約網域的註冊
- 將網域轉移到 Amazon Route 53
- 變更網域擁有者 (對於某些 TLD，此操作是免費的)

> **Note**
>
> 如果您使用已開發票付款，任何 Route 53 網域註冊交易都會顯示在您的月結 AWS 單中。發票包含每項費用適用的網域名稱和操作。

有時候，您的帳單報告可能會顯示涵蓋未來的帳單週期。這是因為網域自動續約程序會在網域到期前一個月開始。因此，舉例來說，在 8 月的報告中，您可能會看到在 9 月之後開始的帳單週期，直到次年 9 月為止。

當您使用主控台執行報告時，您可以選擇下列選項：

- 過去 12 個月：報告包含從您執行報告前一年到目前日期的費用。例如，如果您在 6 月 3 日執行報告，其中包含從前一年 6 月 3 日到當天的費用。
- 去年的個別月份：報告包含指定月份的費用。

如果您以程式設計方式執行報表，則可以取得從 2014 年 7 月 31 日開始之任何日期範圍的費用。這是 Route 53 開始支援網域註冊的日期。例如，請參閱 AWS CLI 命令參考中的 view-billing。

CSV 格式的帳單報告包含以下值：

- 出現費用的 AWS 商業發票識別碼。
- 操作 (REGISTER_DOMAIN、RENEW_DOMAIN、TRANSFER_IN_DOMAIN 或 CHANGE_DOMAIN_OWNER)。
- 網域的名稱。
- 以美元表示的操作費用。
- 採用 ISO 8601 格式的日期和時間，例如 2016-03-03T19:20:25.177Z。如需有關 ISO 8601 格式的詳細資訊，請參閱 Wikipedia 文章 ISO 8601。

若要下載網域帳單報告

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇 Domain billing report (網域帳單報告)。
4. 選擇報告的日期範圍，然後選擇 Download domain report (下載網域報告)。
5. 依照提示開啟報告或儲存報告。
6. 如果您在下載網域帳單報告時遇到問題，可以免費聯絡 Sup AWS port 務。如需更多詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

可向 Amazon Route 53 註冊的網域

下列一般和地理頂層網域清單顯示可用來向 Amazon Route 53 註冊網域的頂層網域 (TLD)。

向 Route 53 註冊網域

TLD 註冊機構向一些網域名稱指派特殊或優惠的價格。您無法使用 Route 53 註冊具有特殊或高級價格的網域。可以向 Route 53 註冊的 TLD 包含在以下清單中。如果不包含 TLD，則無法向 Route 53 註冊網域。

將網域轉移至 Route 53

如果 TLD 包含在以下清單，您可以將網域轉移至 Route 53。如果不包含 TLD，則無法將網域轉移至 Route 53。

對於大多數 TLD，您需要從目前的註冊商取得授權碼才能轉移網域。若要判斷是否需要授權碼，請參閱您的 TLD 的「需要授權碼才能轉移至 Route 53」一節。

網域註冊和轉移的定價

如需有關註冊網域或將網域轉移至 Route 53 的費用資訊，請參閱 Amazon Route 53 網域註冊的定價。

使用 Route 53 做為您的 DNS 服務

您可以使用 Route 53 做為任何網域的 DNS 服務，即使網域的 TLD 不包含在以下清單。如需有關 Route 53 做為 DNS 服務的詳細資訊，請參閱 如何將網際網路流量路由到您的網站或 Web 應用程式。如需如何將網域的 DNS 服務轉移至 Route 53 的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

國際化網域名稱

並非所有 TLD 都支援國際化網域名稱 (IDN)，即包含 ASCII 字元 a-z、0-9 和 - (連字號) 以外之字元的網域名稱。每個 TLD 的清單表示該 TLD 是否支援 IDN。如需國際化網域名稱的詳細資訊，請參閱DNS 網域名稱格式。

使用 TLD 註冊地理網域

地理 TLD 註冊規則因國家/地區而異。有些國家/地區不受限制，也就是說世界上任何人都可以註冊，而有些國家/地區有特定限制，例如居留權。每個地理 TLD 的清單表示任何限制。

支援的頂層網域的索引

主題

- 一般頂層網域
- 地理頂層網域

一般頂層網域

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, . 啤酒。 ,.bet, . 投標, .bike, .bingo, . 生物。 , .biz, .black, .blue, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, . 聖誕節。 , .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, . 聯繫。 , .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deals, .degree, .delivery, .democrat, .dental, . 設計。 , .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, . 風扇。 , .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, . 樂趣。 , .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, . 法律。, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol, . 有限公司

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub. .pw (帛琉)

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, . 購物。, .show, .singles, .site, . 滑雪。, .soccer, .social, .solar, .solutions, . 軟體。, .space, .store, . 流, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team, .tech,.technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, . 投票。, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, . 工作。, .works, .world, .wtf, .xyz, .zone

地理頂層網域

非洲

.ac (亞森欣島), .co.za (南非), .sh (聖赫勒拿島)

美洲

.ca (加拿大), .cl (智利), .co (哥倫比亞), .com.ar (阿根廷), .com.br (巴西), com.mx (墨西哥), .mx (墨西哥), .us (美國), .vc (聖文森及格瑞那丁), .vg (英屬維京群島)

亞洲/大洋洲

.au (澳洲), .cc (可可斯群島), .co.nz (紐西蘭), .com.au (澳洲), .com.sg (新加坡共和國), .fm (密克羅尼西亞聯邦), .in (印度), .jp (日本), .io (英屬印度洋領地), .net.au (澳洲), .net.nz (紐西蘭), .org.nz (紐西蘭), .pw (帛琉), .qa (卡達), .ru (俄羅斯聯邦), .sg (新加坡共和國)

歐洲

.be (比利時), .berlin (德國柏林市), .ch (瑞士), .co.uk (英國), .cz (捷克共和國), .de (德國), .es (西班牙) , .eu (歐盟), .fi (芬蘭), .fr (法國), .gg (耿西島), .im (曼島), .it (義大利), .me (蒙特內哥羅), .me.uk (英國), .nl (荷蘭), .org.uk (英國), .ruhr (魯爾區，位於德國西部), .se (瑞典), .uk (英國), .wien (奧地利維也納市)

一般頂層網域

一般頂層網域 (gTLD) 是全球使用且公認的全球網域域名，例如 .com、.net 和 .org。一般頂層網域也包含專業網域，例如 .bike、.condos 和 .marketing。

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, . 啤酒。, .bet, . 投標, .bike, .bingo, . 生物。, .biz, .black, .blue, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .church, . 聖誕節。, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, . 聯繫。, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deals, .degree, .delivery, .democrat, .dental, . 設計。, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, . 風扇。, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, . 樂趣。, .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, . 法律。 , .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol , . 有限公司

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, . 購物。, .show, .singles, .site, . 滑雪。, .soccer, .social, .solar, .solutions, . 軟體。, .space, .store, . 流, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team,.tech, .technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, . 投票。, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, . 工作。, .works, .world, .wtf, .xyz, .zone

.ac

請參閱 .ac (亞森欣島)。

Return to index

.academy

供學校和大學等教育機構使用。此外，教育機構附屬的招募人員、顧問、廣告商、學生、老師和行政人員也使用該網域域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.accountants

供會計業附屬的企業、集團和個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.actor

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天

- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.adult

供僅託管成人內容的網站使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.agency

供識別為代理機構的任何企業或集團使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.airforce

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.apartments

供房仲業者、房東和房客使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.associates

供名稱中包含 "associates" 一字的企業和公司使用。想要指出其組織專業性質的任何集團或代理機構也使用該網域域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.auction

用於與拍賣相關的活動以及拍賣型購買和銷售。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、西班牙文和拉丁文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.audio

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .audio 網域或將 .audio 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .audio 網域。

供影音產業以及對廣播、音響設備、音訊製作和音訊串流有興趣的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .audio 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.band

用於分享樂團和樂團活動的資訊。此外，音樂家也使用該網域域名與其粉絲交流及銷售樂團相關的商品。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、西班牙文和拉丁文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.bargains

用於銷售和促銷活動的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 啤酒。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.bet

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 投標

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天

- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.bike

供為自行車騎士提供服務的企業或集團使用，例如自行車店、摩托車行和修車店。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.bingo

供線上遊戲網站使用或用於分享有關賓果遊戲的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 生物。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.biz

供企業或商業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援簡體中文、繁體中文、丹麥文、芬蘭文、德文、匈牙利文、日文、韓文、拉脫維亞文、立陶宛文、挪威文、波蘭文、葡萄牙文、西班牙文和瑞典文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.black

供喜歡黑色或希望黑色與其企業或品牌關聯的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.blue

供喜歡藍色或希望藍色與其企業或品牌關聯的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.boutique

用於提供有關精品店和小型專賣店的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.builders

供附屬於建築業的公司和個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.business

供任何類型的企業使用。可用來替代 .biz 域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.buzz

用於提供有關最新新聞和活動的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cab

供計程車業的公司和個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cafe

供咖啡館企業和對咖啡館文化感興趣的人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.camera

供攝影愛好者和想要分享相片的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.camp

供遊樂園及休閒部門、夏令營、作家研習營、健身營和露營愛好者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.capital

做為一般類別，用來描述任何類型的首都，例如金融首都或城市首都。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cards

供專營電子卡片、印刷賀卡、名片和紙牌等卡片的企業使用。此外，也適合希望討論卡牌遊戲規則和策略的遊戲玩家。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.care

供照護領域的企業或代理機構使用。也供慈善組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.careers

用於提供有關工作招募的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.cash

供參與金錢相關活動的任何組織、群體或個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.casino

供賭博業或希望分享賭博和賭場遊戲資訊的遊戲玩家使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.catering

供餐飲業或分享美食相關活動資訊的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cc

請參閱 .cc (可可斯群島)。

Return to index

.center

做為從研究組織到社群中心的一般域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.ceo

用於提供 CEO 及其同輩的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援德文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.chat

供任何類型的線上聊天網站使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cheap

供電子商務網站用來促銷和銷售便宜的產品。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

. 聖誕節。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- 可以通過 53 號路線延遲更新：到期後 43 天
- 網域已從 Route 53 刪除：過期後 44 天
- 可以通過註冊表恢復：到期後的 44 天到 86 天
- 網域已自註冊表中刪除：到期後 86 天

.church

供任何規模或宗派的教會用來與其信眾交流，以及發佈教會相關和活動的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.city

用於提供有關特定城市的資訊，例如景點、當地熱門觀光點、或里民活動。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.claims

供處理保險理賠或提供法律服務的公司使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cleaning

供提供清潔服務的企業或個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.click

供要將點選動作與其網站 (例如，在網站上按一下產品即可購買) 關聯的企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.clinic

供醫療保健產業和醫療專業人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.clothing

供時裝業的企業和個人使用，包括零售商、百貨公司、設計師、裁縫師和 Outlet 購物中心。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cloud

做為一般域名，但最適合提供雲端運算技術和服務的公司。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.club

供任何類型的俱樂部或組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援西班牙文和日文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.coach

供對教導感興趣的任何人使用，例如運動專業人員、生活方式教練或企業講師。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.codes

做為各種 Code 的一般域名，例如行為準則、建築法規或程式設計。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止

- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.coffee

供咖啡產業的企業和個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.college

供學校和大學等教育機構使用。此外，教育機構附屬的招募人員、顧問、廣告商、學生、老師和行政人員也使用該網域域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、簡體中文和繁體中文、斯拉夫文、希臘文、希伯來文、日文和泰文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.com

用於商業網站。這是網際網路上最熱門的網域域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.community

供任何類型的社群、俱樂部、組織或特殊興趣群體使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.company

做為各種公司的一般域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.computer

做為電腦相關資訊的一般域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.condos

供與公寓關聯的個人和企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.construction

供建築業從業者使用，例如建商和承包商。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.consulting

供顧問和附屬於諮詢產業的其他人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、中文、法文、斯拉夫文、梵文字母、德文、希臘文、希伯來文、日文、韓文、拉丁文、西班牙文、坦米爾文和泰文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 聯繫。

供任何規模或宗派的教會用來與其信眾交流，以及發佈教會相關和活動的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.contractors

供承包商使用，例如建築業承包商。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cool

供需要將其品牌與最新趨勢關聯的組織和群組使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.coupons

供提供線上優惠券和優惠券代碼的零售商和製造商使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.credit

供信貸產業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.creditcard

供發行信用卡的公司或銀行使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.cruises

供郵輪產業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.dance

供舞者、舞蹈講師和舞蹈學校使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.dating

用於交友約會網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.deals

用於提供有關線上優惠和特賣的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.degree

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.delivery

供提供各種商品或服務的公司使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.democrat

用於提供有關美國民主黨的資訊。另外想要競選公職的官員、民選官員、政治熱衷者和顧問也使用該網域域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.dental

供牙科專業人員和牙科供應商使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 設計。

供任何規模或宗派的教會用來與其信眾交流，以及發佈教會相關和活動的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.diamonds

供鑽石愛好者和鑽石業者 (包括賣方、經銷商和商家) 使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.diet

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .diet 網域或將 .diet 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .diet 網域。

供健康和健身專業人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .diet 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.digital

用於與數位相關的一切，但最適用於科技企業。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.direct

做為一般域名，但最適合透過電子商務網站直接向客戶銷售產品的人員。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.directory

供媒體業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.discount

用於大幅度降價的折扣網站和企業。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.dog

供愛狗人士以及寵物犬服務和產品提供者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.domains

用來提供網域名稱的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.education

用於提供教育相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.email

用於提供促銷電子郵件的相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.energy

做為一般域名，但最適合能源或節能領域的企業和個人。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.engineering

供工程公司和專業人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.enterprises

用於提供有關企業和業務的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.equipment

用於提供有關設備、設備零售商或製造商以及租賃中心的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.estate

用於提供房屋置產和地產業的相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.events

用於提供各種活動的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.exchange

用於任何類型的交易/交換：股票交易、商品交易，或甚至是簡單的資訊交換。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.expert

供在各領域擁有專業知識的人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.exposed

做為各種主題的一般域名，包括攝影、小報和調查報導。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.express

做為一般域名，但最適合希望強調快速交付商品或服務的企業或個人。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.fail

供犯錯的任何人使用，但最適合發佈幽默的「失敗」失誤和出糗。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 風扇。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.farm

供農業從業者使用，例如農民和農業工程師。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.finance

供金融業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.financial

供金融業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.fish

做為一般域名，但最適合與魚類和釣魚相關的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.fitness

用於推廣健身和健身服務。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.flights

由旅行社、航空公司和任何人的旅遊公司隸屬於產業。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.florist

供花店使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.flowers

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .flowers 網域，或將 .flowers 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .flowers 網域。

用於與花卉相關的一切，例如線上花卉銷售或有關花卉種植和培育的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .flowers 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.fm

請參閱 .fm (密克羅尼西亞聯邦)。

Return to index

.football

供與足球運動相關的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.forsale

用於銷售產品和服務。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.foundation

供非營利組織、慈善機構和其他類型的基金會使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 樂趣。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.fund

做為基金相關一切的一般域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.furniture

供家具製造商和賣方以及附屬於家具產業的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.futbol

用於提供足球的相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.fyi

做為一般域名，但最適合分享各種資訊。"FYI" 是由 "for your information" (僅供參考) 的縮寫。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gallery

供藝廊擁有者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.games

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gift

供銷售禮物或提供禮物相關服務的企業或組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gifts

供銷售禮物或提供禮物相關服務的企業或組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gives

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.glass

供玻璃產業從業者使用，例如玻璃切割者和窗戶安裝者。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.global

供具有國際市場或願景的任何企業或集團使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、白俄羅斯文、波士尼亞文、保加利亞文、簡體中文、繁體中文、丹麥文、德文、印度文、匈牙利文、冰島語、韓文、拉脫維亞文、立陶宛文、馬其頓文、蒙特內哥羅文、波蘭文、俄文、塞爾維亞文、西班牙文、瑞典文和烏克蘭文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gmbh

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gold

做為一般域名，但最適合購買或銷售黃金或黃金相關產品的公司。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.golf

用於致力推廣高爾夫球運動的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.graphics

供圖形產業的企業和個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gratis

用於提供免費產品 (例如促銷項目、下載或優惠券) 的網站。"Gratis" 是西班牙單字，表示「免費」。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.green

用於致力於保育、生態、環境和綠色生活方式的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.gripe

用於分享抱怨和批評。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.group

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.guide

做為一般域名，但最適合專注於旅遊目的地、服務和產品的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.guitars

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .guitars 網域，或將 .guitars 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .guitars 網域。

供吉他愛好者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .guitars 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.guru

供想要分享各種主題知識的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.haus

供房地產與建築產業使用。"Haus" 是德文單字，表示「房屋」。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.healthcare

用於醫療保健部門。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.help

做為一般域名，但最適合提供線上說明和資訊的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.hiv

用於致力於對抗 HIV 的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.hockey

用於致力推廣曲棍球運動的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.holdings

供財務顧問、股票經紀人，以及投資從業者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.holiday

供旅遊業者以及從事派對策劃和特殊場合策劃的個人和企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.host

供提供 Web 託管平台和服務的公司使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、簡體中文、繁體中文、希臘文、希伯來文、韓文和泰文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.hosting

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .hosting 網域或將 .hosting 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .hosting 網域。

用於託管網站或供主機代管業者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .hosting 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.house

供房地產代理以及房屋的買方和賣方使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.im

請參閱 .im (曼島)。

Return to index

.immo

供房地產業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.immobilien

用於提供房地產相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.industries

供希望識別為工業的任何公司或商業企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.info

用於傳播資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.ink

供紋身花紋愛好者或與油墨相關的任何產業 (例如印刷和出版業) 使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文和拉丁文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.institute

供任何組織或群體使用，尤其是研究和教育組織。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.insure

供保險公司和保險經紀人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.international

供具有國際連鎖的企業、國際旅遊的個人或具有國際影響的慈善組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.investments

做為一般域名，但最適合推廣投資機會。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.io

請參閱 .io (英屬印度洋領地)。

Return to index

.irish

用於推廣愛爾蘭文化和組織。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、簡體中文、繁體中文、法文、德文、希臘文、希伯來文、日文、韓文、西班牙文、坦米爾文和泰文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.jewelry

供珠寶賣方和買方使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.juegos

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .juegos 網域，或將 .juegos 網域轉移至 。我們會繼續支援已向 Route 53 註冊的 .juegos 網域。

用於所有類型的遊戲網站。"Juegos" 是西班牙單字，表示「遊戲」。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .juegos 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.kaufen

用於提供電子商務相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.kim

供名字或姓氏為 Kim 的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.kitchen

供廚房零售商、廚師、美食部落客，以及食品業者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.kiwi

供希望支持紐西蘭 kiwi 文化的公司和個人使用。也做為基督城重建慈善援助的平台，基督城在 2010 和 2011 年因地震而毀壞。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援毛利文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.land

供農民、房仲業者、商業開發商以及對地產感興趣的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 法律。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.lease

供房仲業者、房東和房客使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.legal

供法律專業人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.lgbt

供女同性戀者、男同性戀者、雙性戀者和跨性別者的社群使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.life

做為一般域名，並適合多種企業、群體和個人。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.lighting

供攝影師、設計人員、建築師、工程師，以及對照明感興趣的其他人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.limited

做為一般域名，並適合多種企業、群體和個人。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.limo

供司機、豪華禮車公司和租車機構使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.link

用於提供有關建立線上捷徑連結的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

Uniregistry 是 .LINK 域名的註冊機構。由於 Uniregistry 的政策，註冊機構級 WHOIS 顯示 REDACTED FOR PRIVACY (出於保護隱私權進行遮蔽)。刪除我們的隱私權保護功能只會影響在註冊服務商級別 Amazon Registrar WHOIS 顯示的信息。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.live

做為一般域名，並適合多種企業、群體和個人。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止

- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.llc

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.loan

供貸方、借方和信貸專業人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援丹麥文、德文、挪威文和瑞典文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.loans

供貸方、借方和信貸專業人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.lol

用於幽默和喜劇網站。"LOL" 是 "laugh out loud" (大笑) 的縮寫。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 有限公司

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.maison

供房地產業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.management

用於提供有關商務世界和公司管理的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.marketing

供行銷業用於各種用途。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.mba

用於提供有關企業管理碩士學位 (MBA) 資訊的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.media

供媒體和娛樂產業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.memorial

供緬懷事件和先人的紀念組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.mobi

供希望自己的網站可在行動電話上存取的公司和個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.moda

用於提供時裝相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.money

用於專注於金錢和金錢相關活動的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.mortgage

供房貸產業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.movie

用於提供有關電影和影片製作資訊的網站。適合專業人員和粉絲。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.name

供想要建立個人化 Web 空間的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

Verisign (.name TLD 的註冊機構) 可讓您註冊第二層網域 (name) 和第三層網域 (firstname.lastname.name) Route 53 在註冊網域和將現有的網域轉移至 Route 53 時僅支援第二層網域。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.net

用於所有類型的網站。.net 域名是 "network" (網路) 的縮寫。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.network

供從事網路產業或希望運用人際網路建立關係的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.news

用於散發任何有新聞價值的資訊，例如與報導和通訊相關的目前事件或資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.ninja

供想要將自身與忍者能力關聯的個人和企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.onl

.onl 域名是 "online" (線上) 的縮寫，而且也是西班牙文中非營利組織的縮寫。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、白俄羅斯文、波士尼亞文、保加利亞文、簡體中文、繁體中文、丹麥文、德文、印地語、匈牙利文、冰島語、韓文、立陶宛文、拉脫維亞文、馬其頓文、波蘭文、俄文、塞爾維亞文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.online

.onl 域名是 "online" (線上) 的縮寫，而且也是西班牙文中非營利組織的縮寫。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.org

供所有類型的組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.partners

供法律事務所、投資人和各種公司使用。同時也用於建立關係的社交網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止

- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.parts

做為一般域名，但最適合零件造商、賣方和買方。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.photo

供攝影師和對相片感興趣的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.photography

供攝影師和對相片感興趣的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.photos

供攝影師和對相片感興趣的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.pics

供攝影師和對相片感興趣的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.pictures

供對攝影師、藝術和媒體感興趣的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.pink

供喜歡粉紅色或希望粉紅色與其企業或品牌關聯的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.pizza

供披薩餐廳和披薩愛好者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.place

做為一般域名，但最適合家庭和旅遊業。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.plumbing

供裝修水管業的企業和個人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.plus

做為一般域名，但最適合大號衣物、附加軟體或可提供「額外」功能或尺寸的任何產品。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.poker

供撲克牌玩家和遊戲網站使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.porn

用於僅限成人網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.press

用於僅限成人網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.pro

供獲證書認可的專業人員和專業組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.productions

供製作廣告、廣播廣告和音樂影片的工作室與製作公司使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.properties

用於任何財產類型的資訊，包括房地產或智慧財產。此外，也供有待銷售、租賃或出租之房屋、建築物或土地的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.property

用於任何財產類型的資訊，包括房地產或智慧財產。此外，也供有待銷售、租賃或出租之房屋、建築物或土地的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .property 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.pub

供出版、廣告或釀酒業從業者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.qpon

用於優惠券和促銷代碼。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.recipes

供要分享食譜的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.red

供喜歡紅色或希望紅色與其企業或品牌關聯的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.reise

用於旅遊或旅程相關的網站。"Reise" 是德文單字，表示「上升」、「升起」或「踏上旅程」。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.reisen

用於旅遊或旅程相關的網站。「Reisen」是德文單字，表示「旅程」。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.rentals

用於所有類型的出租業務。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.repair

供維修服務或是想要使用這些教導他人如何修復各種物品的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.report

做為一般域名，但最適用於有關業務報告、社群出版、書籍報告或新聞報告的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.republican

用於提供有關美國共和黨的資訊。另外想要競選公職的官員、民選官員、政治熱衷者和顧問也使用該網域域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.restaurant

供餐廳業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.reviews

供想要提供意見和讀取他人評論的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.rip

用於死亡和紀念專用網站。"RIP" 是 "rest in peace" (願死者安息) 的縮寫。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.rocks

做為一般域名，但最適合與 “rocks” 相關的任何人：音樂家、地理學家、珠寶商、攀岩者等等。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.run

做為一般域名，但最適合健身和運動業。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.sale

供電子商務網站使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.sarl

供通常位於法國的有限責任公司使用。"SARL" 是 Société à Responsabilité Limité 的縮寫。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.school

用於提供有關教育、教育機構和學校相關活動的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.schule

用於提供以德文為基礎的教育、教育機構和學校相關活動的資訊。"Schule" 是德文單字，表示「學校」。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天

- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.services

用於專注於各種服務的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.sex

用於僅限成人內容。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.sexy

用於提供與性相關的內容。同時也用於描述最熱門和令人興奮的品牌、產品、資訊和網站。

Return to index

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .sexy 網域，或將 .sexy 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .sexy 網域。

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .sexy 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.shiksha

供教育機構使用。"Shiksha" 是印度字，表示學校。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.shoes

供鞋零售商、設計人員、製造商或時尚部落客使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 購物。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止

- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.show

做為一般域名，但最適合娛樂業。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.singles

供交友服務、度假村，以及為希望建立關係的人員提供服務的其他企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.site

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 滑雪。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.soccer

用於致力推廣足球運動的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.social

用於提供有關社交媒體、論壇和線上交談的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.solar

用於提供有關太陽系或太陽能的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.solutions

由各種顧問， do-it-yourself 服務和顧問使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 軟體。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.space

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.store

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 流

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.studio

做為一般域名，但最適合房地產、藝術或娛樂業的從業者。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.style

做為一般域名，但最適合致力於最新趨勢 (尤其是時尚、設計、建築和藝術方面的趨勢) 的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.sucks

做為一般域名，但最適合要分享負面體驗或向他人警告騙局、詐騙或瑕疵產品的人。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.supplies

供線上銷售商品的企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止

- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.supply

供線上銷售商品的企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.support

供提供各種支援 (包括客戶、產品或系統支援或情感、財務或精神支持) 的企業、群體或慈善機構使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.surgery

用於提供有關外科手術、醫學和醫療保健的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.systems

主要供科技產業及科技服務提供者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tattoo

供紋身愛好者和紋身業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援斯拉夫文 (主要是俄文)、法文、德文、義大利文、葡萄牙文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tax

用於提供稅務、稅務準備和稅法相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.taxi

供計程車、司機和接駁車公司使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.team

供希望識別為團隊的任何公司或組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tech

供科技愛好者以及致力於公司、服務和製造商方面的科技的人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.technology

供科技愛好者以及致力於公司、服務和製造商方面的科技的人員使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tennis

用於提供網球運動的相關資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.theater

用於致力於戲劇院、戲劇和音樂劇的網站。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tienda

供要與西班牙語系的消費者聯繫的零售企業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.tips

供想要分享幾乎任何主題知識和建議的人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tires

供輪胎的製造商、代理商或買方使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.today

用於提供有關目前活動、新聞、天氣、娛樂等的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tools

用於提供有關任何工具類型的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tours

做為一般域名，但最適合旅遊公司。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.town

用於推廣城市的地區、文化和社群。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.toys

供玩具產業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.trade

做為一般域名，但最適合商務網站或貿易服務。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援丹麥文、德文、挪威文和瑞典文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.training

供講師、輔導員和教育工作者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.tv

用於提供有關電視和媒體的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

無。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.university

供大學和其他教育組織使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.uno

用於提供有關西班牙、葡萄牙文和義大利文社群的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.vacations

供旅遊和觀光業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

.vegas

用於推廣拉斯維加斯市和拉斯維加斯生活方式。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.ventures

供企業家、新創公司、創業投資者、投資銀行和金融家使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.vg

請參閱 .vg (英屬維京群島)。

Return to index

.viajes

供旅遊社、旅行社人員、旅遊部落格、旅遊公司、租賃服務、旅遊部落客和旅遊零售商使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.video

供媒體和視訊業使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文、拉丁文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.villas

供要出售、出租或租賃別墅的房地產代理和房地產擁有者使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.vision

做為一般域名，但最適合驗光師和眼科醫生等眼科專家。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

. 投票。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.voyage

供旅遊社、旅行社人員、旅遊部落格、旅遊公司、租賃服務、旅遊部落客和旅遊零售商使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.watch

用於提供有關串流網站、Web 電視、影片或手錶的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.website

用於提供有關網站開發、促銷、改進和體驗的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、簡體中文、繁體中文、希臘文、希伯來文、日文、韓文和泰文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.wedding

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

無。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援中文、法文、德文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.wiki

用於提供有關線上文件的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文和拉丁文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.wine

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護

支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 75 天

. 工作。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.works

供企業、組織和個人用來提供工作、任務和雇用服務的相關資訊。此域名可用來替代 .com、.net 或 .org 域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.world

供想要提供全球主題資訊的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.wtf

供想要與常見但不雅的縮寫 "WTF" 關聯的任何人使用。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.xyz

做為任何用途的一般域名。

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

.xyz 網域的登錄機構 Generation XYZ，會將某些網域名稱視為高級的網域名稱。您無法向 Route 53 註冊或轉移高級的 .xyz 網域。如需詳細資訊，請參閱 Generation XYZ 網站。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.zone

用於提供有關任何區域類型 (包括時區、氣候區域和運動區域) 的資訊。

Return to index

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援法文和西班牙文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止

- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

地理頂層網域

以下網域域名依地理位置分組，並包含國家特定的官方域名，稱為國家/地區代碼頂層網域(ccTLD)。範例包含 .be (比利時)、.in (印度) 和 .mx (墨西哥)。ccTLD 註冊規則因國家/地區而異。有些國家/地區不受限制，也就是說世界上任何人都可以註冊，而有些國家/地區有特定限制，例如居留權。每個 ccTLD 的清單表示任何限制。

> **Important**
>
> 在將任何 ccTLDs 傳輸至 Route 53 的期間 (.cc 和 .tv 除外)，系統會忽略擁有者聯絡資訊的更新，並使用登錄檔中的擁有者聯絡資訊。您可以在傳輸完成後更新聯絡資訊。如需詳細資訊，請參閱 更新網域的聯絡資訊和所有權。

Return to index

非洲

.ac (亞森欣島), .co.za (南非), .sh (聖赫勒拿島)

美洲

.ca (加拿大), .cl (智利), .co (哥倫比亞), .com.ar (阿根廷), .com.br (巴西), com.mx (墨西哥), .mx (墨西哥), .us (美國), .vc (聖文森及格瑞那丁), .vg (英屬維京群島)

亞洲/大洋洲

.au (澳洲), .cc (可可斯群島), .co.nz (紐西蘭), .com.au (澳洲), .com.sg (新加坡共和國), .fm (密克羅尼西亞聯邦), .in (印度), .jp (日本), .io (英屬印度洋領地), .net.au (澳洲), .net.nz (紐西蘭), .org.nz (紐西蘭), .pw (帛琉), .qa (卡達), .ru (俄羅斯聯邦), .sg (新加坡共和國)

歐洲

.be (比利時), .berlin (德國柏林市), .ch (瑞士), .co.uk (英國), .cz (捷克共和國), .de (德國), .es (西班牙) , .eu (歐盟), .fi (芬蘭), .fr (法國), .gg (耿西島), .im (曼島), .it (義大利), .me (蒙特內哥羅), .me.uk (英國), .nl (荷蘭), .org.uk (英國), .ruhr (魯爾區，位於德國西部), .se (瑞典), .uk (英國), .wien (奧地利維也納市)

非洲

您可以使用下列適用於非洲的頂層網域 (TLD) 向 Amazon Route 53 註冊網域。

, ,

Return to index

.ac (亞森欣島)

Return to index

另外，也是學術界中常用的一般 TLD。

註冊和續約的租用期間

一年。

限制

沒有限制地開放給大眾使用。

隱私權保護

由註冊機構決定。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：過期後 80 天

.co.za (南非)

Return to index

註冊和續約的租用期間

一年。

限制

.za 域名只提供第二層網域。Route 53 支援第二層網域 .co.za。

開放給大眾使用，但有些限制。

- 註冊開放給可識別身分的法人實體 (個人和法人)。
- 網域名稱在註冊過程中必須通過區域檢查。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。為了防止未經授權的轉移，請限制對註冊人電子郵件地址和 Route 53 API 的訪問，這些 API 可能允許更改所有權，UpdateDomainContact例如。如需詳細資訊，請參閱《服務授權參考》中的 Route 53 網域的動作、資源和條件索引鍵和 網域記錄擁有者的許可範例。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

否

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期的前 1 天為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期的前 1 天
- 可透過註冊商進行還原：過期後 1 天至 9 天之間

- 網域已由註冊商刪除：過期後 9 天

.sh (聖赫勒拿島)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 80 天

美洲

您可以使用下列適用於美洲的頂層網域 (TLD) 向 Amazon Route 53 註冊網域。

, , , , , , , , ,

Return to index

.ca (加拿大)

Return to index

域名的變體（à）或不帶有（a）重音符號）將自動保留給註冊人，並成為管理服務包的一部分。若要啟用套裝軟體中的網域，註冊人必須提出網域的註冊要求。套裝軟體中的所有網域都必須由相同的註冊人和同一個註冊商註冊。註冊人還需要提交組合中所有網域的轉移申請，才能完成轉移作業。

來自 TLD 註冊機構的確認電子郵件

當您註冊 .ca 網域，您會收到一封包含連結的電子郵件，該連結指向註冊合約的接受程序。您必須在七天內完成程序，否則將無法註冊網域。

註冊和續約的租用期間

1 到 10 年。

限制

開放給大眾使用，但有些限制。

- 註冊開放給加拿大相關個人或組織，如「加拿大註冊者要求」所述。
- 註冊聯絡人：您必須提供網域擁有者的完整和確切法律名稱。
- 管理員和技術聯絡人：您必須指定 Person (個人) 做為聯絡人類型，並提供居住在加拿大的個人的聯絡資訊。
- 在註冊程序中，必須選擇其中一個法律類型：
  - ABO：加拿大原住民 (個人或團體)
  - ASS：加拿大非公司協會。
  - CCO：加拿大公司或加拿大省或領土
  - CCT：加拿大公民
  - EDU：加拿大教育機構
  - GOV：加拿大政府或政府機關
  - HOP：加拿大醫院
  - INB：加拿大印地安法認可的印地安社
  - LAM：加拿大圖書館、檔案管理局或博物館
  - LGR：加拿大公民或永久居民的法人代表

- MAJ：加拿大女王/加拿大國王
- OMK：在加拿大登記的官方商標
- PLT：加拿大政黨
- PRT：在加拿大登記的合夥企業
- RES：加拿大永久居民
- TDM：在加拿大登記的商標 (非加拿大擁有者類型)
- TRD: 加拿大工會
- TRS：在加拿大成立的信託

隱私權保護

- 人員 — 對於所有聯繫人，聯繫人姓名，地址，電話號碼，傳真號碼和電子郵件地址都會隱藏，因為 CIRA 會自動將其隱私保護應用於某個人。隱私權保護選項僅適用於註冊商 Whois。
- 公司、關聯或公共機構 — 登錄層級不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：各有不同。聯絡 AWS 支援。

刪除網域註冊

.ca 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

.cl (智利)

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .cl 網域，或將 .cl 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .cl 網域。

Return to index

續約期間

兩年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .cl 網域轉移至 Route 53。

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：請聯絡 AWS Support。
- Route 53 可延遲續約：請聯絡 AWS Support。
- 網域已從 Route 53 刪除：請聯絡 AWS Support。
- 可透過註冊商進行還原：請聯絡 AWS Support。
- 網域已由註冊商刪除：請聯絡 AWS Support。

.co (哥倫比亞)

Return to index

註冊和續約的租用期間

1 到 5 年。

限制

.co 網域的登錄機構 Go.co 會將某些網域名稱視為高級的網域名稱。您無法向 Route 53 註冊或轉移高級 .co 網域。如需詳細資訊，請參閱 Go.co 網站。

隱私保護（適用於：個人）

所有資訊都會隱藏。

如果聯絡人類型並非人員，WHOIS 會顯示公司名稱和國家。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：過期後 30 天至 45 天之間
- 網域已由註冊商刪除：過期後 50 天

.com.ar (阿根廷)

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .com.ar 網域，或將 .com.ar 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .com.ar 網域。

Return to index

續約期間

一年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。為了防止未經授權的轉移，請限制對註冊人電子郵件地址和 Route 53 API 的訪問，這些 API 可能允許更改所有權，UpdateDomainContact例如。如需詳細資訊，請參閱《服務授權參考》中的 Route 53 網域的動作、資源和條件索引鍵和 網域記錄擁有者的許可範例。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .com.ar 網域轉移至 Route 53。

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：請聯絡 AWS Support。
- Route 53 可延遲續約：請聯絡 AWS Support。
- 網域已從 Route 53 刪除：請聯絡 AWS Support。
- 可透過註冊商進行還原：請聯絡 AWS Support。
- 網域已由註冊商刪除：請聯絡 AWS Support。

.com.br (巴西)

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .com.br 網域，或將 .com.br 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .com.br 網域。

Return to index

續約期間

一年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .com.br 網域轉移至 Route 53。

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：過期前 30 天至過期日期之間
- Route 53 可延遲續約：至過期後 119 天為止
- 網域已從 Route 53 刪除：過期後 119 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 119 天

com.mx (墨西哥)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

由註冊機構決定。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.mx (墨西哥)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

由註冊機構決定。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.us (美國)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

.us 網域的註冊機構不允許網域名稱中包含 Federal Communications Commission v. Pacifica Foundation No. 77-528 的「法院意見的附錄」中標識的任何七個字詞。

開放給大眾使用，但有一項限制：

- .us 域名用於美國境內的網站或活動。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：過期後 30 天至 60 天之間
- 網域已由註冊商刪除：過期後 65 天

.vc (聖文森及格瑞那丁)

此外，創業投資金融、Varsity 學院等也將其用做一般 TLD。

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 80 天

.vg (英屬維京群島)

此外，視訊遊戲相關組織也將其用做一般 TLD。

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期後的 44 天為止
- Route 53 可延遲續約：是

- 網域已從 Route 53 刪除：過期後 45 天
- 網域已由註冊商刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 74 天之間
- 網域再次公開提供：過期後 80 天

亞洲/大洋洲

您可以使用下列適用於亞洲和大洋洲的頂層網域 (TLD) 向 Amazon Route 53 註冊網域。

, , , , , , , , , , , , , , ,

Return to index

.au (澳洲)

Return to index

來自 TLD 註冊機構的確認電子郵件

我們的註冊商助理 Gandi 透過以下方式轉售 .au 網域。DomainDirectors當您將網域名稱轉移到 Route 53 時，DomainDirectors 會傳送電子郵件給該網域的註冊人聯絡人，以驗證聯絡人資訊或授權轉移請求。

註冊和續約的租用期間

一年。

限制

開放給大眾使用，但有些限制。

- .au 網域開放給下列對象：在澳洲註冊的法人、貿易、合作夥伴關係或獨立貿易商；獲授權可在澳洲進行交易的外國公司；以及澳洲註冊商標的擁有者或申請人。個人無法註冊 .au 網域。註冊機構聯絡人必須是公司。
- 您的網域名稱必須與名稱 (已向澳洲相關機構註冊) 或商標 (或縮寫) 相同。
- 網域名稱應該指出您的活動。例如，它應該指出您銷售的產品或提供的服務。
- 在註冊過程中，您必須指出下列資訊：
  - 您的註冊類型：ABN (澳洲企業號碼)、ACN (澳洲公司註冊編號) 或 TM (商標，如果網域名稱對應到商標)。
  - 您的 ID 號碼，可以是醫療保險卡號、稅務檔案編號 (TFN)、州駕照號碼或澳洲企業號碼 (ABN)。

- 您所在的州或省。
- 不正確或不相符的聯絡資訊，包括姓名、ABN 或商標 (TM) 號碼，將導致註冊、交易和續約失敗。您可能需要變更擁有權才能更正現有網域的資訊。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。設定金鑰時，您必須選擇 DNS 安全性演算法 2 (DH)。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：過期前 60 天至過期日期之間
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 29 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 30 天

刪除網域註冊

.au 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

變更擁有權

使用 Route 53 主控台變更擁有者。請參閱 更新網域的聯絡人資訊。然後完成以下程序以完成所有權變更：

1. 舊註冊人和新註冊人都必須單擊他們在電子郵件中收到的鏈接，從 transfers@1api.net 發送到他們列出的電子郵件地址。如果未在 14 天內完成此程序，您必須從頭開始本程序：

2. 回覆確認後，將在短時間內處理註冊機構中的擁有者變更，無需進一步確認。

.cc (可可斯群島)

Return to index

此外，名稱中有 "cc" 的組織 (例如諮詢公司、雲端運算公司或自行車俱樂部) 也將其用做一般 TLD。此域名是 ".com" 的常見替代名稱。

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

- 隱藏 – 地址、電話號碼、傳真號碼和電子郵件地址
- 不隱藏 – 聯絡人姓名和組織名稱

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止

- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 30 天至 60 天之間
- 網域已由註冊商刪除：過期後 65 天

.co.nz (紐西蘭)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

可向 Route 53 註冊以下第二層網域：.co.nz、.net.nz 和 .org.nz。您無法向 Route 53 註冊 .nz (第一級) 網域，或將 .nz 網域轉移至 Route 53。

開放給大眾使用，但有些限制。

- 個人必須年滿 18 歲。
- 組織必須已註冊。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 44 天
- 可透過註冊機構進行還原：過期後 44 天至 134 天之間
- 網域已由註冊機構刪除：過期後 134 天

.com.au (澳洲)

Return to index

來自 TLD 註冊機構的確認電子郵件

我們的註冊商助理 Gandi 透過以下方式轉售 .au 域名。DomainDirectors當您將網域名稱轉移到 Route 53 時，DomainDirectors 會傳送電子郵件給該網域的註冊人聯絡人，以驗證聯絡人資訊或授權轉移請求。

註冊和續約的租用期間

1 到 5 年。

限制

開放給大眾使用，但有些限制。

- .com.au 和 .net.au 網域開放給下列對象：在澳洲註冊的合作夥伴關係或獨立貿易商；獲授權可在澳洲進行交易的外國公司；以及澳洲註冊商標的擁有者或申請人。個人無法註冊 .com.au/.au 網域。註冊機構聯絡人必須是公司。
- 您的網域名稱必須與名稱 (已向澳洲相關機構註冊) 或商標 (或商標的縮寫) 相同。
- 網域名稱應該指出您的活動。例如，它應該指出您銷售的產品或提供的服務。
- 在註冊過程中，您必須提供下列資訊：
  - 您的註冊類型：ABN (澳洲企業號碼)、ACN (澳洲公司註冊編號) 或 TM (商標，如果網域名稱對應到商標)。
  - 您的 ID 編號：可以是 ABN (澳洲企業號碼)、ACN (澳洲公司註冊編號) 或 TM (商標，如果網域名稱對應到商標)。
  - 您所在的州或省。
- 不正確或不相符的聯絡資訊，包括姓名、ABN 或商標 (TM) 號碼，將導致註冊、交易和續約失敗。您可能需要變更擁有權才能更正現有網域的資訊。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。設定金鑰時，您必須選擇 DNS 安全性演算法 2 (DH)。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：過期前 60 天至過期日期之間
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 29 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 30 天

刪除網域註冊

.com.au 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

變更擁有權

變更擁有者，可採用程式設計的方式或使用 Route 53 主控台。請參閱 更新網域的聯絡人資訊。然後完成以下程序以完成所有權變更：

1. 舊註冊人和新註冊人都必須單擊他們在電子郵件中收到的鏈接，從 transfers@1api.net 發送到他們列出的電子郵件地址。如果未在 14 天內完成此程序，您必須從頭開始本程序：

2. 回覆確認後，將在短時間內處理註冊機構中的擁有者變更，無需進一步確認。

.com.sg (新加坡共和國)

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .com.sg 網域，或將 .com.sg 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .com.sg 網域。

Return to index

續約期間

一年或兩年。

刪除網域註冊

.com.sg 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .com.sg 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：過期後 30 天至 60 天之間
- 網域已由註冊商刪除：過期後 60 天

.fm (密克羅尼西亞聯邦)

此外，線上媒體和廣播相關組織也將其用做一般 TLD。

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 44 天
- 可透過註冊商進行還原：過期後 44 天至 79 天之間
- 網域已由註冊商刪除：過期後 84 天

.in (印度)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：過期後 30 天至 60 天之間
- 網域已由註冊商刪除：過期後 65 天

.jp (日本)

Return to index

註冊和續約的租用期間

一年。

限制

開放給大眾使用，但有一項限制：

- 只有在日本的個人或公司可以註冊 .jp 網域名稱。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。為了防止未經授權的轉移，請限制對註冊人電子郵件地址和 Route 53 API 的訪問，這些 API 可能允許更改所有權，UpdateDomainContact例如。如需詳細資訊，請參閱《服務授權參考》中的 Route 53 網域的動作、資源和條件索引鍵和 網域記錄擁有者的許可範例。

國際化網域名稱

支援日文。

需要授權碼才能轉移至 Route 53

是。

需要授權碼才能從 Route 53 轉移

是。

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：過期日期前 30 天至 7 天之間
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期的前 6 天
- 可透過註冊商進行還原：請聯絡 AWS Support。
- 網域已由註冊商刪除：請聯絡 AWS Support。

> **Note**
>
> 目前無法註冊 non-general-purpose .co.jp 和 .or .jp 等 JP 網域。

.io (英屬印度洋領地)

此外，電腦相關組織 (例如線上服務、以瀏覽器為基礎的遊戲和新創公司) 也將其用做一般 TLD。

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

州/省和國家/地區除外，隱藏其他所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

.io 網域的註冊機構也將授權碼用做某些操作 (如啟用或停用隱私權保護) 的一次性密碼。如果要執行多個需要密碼的操作，則必須為每個操作產生另一個授權碼。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已自註冊表中刪除：到期後 90 天

.net.au (澳洲)

Return to index

來自 TLD 註冊機構的確認電子郵件

我們的註冊商助理 Gandi 透過以下方式轉售 .net.au 域名。DomainDirectors當您將網域名稱轉移到 Route 53 時，DomainDirectors 會傳送電子郵件給該網域的註冊人聯絡人，以驗證聯絡人資訊或授權轉移請求。

註冊和續約的租用期間

1 到 5 年。

限制

只提供第二層網域。Route 53 支援第二層網域 .com.au 和 .net.au。

開放給大眾使用，但有些限制。

- .com.au 和 .net.au 網域開放給下列對象：在澳洲註冊的法人、貿易、合作夥伴關係或獨立貿易商；獲授權可在澳洲進行交易的外國公司；以及澳洲註冊商標的擁有者或申請人。
- 您的網域名稱必須與名稱 (已向澳洲相關機構註冊) 或商標 (或縮寫) 相同。
- 網域名稱應該指出您的活動。例如，它應該指出您銷售的產品或提供的服務。
- 在註冊過程中，您必須指出下列資訊：
  - 您的註冊類型：ABN (澳洲企業號碼)、ACN (澳洲公司註冊編號) 或 TM (商標，如果網域名稱對應到商標)。
  - 您的 ID 編號：可以是 ABN (澳洲企業號碼)、ACN (澳洲公司註冊編號) 或 TM (商標，如果網域名稱對應到商標)。
  - 您所在的州或省。
- 不正確或不相符的聯絡資訊，包括姓名、ABN 或商標 (TM) 號碼，將導致註冊、交易和續約失敗。您可能需要變更擁有權才能更正現有網域的資訊。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。設定金鑰時，您必須選擇 DNS 安全性演算法 2 (DH)。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：過期前 60 天至過期日期之間
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 29 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 30 天

刪除網域註冊

.net.au 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

變更擁有權

變更擁有者，可採用程式設計的方式或使用 Route 53 主控台。請參閱 更新網域的聯絡人資訊。然後完成以下程序以完成所有權變更：

1. 舊註冊人和新註冊人都必須單擊他們在電子郵件中收到的鏈接，從 transfers@1api.net 發送到他們列出的電子郵件地址。如果未在 14 天內完成此程序，您必須從頭開始本程序：

2. 回覆確認後，將在短時間內處理註冊機構中的擁有者變更，無需進一步確認。

.net.nz (紐西蘭)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

可向 Route 53 註冊以下第二層網域：.co.nz、.net.nz 和 .org.nz。您無法向 Route 53 註冊 .nz (第一級) 網域，或將 .nz 網域轉移至 Route 53。

開放給大眾使用，但有些限制。

- 個人必須年滿 18 歲。
- 組織必須已註冊。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 44 天
- 可透過註冊機構進行還原：過期後 44 天至 134 天之間
- 網域已由註冊機構刪除：過期後 134 天

.org.nz (紐西蘭)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

可向 Route 53 註冊以下第二層網域：.co.nz、.net.nz 和 .org.nz。您無法向 Route 53 註冊 .nz (第一級) 網域，或將 .nz 網域轉移至 Route 53。

開放給大眾使用，但有些限制。

- 個人必須年滿 18 歲。
- 組織必須已註冊。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 44 天
- 可透過註冊機構進行還原：過期後 44 天至 134 天之間
- 網域已由註冊機構刪除：過期後 134 天

.pw (帛琉)

Return to index

.pw 最初是為帕勞的居民保留的，帕勞是西太平洋大洋洲密克羅尼西亞次區的一個島國，但是，現在它通常用於代表「專業網絡」，並且每個人都可以使用。

註冊和續約的租用期間

1 到 10 年。

隱私權保護 (適用於所有聯絡人類型：個人、公司、協會和公共機構)

除組織名稱以外，隱藏所有資訊。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 75 天

.qa (卡達)

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .qa 網域，或將 .qa 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .qa 網域。

Return to index

續約期間

1 到 5 年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .qa 網域轉移至 Route 53。

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 31 天

.ru (俄羅斯聯邦)

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .ru 網域，或將 .ru 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .ru 網域。

Return to index

註冊和續約的租用期間

一年。

> **Note**
>
> .ru 網域的註冊機構會在網域過期當天，更新網域的過期日期。無論您何時向 Route 53 續訂網域，在該日期之前，WHOIS 查詢會顯示網域的舊過期日期。

限制

開放給大眾使用，但有些限制。

- 個人可能需要提供護照號碼或政府核發的 ID 號碼。
- 外國公司可能需要提供公司 ID 或公司註冊。

隱私權保護

由註冊機構決定。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台，AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .ru 網域轉移至 Route 53。

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期的前 2 天為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期的前 2 天
- 可透過註冊商進行還原：過期前 2 天至過期後 28 天之間
- 網域已由註冊商刪除：過期後 28 天

刪除網域註冊

.ru 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

.sg (新加坡共和國)

> **Important**
>
> 您無法再使用 Route 53 註冊新的 .sg 網域，或將 .sg 網域轉移至 Route 53。我們會繼續支援已向 Route 53 註冊的 .sg 網域。

Return to index

續約期間

一年或兩年。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

需要授權碼才能轉移至 Route 53

不支援。您無法再將 .sg 網域轉移至 Route 53。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：過期後 30 天至 60 天之間
- 網域已由註冊商刪除：過期後 60 天

刪除網域註冊

.sg 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

歐洲

您可以使用下列適用於歐洲的頂層網域 (TLD) 向 Amazon Route 53 註冊網域。

, ,

Return to index

.be (比利時)

Return to index

註冊和續約的租用期間

一年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是。您可以從 DNS 澳門網站獲取轉移代碼。

需要授權碼才能從 Route 53 轉移

是。您可以從 DNS 澳門網站獲取轉移代碼。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期日期當天
- 可透過註冊商進行還原：過期後 40 天之前
- 網域已由註冊商刪除：過期後 40 天

.berlin (德國柏林市)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

開放給大眾使用，但有些限制。

- 擁有者、管理或技術聯絡人必須提供位於柏林的地址，而且管理聯絡人必須為個人。
- 您必須在網域註冊後 12 個月內啟用和使用 .berlin 網域 (適用於網站、重新引導或電子郵件地址)。
- 如果在 .berlin 網域下發佈網站，或者 .berlin 網域重新引導到另一個網站，則該網站的內容必須與柏林相關。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援拉丁文和斯拉夫文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 80 天

.ch (瑞士)

Return to index

註冊和續約的租用期間

一年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止

- Route 53 可延遲續約：至過期後 9 天為止
- 網域已從 Route 53 刪除：過期後 9 天
- 可透過註冊商進行還原：過期後 9 天至 49 天之間
- 網域已由註冊商刪除：過期後 49 天

.co.uk (英國)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

如果要轉移 .co.uk 網域至 Route 53，不需要取得授權碼。相反地，請使用目前網域註冊機構提供的方法，將網域 IPS 標籤的值更新為全部大寫的 GANDI。(.uk 網域名稱的註冊機構 Nominet 需要 IPS 標籤。) 如果您的註冊機構不會變更 IPS 標籤的值，請聯絡 Nominet。

> **Note**
>
> 當您註冊 .co.uk 網域時，Route 53 會自動將網域的 IPS 標籤設為 GANDI。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：過期日期前 180 天至過期日期後 30 天之間
- Route 53 可延遲續約：過期後 30 天至 90 天之間
- 網域已從 Route 53 刪除：過期後 90 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 92 天

刪除網域註冊

.co.uk 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

.cz (捷克共和國)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援，但所有連絡人的電子郵件地址和電話號碼都會隱藏。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

如果您目前的註冊商沒有提供授權碼，請前往 `https://www.nic.cz/whois/send-password/` 提出要求，由 CZ 網域註冊機構將其傳送至註冊人的電子郵件地址。

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 58 天為止
- 網域已從 Route 53 刪除：過期後 59 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 60 天

.de (德國)

Return to index

註冊和續約的租用期間

一年。

限制

開放給大眾使用，但有些限制。

- 您必須居住在德國，或者您的管理聯絡人 (自然人) 居住在德國並且具有郵政信箱以外的地址。
- 在註冊時，網域名稱的 DNS (A、MX 和 CNAME) 必須正確設定，才能通過註冊的區域檢查。需要兩種不同 C 類別的三部伺服器。
- 如果您使用的是 Route 53 以外的 DNS 服務，則網域的名稱伺服器必須通過檢查，以確保它們已正確設定。若要判斷您的網域之名稱伺服器是否會通過檢查，請參閱 https://www.denic.de/en/service/tools/nast/。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台，AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期日期當天
- 可透過註冊商進行還原：請聯絡 AWS Support。
- 網域已由註冊商刪除：請聯絡 AWS Support。

.es (西班牙)

Return to index

網域購買或轉移

> **Important**
>
> 如果註冊聯絡人的聯絡人類型為 Person (個人)，您現在可以購買新的 .es 網域名稱或將 .es 網域轉移 Route 53。如果註冊聯絡人的聯絡人類型為 Company (公司)、Association (協會) 或 Public Body (公共機構)，則無法購買或轉移 .es 網域。
> 您也無法將註冊聯絡人的聯絡人類型變更為公司。

註冊和續約的租用期間

1 到 5 年。

限制

開放給對西班牙感興趣或與之有關係的大眾。

從 2016 年起，.ES 網域註冊者必須提供註冊者聯絡電子郵件。如果您尚未提供此資訊，則需要先向目前註冊商提供此資訊，然後才能將網域轉移至 Route 53。

您需要下列資訊：

- 類似於 *AAAA0-ESNIC-F0* 的 ESNIC 識別符。
- 如果您不知道自己的 ESNIC 識別符，可以從目前註冊商取得它。您可以在以下網址找到您的註冊商：https://www.dominios.es/en。

根據您是否記得您在註冊商的密碼，可以遵循下列其中一個程序更新您的註冊者電子郵件：

- 如果您記得密碼，請使用 ESNIC 識別符和密碼登入 https://www.nic.es/sgnd/login.action。

  登入之後，您可以選擇登錄檔頁面上的編輯標籤，來編輯註冊者電子郵件聯絡人。
- 如果您忘記密碼，請瀏覽至 https://www.nic.es/sgnd/peticion/editCorreo.action?request_locale=en。

  使用您的 ESNIC 識別符、您新的有效註冊者電子郵件聯絡人填寫表單。然後，透過選擇不使用 eID/憑證處理來驗證表單，並上傳請求的身分文件。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。為了防止未經授權的轉移，請限制對註冊人電子郵件地址和 Route 53 API 的訪問，這些 API 可能允許更改所有權，UpdateDomainContact例如。如需詳細資訊，請參閱《服務授權參考》中的 Route 53 網域的動作、資源和條件索引鍵和 網域記錄擁有者的許可範例。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

否

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期的前 6 天為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期的前 6 天

- 可透過註冊商進行還原：過期前 6 天至過期後 4 天之間
- 網域已由註冊商刪除：過期後 4 天

.eu (歐盟)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

開放給大眾使用，但有一項限制：

- 您必須提供歐洲經濟區 (EEA) 30 個州之一的有效郵寄地址，或者如果您是歐盟 27 個成員國之一的公民，則必須指定您所在的歐盟國籍國家/地區。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期日期當天

- 可透過註冊商進行還原：過期後 40 天之前
- 網域已由註冊商刪除：過期後 40 天

WHOIS 搜尋

如需有關現有 .eu 網域的詳細資訊，請參閱 https://whois.eurid.eu/en/。

.fi (芬蘭)

Return to index

註冊和續約的租用期間

1 到 5 年。

限制

開放給大眾使用，但有些限制。

- .fi 域名可用於在芬蘭有永久居住地並且具有芬蘭身分證號碼的個人，以及在芬蘭註冊的法人或私營企業主。
- 如果註冊人聯絡地址在芬蘭，則個人註冊人需要芬蘭的身分證號碼，而公司註冊人則需要芬蘭的公司編號，且您在註冊時必須提供以下資訊：
  - 聯絡人是否為居住在芬蘭的自然人或法人。
  - 如果是根據法人的名字，則需提供記錄該名稱的註冊機構的識別碼。
  - 如果是根據法人的名字，則需提供記錄該名稱的註冊機構中的記錄編號。
  - 法人在芬蘭的識別號碼。
  - 自然人在芬蘭的識別號碼。
  - 如果註冊人是非芬蘭公司，則您必須提供業務編號作為 VAT_Number。
- 如果註冊人地址不在芬蘭，則不需要芬蘭的身分證號碼或公司號碼。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：否

刪除網域註冊

如需刪除網域的相關資訊，請參閱 刪除網域名稱註冊。

.fr (法國)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

開放給大眾使用，但有些限制。

- 個人必須年滿 18 歲，並且必須提供他們的date-of-birth.
- 組織必須位於歐盟經濟區或瑞士。
- 組織應該填寫所有公司識別欄位 (加值稅號碼、SIREN、WALDEC、DUNS 等)，以便 AFNIC 日後執行任何驗證。
- 相同的資格條件也適用於管理聯絡人。
- 名稱和條款需經 AFNIC 事先審查 (命名章程第 2.4 款) 並滿足以下附加條件：
  - 先前保留或禁止的網域名稱開放給有合法權利並且出於善意行事的申請人。

- 以 ville、mairie、agglo、cc、cg 開頭的名稱需符合 AFNIC 命名慣例。

隱私權保護

由註冊機構決定。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 27 天為止
- 網域已從 Route 53 刪除：過期後 28 天
- 可透過註冊商進行還原：過期後 28 天至 58 天之間
- 網域已由註冊商刪除：過期後 58 天

.gg (耿西島)

Return to index

註冊和續約的租用期間

一年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：過期後 30 天至 35 天之間
- 網域已由註冊商刪除：過期後 35 天

.im (曼島)

此外，即時訊息服務或要開發 "I am" 品牌的個人也將其用做一般 TLD。

Return to index

註冊和續約的租用期間

一年或兩年。

限制

沒有限制地開放給大眾使用。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 30 天

.it (義大利)

Return to index

註冊和續約的租用期間

一年。

限制

開放給大眾使用，但有些限制。

- 個人或組織都必須有在歐盟境內的註冊地址。
- 如果原產國為義大利，您必須輸入稅號 (Fiscal Code)。如果原產國是在歐盟境內，您必須輸入身分證號碼 (ID 號碼)。
- 如果您為聯絡人類型指定 Company (公司)、Association (協會) 或 Public Body (公共機構)，則需提供加值稅號碼 (加值稅識別碼)。
- 網域的名稱伺服器必須通過 DNS 檢查。我們建議您檢查名稱伺服器 https://dns-check.nic.it/，然後再提交變更要求。如果網域名稱不符合技術要求 (例如，它未與選用的名稱伺服器關聯)，而且未在 30 天內更正，註冊機構將會刪除您的網域名稱。對於因為不符合技術要求而刪除的網域，我們不會發出退款。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

不支援。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 13 天為止
- 網域已由註冊商刪除：過期後 49 天
- 可透過註冊商進行還原：過期後 14 天至 44 天之間
- 網域已由註冊商刪除：請聯絡 AWS Support。

.me (蒙特內哥羅)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

Domain.me (.me 網域的註冊機構) 將兩個字母的網域名稱和一些更長的網域名稱視為高級網域名稱。您無法向 Route 53 註冊高級 .me 網域或向其轉移這類網域。如需高級 .me 網域名稱的詳細資訊，請參閱 domain.me 網站。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援阿拉伯文、白俄羅斯文、波斯尼亞文、保加利亞文、簡體中文、繁體中文、克羅埃西亞文、丹麥文、法文、德文、印地語、匈牙利文、冰島文、義大利文、韓文、拉脫維亞文、立陶宛文、蒙古文、蒙特內哥羅文、波蘭文、葡萄牙文、俄文、塞爾文、西班牙文、瑞典文、土耳其文和烏克蘭文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 29 天為止
- 網域已從 Route 53 刪除：過期後 30 天
- 可透過註冊商進行還原：過期後 30 天至 60 天之間
- 網域已由註冊商刪除：過期後 65 天

.me.uk (英國)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

如果要轉移 .me.uk 網域至 Route 53，不需要取得授權碼。相反地，請使用目前網域註冊機構提供的方法，將網域 IPS 標籤的值更新為全部大寫的 GANDI。(.uk 網域名稱的註冊機構 Nominet 需要 IPS 標籤。) 如果您的註冊機構不會變更 IPS 標籤的值，請聯絡 Nominet。

> **Note**
>
> 當您註冊 .me.uk 網域時，Route 53 會自動將網域的 IPS 標籤設為 GANDI。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：過期日期前 180 天至過期日期後 30 天之間
- Route 53 可延遲續約：過期後 30 天至 90 天之間
- 網域已從 Route 53 刪除：過期後 90 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 92 天

刪除網域註冊

.me.uk 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

.nl (荷蘭)

Return to index

註冊和續約的租用期間

一年。

限制

開放給大眾使用，但有些限制。

- 擁有者或管理聯絡人必須提供位於荷蘭的有效地址。必須有當地業務。
- 如果您沒有位於荷蘭的有效地址，註冊機構 SIDN 將根據戶籍地址步驟，為您提供戶籍地址。
- 網域名稱必須為 3-63 個字元，但不包括 .nl。

隱私權保護

由註冊機構決定。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期的前 1 天為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期的前 1 天
- 可透過註冊商進行還原：過期前 1 天至過期後 39 天之間
- 網域已由註冊商刪除：過期後 39 天

.org.uk (英國)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

如果要轉移 .org.uk 網域至 Route 53，不需要取得授權碼。相反地，請使用目前網域註冊機構提供的方法，將網域 IPS 標籤的值更新為全部大寫的 GANDI。(.uk 網域名稱的註冊機構 Nominet 需要 IPS 標籤。) 如果您的註冊機構不會變更 IPS 標籤的值，請聯絡 Nominet。

> **Note**
>
> 當您註冊 .org.uk 網域時，Route 53 會自動將網域的 IPS 標籤設為 GANDI。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：過期日期前 180 天至過期日期後 30 天之間
- Route 53 可延遲續約：過期後 30 天至 90 天之間
- 網域已從 Route 53 刪除：過期後 90 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 92 天

刪除網域註冊

.org.uk 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

.ruhr (魯爾區，位於德國西部)

Return to index

.ruhr 域名用於魯爾區 (德國西部)。

註冊和續約的租用期間

1 到 10 年。

限制

開放給大眾使用，但有一項限制：

- 管理聯絡人必須是擁有德國地址的個人。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援 (ä、ö、ü、ß)。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止
- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間

- 網域已由註冊商刪除：請聯絡 AWS Support。

.se (瑞典)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

開放給大眾使用，但有些限制。

- 如果您位於瑞典，則必須提供有效的瑞典 ID 號碼。ID 號碼格式為YYMMDD-NNNN。
- 如果您是在瑞典境外，則必須輸入有效的 ID 號碼，如稅務 ID 號碼。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

不支援。我們建議您限制 RetrieveDomainAuthCodeAPI 動作的存取權限，以防止未經授權的轉移。（當您限制對此 Route 53 API 的訪問時，還可以限制誰可以使用 Route 53 控制台， AWS SDK 和其他程序化方法生成授權代碼。）如需詳細資訊，請參閱 Amazon Route 53 中的身分和存取管理。

國際化網域名稱

支援拉丁文、瑞典文和意第緒文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期的前 1 天為止
- Route 53 可延遲續約：否
- 網域已從 Route 53 刪除：過期的前 1 天
- 可透過註冊商進行還原：過期前 1 天至過期後 59 天之間

- 網域已由註冊商刪除：過期後 64 天

.uk (英國)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

沒有限制地開放給大眾使用。

隱私權保護

所有資訊都會隱藏。

網域鎖定，以防止未經授權的轉移

支援

國際化網域名稱

不支援。

需要授權碼才能轉移至 Route 53

如果要轉移 .uk 網域至 Route 53，不需要取得授權碼。相反地，請使用目前網域註冊機構提供的方法，將網域 IPS 標籤的值更新為全部大寫的 GANDI。(.uk 網域名稱的註冊機構 Nominet 需要 IPS 標籤。) 如果您的註冊機構不會變更 IPS 標籤的值，請聯絡 Nominet。

> **Note**
>
> 當您註冊 .uk 網域，Route 53 會自動將網域的 IPS 標籤設為 GANDI。

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：過期日期前 180 天至過期日期後 30 天之間
- Route 53 可延遲續約：過期後 30 天至 90 天之間

- 網域已從 Route 53 刪除：過期後 90 天
- 可透過註冊商進行還原：否
- 網域已由註冊商刪除：過期後 92 天

刪除網域註冊

.uk 網域的註冊機構不允許您刪除網域註冊。相反地，您必須停用自動續約並等待網域過期。如需詳細資訊，請參閱 刪除網域名稱註冊。

.wien (奧地利維也納市)

Return to index

註冊和續約的租用期間

1 到 10 年。

限制

開放給大眾使用，但有些限制。

- 您必須展示奧地利維也納市的經濟、文化、旅遊、歷史、社會或其他吸引力。
- 在整個註冊期限內，必須將 .wien 網域名稱與上述條件結合。

隱私權保護

不支援。

網域鎖定，以防止未經授權的轉移

支援。

國際化網域名稱

支援拉丁文。

需要授權碼才能轉移至 Route 53

是

DNSSEC

支援網域註冊。如需詳細資訊，請參閱 設定網域的 DNSSEC。

續約及還原網域的截止日期

- 可續約：至過期日期為止

- Route 53 可延遲續約：至過期後 44 天為止
- 網域已從 Route 53 刪除：過期後 45 天
- 可透過註冊商進行還原：過期後 45 天至 75 天之間
- 網域已由註冊商刪除：過期後 80 天

將 Amazon Route 53 設定為 DNS 服務

Amazon Route 53 可以用做網域 (例如 example.com) 的 DNS 服務。當 Route 53 做為您的 DNS 服務，它會透過將易記網域名稱 (如 www.example.com) 轉譯為數字 IP 地址 (如 192.0.2.1，供電腦用於互相連線)，將網際網路流量路由到您的網站。當有人在瀏覽器中輸入您的網域名稱或傳送電子郵件給您，DNS 查詢會轉送到 Route 53，以適當的值回應。例如，Route 53 可能會以 example.com 之 Web 伺服器的 IP 地址回應。

在本章中，我們說明如何設定 Route 53 以將網際網路流量路由至適當位置。我們也會說明如果您目前正在使用其他 DNS 服務，可如何將 DNS 服務遷移至 Route 53，以及如何將 Route 53 用為新網域的 DNS 服務。

主題

- 將 Amazon Route 53 設定為現有網域的 DNS 服務
- 設定新網域的 DNS 路由
- 將流量路由至您的資源
- 使用託管區域
- 處理記錄
- 使用流量流程來路由 DNS 流量
- 在 Amazon Route 53 中設定 DNSSEC 簽署
- 使用 AWS Cloud Map 建立記錄和運作狀態檢查
- DNS 限制和行為

將 Amazon Route 53 設定為現有網域的 DNS 服務

如果您將一或多個網域註冊遷移至 Route 53，並且您目前正在使用不提供付費 DNS 服務的網域註冊機構，則需要先遷移 DNS 服務，再遷移網域。否則，當您傳輸您的網域時，註冊機構將停止提供 DNS 服務，而相關的網站和 Web 應用程式將無法在網際網路上使用。(您也可以將 DNS 服務從目前的註冊商遷移至另一個 DNS 服務提供者。我們不要求您使用 Route 53 做為向 Route 53 註冊之網域的 DNS 服務提供者。)

此程序取決於您目前是否使用該網域：

- 如果該網域目前正在取得流量—例如，如果您的使用者正在使用該網域名稱瀏覽網站或存取 Web 應用程式—請參閱 將 Route 53 做為使用中網域的 DNS 服務。

- 如果該網域未取得任何流量 (或是取得極少的流量)，請參閱將 Route 53 設定為非作用中網域的 DNS 服務。

對於這兩個選項，網域都應該在整個遷移程序期間保持可用。不過在極少的情況下，如果出現問題，第一個選項可讓您快速復原遷移。如果使用第二個選項，您的網域可能在幾天內不可用。

如果您想要與 AWS 中的專家聯絡，請造訪銷售支援。

將 Route 53 做為使用中網域的 DNS 服務

如果要為目前正在取得流量—例如，如果您的使用者正在使用該網域名稱瀏覽網站或存取 Web 應用程式—的網域將 DNS 服務遷移至 Amazon Route 53，請執行本節中的程序。

主題

- 步驟 1：從目前的 DNS 服務提供者取得您目前的 DNS 組態 (選用但建議)
- 步驟 2：建立託管區域
- 步驟 3：建立記錄
- 步驟 4：較低的 TTL 設定
- 步驟 5：(如果您已設定 DNSSEC) 從父區域移除 DS 記錄
- 步驟 6：等待舊 TTL 過期
- 步驟 7：更新 NS 記錄，以使用 Route 53 名稱伺服器
- 步驟 8：監控網域的流量
- 步驟 9：將 NS 記錄的 TTL 變更回較高的值
- 步驟 10：將網域註冊轉移到 Amazon Route 53
- 步驟 11：重新啟用 DNSSEC 簽署 (如果需要)

步驟 1：從目前的 DNS 服務提供者取得您目前的 DNS 組態 (選用但建議)

當您將 DNS 服務從另一個提供者遷移至 Route 53 時，您將在 Route 53 中重現目前的 DNS 組態。在 Route 53 中，您建立一個與您的網域同名的託管區域，而且您在該託管區域中建立記錄。每個記錄表示您希望如何針對指定的網域名稱或子網域名稱路由流量。例如，當有人在 Web 瀏覽器中輸入您的網域名稱，您希望流量路由到資料中心的 Web 伺服器、Amazon EC2 執行個體、CloudFront 分佈或其他位置？

您使用的程序取決於目前 DNS 組態的複雜性：

- 在目前 DNS 組態是簡單的情況下 – 如果您只是將幾個子網域的網際網路流量路由到少數資源 (例如，Web 伺服器或 Amazon S3 儲存貯體)，則可以在 Route 53 主控台中手動建立幾個記錄。
- 在目前 DNS 組態更複雜而且您只希望重現目前組態的情況下 – 如果您可以從目前 DNS 服務提供者取得區域檔案並將該區域檔案匯入 Route 53 中，則可簡化遷移程序。(並非所有 DNS 服務提供者都提供區域檔案。) 當您匯入區域檔案時，Route 53 會在您的託管區域中建立對應記錄來自動重現現有的組態。

  請嘗試詢問您目前 DNS 服務提供者的客戶支援如何取得區域檔案或記錄清單。如需所需區域檔案格式的資訊，請參閱透過匯入區域檔案建立記錄。
- 在目前 DNS 組態更加複雜，而且您對 Route 53 路由功能感興趣的情況下 – 檢閱下列文件，了解您是否需要使用其他 DNS 服務提供者未提供的 Route 53 功能。若是如此，您可以手動建立記錄，也可以匯入區域檔案，並稍後建立或更新記錄：
  - 選擇別名或非別名記錄 說明 Route 53 別名記錄的優勢，這些記錄可免費將流量路由到一些 AWS 資源 (例如 CloudFront 分佈和 Amazon S3 儲存貯體)。
  - 選擇路由政策 說明 Route 53 路由選項，例如，根據使用者位置的路由、根據使用者和資源之間延遲的路由、根據資源是否正常運作的路由，以及根據您指定的權重來路由到資源。

> **Note**
>
> 您也可以匯入區域檔案，並在稍後變更組態以利用別名記錄和複雜的路由政策。

如果您無法取得區域檔案，或者如果您要在 Route 53 中手動建立記錄，則可能要遷移的記錄包括：

- A (地址) 記錄 – 將網域名稱或子網域名稱與對應資源的 IPv4 地址 (例如，192.0.2.3) 建立關聯
- AAAA (地址) 記錄 – 將網域名稱或子網域名稱與對應資源的 IPv6 地址 (例如，2001:0db8:85a3:0000:0000:abcd:0001:2345) 建立關聯
- 郵件伺服器 (MX) 記錄 – 將流量路由至郵件伺服器
- CNAME 記錄 – 將單一網域名稱 (example.net) 的流量重新路由至另一個網域名稱 (example.com)
- 其他支援的 DNS 記錄類型記錄 – 如需支援的記錄類型清單，請參閱 支援的 DNS 記錄類型。

步驟 2：建立託管區域

為了告知 Amazon Route 53 您希望如何路由網域的流量，您建立一個與網域同名的託管區域，然後在該託管區域中建立記錄。

> **Important**
>
> 您只能針對擁有管理許可的網域建立託管區域。一般而言，這表示您擁有網域，但也可能是您為網域註冊者開發應用程式。

當您建立託管區域時，Route 53 會為此區域自動建立名稱伺服器 (NS) 記錄和起始授權 (SOA) 記錄。NS 記錄識別透過 Route 53 與您的託管區域關聯的四個名稱伺服器。為了讓 Route 53 成為網域的 DNS 服務，您需要更新網域註冊以使用這四個名稱伺服器。

> **Important**
>
> 請勿建立其他名稱伺服器 (NS) 或起始授權 (SOA) 記錄，也請勿刪除現有的 NS 和 SOA 記錄。

若要建立託管區域

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 如果您是 Route 53 的新手，請選擇 DNS management (DNS 管理) 下的 Get Started (開始)，然後選擇 Create hosted zones (建立託管區域)。

   如果您已經在使用 Route 53，請在導覽窗格中選擇 Hosted zones (託管區域)，然後選擇 Create hosted zones (建立託管區域)。
3. 在 Create hosted zone (建立託管區域) 窗格中，輸入網域名稱並選擇性輸入註解。如需有關設定的詳細資訊，請選擇開啟右側的說明面板。

   如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。
4. 針對 Type (類型)，接受 Public hosted zone (公有託管區域) 的預設值。
5. 選擇 Create hosted zone (建立託管區域)。

步驟 3：建立記錄

建立託管區域後，您可在該託管區域中建立記錄，這些記錄定義您要將網域 (example.com) 或子網域 (www.example.com) 的流量路由到的位置。例如，如果您希望將 example.com 和 www.example.com

的流量路由到 Amazon EC2 執行個體上的 Web 伺服器，則可建立兩個記錄，一個記錄名為 example.com，另一個記錄名為 www.example.com。在每個記錄，指定 EC2 執行個體的 IP 地址。

您可以透過各種方式建立記錄：

匯入區域檔案

如果您已在 步驟 1：從目前的 DNS 服務提供者取得您目前的 DNS 組態 (選用但建議) 中從目前 DNS 服務取得區域檔案，這是最輕鬆的方式。Amazon Route 53 無法預測何時建立別名記錄或使用特殊路由類型 (例如，加權或容錯移轉)。因此，如果您匯入區域檔案，Route 53 會使用簡單路由政策建立標準 DNS 記錄。

如需更多詳細資訊，請參閱 透過匯入區域檔案建立記錄。

在主控台中個別建立記錄

如果您沒有取得區域檔案，並且您只想建立幾個具有簡單路由政策的記錄來開始操作，則可在 Route 53 主控台中建立記錄。您可以建立別名和非別名記錄。

如需詳細資訊，請參閱下列主題：

- 選擇路由政策
- 選擇別名或非別名記錄
- 使用 Amazon Route 53 主控台來建立記錄

以程式設計方式建立記錄

您可以使用 AWS 開發套件、AWS CLI 或 AWS Tools for Windows PowerShell 建立記錄。如需詳細資訊，請參閱 AWS 文件。

如果您使用 AWS 未提供開發套件的程式設計語言，您也可以使用 Route 53 API。如需詳細資訊，請參閱 Amazon Route 53 API 參考。

步驟 4：較低的 TTL 設定

記錄的 TTL (存留時間) 設定指定您希望 DNS 解析程式快取記錄和使用快取資訊的時間。當 TTL 過期，解析程式會向網域的 DNS 服務提供者傳送另一個查詢以取得最新資訊。

NS 記錄的典型 TTL 設定為 172800 秒或兩天。NS 記錄列出網域名稱系統 (DNS) 可用來取得有關如何路由網域流量的資訊的名稱伺服器。透過為目前 DNS 服務提供者和 Amazon Route 53 降低 NS 記錄的 TTL，可在您將 DNS 遷移至 Route 53 的過程中發現問題時，縮短網域的停機時間。如果未降低 TTL，您的網域可能會在出現問題時最多兩天內在網際網路上無法使用。

> **Note**
>
> 某些完整解析器可能會快取父授權伺服器之 NS 記錄的 TTL，因此也必須減少在父授權 DNS 伺服器上註冊之 NS 記錄的 TTL。

我們建議您針對以下 NS 記錄變更 TTL：

- 目前 DNS 服務提供者的託管區域中的 NS 記錄。(目前提供者可能使用不同的術語。)
- 您在步驟 2：建立託管區域中建立的託管區域中的 NS 記錄。

若要為目前 DNS 服務提供者降低 NS 記錄的 TTL 設定

- 使用網域目前的 DNS 服務提供者提供的方法，來變更網域的託管區域中的 NS 記錄的 TTL。

若要降低 Route 53 託管區域中 NS 記錄的 TTL 設定

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 選擇導覽窗格中的 Hosted Zones (託管區域)。
3. 選擇託管區域的名稱。
4. 選擇 NS 記錄，然後選擇 Edit (編輯)。
5. 變更 TTL (Seconds) (TTL (秒)) 的值。我們建議您指定介於 60 秒和 900 秒 (15 分鐘) 之間的值。
6. 選擇 Save changes (儲存變更)。

步驟 5：(如果您已設定 DNSSEC) 從父區域移除 DS 記錄

如果您已為網域設定 DNSSEC，請先從父區域移除委派簽署人 (DS) 記錄，然後再將網域遷移至 Route 53。

如果父區域託管是透過 Route 53 或其他註冊商託管，請聯絡他們以移除 DS 記錄。

目前無法跨兩個提供者啟用 DNSSEC 簽署，因此您必須移除任何 DS 或 DNSKEY 來停用 DNSSEC。這會暫時向 DNS 解析程式發出訊號，以停用 DNSSEC 驗證。在步驟 11 中，您可以在完成轉換至 Route 53 之後，視需要重新啟用 DNSSEC 驗證。

如需更多詳細資訊，請參閱 刪除網域的公開金鑰。

步驟 6：等待舊 TTL 過期

如果您的網域正在使用中—例如，如果您的使用者正在使用該網域名稱瀏覽網站或存取 Web 應用程式—則 DNS 解析程式已快取目前 DNS 服務提供者所提供的名稱伺服器的名稱。已在幾分鐘前快取該資訊的 DNS 解析程式會將其儲存近兩天。

為了確保一次性完成 DNS 服務到 Route 53 的遷移，請在降低 TTL 後等待兩天。為期兩天的 TTL 過期且解析程式請求您的網域的名稱伺服器後，解析程式將取得目前名稱伺服器，並且還將取得您在步驟 4：較低的 TTL 設定中指定的新 TTL。

步驟 7：更新 NS 記錄，以使用 Route 53 名稱伺服器

如果要開始使用 Amazon Route 53 做為網域的 DNS 服務，請使用註冊商或父區域所提供的方法，以 Route 53 名稱伺服器取代 NS 記錄中目前的名稱伺服器。

> **Note**
>
> 當您使用目前的 DNS 服務提供者來更新 NS 記錄以使用 Route 53 名稱伺服器時，您會更新網域的 DNS 組態。(這相當於更新網域的 Route 53 託管區域中的 NS 記錄，差別在於使用要移出的 DNS 服務來更新設定。)

若要更新註冊商或父區域的 NS 記錄，以使用 Route 53 名稱伺服器

1. 在 Route 53 主控台中，取得託管區域的名稱伺服器：
   a. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
   b. 在導覽窗格中，選擇 Hosted zones (託管區域)。
   c. 在 Hosted zones (託管區域) 頁面上，選擇適用託管區域的名稱。
   d. 記下 Hosted zone details (託管區域詳細資訊)中 Name servers (名稱伺服器) 下列出的四個名稱。
2. 使用網域目前的 DNS 服務提供的方法，更新託管區域的 NS 記錄。如果此網域已向 Route 53 註冊，請參閱 新增或變更網域的名稱伺服器和黏附記錄。具體程序取決於目前的 DNS 服務是否可讓您刪除名稱伺服器：

   如果您可以刪除名稱伺服器

- 記下託管區域 NS 記錄中目前名稱伺服器的名稱。如果您需要恢復到目前的 DNS 組態，這些是您要指定的伺服器。
- 從 NS 記錄刪除目前的名稱伺服器。
- 使用您在此程序的步驟 1 中取得的四個 Route 53 名稱伺服器名稱來更新 NS 記錄。

> **Note**
>
> 完成後，NS 記錄的名稱伺服器只會有四個 Route 53 名稱伺服器。

如果您無法刪除名稱伺服器

- 選擇使用自訂名稱伺服器的選項。
- 新增全部四個在此程序步驟 1 中取得的 Route 53 名稱伺服器。

步驟 8：監控網域的流量

監控網域的流量，包括網站或應用程式流量和電子郵件：

- 如果流量慢或停止 – 使用上一個 DNS 服務提供的方法，將網域名稱伺服器變更回之前的名稱伺服器。這些是您在 若要更新註冊商或父區域的 NS 記錄，以使用 Route 53 名稱伺服器 的步驟 7 中記下的名稱伺服器。然後判斷發生什麼錯誤。
- 如果流量不受影響 – 繼續執行 步驟 9：將 NS 記錄的 TTL 變更回較高的值。

步驟 9：將 NS 記錄的 TTL 變更回較高的值

在網域的 Amazon Route 53 託管區域中，將 NS 記錄的 TTL 變更為更典型的值，例如，172800 秒 (兩天)。這減少使用者的延遲，因為他們不必像 DNS 解析程式一樣通常需要等待為網域的名稱伺服器傳送查詢。

若要變更 Route 53 託管區域中 NS 記錄的 TTL

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 選擇導覽窗格中的 Hosted Zones (託管區域)。
3. 選擇託管區域的名稱。

4. 在託管區域的記錄清單中，選擇 NS 記錄。
5. 選擇 編輯 。
6. 將 TTL (Seconds) (TTL (秒)) 變更為您希望 DNS 解析程式快取網域之名稱伺服器名稱的秒數。我們建議值 172800 秒。
7. 選擇 Save changes (儲存變更)。

步驟 10：將網域註冊轉移到 Amazon Route 53

現在您已將網域的 DNS 服務轉移到 Amazon Route 53，您可以選擇將網域的註冊轉移到 Route 53。如需更多詳細資訊，請參閱 將網域註冊轉移到 Amazon Route 53。

步驟 11：重新啟用 DNSSEC 簽署 (如果需要)

現在您已將網域的 DNS 服務轉移到 Amazon Route 53，接下來可以重新啟用 DNSSEC 簽署。

啟用 DNSSEC 簽章有兩個步驟：

- 步驟 1：啟用 Route 53 的 DNSSEC 簽署，並要求 Route 53 根據 AWS Key Management Service (AWS KMS) 中的客戶受管金鑰建立金鑰簽署金鑰 (KSK)。
- 步驟 2：將委派簽署人 (DS) 記錄新增至父區域，以建立託管區域的信任鏈，以便透過受信任的密碼編譯簽章驗證 DNS 回答。

  如需說明，請參閱 啟用 DNSSEC 簽署並建立信任鏈。

將 Route 53 設定為非作用中網域的 DNS 服務

如果要為不取得任何流量 (或取得非常少的流量) 的網域將 DNS 服務遷移到 Amazon Route 53，請執行本節中的程序。

主題

- 步驟 1：從目前的 DNS 服務提供者取得您目前的 DNS 組態 (非作用中網域)
- 步驟 2：建立託管區域 (非作用中網域)
- 步驟 3：建立記錄 (非作用中網域)
- 步驟 4：更新網域註冊以使用 Amazon Route 53 名稱伺服器 (非作用中網域)

步驟 1：從目前的 DNS 服務提供者取得您目前的 DNS 組態 (非作用中網域)

當您將 DNS 服務從另一個提供者遷移至 Route 53 時，您將在 Route 53 中重現目前的 DNS 組態。在 Route 53 中，您建立一個與您的網域同名的託管區域，而且您在該託管區域中建立記錄。每個記錄表示您希望如何針對指定的網域名稱或子網域名稱路由流量。例如，當有人在 Web 瀏覽器中輸入您的網域名稱，您希望流量路由到資料中心的 Web 伺服器、Amazon EC2 執行個體、CloudFront 分佈或其他位置？

您使用的程序取決於目前 DNS 組態的複雜性：

- 在目前 DNS 組態是簡單的情況下 – 如果您只是將幾個子網域的網際網路流量路由到少數資源 (例如，Web 伺服器或 Amazon S3 儲存貯體)，則可以在 Route 53 主控台中手動建立幾個記錄。
- 在目前 DNS 組態更複雜而且您只希望重現目前組態的情況下 – 如果您可以從目前 DNS 服務提供者取得區域檔案並將該區域檔案匯入 Route 53 中，則可簡化遷移程序。(並非所有 DNS 服務提供者都提供區域檔案。) 當您匯入區域檔案時，Route 53 會在您的託管區域中建立對應記錄來自動重現現有的組態。

  請嘗試詢問您目前 DNS 服務提供者的客戶支援如何取得區域檔案或記錄清單。如需所需區域檔案格式的資訊，請參閱透過匯入區域檔案建立記錄。
- 在目前 DNS 組態更加複雜，而且您對 Route 53 路由功能感興趣的情況下 – 檢閱下列文件，了解您是否需要使用其他 DNS 服務提供者未提供的 Route 53 功能。若是如此，您可以手動建立記錄，也可以匯入區域檔案，並稍後建立或更新記錄：
  - 選擇別名或非別名記錄 說明 Route 53 別名記錄的優勢，這些記錄可免費將流量路由到一些 AWS 資源 (例如 CloudFront 分佈和 Amazon S3 儲存貯體)。
  - 選擇路由政策 說明 Route 53 路由選項，例如，根據使用者位置的路由、根據使用者和資源之間延遲的路由、根據資源是否正常運作的路由，以及根據您指定的權重來路由到資源。

> **Note**
>
> 您也可以匯入區域檔案，並在稍後變更組態以利用別名記錄和複雜的路由政策。

如果您無法取得區域檔案，或者如果您要在 Route 53 中手動建立記錄，則可能要遷移的記錄包括：

- A (地址) 記錄 – 將網域名稱或子網域名稱與對應資源的 IPv4 地址 (例如，192.0.2.3) 建立關聯
- AAAA (地址) 記錄 – 將網域名稱或子網域名稱與對應資源的 IPv6 地址 (例如，2001:0db8:85a3:0000:0000:abcd:0001:2345) 建立關聯

- 郵件伺服器 (MX) 記錄 – 將流量路由至郵件伺服器
- CNAME 記錄 – 將單一網域名稱 (example.net) 的流量重新路由至另一個網域名稱 (example.com)
- 其他支援的 DNS 記錄類型記錄 – 如需支援的記錄類型清單，請參閱 支援的 DNS 記錄類型。

步驟 2：建立託管區域 (非作用中網域)

為了告知 Amazon Route 53 您希望如何路由網域的流量，您建立一個與網域同名的託管區域，然後在該託管區域中建立記錄。

> **Important**
>
> 您只能針對擁有管理許可的網域建立託管區域。一般而言，這表示您擁有網域，但也可能是您為網域註冊者開發應用程式。

當您建立託管區域時，Route 53 會為此區域自動建立名稱伺服器 (NS) 記錄和起始授權 (SOA) 記錄。NS 記錄識別透過 Route 53 與您的託管區域關聯的四個名稱伺服器。為了讓 Route 53 成為網域的 DNS 服務，您需要更新網域註冊以使用這四個名稱伺服器。

> **Important**
>
> 請勿建立其他名稱伺服器 (NS) 或起始授權 (SOA) 記錄，也請勿刪除現有的 NS 和 SOA 記錄。

若要建立託管區域

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 若您是初次使用 Route 53，請選擇 Get Started (開始使用)。

   如果您已經在使用 Route 53，請在導覽窗格中選擇 Hosted zones (託管區域)。
3. 選擇 Create hosted zone (建立託管區域)。
4. 在 Create hosted zone (建立託管區域) 窗格中，輸入網域名稱並選擇性輸入註解。如需設定的詳細資訊，請將滑鼠指標停留在其標籤上，以查看工具提示。

   如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。

5. 針對 Record Type (記錄類型)，接受 Public hosted zone (公有託管區域) 的預設值。
6. 選擇 Create hosted zone (建立託管區域)。

步驟 3：建立記錄 (非作用中網域)

建立託管區域後，您可在該託管區域中建立記錄，這些記錄定義您要將網域 (example.com) 或子網域 (www.example.com) 的流量路由到的位置。例如，如果您希望將 example.com 和 www.example.com 的流量路由到 Amazon EC2 執行個體上的 Web 伺服器，則可建立兩個記錄，一個記錄名為 example.com，另一個記錄名為 www.example.com。在每個記錄，指定 EC2 執行個體的 IP 地址。

您可以透過各種方式建立記錄：

匯入區域檔案

如果您已在 步驟 1：從目前的 DNS 服務提供者取得您目前的 DNS 組態 (非作用中網域) 中從目前 DNS 服務取得區域檔案，這是最輕鬆的方式。Amazon Route 53 無法預測何時建立別名記錄或使用特殊路由類型 (例如，加權或容錯移轉)。因此，如果您匯入區域檔案，Route 53 會使用簡單路由政策建立標準 DNS 記錄。

如需更多詳細資訊，請參閱 透過匯入區域檔案建立記錄。

在主控台中個別建立記錄

如果您沒有取得區域檔案，並且您只想建立幾個具有簡單路由政策的記錄來開始操作，則可在 Route 53 主控台中建立記錄。您可以建立別名和非別名記錄。

如需詳細資訊，請參閱下列主題：

- 選擇路由政策
- 選擇別名或非別名記錄
- 使用 Amazon Route 53 主控台來建立記錄

以程式設計方式建立記錄

您可以使用 AWS 開發套件、AWS CLI 或 AWS Tools for Windows PowerShell 建立記錄。如需詳細資訊，請參閱 AWS 文件。

如果您使用 AWS 未提供開發套件的程式設計語言，您也可以使用 Route 53 API。如需詳細資訊，請參閱 Amazon Route 53 API 參考。

步驟 4：更新網域註冊以使用 Amazon Route 53 名稱伺服器 (非作用中網域)

當您完成建立網域的記錄，您可以將網域的 DNS 服務變更為 Amazon Route 53。執行下列程序以更新網域註冊商的設定。

若要更新網域的名稱伺服器

1. 在 Route 53 主控台中，取得 Route 53 託管區域的名稱伺服器：
   a. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
   b. 在導覽窗格中，選擇 Hosted zones (託管區域)。
   c. 在 Hosted zones (託管區域) 頁面上，選擇託管區域的選項按鈕 (而非名稱)，然後選擇 View details (檢視詳細資訊)。
   d. 在託管區域的詳細資訊頁面上，選擇託管區域詳細資訊。
   e. 記下 Name Servers (名稱伺服器) 下所列的四個名稱。
2. 使用網域註冊商提供的方法，將網域的名稱伺服器變更為使用您在此程序的步驟 2 中取得的四個 Route 53 名稱伺服器。

   如果此網域已向 Route 53 註冊，請參閱 新增或變更網域的名稱伺服器和黏附記錄。

設定新網域的 DNS 路由

當您以 Route 53 註冊網域時，我們會自動將 Route 53 用為網域的 DNS 服務。Route 53 會建立與域網名稱相同的託管區域、為託管區域指派四個名稱伺服器，並更新網域以使用這些名稱伺服器。

若要指定您希望 Route 53 如何路由網域的網際網路流量，請在託管區域中建立記錄。例如，如果您希望將 example.com 的請求路由至在 Amazon EC2 執行個體上執行的 Web 伺服器，您可以在 example.com 託管區域中建立記錄，並指定 EC2 執行個體的彈性 IP 地址。如需詳細資訊，請參閱下列主題：

- 如需如何在託管區域中建立記錄的詳細資訊，請參閱 處理記錄。
- 如需如何將流量路由至所選 AWS 資源的資訊，請參閱 將網際網路流量路由到您的 AWS 資源。
- 如需 DNS 運作方式的資訊，請參閱如何將網際網路流量路由到您的網站或 Web 應用程式。

將流量路由至您的資源

例如，當使用者在 Web 瀏覽器中輸入您的網域名稱，以請求您的網站或 Web 應用程式，Amazon Route 53 可將使用者路由至您的資源 (例如您資料中心的 Amazon S3 儲存貯體或 Web 伺服器)。若要設定 Route 53 將流量路由至您的資源，請執行下列操作：

1. 建立託管區域。您可以建立公有託管區域或私有託管區域：

   公有託管區域

   例如，如果您希望將網際網路流量路由至您的資源，您可以建立公有託管區域，以便客戶檢視您在 EC2 執行個體上託管的公司網站。如需更多詳細資訊，請參閱 使用公有託管區域。

   私有託管區域

   如果您希望在 Amazon VPC 內路由流量，您可以建立私有託管區域。如需更多詳細資訊，請參閱 使用私有託管區域。

2. 在託管區域中建立記錄。記錄會定義您希望為每個網域名稱或子網域名稱路由流量的位置。例如，若要將 www.example.com 流量路由至您資料中心的 Web 伺服器，一般做法是在 example.com 託管區域中建立 www.example.com 記錄。

   如需詳細資訊，請參閱下列主題：

   - 處理記錄
   - 路由傳送子網域的流量
   - 將網際網路流量路由到您的 AWS 資源

路由傳送子網域的流量

若要將流量路由至子網路的資源 (例如 acme.example.com 或 zenith.examplec.com)，您有兩種選擇：

在網域的託管區域中建立記錄

一般而言，若要路由子網域的流量，需要在與網域名稱相同的託管區域中建立記錄。例如，若要將 acme.example.com 網際網路流量路由至您資料中心的 Web 伺服器，請在 example.com 託管區域中建立名為 acme.example.com 的記錄。如需詳細資訊，請參閱主題 處理記錄 及其子主題。

建立子網域的託管區域，並在新的託管區域中建立記錄

您也可以為子網域建立託管區域。使用個別託管區域將網際網路流量路由至子網域，有時稱為「將子網域的責任委派給託管區域」、「將子網域委派給其他的名稱伺服器」或類似的術語組合。以下概述運作方式：

1. 您建立託管區域與您想要路由傳送流量的子網域名稱相同，例如 acme.example.com。
2. 您可以在新的託管區域中建立記錄，以定義要如何路由子網域 (acme.example.com) 及其子網域 (例如 backend.acme.example.com) 的流量。
3. 您會取得建立新託管區域時 Route 53 指派給新託管區域之名稱伺服器的名稱。
4. 您可以為網域在託管區域中建立新的 NS 記錄 (example.com)，並指定您在步驟 3 中取得的四個名稱伺服器。

使用個別託管區域來路由子網域的流量時，您可以使用 IAM 許可來限制存取子網域的託管區域。如果您有多個由不同群組管理的子網域，為每個子網域建立託管區域可大幅減少必須存取網域託管區域中記錄的人員數量。

為子網域使用個別託管區域，也可讓您為網域和子網域使用不同的 DNS 服務。如需更多詳細資訊，請參閱 將 Amazon Route 53 做為子網域的 DNS 服務，而不需遷移父系網域。

對於來自每個 DNS 解析程式的第一個 DNS 查詢，此組態具有微小的效能影響。解析程式必須從根網域的託管區域取得資訊，然後從子網域的託管區域取得資訊。在子網域的第一次 DNS 查詢之後，解析程式會快取資訊，並且直到 TTL 過期、其他用戶端請求該解析程式的子網域前，不需要再次取得該資訊。如需詳細資訊，請參閱 您在建立或編輯 Amazon Route 53 記錄指定的值 一節中的 TTL (秒)。

主題

- 建立另一個託管區域來路由子網域的流量
- 路由其他子網域層級的流量

建立另一個託管區域來路由子網域的流量

路由子網域流量的其中一種方法，是為子網域建立託管區域，然後在新託管區域中為子網域建立記錄。(較常見的選項是在網域託管區域中建立子網域的記錄)。

> **Note**
>
> 雖然我們在此說明於 Route 53 上建立及委派給子網域託管區域的程序，但您也可以在其他名稱伺服器上建立 DNS 區域，以及類似地建立將責任委派給這些名稱伺服器的名稱伺服器 (NS) 記錄。

下列為此程序的概觀：

1. 為子網域建立 託管區域。如需更多詳細資訊，請參閱 為子網域建立新託管區域。
2. 將記錄新增至子網域的託管區域。如果網域託管區域包含屬於子網域託管區域的任何記錄，請在子網域的託管區域中複製這些記錄。如需詳細資訊，請參閱 在子網域的託管區域中建立記錄
3. 在網域託管區域中為子網域建立 NS 記錄，將子網域的責任委派給新託管區域中的名稱伺服器。如果網域託管區域包含屬於子網域託管區域的任何記錄，請從網域託管區域中刪除這些記錄。(您已在步驟 2 建立子網域託管區域的複本。) 如需更多詳細資訊，請參閱 更新網域的託管區域。

為子網域建立新託管區域

若要使用 Route 53 主控台為子網域建立託管區域，請執行下列程序。

為子網域建立託管區域 (主控台)

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 若您是初次使用 Route 53，請選擇 Get Started (開始使用)。

   如果您已經在使用 Route 53，請在導覽窗格中選擇 Hosted zones (託管區域)。
3. 選擇 Create Hosted Zone (建立託管區域)。
4. 在右窗格中，輸入子網域的名稱，例如 acme.example.com。您也可以選擇輸入註解。

   如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。
5. 針對 Type (類型)，接受 Public Hosted Zone (公有託管區域) 的預設值。
6. 在右窗格底部，選擇 Create hosted zone (建立託管區域)。

在子網域的託管區域中建立記錄

若要定義 Route 53 該如何路由子網域 (acme.example.com) 及其子網域 (例如 backend.acme.example.com) 的流量，您可以在子網域的託管區域中建立記錄。

請注意下列在子網域託管區域中建立記錄的相關資訊：

- 請勿在子網域託管區域中建立其他名稱伺服器 (NS) 或起始授權 (SOA) 記錄，也請勿刪除現有的 NS 和 SOA 記錄。
- 在子網域託管區域中建立子網域的所有記錄。例如，如果您擁有 example.com 和 acme.example.com 網域的託管區域，請在 acme.example.com 託管區域中，為 acme.example.com 子網域建立所有記錄。包括諸如 backend.acme.example.com 和 beta.backend.acme.example.com 等記錄。
- 如果網域 (example.com) 託管區域已包含屬於子網域 (acme.example.com) 託管區域的記錄，請在子網域的託管區域中複製這些記錄。在程序最後一個步驟中，您稍後會從網域託管區域刪除重複的記錄。

> **Important**
>
> 如果您在網域託管區域和子網域託管區域中都擁有子網域的某些記錄，DNS 的行為將會不一致。行為取決於 DNS 解析程式已快取哪些名稱伺服器、網域託管區域 (example.com) 的名稱伺服器或子網域託管區域 (acme.example.com) 的名稱伺服器。在某些情況下，如已存在記錄，Route 53 會傳回 NXDOMAIN (不存在的網域)，但不會在 DNS 解析程式提交查詢至的託管區域中。

如需更多詳細資訊，請參閱 處理記錄。

更新網域的託管區域

建立託管區域時，Route 53 會自動將四個名稱伺服器指派給區域。託管區域的 NS 記錄會找出回應網域或子網域 DNS 查詢的名稱伺服器。若要開始使用子網域託管區域的記錄來路由網際網路流量，請在建立網域 (example.com) 託管區域中建立新的 NS 記錄，並為其指定子網域 (acme.example.com) 名稱。針對 NS 記錄的值，請指定子網域託管區域中名稱伺服器的名稱。

當 Route 53 從子網域 acme.example.com 或其子網域之一收到 DNS 解析程式的 DNS 查詢，會發生下列情況：

1. Route 53 會在網域 (example.com) 託管區域中找出子網域 (acme.example.com) 的 NS 記錄。

2. Route 53 會從網域 (example.com) 託管區域的 acme.example.com NS 記錄取得名稱伺服器，並將這些名稱伺服器傳回 DNS 解析程式。
3. 解析程式會將 acme.example.com 的查詢，重新提交給 acme.example.com 託管區域的名稱伺服器。
4. Route 53 會使用 acme.example.com 託管區域的記錄來回應查詢。

若要設定 Route 53 子網域使用託管區域來路由子網域流量，並從網域託管區域刪除任何重複的記錄，請執行下列程序：

設定 Route 53 使用子網域託管區域 (主控台)

1. 在 Route 53 主控台中，取得子網域託管區域的名稱伺服器：
   a. 在導覽窗格中，選擇 Hosted zones (託管區域)。
   b. 在 Hosted Zones (託管區域) 頁面上，選擇子網域的託管區域的名稱。
   c. 在右窗格中，複製 Hosted zones details (託管區域詳細資訊) 部分中 Name Servers (名稱伺服器) 下所列的四個伺服器名稱。
2. 選擇網域 (example.com) 託管區域的名稱，而不是子網域託管區域的名稱。
3. 選擇 Create record (建立記錄)。
4. 選擇 Simple routing (簡易路由)，然後選擇 Next (下一步)。
5. 選擇 Define simple record (定義簡易記錄)。
6. 指定下列值：

   名稱

   輸入子網域的名稱。

   值/將流量路由到

   選擇IP 地址或其他值，視紀錄類型而定，然後貼上您在步驟 1 中複製的名稱伺服器的名稱。

   記錄類型

   選擇 NS — 託管區域的名稱伺服器。

   TTL (秒)

   將 NS 記錄變更為更常用的值，例如 172800 秒。
7. 選擇 Define simple record (定義簡易記錄)，然後選擇 Create records (建立記錄)。

8. 如果網域託管區域包含您在子網域託管區域中重新建立的任何記錄，請從網域託管區域中刪除這些記錄。如需更多詳細資訊，請參閱 刪除記錄。

   完成後，子網域的所有記錄應該會位於子網域託管區域中。

路由其他子網域層級的流量

將流量路由至子網域的子網域 (例如 backend.acme.example.com)，方法與將流量路由至子網域 (例如 acme.example.com) 相同。您可以在網域託管區域中建立記錄，或是在為較低層級的子網域建立託管區域，然後在該新託管區域中建立記錄。

如果您選擇為較低層級的子網域建立個別託管區域，請為託管區域中較低層級的子網域 (距離網域名稱較近一級) 建立 NS 記錄。這有助於確保流量正確路由至您的資源。例如，假設您希望路由下列子網域的流量：

- subdomain1.example.com
- subdomain2.subdomain1.example.com

若要使用另一個託管區域來路由 subdomain2.subdomain1.example.com 的流量，請執行下列操作：

1. 建立名為 subdomain2.subdomain1.example.com 的託管區域。
2. 在 subdomain2.subdomain1.example.com 託管區域中建立記錄。如需更多詳細資訊，請參閱 在子網域的託管區域中建立記錄。
3. 複製 subdomain2.subdomain1.example.com 託管區域名稱伺服器的名稱。
4. 在 subdomain1.example.com 託管區域中，建立名為 subdomain2.subdomain1.example.com 的 NS 記錄，並貼在 subdomain2.subdomain1.example.com 託管區域的名稱伺服器名稱中。

   此外，刪除 subdomain1.example.com 中任何重複的記錄。如需更多詳細資訊，請參閱 更新網域的託管區域。

   建立此 NS 記錄後，Route 53 會開始使用 subdomain2.subdomain1.example.com 託管區域來路由 subdomain2.subdomain1.example.com 子網域的流量。

使用託管區域

託管區域是記錄的容器，記錄包含您希望如何路由特定網域 (如 example.com) 或其子網域 (acme.example.com、zenith.example.com) 的網際網路流量等相關資訊。託管區域和對應的網域具有相同名稱。有兩種類型的託管區域：

- 公有託管區域包含指定您希望如何在網際網路上路由流量的記錄。如需更多詳細資訊，請參閱 使用公有託管區域。
- 私有託管區域包含指定您希望如何在 Amazon VPC 中路由流量的記錄。如需更多詳細資訊，請參閱使用私有託管區域。

使用公有託管區域

公有託管區域是一種容器，其中包含您希望如何路由特定網域 (如 example.com) 或其子網域 (acme.example.com、zenith.example.com) 的網際網路流量等相關資訊。您可以使用下列兩種方式之一來取得公有託管區域：

- 當您向 Route 53 註冊網域時，我們會自動為您建立託管區域。
- 當您將現有網域的 DNS 服務轉移至 Route 53 時，您會先從建立網域的託管區域開始。如需更多詳細資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

在這兩種情況下，您都要在託管區域中建立記錄以指定您希望如何路由網域和子網域的流量。例如，您可以建立一個記錄將 www.example.com 的流量路由到 CloudFront 分佈或資料中心的 Web 伺服器。如需記錄的詳細資訊，請參閱 處理記錄。

本主題說明如何使用 Amazon Route 53 主控台來建立、列出和刪除公有託管區域。

> **Note**
>
> 您也可以使用 Route 53 的私有託管區域路由一或多個您透過 Amazon VPC 服務所建立之 VPC 內的流量。如需更多詳細資訊，請參閱 使用私有託管區域。

主題

- 使用公有託管區域的考量
- 建立公有託管區域

- 取得公有託管區域的名稱伺服器
- 列出公有託管區域
- 檢視公有託管區域的 DNS 查詢指標
- 刪除公有託管區域
- 檢查來自 Route 53 的 DNS 回答
- 設定白標籤名稱伺服器
- Amazon Route 53 為公有託管區域建立的 NS 和 SOA 記錄

使用公有託管區域的考量

使用公有託管區域時請注意以下考量：

NS 和 SOA 記錄

當您建立託管區域時，Amazon Route 53 會為此區域自動建立名稱伺服器 (NS) 記錄和起始授權 (SOA) 記錄。NS 記錄會識別您提供給註冊商或 DNS 服務的四個名稱伺服器，以便系統將 DNS 查詢路由到 Route 53 名稱伺服器。如需 NS 和 SOA 記錄的詳細資訊，請參閱 Amazon Route 53 為公有託管區域建立的 NS 和 SOA 記錄。

名稱相同的多個託管區域

您可以建立多個具有相同名稱的託管區域，然後將不同的記錄新增至每個託管區域。Route 53 會將四個名稱伺服器指派給每個託管區域，而且每個託管區域的名稱伺服器各不相同。當您更新註冊商的名稱伺服器記錄，請謹慎將 Route 53 名稱伺服器用於正確的託管區域 (其中包含您希望 Route 53 在回應網域查詢時使用的記錄)。對於名稱相同的其他託管區域中的記錄，Route 53 永遠不會傳回值。

可重複使用的委派組

在預設情況下，Route 53 會將一組四個唯一的名稱伺服器 (統稱為委派組) 指派給每個您建立的託管區域。如果您要建立大量託管區域，可透過編寫程式的方式建立可重複使用的委派組。(Route 53 主控台不提供可重複使用的委派集。) 然後，您可採用程式設計方式建立託管區域，並將同一組可重複使用的委派組 (相同的四個名稱伺服器) 指派給每個託管區域。

可重複使用的委派組可簡化將 DNS 服務遷移至 Route 53 的程序，因為您可以指示網域名稱註冊商針對您要讓 Route 53 成為其 DNS 服務的所有網域，使用相同的四個名稱伺服器。如需詳細資訊，請參閱 Amazon Route 53 API 參考中的 CreateCloudFrontOriginAccessIdentity。

建立公有託管區域

公有託管區域是一種容器，其中包含您希望如何路由特定網域 (如 example.com) 或其子網域 (acme.example.com、zenith.example.com) 的網際網路流量等相關資訊。建立託管區域之後，您可以建立記錄以指定您希望如何路由網域和子網域的流量。

> **Important**
>
> 您只能針對擁有管理許可的網域建立託管區域。一般而言，這表示您擁有網域，但也可能是您為網域註冊者開發應用程式。

使用 Route 53 主控台建立公有託管區域

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 如果您剛開始使用 Route 53，請在 DNS Management (DNS 管理) 下選擇 Get Started (開始使用)。

   如果您已經在使用 Route 53，請在導覽窗格中選擇 Hosted zones (託管區域)。
3. 選擇 Create Hosted Zone (建立託管區域)。
4. 在 Create Hosted Zone (建立託管區域) 窗格中，輸入要將流量路由所至的網域。您也可以選擇輸入註解。

   如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。
5. 針對 Type (類型)，接受 Public Hosted Zone (公有託管區域) 的預設值。
6. 選擇 Create (建立)。
7. 建立記錄以指定您想如何路由網域和子網域的流量。如需更多詳細資訊，請參閱 處理記錄。
8. 若要使用新託管區域中的記錄來路由網域的流量，請參閱適用的主題：
   - 如果您的網域已向其他網域註冊商註冊，要將 Route 53 設為該網域的 DNS 服務時，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。
   - 如果此網域已向 Route 53 註冊，請參閱 新增或變更網域的名稱伺服器和黏附記錄。

取得公有託管區域的名稱伺服器

若要變更網域註冊的 DNS 服務，您需要取得公有託管區域的名稱伺服器。如需如何變更 DNS 服務的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

> **Note**
>
> 有些註冊商只允許使用 IP 地址指定名稱伺服器；不允許指定完整網域名稱。如果您的註冊商要求使用 IP 地址，您可以使用 dig 公用程式 (適用於 Mac、Unix 或 Linux) 或 nslookup 公用程式 (適用於 Windows) 來取得名稱伺服器的 IP 地址。我們很少變更名稱伺服器的 IP 地址；如果需要變更 IP 地址，我們會提前通知您。

若要使用 Route 53 主控台來取得託管區域的名稱伺服器

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，按一下 Hosted zones (託管區域)。
3. 在 Hosted zones (託管區域) 頁面上，選擇託管區域的選項按鈕 (而非名稱)，然後選擇 View details (檢視詳細資訊)。
4. 在託管區域的詳細資訊頁面上，選擇託管區域詳細資訊。
5. 記下 Name Servers (名稱伺服器) 下所列的四個伺服器。

列出公有託管區域

您可以使用 Amazon Route 53 主控台，列出目前 AWS 帳戶建立的所有託管區域。如需有關如何使用 Route 53 API 列出託管區域的資訊，請參閱 Amazon Route 53 API 參考中的 ListHostedZones。

若要使用 Route 53 主控台列出與 AWS 帳戶關聯的公有託管區域

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。該頁面會自動顯示與您目前登入的 AWS 帳戶相關聯的託管區域清單。
3. 若要篩選託管區域，請使用資料表頂端的搜尋列。

   搜尋行為取決於託管區域最多包含 2,000 個記錄或超過 2,000 個記錄：

最多 2,000 個託管區域

- 若要顯示具有特定值的記錄，請按一下搜尋列，從下拉式清單中選擇屬性，然後輸入值。您也可以直接在搜尋列輸入值，然後按 Enter 鍵。例如，若要顯示名稱以 **abc** 開頭的託管區域，請在搜尋列輸入該值，然後按 Enter 鍵。
- 若只要顯示類型相同的託管區域，請從下拉式清單中選取該類型，然後輸入類型。

超過 2,000 個託管區域

- 您可以根據確切的網域名稱、所有內容和類型來搜尋內容。
- 使用確切的網域名稱搜尋，以更快取得搜尋結果。

檢視公有託管區域的 DNS 查詢指標

您可以針對 Route 53 回應指定的公有託管區域或公有託管區域組合來檢視 DNS 查詢總數。指標會出現在 CloudWatch 中，可讓您檢視圖形、選擇您要檢視的時段，以及以各種其他方式自訂指標。您也可以建立警示和設定通知，以便在指定期間內 DNS 查詢數量超過或低於指定層級時收到通知。

> **Note**
>
> Route 53 會自動針對所有公有託管區域，將 DNS 查詢數量傳送至 CloudWatch，因此您不需要設定任何項目，即可檢視查詢指標。DNS 查詢指標無須付費。

會將哪些 DNS 查詢列入計算？

指標只包含 DNS 解析程式轉送至 Route 53 的查詢。如果 DNS 解析程式已快取對查詢的回應 (如 example.com 的負載平衡器的 IP 地址)，解析程式會繼續傳回快取的回應而不將查詢轉送到 Route 53，直到對應記錄的 TTL 到期為止。

根據為網域名稱 (example.com) 或子網域名稱 (www.example.com) 提交的 DNS 查詢數量、使用者正在使用的解析程式，以及記錄的 TTL，DNS 查詢指標可能只包含提交到 DNS 解析程式的數千個查詢中的一個查詢的資訊。如需 DNS 運作方式的詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

託管區域的查詢指標何時開始出現在 CloudWatch 中？

建立託管區域之後，會延遲幾個小時，之後託管區域才會出現在 CloudWatch 中。此外，您必須提交託管區域中記錄的 DNS 查詢，才能顯示資料。

指標僅在美國東部 (維吉尼亞北部) 區域提供。

若要在控制台上取得該指標，您必須選擇美國東部 (維吉尼亞北部) 區域。若要使用 AWS CLI 取得指標，您必須未指定 AWS 區域，或者指定 `us-east-1` 作為區域。如果您選擇任何其他區域，Route 53 指標將無法使用。

DNS 查詢的 CloudWatch 指標和維度

如需 DNS 查詢的 CloudWatch 指標和維度的詳細資訊，請參閱 使用 Amazon 監控託管區域 CloudWatch。如需 CloudWatch 指標的資訊，請參閱 Amazon CloudWatch 使用者指南中的使用 Amazon CloudWatch 指標。

取得關於 DNS 查詢的詳細資訊

若要取得 Route 53 回應之每個 DNS 查詢的詳細資訊 (包括下列值)，您可以設定查詢記錄：

- 請求的網域或子網域
- 請求的日期和時間
- DNS 記錄類型 (例如 A 或 AAAA)
- 回應 DNS 查詢的 Route 53 節點。
- DNS 回答代碼，例如 `NoError` 或 `ServFail`

如需更多詳細資訊，請參閱 公有 DNS 查詢日誌記錄。

如何取得 DNS 查詢指標

在您建立託管區域之後不久，Amazon Route 53 會每分鐘將指標和維度傳送到 CloudWatch 一次。您可以使用以下程序，在 CloudWatch 主控台中檢視指標，或透過使用 AWS Command Line Interface (AWS CLI) 檢視指標。

主題

- 在 CloudWatch 主控台中檢視公有託管區域的 DNS 查詢指標
- 使用 AWS CLI 取得 DNS 查詢指標

在 CloudWatch 主控台中檢視公有託管區域的 DNS 查詢指標

若要在 CloudWatch 主控台中檢視公有託管區域的 DNS 查詢指標，請執行下列程序。

在 CloudWatch 主控台上檢視公有託管區域的 DNS 查詢指標

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/cloudwatch/ 的 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Metrics (指標)。
3. 在主控台視窗右上角的 AWS 區域清單中，選擇美國東部 (維吉尼亞北部)。如果您選擇任何其他 AWS 區域，Route 53 指標將無法使用。
4. 在 All metrics (所有指標) 標籤上，選擇 Route 53。
5. 選擇 Hosted Zone Metrics (託管區域指標)。
6. 選取一或多個具有指標名稱 DNSQueries 之託管區域的核取方塊。
7. 在 Graphed metrics (圖表化指標) 索引標籤上，變更適用的值，以您想要的格式檢視指標。

   對於 Statistic (統計資料)，選擇 Sum (總和) 或 SampleCount；這些統計資料都會顯示相同的值。

使用 AWS CLI 取得 DNS 查詢指標

若要使用 AWS CLI 取得 DNS 查詢指標，您可以使用 get-metric-data 命令。注意下列事項：

- 您可以在個別的 JSON 檔案中，為命令指定大多數值。如需詳細資訊，請參閱 get-metric-data。
- 命令會為您 `Period` 在 JSON 檔案中，為指定的每個間隔傳回一個值。`Period` 是以秒為單位，因此如果您指定 5 分鐘的時段並為 `Period` 指定 `60`，您會得到五個值。如果您指定 5 分鐘的時段，並為 `Period` 指定 `300`，您會得到一個值。
- 在 JSON 檔案中，您可以為 `Id` 指定任何值。
- 要么保持未指定 AWS 區域，要麼指定 `us-east-1` 作為區域。如果您選擇任何其他區域，Route 53 指標將無法使用。如需詳細資訊，請參閱 AWS Command Line Interface 使用者指南中的設定 AWS CLI。

以下 AWS CLI 命令可用於取得 2019 年 5 月 1 日 4:01 到 4:07 之間五分鐘期間的 DNS 查詢指標。`metric-data-queries` 參數會參考遵循命令的範例 JSON 檔案。

```
aws cloudwatch get-metric-data --metric-data-queries file://./metric.json --start-time
 2019-05-01T04:01:00Z --end-time 2019-05-01T04:07:00Z
```

以下是範例 JSON 檔案：

```
[
```

```
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

以下是此命令的輸出。注意下列事項：

- 命令中的開始時間和結束時間涵蓋 7 分鐘的時段：2019-05-01T04:01:00Z 至 2019-05-01T04:07:00Z。
- 只有六個傳回值。因為在這一分鐘內沒有 DNS 查詢，所以 2019-05-01T04:05:00Z 沒有值。
- JSON 檔案中指定 Period 的值是 60 (秒)，因此會以一分鐘為間隔回報值。

```
{
    "MetricDataResults": [
        {
            "Id": "my_dns_queries_id",
            "StatusCode": "Complete",
            "Label": "DNSQueries",
            "Values": [
                101.0,
                115.0,
                103.0,
                127.0,
                111.0,
                120.0
            ],
```

```
            "Timestamps": [
                "2019-05-01T04:07:00Z",
                "2019-05-01T04:06:00Z",
                "2019-05-01T04:04:00Z",
                "2019-05-01T04:03:00Z",
                "2019-05-01T04:02:00Z",
                "2019-05-01T04:01:00Z"
            ]
        }
    ]
}
```

刪除公有託管區域

本節說明如何使用 Amazon Route 53 主控台刪除公有託管區域。

只有在沒有預設 SOA 和 NS 記錄以外的任何記錄時，才可以刪除託管區域。如果託管區域包含其他記錄，則必須先刪除記錄，才能刪除託管區域。如此可避免意外刪除仍然包含記錄的託管區域。

主題

- 防止流量路由傳送到您的網域
- 刪除其他服務所建立的公有託管區域
- 使用 Route 53 主控台刪除公有託管區域。

防止流量路由傳送到您的網域

如果您想要保留您的網域註冊，但想要停止將網際網路流量路由到您的網站或 Web 應用程式，則建議您刪除託管區域中的記錄，而不是刪除託管區域。

> **Important**
>
> 如果您刪除託管區域，就無法取消刪除。您必須建立新的託管區域，並更新您網域註冊的名稱伺服器；這最多需要 48 小時才能生效。此外，如果您刪除託管區域，有心人士可能會攔截網域，並使用您的網域名稱將流量路由到他們自己的資源。
>
> 如果您將子系網域的責任委派給託管區域，並想要刪除子系託管區域，則您也必須刪除與子系託管區域名稱相同的 NS 記錄，以更新父系託管區域。例如，如果您想要刪除託管區域 acme.example.com，則您也必須從 acme.example.com 託管區域中刪除該 NS 記錄。我們建議您先刪除 NS 記錄，並等待 NS 記錄上的 TTL 持續時間經過後，再刪除子系託管區域。這可

確保當 DNS 解析程式仍在處理所快取子系託管區域的名稱伺服器時，無人可攔截該子系託管區域。

如果您想要避免託管區域的每月費用，您可以將網域的 DNS 服務轉移至免費 DNS 服務。當您轉移 DNS 服務時，您必須更新網域註冊的名稱伺服器。如果網域是向 Route 53 註冊，請參閱 新增或變更網域的名稱伺服器和黏附記錄 以了解如何將 Route 53 名稱伺服器取代為新 DNS 服務的名稱伺服器。如果此網域已向其他註冊商註冊，請使用註冊商提供的方法來更新網域註冊的名稱伺服器。如需詳細資訊，請在網際網路上搜尋「免費 DNS 服務」。

刪除其他服務所建立的公有託管區域

如果託管區域是由其他服務所建立，您無法使用 Route 53 主控台刪除它。反之，您需要使用適合該其他服務的程序：

- AWS Cloud Map – 若要刪除當您建立公有 DNS 命名空間時由 AWS Cloud Map 建立的託管區域，請刪除該命名空間。AWS Cloud Map 會自動刪除該託管區域。如需詳細資訊，請參閱 AWS Cloud Map 開發人員指南中的刪除命名空間。
- Amazon Elastic Container Service (Amazon ECS) 服務探索 – 若要刪除當您使用服務探索建立服務時由 Amazon ECS 建立的公有託管區域，請刪除使用命名空間的 Amazon ECS 服務，然後刪除該命名空間。如需詳細資訊，請參閱 Amazon Elastic Container Service 開發人員指南中的刪除服務。

使用 Route 53 主控台刪除公有託管區域。

若要使用 Route 53 主控台刪除公有託管區域，請執行下列程序。

使用 Route 53 主控台刪除公有託管區域。

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted Zones (託管區域)，然後選擇所要刪除託管區域的反白顯示連結。
3. 確認要刪除的託管區域只包含 NS 和 SOA 記錄。如果包含其他記錄，請刪除它們。您還需要停用 DNSSEC 簽署：

    - 在託管區域詳細資訊頁面的 Records (記錄) 清單中，如果有任何記錄的 Type (類型) 欄值不是 NS 或 SOA，請選擇該列，然後選擇 Delete (刪除)。

      若要選取多個連續的記錄，請選擇第一列，按住 Shift 鍵，然後選擇最後一列。若要選取多個非連續的記錄，請選擇第一列，按住 Ctrl 鍵，然後選擇其餘列。

> **Note**
>
> 如果您在託管區域中為子網域建立任何 NS 記錄，也請刪除這些記錄。

4. 返回 Hosted Zones (託管區域) 頁面，然後選擇所要刪除託管區域的對應列。
5. 選擇 Delete (刪除)。
6. 輸入確認金鑰，然後選擇 Delete (刪除)。
7. 如果您想要讓網域無法在網際網路上使用，我們建議您將 DNS 服務轉移至免費的 DNS 服務，然後刪除 Route 53 託管區域。這可避免往後的 DNS 查詢發生路由錯誤。

   如果網域是向 Route 53 註冊，請參閱 新增或變更網域的名稱伺服器和黏附記錄 以了解如何將 Route 53 名稱伺服器取代為新 DNS 服務的名稱伺服器。如果此網域已向其他註冊商註冊，請使用註冊商提供的方法變更網域的名稱伺服器。

   > **Note**
   >
   > 如果您刪除子網域 (acme.example.com) 的託管區域，則不需要變更網域 (example.com) 的名稱伺服器。

檢查來自 Route 53 的 DNS 回答

如果您為網域建立 Amazon Route 53 託管區域，可以使用主控台中的 DNS 檢查工具，了解在設定網域使用 Route 53 做為 DNS 服務時 Route 53 會如何回應 DNS 查詢。對於地理位置、地理位置鄰近性及延遲記錄，您也可以模擬來自特定 DNS 解析程式和/或用戶端 IP 地址的查詢，來了解 Route 53 會傳回的回應。

> **Important**
>
> 此工具不會將查詢提交至網域名稱系統，它只會根據託管區域中記錄的設定加以回應。無論託管區域目前是否正用來路由網域的流量，此工具都會傳回相同的資訊。

DNS 檢查工具只適用於公有託管區域。

> **Note**
>
> DNS 檢查工具會傳回類似於您在 `dig` 命令的回答區段所預期的資訊。因此，如果您查詢的子網域名稱伺服器指向父名稱伺服器，則不會傳回這些名稱伺服器。

主題

- 使用檢查工具，了解 Amazon Route 53 如何回應 DNS 查詢
- 使用檢查工具，模擬來自特定 IP 地址的查詢 (僅限地理位置及延遲記錄)

使用檢查工具，了解 Amazon Route 53 如何回應 DNS 查詢

您可以使用此工具，查看 Amazon Route 53 傳回哪些回應，以回應記錄的 DNS 查詢。

若要使用檢查工具，了解 Route 53 如何回應 DNS 查詢

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted Zones (託管區域)。
3. 在 Hosted Zones (託管區域) 頁面上，選擇託管區域的名稱。主控台會顯示該託管區域的記錄清單。
4. 若要直接移至 Check response from Route 53 (檢查來自 Route 53 的回應) 頁面，請選擇 Test record (測試記錄)。
5. 指定下列值：
   - 記錄的名稱，不包括託管區域的名稱。例如，若要檢查 www.example.com，請輸入 www。若要檢查 example.com，請將 Record name (記錄名稱) 欄位保留空白。
   - 您要檢查的記錄類型，例如 A 或 CNAME。
6. 選擇 Get Response (取得回應)。
7. Response returned by Route 53 (Route 53 傳回的回應) 區段包含以下值：

   DNS 回答代碼

   指出查詢是否有效的代碼。最常見的回應代碼是 NOERROR，表示查詢有效。如果回應無效，Route 53 會傳回說明無效原因的回應代碼。如需可能的回應代碼清單，請參閱 IANA 網站上的 DNS RCODES。

通訊協定

Amazon Route 53 在回應查詢時使用的通訊協定，可能是 UDP 或 TCP。

Route 53 傳回的回應

Route 53 會傳回給 Web 應用程式的值。值可以是下列其中一項：

- 對於非別名記錄，回應包含記錄中的值。
- 對於具有相同名稱和類型 (包含加權、延遲、地理位置和容錯移轉) 的多個記錄，回應會根據請求包含適當記錄的值。
- 對於參照 AWS 資源 (而非另一個記錄) 的別名記錄，回應會根據資源類型包含 AWS 資源的 IP 地址或網域名稱。
- 對於參照其他記錄的別名記錄，回應會包含所參照記錄的值。

使用檢查工具，模擬來自特定 IP 地址的查詢 (僅限地理位置及延遲記錄)

如果您已經建立延遲或地理位置記錄，可以使用檢查工具模擬來自 DNS 解析程式和用戶端 IP 地址的查詢。

若要使用檢查工具模擬來自特定 IP 地址的查詢

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted Zones (託管區域)。
3. 在 Hosted Zones (託管區域) 頁面上，選擇託管區域的名稱。主控台會顯示該託管區域的記錄清單。
4. 若要直接移至 Check response from Route 53 (檢查來自 Route 53 的回應) 頁面，請選擇 Test record set (測試記錄集)。

   若要前往特定記錄的 Check response from Route 53 (檢查來自 Route 53 的回應) 頁面，請選擇該記錄的核取方塊，然後選擇 Test record set (測試記錄集)。
5. 如果您選擇了 Test record set (測試記錄集) 但未先選擇記錄，請指定下列值：
   - 記錄的名稱，不包括託管區域的名稱。例如，若要檢查 www.example.com，請輸入 www。若要檢查 example.com，請將 Record name (記錄名稱) 欄位保留空白。
   - 您要檢查的記錄類型，例如 A 或 CNAME。
6. 指定適用的值：

解析程式 IP 地址

指定 IPv4 或 IPv6 地址，以模擬用戶端在發出請求時使用的 DNS 解析程式的位置。這對測試延遲和地理位置記錄十分實用。如果您省略這個值，工具會使用 AWS 美國東部 (維吉尼亞北部) 區域 (us-east-1) 中 DNS 解析程式的 IP 地址。

EDNS0 用戶端子網路 IP

如果解析程式支援 EDNS0，請輸入適用的地理位置中 IP 地址的用戶端子網路 IP，例如 192.0.2.0 或 2001:db8:85a3::8a2e:370:7334。

子網遮罩

如果您指定 EDNS0 client subnet IP (EDNS0 用戶端子網路 IP) 的 IP 地址，則可以選擇性指定您希望檢查工具包含在 DNS 查詢中的 IP 地址位元數。例如，如果您為 EDNS0 client subnet IP (EDNS0 用戶端子網路 IP) 指定 192.0.2.44，並為 Subnet mask (子網路遮罩) 指定 24，檢查工具就會模擬來自 192.0.2.0/24 的查詢。預設值為 24 個位元 (適用於 IPv4 地址) 和 64 個位元 (適用於 IPv6 地址)。

7. 選擇 Get Response (取得回應)。
8. Response returned by Route 53 (Route 53 傳回的回應) 區段包含以下值：

傳送到 Route 53 的 DNS 查詢

檢查工具傳送到 Route 53 的 BIND 格式查詢。這種格式與 Web 應用程式在傳送查詢時使用的格式相同。這三個值通常是記錄名稱、IN (表示網際網路)，以及記錄類型。

DNS 回答代碼

指出查詢是否有效的代碼。最常見的回應代碼是 NOERROR，表示查詢有效。如果回應無效，Route 53 會傳回說明無效原因的回應代碼。如需可能的回應代碼清單，請參閱 IANA 網站上的 DNS RCODES。

通訊協定

Amazon Route 53 在回應查詢時使用的通訊協定，可能是 UDP 或 TCP。

Route 53 傳回的回應

Route 53 會傳回給 Web 應用程式的值。值可以是下列其中一項：

- 對於非別名記錄，回應包含記錄中的值。
- 對於具有相同名稱和類型 (包含加權、延遲、地理位置和容錯移轉) 的多個記錄，回應會根據請求包含適當記錄的值。

- 對於參照 AWS 資源 (而非另一個記錄) 的別名記錄，回應會根據資源類型包含 AWS 資源的 IP 地址或網域名稱。
- 對於參照其他記錄的別名記錄，回應會包含所參照記錄的值。

設定白標籤名稱伺服器

每個 Amazon Route 53 託管區域與四個名稱伺服器 (統稱為委派組) 相關聯。預設情況下，名稱伺服器有如 ns-2048.awsdns-64.com 的名稱。如果您希望名稱伺服器的網域名稱與託管區域的網域名稱相同 (例如 ns1.example.com)，可以設定白標籤名稱伺服器 (也稱為虛名伺服器或私有名稱伺服器)。

以下步驟說明如何設定一組四個白標籤名稱伺服器，以重複使用於多個網域。例如，假設您擁有網域 example.net、example.org 和 example.com。透過以下步驟，您可以為 example.com 設定白標籤名稱伺服器，並將其重複使用於 example.org 和 example.net。

主題

- 步驟 1：建立 Route 53 可重複使用的委派組
- 步驟 2：建立或重新建立 Amazon Route 53 託管區域，以及變更 NS 和 SOA 記錄的 TTL
- 步驟 3：重新建立託管區域的記錄
- 步驟 4：取得 IP 地址
- 步驟 5：為白標籤名稱伺服器建立記錄
- 步驟 6：更新 NS 和 SOA 記錄
- 步驟 7：建立黏附記錄和變更註冊商的名稱伺服器
- 步驟 8：監控網站或應用程式的流量
- 步驟 9：將 TTL 變更回其原始值
- 步驟 10：(選用) 聯絡遞迴 DNS 服務

步驟 1：建立 Route 53 可重複使用的委派組

白標籤名稱伺服器會與 Route 53 可重複使用的委派組建立關聯。只有在託管區域和可重複使用的委派組均由相同的 AWS 帳戶建立時，您才能使用託管區域的白標籤名稱伺服器。

若要建立可重複使用的委派組，您可以使用 Route 53 API、AWS CLI 或 AWS 開發套件。如需詳細資訊，請參閱下列文件：

- Route 53 API - 請參閱 Amazon Route 53 API 參考中的 CreateReusableDelegationSet

- AWS CLI - 請參閱 AWS CLI 命令參考中的 create-reusable-delegation-set
- AWS 開發套件 – 請參閱 AWS 說明文件頁面上適用的開發套件說明文件

步驟 2：建立或重新建立 Amazon Route 53 託管區域，以及變更 NS 和 SOA 記錄的 TTL

建立或重新建立 Amazon Route 53 託管區域：

- 如果您目前未將 Route 53 做為要使用白標籤名稱伺服器之網域的 DNS 服務 – 請建立託管區域，並指定您在上一個步驟中為每個託管區域建立的可重複使用委派組。如需詳細資訊，請參閱 Amazon Route 53 API 參考中的 CreateHostedZone。
- 如果您目前將 Route 53 做為要使用白標籤名稱伺服器之網域的 DNS 服務 – 您必須重新建立要使用白標籤名稱伺服器的託管區域，並指定您在上一個步驟中為每個託管區域建立的可重複使用委派組。

> **Important**
>
> 您不能變更與現有託管區域關聯的名稱伺服器。只在建立託管區域時，才可將可重複使用的委派組與託管區域關聯。

當您建立託管區域時，並在嘗試存取對應網域的資源之前，變更每個託管區域的以下 TTL 值：

- 將託管區域的 NS 記錄的 TTL 變更為 60 秒以下。
- 將託管區域的 SOA 記錄的最小 TTL 變更為 60 秒以下。這是 SOA 記錄中的最後一個值。

如果您不小心向註冊商提供白標籤名稱伺服器的錯誤 IP 地址，您的網站會變得無法使用，並在您更正問題之後的 TTL 持續期間仍然無法使用。透過設定 TTL 低值，可縮短網站無法使用的時間。

如需有關建立託管區域，並為託管區域的名稱伺服器指定可重複使用委派組的詳細資訊，請參閱 Amazon Route 53 API 參考中的 CreateHostedZone。

步驟 3：重新建立託管區域的記錄

在您於步驟 2 中建立的託管區域中建立記錄：

- 如果您要將網域的 DNS 服務遷移到 Amazon Route 53 – 可透過匯入現有記錄的相關資訊來建立記錄。如需更多詳細資訊，請參閱 透過匯入區域檔案建立記錄。
- 如果您要取代現有的託管區域以使用白標籤名稱伺服器 – 在新的託管區域，重新建立目前託管區域中顯示的記錄。Route 53 不提供從託管區域匯出記錄的方法，但一些第三方廠商提供。然後，您可

以使用 Route 53 匯入功能來匯入路由政策為簡便的非別名記錄。無法匯出和重新匯入別名記錄或路由政策不是簡便的記錄。

如需使用 Route 53 API 建立記錄的詳細資訊，請參閱 Amazon Route 53 API 參考中的 CreateHostedZone。如需如何使用 Route 53 主控台建立記錄的資訊，請參閱 處理記錄。

步驟 4：取得 IP 地址

取得可重複使用的委派組中名稱伺服器的 IPv4 和 IPv6 地址，並填寫下表。

可重複使用委派組中名稱伺服器的名稱 (例如：Ns-2048.awsdns-64.com)	IPv4 和 IPv6 地址	要指派給白標籤名稱伺服器的名稱 (例如：ns1.example.com)
	IPv4： IPv6：	
	IPv4： IPv6：	
	IPv4： IPv6：	
	IPv4： IPv6：	

例如，假設可重複使用委派組的四個名稱伺服器是：

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

若要取得四個名稱伺服器中第一個伺服器的 IP 地址，請執行以下 Linux 和 Windows 命令：

適用於 Linux 的 dig 命令

```
% dig A ns-2048.awsdns-64.com +short
192.0.2.117
```

```
% dig AAAA ns-2048.awsdns-64.com +short
2001:db8:85a3::8a2e:370:7334
```

適用於 Windows 的 nslookup 命令

```
c:\> nslookup ns-2048.awsdns-64.com
Non-authoritative answer:
Name:    ns-2048.awsdns-64.com
Addresses:  2001:db8:85a3::8a2e:370:7334
          192.0.2.117
```

步驟 5：為白標籤名稱伺服器建立記錄

在網域名稱 (如 example.com) 與白標籤名稱伺服器 (如 ns1.example.com) 的網域名稱相同的託管區域中，建立八個記錄：

- 每個白標籤名稱伺服器一個 A 記錄
- 每個白標籤名稱伺服器一個 AAAA 記錄

> **Important**
>
> 如果您為兩個或更多託管區域使用相同的白標籤名稱伺服器，請勿針對其他託管區域執行此步驟。

對於每個記錄指定以下值。請參閱您在上一步填寫的表格：

路由政策

指定簡便路由。

記錄名稱

要指派給其中一個白標籤名稱伺服器的名稱 (例如：ns1.example.com)。對於字首 (此範例中的 ns1 值)，您可以使用網域名稱中任何有效的值。

值/將流量路由到

可重複使用委派組中其中一個 Route 53 名稱伺服器的 IPv4 或 IPv6 地址。

> **Important**
>
> 如果您在為白標籤名稱伺服器建立記錄時指定錯誤的 IP 地址，則在執行後續步驟時，網站或 Web 應用程式會變成無法在網際網路上使用。即使您立即更正 IP 地址，網站或 Web 應用程式在 TTL 持續期間仍然無法使用。

記錄類型

在建立 IPv4 地址的記錄時指定 A。

在建立 IPv6 地址的記錄時指定 AAAA。

TTL (秒)

這個值是 DNS 解析程式在將另一個 DNS 查詢轉送至 Route 53 之前快取此記錄相關資訊的時間。我們建議您指定 60 秒以下的起始值，這樣當您不小心在這些記錄中指定錯誤值時，可以快速恢復。

步驟 6：更新 NS 和 SOA 記錄

更新要使用白標籤名稱伺服器之託管區域中的 SOA 和 NS 記錄。每次針對一個託管區域和對應網域執行步驟 6 到步驟 8，然後針對另一個託管區域和網域重複這些步驟。

> **Important**
>
> 先從網域名稱 (如 example.com) 與白標籤名稱伺服器 (如 ns1.example.com) 的網域名稱相同的 Amazon Route 53 託管區域開始。

1. 將 Route 53 名稱伺服器的名稱取代為其中一個白標籤名稱伺服器的名稱，以更新 SOA 記錄

   範例

   將 Route 53 名稱伺服器的名稱：

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

取代為其中一個白標籤名稱伺服器的名稱：

```
ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
```

> **Note**
>
> 您在 步驟 2：建立或重新建立 Amazon Route 53 託管區域，以及變更 NS 和 SOA 記錄的 TTL 中已變更最後一個值，即存留時間 (TTL)。

如需如何使用 Route 53 主控台更新記錄的詳細資訊，請參閱 編輯記錄。

2. 在 NS 記錄，記下網域目前的名稱伺服器的名稱，以便在必要時恢復為這些名稱伺服器。
3. 更新 NS 記錄。將 Route 53 名稱伺服器的名稱取代為四個白標籤名稱伺服器的名稱，例如 `ns1.example.com`、`ns2.example.com`、`ns3.example.com` 和 `ns4.example.com`。

步驟 7：建立黏附記錄和變更註冊商的名稱伺服器

使用註冊商提供的方法建立黏附記錄和變更註冊商的名稱伺服器：

1. 新增黏附記錄：
   - 如果您要更新網域名稱與白標籤名稱伺服器的網域名稱相同的網域 – 請建立四個黏附記錄，其名稱和 IP 地址符合您在步驟 4 中取得的值。在對應黏附記錄中包含白標籤名稱伺服器的 IPv4 和 IPv6 地址，例如：

     ns1.example.com – IP 地址 = 192.0.2.117 and 2001:db8:85a3::8a2e:370:7334

     註冊商對黏附記錄使用各種不同的術語。您也可能看到它被稱為註冊新的名稱伺服器或類似內容。
   - 如果您要更新其他網域 - 如果 Route 53 是您的 DNS 服務，您必須先完成上一個項目符號中的步驟並建立符合網域名稱的黏附記錄。接著跳至本程序的步驟 2。
2. 將網域的名稱伺服器變更為白標籤名稱伺服器的名稱。

如果您要將 Amazon Route 53 做為 DNS 服務，請參閱 新增或變更網域的名稱伺服器和黏附記錄。

步驟 8：監控網站或應用程式的流量

監控您在步驟 7 中建立黏附記錄和變更名稱伺服器的網站或應用程式的流量：

- 如果流量停止 – 請使用註冊商提供的方法，將網域的名稱伺服器變更回之前的 Route 53 名稱伺服器。這些是您在步驟 6b 中記下的名稱伺服器。然後判斷發生什麼錯誤。
- 如果流量不受影響 – 請針對要使用相同白標籤名稱伺服器的其餘託管區域，重複步驟 6 到步驟 8。

步驟 9：將 TTL 變更回其原始值

針對現在使用白標籤名稱伺服器的所有託管區域，變更以下值：

- 將託管區域的 NS 記錄的 TTL 變更為更典型的 NS 記錄值，例如，172800 秒 (兩天)。
- 將託管區域的 SOA 記錄的最小 TTL 變更為更典型的 SOA 記錄值，例如，900 秒。這是 SOA 記錄中的最後一個值。

步驟 10：(選用) 聯絡遞迴 DNS 服務

選用如果您使用 Amazon Route 53 地理位置路由，請聯絡支援 EDNS0 之 edns-client-subnet 延伸模組的遞迴 DNS 服務，並向他們提供白標籤名稱伺服器的名稱。這可確保這些 DNS 服務會根據查詢的大致來源地理位置，繼續將 DNS 查詢路由到最佳 Route 53 位置。

Amazon Route 53 為公有託管區域建立的 NS 和 SOA 記錄

針對您建立的每個公有託管區域時，Amazon Route 53 會自動建立名稱伺服器 (NS) 記錄和起始授權 (SOA) 記錄。需要變更這些記錄的機會非常少。

主題

- 名稱伺服器 (NS) 記錄
- 起始授權 (SOA) 記錄

名稱伺服器 (NS) 記錄

Amazon Route 53 會自動建立與託管區域同名的名稱伺服器 (NS) 記錄。它列出的四個名稱伺服器是託管區域的授權名稱伺服器。除了極少數的情況以外，建議您不要新增、變更或刪除此記錄中的名稱伺服器。

以下範例顯示 Route 53 名稱伺服器的名稱格式 (這些僅為範例；在更新您的註冊商的名稱伺服器記錄時請勿使用它們)：

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net

- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

若要取得託管區域的名稱伺服器清單：

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，按一下 Hosted zones (託管區域)。
3. 在 Hosted zones (託管區域) 頁面上，選擇託管區域的選項按鈕 (而非名稱)，然後選擇 View details (檢視詳細資訊)。
4. 在託管區域的詳細資訊頁面上，選擇託管區域詳細資訊。
5. 記下 Name Servers (名稱伺服器) 下所列的四個伺服器。

如需如何將 DNS 服務從其他 DNS 服務提供者遷移到 Route 53 的詳細資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

起始授權 (SOA) 記錄

起始授權 (SOA) 記錄識別網域的基本 DNS 相關資訊，例如：

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

SOA 記錄包含下列元素：

- 建立 SOA 記錄的 Route 53 名稱主機，例如 `ns-2048.awsdns-64.net`。
- 管理員的電子郵件地址。其 @ 符號取代為句號，例如 `hostmaster.example.com`。預設值是不受監控的 amazon.com 電子郵件地址。
- 每當您更新託管區域中的記錄時選擇要遞增的序號。Route 53 不會自動遞增號碼。(DNS 服務會使用序號來支援輔助 DNS。) 在範例中，此值為 `1`。
- DNS 輔助伺服器在查詢 DNS 主伺服器的 SOA 記錄以檢查變更之前等待的重新整理時間 (以秒為單位)。在範例中，此值為 `7200`。
- 輔助伺服器在重新嘗試失敗的區域轉移之前等待的重試間隔 (以秒為單位)。通常，重試時間小於重新整理時間。在範例中，此值為 `900` (15 分鐘)。
- 輔助伺服器會持續嘗試完成區域轉移的時間 (以秒為單位)。如果過了此時間仍未成功轉移區域，輔助伺服器會停止回答查詢，因為它認為其資料過舊、不可靠。在範例中，此值為 `1209600` (兩週)。

- 最小存留時間 (TTL)。此值有助於定義遞迴解析程式應從 Route 53 快取下列回應的時間長短：

  NXDOMAIN

  無任何類型的記錄擁有在 DNS 查詢中指定的名稱，例如 example.com。也沒有記錄屬於在 DNS 查詢中指定之名稱的子項，例如 zenith.example.com。

  NODATA

  至少一筆記錄擁有在 DNS 查詢中指定的名稱，但沒有記錄擁有在DNS 查詢中指定的類型 (如 A)。

  當 DNS 解析程式快取 NXDOMAIN 或 NODATA 回應時，其稱為負快取。

  負快取的持續時間低於下列值：

  - 這個值—SOA 記錄中的最小 TTL。在範例中，值為 86400 (一天)。
  - SOA 記錄的 TTL 值。預設值為 900 秒。如需如何變更此值的詳細資訊，請參閱編輯記錄。

  當 Route 53 以 NXDOMAIN 或 NODATA 回應 (負向回應) 對 DNS 查詢進行回應時，您只需針對標準查詢的費率付費。(請參閱 Amazon Route 53 定價中的「查詢」)。如果您擔心負向回應的費用，其中一種選項是變更 SOA 記錄的 TTL、SOA 記錄中的最小 TTL (此值) 或兩者。請注意，提高適用於整個託管區域之負向回應的這些 TTL，會有正面和負面效果：

  - 網際網路的 DNS 解析程式會以較長的時間快取不存在的記錄，進而減少轉送至 Route 53 的查詢數目。這樣可以減少 DNS 查詢的 Route 53 費用。
  - 不過，如果您曾刪錯有效的記錄，並在日後重新建立該記錄，DNS 解析程式則會以較長的時間快取負面回應 (此記錄不存在)。這會加長您的客戶或使用者無法連接對應資源 (如 acme.example.com 的 Web 伺服器) 的時間量。

若要在 Route 53 找到您的 SOA 記錄

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選取要為其檢視記錄的網域之連結名稱。
4. 在 Records (記錄) 區段中，您可以看到列出的所有記錄，也可以篩選記錄以找到您的 SOA 值。

使用私有託管區域

私有託管區域是一種容器，包含您希望 Amazon Route 53 如何回應針對網域及其子網域之 DNS 查詢的資訊，這些網域都位在一或多個您使用 Amazon VPC 服務建立的 VPC 中。以下是私有託管區域運作的方式：

1. 您建立私有託管區域 (例如 example.com)，並指定要與該託管區域關聯的 VPC。建立託管區域後，即可將更多 VPC 與其關聯。
2. 您在託管區域中建立的記錄，決定 Route 53 如何回應針對您位在各 VPC 中之網域和子網域的 DNS 查詢。例如，假設您的資料庫伺服器在與您私有託管區域相關聯的一個 VPC 的 EC2 執行個體上執行。您建立一筆 A 或 AAAA 記錄 (例如 db.example.com)，並指定資料庫伺服器的 IP 地址。

   如需記錄的詳細資訊，請參閱 處理記錄。如需有關使用私有託管區域的 Amazon VPC 要求的資訊，請參閱 Amazon VPC 使用者指南中的使用私有託管區域。
3. 當應用程式提交針對 db.example.com 的 DNS 查詢時，Route 53 會傳回對應的 IP 地址。為了收到從私有託管區域傳來的回應，您還必須在其中一個關聯的 VPC 中執行 EC2 執行個體 (或在混合設定中設定一個傳入端點)。如果您嘗試在 VPC 外部或混合設定中查詢私有託管區域，則會在網際網路上以遞迴方式解析查詢。
4. 應用程式會使用它從 Route 53 取得的 IP 地址，建立與資料庫伺服器的連線。

建立私有託管區域時，會使用以下名稱伺服器：

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

使用這些名稱伺服器是因為 DNS 通訊協定要求每個託管區域都必須有 NS 記錄集。Route 53 公有託管區域絕不會使用這些預留的名稱伺服器。您只能透過 Route 53 Resolver 在與託管區域相關聯的 VPC 中查詢這些區域，方法是使用與私有託管區域中指定之 VPC 連線的傳入端點。

雖然名稱伺服器會顯示在網際網路上，但 Route 53 Resolver 不會與名稱伺服器位址連線。此外，如果您直接在網際網路上查詢名稱伺服器，並不會傳回私有託管區域資訊。反之，Route 53 Resolver會發現這些查詢位於與託管區域相關聯的 VPC 型私有命名空間內，然後直接使用私有連線功能與私有 DNS 伺服器連線。

> **Note**
>
> 如果您希望私有 DNS 解析仍能發揮效果，可更改私有託管區域中的 NS 記錄集。我們不建議這麼做，但如果您選擇這麼做，就必須使用公有 DNS 伺服器不會使用的預留網域名稱。

如果您想要在網際網路上路由您網域的流，您要使用 Route 53 的公有託管區域。如需更多詳細資訊，請參閱 使用公有託管區域。

主題

- 使用私有託管區域的考量
- 建立私有託管區域
- 列出私有託管區域
- 建立多個 VPC 與一個私有託管區域的關聯
- 將您用不同 AWS 帳戶建立的 Amazon VPC 與私有託管區域關聯
- 取消 VPC 與私有託管區域的關聯
- 刪除私有託管區域

使用私有託管區域的考量

使用私有託管區域時，請注意下列注意事項：

- Amazon VPC settings
- Route 53 health checks
- Supported routing policies for records in a private hosted zone
- Split-view DNS
- Public and private hosted zones that have overlapping namespaces
- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules
- Delegating responsibility for a subdomain
- Custom DNS servers
- Required IAM permissions

Amazon VPC 設定

若要使用私有託管區域，您必須將下列 Amazon VPC 設定設為 `true`：

- `enableDnsHostnames`
- `enableDnsSupport`

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的更新 VPC 的 DNS 支援。

Route 53 運作狀態檢查

在私有託管區域中，只能將 Route 53 運作狀態檢查與容錯移轉、多值回答、加權、延遲和地理位置記錄相關聯。如需將運作狀態檢查與容錯移轉記錄關聯的資訊，請參閱 在私有託管區域中設定容錯移轉。

支援的私有託管區域中記錄的路由政策

在私有託管區域中建立記錄時，可以使用以下路由政策：

- 簡便路由
- 容錯移轉路由
- 多值回答路由
- 加權路由
- 以延遲為基礎的路由
- 地理位置路由

不支援使用其他路由政策在私有託管區域中建立記錄。

分割檢視 DNS

可以使用 Route 53 設定分割檢視 DNS，也稱為水平分割 DNS。在分割檢視 DNS 中，您會針對內部用途 (accounting.example.com) 和外部用途 (例如，您的公有網站 (www.example.com)) 使用相同的網域名稱 (example.com)。您可能還需要在內部和外部使用相同的子網域名稱，但提供不同的內容，或需要對內部和外部使用者進行不同的身分驗證。

若要設定分割檢視 DNS，請執行下列步驟：

1. 建立具有相同名稱的公有和私有託管區域。(如果您針對公有託管區域使用其他 DNS 服務，則分割檢視 DNS 仍可運作。)
2. 將一或多個 Amazon VPC 與私有託管區域建立關聯。Route 53 Resolver 會使用私有託管區域來路由指定 VPC 中的 DNS 查詢。

3. 在每個託管區域中建立記錄。公有託管區域中的記錄會控制網際網路流量的路由方式，私有託管區域中的記錄會控制流量在 Amazon VPC 中路由的方式。

如果您需要同時執行 VPC 和現場部署工作負載的名稱解析，您可以使用 Route 53 Resolver。如需更多詳細資訊，請參閱 什麼是 Amazon Route 53 Resolver？。

具有重疊命名空間的公有和私有託管區域

如果您的私有和公有託管區域具有重疊的命名空間，例如 example.com 和 accounting.example.com，則 Resolver 會根據最明確的匹配結果來路由傳送流量。當使用者在 Amazon VPC 中登入與私有託管區域相關聯的 EC2 執行個體時，以下是 Route 53 Resolver 處理 DNS 查詢的方式：

1. Resolver 評估私有託管區域的名稱是否與請求中的網域名稱相符，例如 accounting.example.com。符合定義為下列任一項：
   - 完全符合
   - 私有託管區域的名稱是請求中網域名稱的父系。例如，假設請求中的網域名稱如下：

     seattle.accounting.example.com

     以下託管區域相符，因為它們是 seattle.accounting.example.com 的父系：
     - accounting.example.com
     - example.com

   如果沒有相符的私有託管區域，Resolver 會將請求轉送到公有 DNS 解析程式，您的請求會被解析一般的 DNS 查詢。
2. 如果有與請求中的網域名稱相符的私有託管區域名稱，則會在該託管區域中搜尋與請求中的網域名稱和 DNS 類型相符的記錄，如 accounting.example.com 的 A 記錄。

> **Note**
>
> 如果有相符的私有託管區域名稱，但沒有與請求中的網域名稱和類型相符的記錄，Resolver 不會將請求轉送到公有 DNS 解析程式，而是將 NXDOMAIN (不存在的網域) 傳回給用戶端。

具有重疊命名空間的私有託管區域

如果您的兩個或更多個私有託管區域具有重疊的命名空間，例如 example.com 和 accounting.example.com，則 Resolver 會根據最明確的匹配結果來路由傳送流量。

> **Note**
>
> 如果您有私有託管區域 (example.com)，以及將流量路由到相同網域名稱之網路的 規則，則 Route 53 Resolver 規則優先。請參閱 Private hosted zones and Route 53 Resolver rules。

當使用者在 Amazon VPC 中登入與全部私有託管區域相關聯的 EC2 執行個體時，以下是 Resolver 處理 DNS 查詢的方式：

1. Resolver 評估請求中的網域名稱，例如 accounting.example.com，是否與其中一個私有託管區域的名稱相符。
2. 如果沒有完全符合請求中之網域名稱的託管區域，Resolver 會在請求中檢查具有網域名稱父系名稱的託管區域。例如，假設請求中的網域名稱如下：

   `seattle.accounting.example.com`

   下列託管區域相符，因為它們是 `seattle.accounting.example.com` 的父系：

   - `accounting.example.com`
   - `example.com`

   Resolver 選擇 `accounting.example.com`，因為它比 `example.com` 更為特定。
3. Resolver 會搜尋 `accounting.example.com` 託管區域中符合請求中網域名稱和 DNS 類型的記錄，例如 `seattle.accounting.example.com` 的 A 記錄。

   如果沒有符合請求中網域名稱和類型的記錄，則 Resolver 會向用戶端傳回 NXDOMAIN (不存在的網域)。

私有託管區域和 Route 53 Resolver 規則

如果您有私有託管區域 (example.com)，以及將流量路由到相同網域名稱之網路的 Resolver 規則，則 Resolver 規則優先。

舉例而言，假設您的組態如下：

- 您有一個名為 example.com 的私有託管區域，並與 VPC 建立關聯。
- 您建立將 example.com 流量轉送到您網路的 Route 53 Resolver 規則，並將規則與相同的 VPC 建立關聯。

在此組態中，Resolver 規則優先於私有託管區域。DNS 查詢會轉送到您的網路，而不是根據私有託管區域中的記錄解析。

委派子網域的責任

您不能在私有託管區域中建立 NS 記錄來委派子網域的責任。

自訂 DNS 伺服器

如果您已在 VPC 中的 Amazon EC2 執行個體上設定自訂 DNS 伺服器，則必須設定這些 DNS 伺服器，將私有 DNS 查詢路由到 Amazon 為您的 VPC 提供的 DNS 伺服器的 IP 地址。此 IP 地址是 VPC 網路範圍基礎上的 IP 地址「加 2」。例如，如果您的 VPC 的 CIDR 範圍是 10.0.0.0/16，DNS 伺服器的 IP 地址就是 10.0.0.2。

如果您想要在 VPC 與您的網路之間路由 DNS 查詢，可以使用 Resolver。如需更多詳細資訊，請參閱 什麼是 Amazon Route 53 Resolver？。

所需的 IAM 許可

若要建立私有託管區域，除了 Route 53 動作許可之外，您還需要授予 Amazon EC2 動作的 IAM 許可。如需詳細資訊，請參閱《服務授權參考》中的 Route 53 的動作、資源和條件索引鍵。

建立私有託管區域

私有託管區域是一個容器，用於存放您在一或多個 Amazon Virtual Private Cloud (VPC) 中託管的網域的記錄。您為網域 (例如 example.com) 建立託管區域，然後建立記錄，以告知 Amazon Route 53 如何在 VPC 之內和之間路由該網域的流量。

> **Important**
>
> 當您建立私有託管區域，必須將 VPC 與託管區域關聯，而且您指定的 VPC 與該託管區域必須是使用同一個帳戶建立的。建立託管區域後，可以將其他 VPC 與該託管區域關聯，包括使用不同的 AWS 帳戶建立的 VPC。
>
> 若要將您用不同帳戶建立的 VPC 與私有託管區域關聯，必須對該關聯授權，然後透過程式設計方式建立關聯。如需更多詳細資訊，請參閱 將您用不同 AWS 帳戶建立的 Amazon VPC 與私有託管區域關聯。

如需使用 Route 53 API 建立私有託管區域的資訊，請參閱 Amazon Route 53 API 參考。

使用 Route 53 主控台建立私有託管區域

1. 對於要與 Route 53 託管區域建立關聯的每個 VPC，請將以下 VPC 設定變更為 `true`：

- `enableDnsHostnames`
- `enableDnsSupport`

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的更新 VPC 的 DNS 支援。

2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 若您是初次使用 Route 53，請選擇 Get Started (開始使用)。

   如果您已經在使用 Route 53，請在導覽窗格中選擇 Hosted zones (託管區域)。
4. 選擇 Create Hosted Zone (建立託管區域)。
5. 在 Create private hosted zone (建立私有託管區域) 窗格中，輸入網域名稱並選擇性地輸入註解。

   如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。
6. 在 Type (類型) 清單中選擇 Private hosted zone (私有託管區域)。
7. 在 VPC ID 清單中，選擇您想要與託管區域建立關聯的 VPC。

   > **Note**
   >
   > 如果主控台顯示下列訊息，表示您嘗試關聯的託管區域使用與同一 VPC 內另一個託管區域相同的名稱空間：
   > "A conflicting domain is already associated with the given VPC or Delegation Set." (衝突網域已經與特定 VPC 或委派組關聯。)
   > 例如，如果託管區域 A 和託管區域 B 具有相同的網域名稱，例如 `example.com`，則無法將兩個託管區域與相同的 VPC 建立關聯。
8. 選擇 Create hosted zone (建立託管區域)。

列出私有託管區域

您可以使用 Amazon Route 53 主控台，列出目前 AWS 帳戶建立的所有託管區域。如需有關如何使用 Route 53 API 列出託管區域的資訊，請參閱 Amazon Route 53 API 參考中的 ListHostedZones。

若要列出與 AWS 帳戶關聯的私有託管區域

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。

   Hosted Zones (託管區域) 頁面會自動顯示使用目前 AWS 帳戶建立的所有託管區域的清單。Type (類型) 欄指出託管區域是私有或公有。選擇欄標題，將所有私有託管區域和所有公有託管區域分組。

建立多個 VPC 與一個私有託管區域的關聯

如果您使用相同 AWS 帳戶建立託管區域和多個 VPC，可以使用 Amazon Route 53 主控台將這些 VPC 與私有託管區域關聯。

> **Important**
>
> 若要將您用不同帳戶建立的 VPC 與私有託管區域關聯，必須先對該關聯授權。此外，您無法使用 AWS 主控台來授權關聯或將 VPC 與託管區域關聯。如需更多詳細資訊，請參閱 將您用不同 AWS 帳戶建立的 Amazon VPC 與私有託管區域關聯。

如需有關如何使用 Route 53 API 將多個 VPC 與一個私有託管區域關聯的資訊，請參閱 Amazon Route 53 API 參考中的 AssociateVPCWithHostedZone。

若要使用 Route 53 主控台將其他 VPC 與私有託管區域關聯

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇要將多個 VPC 與之關聯的私有託管區域的選項按鈕。
4. 選擇 Edit (編輯)。
5. 選擇 Add VPC (新增 VPC)。
6. 選擇您要與此託管區域建立關聯之 VPC 的區域和 ID。
7. 若要將其他 VPC 與此託管區域關聯，請重複步驟 5 和 6。
8. 選擇 Save changes (儲存變更)。

將您用不同 AWS 帳戶建立的 Amazon VPC 與私有託管區域關聯

如果要將使用不同 AWS 帳戶建立的 VPC 與私有託管區域關聯，請執行以下步驟：

要將您用不同 AWS 帳戶建立的 Amazon VPC 與私有託管區域關聯

1. 使用建立託管區域的帳戶，透過以下其中一個方法授權 VPC 與私有託管區域的關聯：

   - AWS CLI – 請參閱 AWS CLI 命令參考中的 create-vpc-association-authorization
   - AWSSDK 或 AWS Tools for Windows PowerShell – 請參閱 AWS 說明文件 頁面上適用的說明文件
   - Amazon Route 53 API – 請參閱 Amazon Route 53 API 參考中的 CreateVPCAssociationAuthorization

   注意下列事項：

   - 如果要將使用不同帳戶建立的多個 VPC 與私有託管區域關聯，必須為每個 VPC 提交一個授權請求。
   - 當您授權關聯，您必須指定託管區域 ID，因此私有託管區域必須已存在。
   - 您無法使用 Route 53 主控台來授權 VPC 與私有託管區域的關聯或建立關聯。
2. 使用建立 VPC 的帳戶，將 VPC 與託管區域關聯。如同授權關聯一樣，您可以使用 AWS 開發套件、Tools for Windows PowerShell、AWS CLI 或 Route 53 API。如果使用 API，請使用 AssociateVPCWithHostedZone 動作。
3. 建議 – 刪除建立 VPC 與託管區域關聯的授權。刪除授權不會影響關聯，只是防止未來將 VPC 與託管區域重新關聯。如果要將 VPC 與託管區域重新關聯，您需要重複此程序的步驟 1 和 2。

   > **Note**
   >
   > 如需可建立的授權數量上限，請參閱 實體的配額。

取消 VPC 與私有託管區域的關聯

您可以使用 Amazon Route 53 主控台取消 VPC 與私有託管區域的關聯。這會造成 Route 53 使用託管區域中針對來自 VPC 之 DNS 查詢的記錄來停止路由流量。例如，如果範例 .com 託管區域與 VPC 相關聯，而您取消託管區域與該 VPC 的關聯，Route 53 會停止解析 DNS 查詢，例如 .com 或 example.com 託管區域中任何其他記錄的 DNS 查詢。

> **Note**
>
> 您無法取消最後一個 VPC 與私有託管區域的關聯。如果您想要取消該 VPC 的關聯，必須先將另一個 VPC 與託管區域建立關聯。

若要取消 VPC 與私有託管區域的關聯

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇要與一或多個 VPC 取消關聯的私有託管區域的選項按鈕。
4. 選擇 Edit(編輯) 。
5. 選擇您想要與此託管區域取消關聯的 VPC 旁邊的 Remove VPC (移除 VPC)。
6. 選擇 Save changes (儲存變更)。

刪除私有託管區域

本節說明如何使用 Amazon Route 53 主控台刪除私有託管區域。

只有在沒有預設 SOA 和 NS 記錄以外的任何記錄時，才可以刪除私有託管區域。如果託管區域包含其他記錄，則必須先刪除記錄，才能刪除託管區域。如此可避免意外刪除仍然包含記錄的託管區域。

主題

- 刪除其他服務所建立的私有託管區域
- 使用 Route 53 主控台刪除私有託管區域。

刪除其他服務所建立的私有託管區域

如果私有託管區域是由其他服務所建立，您無法使用 Route 53 主控台刪除它。反之，您需要使用適合該其他服務的程序：

- AWS Cloud Map – 若要刪除當您建立私有 DNS 命名空間時由 AWS Cloud Map 建立的託管區域，請刪除該命名空間。AWS Cloud Map 會自動刪除該託管區域。如需詳細資訊，請參閱 AWS Cloud Map 開發人員指南中的刪除命名空間。

- Amazon Elastic Container Service (Amazon ECS) 服務探索 – 若要刪除當您使用服務探索建立服務時由 Amazon ECS 建立的私有託管區域，請刪除使用命名空間的 Amazon ECS 服務，然後刪除該命名空間。如需詳細資訊，請參閱 Amazon Elastic Container Service 開發人員指南中的刪除服務。

使用 Route 53 主控台刪除私有託管區域。

若要使用 Route 53 主控台刪除私有託管區域，請執行下列程序。

若要使用 Route 53 主控台刪除私有託管區域。

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 確認要刪除的託管區域只包含 NS 和 SOA 記錄。如果包含其他記錄，請刪除它們：
   a. 選擇要刪除的託管區域的名稱。
   b. 在 Record (記錄) 頁面的記錄清單中，如果有任何記錄的 Type (類型) 欄值不是 NS 或 SOA，請選擇該列，然後選擇 Delete (刪除)。

      若要選取多個連續的記錄，請選擇第一列，按住 Shift 鍵，然後選擇最後一列。若要選取多個非連續的記錄，請選擇第一列，按住 Ctrl 鍵，然後選擇其餘列。
3. 在 Hosted Zones (託管區域) 頁面上，選擇要刪除的託管區域的對應列。
4. 選擇 Delete (刪除)。
5. 輸入確認金鑰，然後選擇 Delete (刪除)。

將託管區域遷移到其他 AWS 帳戶

如果您想要將託管區域從一個 AWS 帳戶移轉到另一個帳戶，您可以透過程式設計方式列出舊託管區域中的記錄、編輯輸出，然後使用編輯的輸出，以程式設計方式在新的託管區域中建立記錄。注意下列事項：

- 如果您只有幾筆記錄，您也可以使用 Route 53 主控台在新的託管區域中建立記錄。如需詳細資訊，請參閱 使用 Amazon Route 53 主控台來建立記錄。
- 某些程序使用 AWS Command Line Interface (AWS CLI)。您也可以使用其中一個開 AWS 發套件、Amazon 路線 53 API 或 AWS Tools for Windows PowerShell. 對於本主題，我們使用， AWS CLI 因為對於少量託管區域來說更容易。
- 如果新的託管區域名稱與現有託管區域不同，但具有相同的記錄，您也可以使用此程序，在這個新的託管區域中建立記錄。

- 如果別名記錄會將流量路由到流量政策執行個體，您就無法遷移此別名記錄。

主題

- 步驟 1：安裝或升級 AWS CLI
- 步驟 2：建立新的託管區域
- 步驟 3：建立檔案以包含您想要遷移的記錄
- 步驟 4：編輯您想要遷移的記錄
- 步驟 5：將大檔案分成較小的檔案
- 步驟 6：在新的託管區域中建立記錄
- 步驟 7：比較舊託管區域和新託管區域中的記錄
- 步驟 8：更新網域註冊以使用新託管區域的名稱伺服器
- 步驟 9：等待 DNS 解析程式開始使用新的託管區域
- 步驟 10：(選用) 刪除舊的託管區域

步驟 1：安裝或升級 AWS CLI

若要取得有關下載、安裝和配置的資訊 AWS CLI，請參閱《AWS Command Line Interface 使用指南》。

> **Note**
>
> 設定 CLI；當您使用建立託管區域的帳戶和要將託管區域遷移至其中的目標帳戶時，會用到。如需詳細資訊，請參閱 AWS Command Line Interface 使用者指南中的設定。

如果您已經在使用 AWS CLI，建議您升級至最新版本的 CLI，以便 CLI 命令支援最新的 Route 53 功能。

步驟 2：建立新的託管區域

下列程序說明如何使用 Route 53 主控台來建立要遷移過去的目標託管區域。

> **Note**
>
> Route 53 會將新的一組四個名稱伺服器指派給新的託管區域。將託管區域移轉到另一個 AWS 帳戶後，您需要更新網域註冊，才能將名稱伺服器用於新託管區域。我們會在此程序稍後提醒您此步驟。

使用不同帳戶建立新的託管區域

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

   使用您要將託管區域遷移至其中的目標帳戶登入資料來登入。
2. 建立託管區域。如需詳細資訊，請參閱 建立公有託管區域。
3. 記下託管區域 ID。在部分情況下，您會於稍後程序中需要這項資訊。
4. 登出 Route 53 主控台。

步驟 3：建立檔案以包含您想要遷移的記錄

若要將記錄從某個託管區域遷移到另一個，您要建立一個檔案以包含您希望遷移的記錄、編輯該檔案，然後使用編輯過的檔案在新託管區域中建立記錄。請執行下列程序以建立檔案。

建立檔案以包含您想要遷移的記錄

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

   使用您已建立要遷移之託管區域的帳戶登入資料來登入。
2. 取得您要遷移之託管區域的託管區域 ID：

   a. 在導覽窗格中，選擇 Hosted zones (託管區域)。

   b. 尋找您要遷移的託管區域。如果您有很多託管區域，則可以選擇 Exact domain name (確切的網域名稱) 並輸入託管區域名稱，然後按下 Enter 鍵來篩選清單。

   c. 取得 Hosted zone ID (託管區域 ID) 欄的值。
3. 執行以下命令：

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

注意下列事項：

- 對於 *hosted-zone-id*，指定您在此程序的步驟 2 中取得的託管區域 ID。
- 對於 *path-to-output-file*，指定要儲存輸出的目錄路徑和檔案名稱。
- > 字元會將輸出傳送到指定的檔案。
- 會 AWS CLI 自動處理包含 100 筆以上記錄的託管區域的分頁。若要取得更多資訊，請參閱《使用指南》中的〈使用指 AWS 令行介面的分頁選項〉。AWS Command Line Interface

  如果您使用其他程式設計方法列出記錄 (例如其中一個 AWS SDK)，則每頁結果最多可以取得 100 筆記錄。如果託管區域包含超過 100 個記錄，您必須提交多個請求以列出所有記錄。
- 若要在 PowerShell 早於 6.0 的 Windows 版本中執行命令，請使用下列語法：

  ```
  aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id | Out-File path-to-output-file -Encoding utf8
  ```

例如，如果您在 Windows 電腦 AWS CLI 上執行，您可以執行下列命令：

```
aws route53 list-resource-record-sets --hosted-zone-id ZOLDZONE12345 > c:\temp\list-records-ZOLDZONE12345.txt
```

如果您在 Windows 電腦 AWS CLI 上執行的是 PowerShell 早於 6.0 的 Windows 版本，您可以執行下列命令：

```
$output = aws route53 list-resource-record-sets --hosted-zone-id <hosted-zone-id>;
 $mypath = <output-path ;
[System.IO.File]::WriteAllLines($mypath,$output)
```

4. 建立此輸出的副本。在新託管區域中建立記錄之後，建議您在新的託管區域上執行 AWS CLI `list-resource-record-sets`命令，並比較兩個輸出，以確保所有記錄都已建立。

步驟 4：編輯您想要遷移的記錄

您在上一個程序中建立的檔案格式與用於在新託管區域中建立記錄的 AWS CLI `change-resource-record-sets`指令所需的格式接近。不過，您仍需要編輯此檔案。您必須為每筆記錄套用一些變更。您可以在適當的文字編輯器中，使用搜尋和取代功能進行這些變更。

開啟您在 步驟 3：建立檔案以包含您想要遷移的記錄 中建立的檔案複本，並進行以下變更：

- 刪除輸出最上方的前兩行：

```
{
    "ResourceRecordSets": [
```

- 刪除 NS 和 SOA 記錄的相關行。新的託管區域已有這些記錄。
- 選用 – 新增 `Comment` 元素。
- 新增 `Changes` 元素。
- 針對每筆記錄，新增 `Action` 和 `ResourceRecordSet` 元素。
- 新增左大括號及右大括號（`{ }`），以讓 JSON 程式碼有效。

> **Note**
>
> 您可以使用 JSON 驗證程式，以驗證所有大括號和括號都位置正確。若要尋找線上 JSON 驗證程式，請在網際網路上搜尋 "`json validator`"。

- 如果託管區域包含任何別名，其參考相同託管區域中的其他記錄，請進行以下變更：
  - 將託管區域 ID 變更為新託管區域的 ID。

> **Important**
>
> 如果別名記錄指向另一個資源 (例如負載平衡器)，請勿將託管區域 ID 變更為資源本身的託管區域 ID，而不是網域的託管區域 ID。如果您不小心變更了託管區域 ID，請將託管區域 ID 回復為資源本身的託管區域 ID，而不是網域的託管區域 ID。您可以從建立資源的 AWS 主控台找到該託管區域 ID。

  - 將別名記錄移至檔案底部。Route 53 必須先建立別名記錄所要參考的記錄，之後才能建立別名記錄。

> **Important**
>
> 如果一或多個別名記錄會參考其他的別名記錄，則別名的目標記錄必須比參考的別名記錄先在檔案中出現。例如，如果 alias.example.com 是 alias.alias.example.com 的別名目標，則 alias.example.com 必須先在檔案中出現。

- 刪除任何會將流量路由到流量政策執行個體的別名記錄。記下這些記錄，以便稍後可以重新建立。

- 您可以使用此程序，在不同名稱的託管區域中建立記錄。針對輸出中的每筆記錄，將 Name 元素的網域名稱部分變更為新託管區域的名稱。例如，如果您列出 example.com 託管區域中的記錄，並想要在 example.net 託管區域中建立記錄，請將每個記錄名稱的 example.com 部分變更為 example.net：

  從：

  - "Name": "example.com."
  - "Name": "www.example.com."

  至：

  - "Name": "example.net."
  - "Name": "www.example.net."

以下範例顯示 example.com 託管區域的已編輯版本記錄。紅色、斜體文字是新的：

```
{
    "Comment": "string",
    "Changes": [
        {
            "Action": "CREATE",
            "ResourceRecordSet":{
                "ResourceRecords": [
                    {
                        "Value": "192.0.2.4"
                    },
                    {
                        "Value": "192.0.2.5"
                    },
                    {
                        "Value": "192.0.2.6"
                    }
```

```
                ],
                "Type": "A",
                "Name": "route53documentation.com.",
                "TTL": 300
            }
        },
        {
            "Action": "CREATE",
            "ResourceRecordSet":{
                "AliasTarget": {
                    "HostedZoneId": "Z3BJ6K6RIION7M",
                    "EvaluateTargetHealth": false,
                    "DNSName": "s3-website-us-west-2.amazonaws.com."
            },
                "Type": "A",
                "Name": "www.route53documentation.com."
            }
        }
    ]
}
```

步驟 5：將大檔案分成較小的檔案

如果您有許多記錄，或是您的記錄有許多值 (例如許多 IP 地址)，您可能需要將檔案分成較小的檔案。以下是上限：

- 每個檔案最多可包含 1,000 筆記錄。
- 所有 `Value` 元素中的值組合最大長度為 32,000 位元組。

步驟 6：在新的託管區域中建立記錄

若要在新託管區域中建立記錄，請使用下列 AWS CLI 指令：

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-new-hosted-zone --
change-batch file://path-to-file-that-contains-records
```

例如：

```
aws route53 change-resource-record-sets --hosted-zone-id ZNEWZONE1245 --change-batch
 file://c:/temp/change-records-ZNEWZONE1245.txt
```

如果您已刪除任何會將流量路由到流量政策執行個體的別名記錄，請使用 Route 53 主控台重新建立這些別名記錄。如需詳細資訊，請參閱 使用 Amazon Route 53 主控台來建立記錄。

步驟 7：比較舊託管區域和新託管區域中的記錄

若要確認您已成功在新的託管區域中建立所有記錄，建議您列出新託管區域中的記錄，並與含舊託管區域記錄清單的輸出進行比較。若要執行此操作，請執行以下程序。

比較舊託管區域和新託管區域中的記錄

1. 執行以下命令：

   ```
   aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id --output json
    > path-to-output-file
   ```

   指定下列值：

   - 對於 *hosted-zone-id*，指定新託管區域的 ID。
   - 對於 *path-to-output-file*，指定要儲存輸出的目錄路徑和檔案名稱。請使用與您在步驟 3：建立檔案以包含您想要遷移的記錄中使用的檔案名稱不同的檔案名稱。使用不同的檔案名稱可確保新的檔案不會覆寫舊檔案。
   - > 字元會將輸出傳送到指定的檔案。

   例如，如果您使用的是 Windows 電腦，您可以執行下列命令：

   ```
   aws route53 list-resource-record-sets --hosted-zone-id ZNEWZONE67890 --output json
    > c:\temp\list-records-ZNEWZONE67890.txt
   ```

2. 將輸出與步驟 3：建立檔案以包含您想要遷移的記錄的輸出進行比較。

   除了 NS 和 SOA 記錄值以及您在步驟 4：編輯您想要遷移的記錄中所做的任何變更 (如不同的託管區域 ID 或網域名稱) 之外，這兩個輸出應該是相同的。

3. 如果新託管區域的記錄與舊託管區域的記錄不符，您可以執行下列其中一項操作：

   - 使用 Route 53 主控台進行小更正。如需詳細資訊，請參閱 編輯記錄。
   - 如果缺少大量記錄，請建立新的文字檔案以包含缺少的記錄，然後重複 步驟 6：在新的託管區域中建立記錄。
   - 刪除新託管區域中除了 NS 和 SOA 記錄以外的所有記錄，並重複以下步驟：

- 步驟 4：編輯您想要遷移的記錄
- 步驟 5：將大檔案分成較小的檔案
- 步驟 6：在新的託管區域中建立記錄
- 步驟 7：比較舊託管區域和新託管區域中的記錄

步驟 8：更新網域註冊以使用新託管區域的名稱伺服器

當您在新託管區域中完成建立記錄之後，請變更您網域註冊的名稱伺服器以使用新託管區域的名稱伺服器。

> **Important**
>
> 如果您未將網域註冊更新為使用新託管區域的名稱伺服器，Route 53 將繼續使用舊託管區域來路由網域的流量。如果您刪除舊託管區域但未更新網域註冊的名稱伺服器，該網域會變成無法在網際網路上使用。如果您新增、更新或刪除新託管區域中的記錄，但未更新網域註冊的名稱伺服器，系統就不會根據這些變更來路由流量。

如需詳細資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

> **Note**
>
> 無論您使用的是遷移使用中網域之 DNS 服務的程序，或非作用中網域的程序，您都可以略過以下步驟，因為您已經建立新的託管區域與該託管區域中的記錄：
>
> - 步驟 1：從目前的 DNS 服務提供者取得您目前的 DNS 組態
> - 步驟 2：建立託管區域
> - 步驟 3：建立記錄

步驟 9：等待 DNS 解析程式開始使用新的託管區域

如果您的網域正在使用中—例如，如果您的使用者正在使用該網域名稱瀏覽網站或存取 Web 應用程式—則 DNS 解析程式已快取目前 DNS 服務提供者所提供的名稱伺服器的名稱。DNS 解析程式會將幾分鐘前快取的那項資訊儲存最多兩天。

> **Note**
>
> 如果您在新託管區域中建立了任何未出現在舊託管區域中的記錄，則必須等到解析程式開始使用新託管區域的名稱伺服器之後，您的使用者才能使用新記錄來存取您的資源。例如，假設您在新託管區域中建立一筆 test.example.com 的記錄，而該新託管區域應該將網際網路流量路由到您的網站。如果該筆記錄未出現在舊的託管區域中，則必須等到解析程式開始使用新的託管區域之後，您才能在 Web 瀏覽器中輸入 test.example.com。

若要確保將託管區域移轉到其他 AWS 帳戶已完成，然後再刪除舊的託管區域，請在更新網域註冊後等待兩天，以便在新託管區域使用名稱伺服器。等過了這兩天的 TTL 且解析程式請求您網域的名稱伺服器之後，解析程式即可取得目前的名稱伺服器。您也可以啟用 解析程式查詢日誌記錄 來監控新託管區域中的查詢。如需 Resolver 查詢日誌記錄定價的資訊，請參閱 CloudWatch 定價。

步驟 10：(選用) 刪除舊的託管區域

當您確信不再需要舊的託管區域時，可以選擇將其刪除。

> **Important**
>
> 在您將網域註冊更新為使用新託管區域的名稱伺服器之後，請至少等待 48 小時再刪除舊託管區域或該託管區域中的任何記錄。如果您在 DNS 解析程式停止使用舊託管區域中的記錄之前就刪除該託管區域，則必須等到解析程式開始使用新的託管區域之後，才能在網際網路上使用您的網域。

託管區域必須空白，預設 NS 和 SOA 記錄除外。如果舊託管區域包含許多記錄，使用主控台刪除這些記錄可能會花很長的時間。其中一個選項是執行以下步驟：

1. 再做一份於步驟 4：編輯您想要遷移的記錄中編輯過的檔案複本。
2. 在該檔案複本中，將每筆記錄的 `"Action": "CREATE"` 變更為 `"Action": "DELETE"`。
3. 使用以下 AWS CLI 命令刪除記錄：

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-old-hosted-zone --
change-batch file:///path-to-file-that-contains-records
```

> **Important**
>
> 請確定您為託管區域 ID 指定的值是舊託管區域的 ID，而非新託管區域的 ID。

4. 刪除任何剩餘記錄和託管區域：

   a. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

      使用您建立舊託管區域的帳戶登入資料來登入。

   b. 在導覽窗格中，選擇 Hosted zones (託管區域)。

   c. 選擇舊託管區域的名稱。如果您有很多託管區域，則可以選擇 Exact domain name (確切的網域名稱) 并輸入託管區域名稱，然後按下 Enter 鍵來篩選清單。

   d. 如果託管區域包含預設 NS 和 SOA 記錄以外的任何記錄 (例如會將流量路由到流量政策執行個體的別名記錄)，請選擇對應的核取方塊，然後選擇 Delete (刪除)。

   e. 在導覽窗格中，選擇 Hosted zones (託管區域)。

   f. 在託管區域清單中，選擇要刪除之託管區域的選項按鈕。

   g. 選擇刪除。

處理記錄

為網域 (例如 example.com) 建立託管區域之後，您需要建立記錄，以告知網域名稱系統 (DNS) 為該網域路由流量的方式。

例如，您可以建立記錄，指示 DNS 執行下列動作：

- 將 example.com 的網際網路流量路由到您資料中心的主機的 IP 地址。
- 將該網域的電子郵件 (ichiro@example.com) 路由到郵件伺服器 (mail.example.com)。
- 將名為 operations.tokyo.example.com 的子網域的流量路由到不同主機的 IP 地址。

每個記錄都包含網域或子網域名稱、記錄類型 (例如，具有 MX 路由電子郵件類型的記錄)，以及適用於該記錄類型的其他資訊 (對於 MX 記錄，一或多個郵件伺服器的主機名稱和每個伺服器的優先順序)。如需不同記錄類型的詳細資訊，請參閱支援的 DNS 記錄類型。

託管區域中每個記錄的名稱必須以託管區域名稱結尾。例如，example.com 託管區域可包含 www.example.com 和 accounting.tokyo.example.com 子網域的記錄，但不能包含 www.example.ca 子網域的記錄。

> **Note**
>
> 若要為複雜路由組態建立記錄，您也可以使用流量流程視覺化編輯器，並將組態儲存為流量政策。然後，您可以將流量政策與相同託管區域或多個託管區域中的一或多個網域名稱 (例如 example.com) 或子網域名稱 (如 www.example.com) 關聯。此外，如果新組態執行不如預期，您可以復原更新。如需詳細資訊，請參閱 使用流量流程來路由 DNS 流量。

對於您新增到託管區域的記錄，Amazon Route 53 不收取費用。如需託管區域中可建立之記錄數目上限的資訊，請參閱配額。

主題

- 選擇路由政策
- 選擇別名或非別名記錄
- 支援的 DNS 記錄類型
- 使用 Amazon Route 53 主控台來建立記錄
- 資源記錄集許可
- 您在建立或編輯 Amazon Route 53 記錄指定的值
- 透過匯入區域檔案建立記錄
- 編輯記錄
- 刪除記錄
- 列出記錄

選擇路由政策

當您建立記錄，需要先選擇路由政策，這會決定 Amazon Route 53 回應查詢的方式：

- 簡便路由政策 – 用於為網域執行指定功能的單一資源，例如，為 example.com 網站提供內容的 Web 伺服器。您可以使用簡易路由在私有託管區域中建立記錄。
- 容錯移轉路由政策 – 如果要設定主動-被動容錯移轉時使用。您可以使用容錯移轉路由在私有託管區域中建立記錄。

- 地理位置路由政策 – 用於根據使用者位置來路由流量。您可以使用地理位置路由在私有託管區域中建立記錄。
- 地理位置鄰近性路由政策：用於根據資源位置路由流量，以及 (選用) 將流量從某個位置的資源轉移到另一個位置的資源。您可以使用地理鄰近路由在私人託管區域中建立記錄。
- 延遲路由政策：如果您的資源位於多個 AWS 區域，並且您希望將流量路由到提供最佳延遲的區域，則可以使用該政策。您可以使用延遲路由在私有託管區域中建立記錄。
- 以 IP 為基礎的路由政策 - 用於在能夠取得流量來源 IP 地址的情況下根據使用者位置路由流量。
- 多值回答路由政策 – 如果您希望 Route 53 用隨機選取的正常記錄 (最多八個) 回應 DNS 查詢，可以使用該政策。您可以使用多值回答路由在私有託管區域中建立記錄。
- 加權路由政策 – 用於按照您指定的比例將流量路由到多個資源。您可以使用加權路由在私有託管區域中建立記錄。

主題

- 簡便路由
- 容錯移轉路由
- 地理位置路由
- 地理鄰近路由
- 以延遲為基礎的路由
- 以 IP 為基礎的路由
- 多值回答路由
- 加權路由
- Amazon Route 53 如何使用 EDNS0 判斷使用者的位置

簡便路由

簡便路由可讓您設定不含特殊 Route 53 路由 (例如加權或延遲) 的標準 DNS 記錄。透過簡便路由，您通常會將流量路由至單一資源，例如您網站的 Web 伺服器。

您可以在私有託管區域中使用簡便路由政策。

如果您在主 Route 53 控台中選擇簡便路由政策，則不能建立具有相同名稱和類型的多個記錄，但您可以在相同記錄中指定多個值 (例如多個 IP 地址)。(如果您為別名記錄選擇簡便路由政策，您可以在目前的託管區域中指定一個 AWS 資源或一個記錄。) 如果您在記錄中指定多個值，Route 53 會以隨機排列

將所有值傳回遞迴解析程式，解析程式會將值傳回給提交 DNS 查詢的用戶端 (例如 Web 瀏覽器)。然後，用戶端會選擇值並重新提交查詢。使用簡便路由政策雖然可以指定多個 IP 地址，但不會檢查這些 IP 地址的運作狀態。

如需在使用簡便路由政策來建立記錄時指定值的資訊，請參閱下列主題：

- 簡單記錄的專用值
- 簡單別名記錄的專用值
- 所有路由政策的常見值
- 所有路由政策的別名記錄常見值

容錯移轉路由

容錯移轉路由可讓您將流量路由到某個資源 (如果該資源正常) 或路由到其他資源 (如果第一個資源狀況不良)。主要和次要記錄可以將流量路由到任何內容，從設定為網站的 Amazon S3 儲存貯體到複雜的記錄樹。如需詳細資訊，請參閱 主動-被動容錯移轉。

您可以在私有託管區域中使用容錯移轉路由政策。

如需在使用容錯移轉路由政策來建立記錄時指定值的資訊，請參閱下列主題：

- 容錯移轉記錄的專用值
- 容錯移轉別名記錄的專用值
- 所有路由政策的常見值
- 所有路由政策的別名記錄常見值

地理位置路由

地理位置路由可讓您根據使用者的地理位置 (即 DNS 查詢的來源位置) 選擇服務流量的資源。例如，您可能想要將來自歐洲的所有查詢路由到位於法蘭克福區域的 Elastic Load Balancing 負載平衡器。

使用地理位置路由時，您可以對內容進行本地化，以使用者使用的語言呈現部分或全部的網站內容。您也可以使用地理位置路由，以便僅向您擁有分佈權利的位置分佈內容。另一個可能的用途是以可預測的 easy-to-manage 方式平衡端點之間的負載，以便每個使用者位置一致地路由到相同的端點。

您可以依洲別、依國家/地區或依美國州別指定地理位置。如果您為重疊的地理區域建立不同的記錄—例如，北美洲一個記錄，加拿大一個記錄—則最小的地理區域具有更高的優先順序。這可讓您將某洲的

部分查詢路由到一個資源，並將該洲上選定國家/地區的查詢路由到另一個資源。(如需每個洲別的國家/地區清單，請參閱位置。)

地理位置的運作方式是將 IP 地址對應到位置。然而，有些 IP 地址並未映射到地理位置，所以即使您建立涵蓋所有七大洲的地理位置記錄，Amazon Route 53 仍會收到一些來自無法識別位置的 DNS 查詢。您可以建立預設記錄，用來處理來自未對應到任何位置的 IP 地址的查詢，以及來自您未建立地理位置記錄的位置的查詢。如果您未建立預設記錄，對於來自這些位置的查詢，Route 53 會傳回「無回答」回應。

您可以對公有和私有託管區域中的記錄使用地理位置路由。

如需詳細資訊，請參閱 Amazon Route 53 如何使用 EDNS0 判斷使用者的位置。

如需在使用地理位置路由政策來建立記錄時指定值的資訊，請參閱下列主題：

- 地理位置記錄的專用值
- 地理位置別名記錄的專用值
- 所有路由政策的常見值
- 所有路由政策的別名記錄常見值

私有託管區域中的地理位置路由

針對私有託管區域，Route 53 會根據查詢源自之 VPC 的AWS 區域 來回應 DNS 查詢。針對 AWS 區域 的清單，請參閱《Amazon EC2 使用者指南》中的區域和分區。

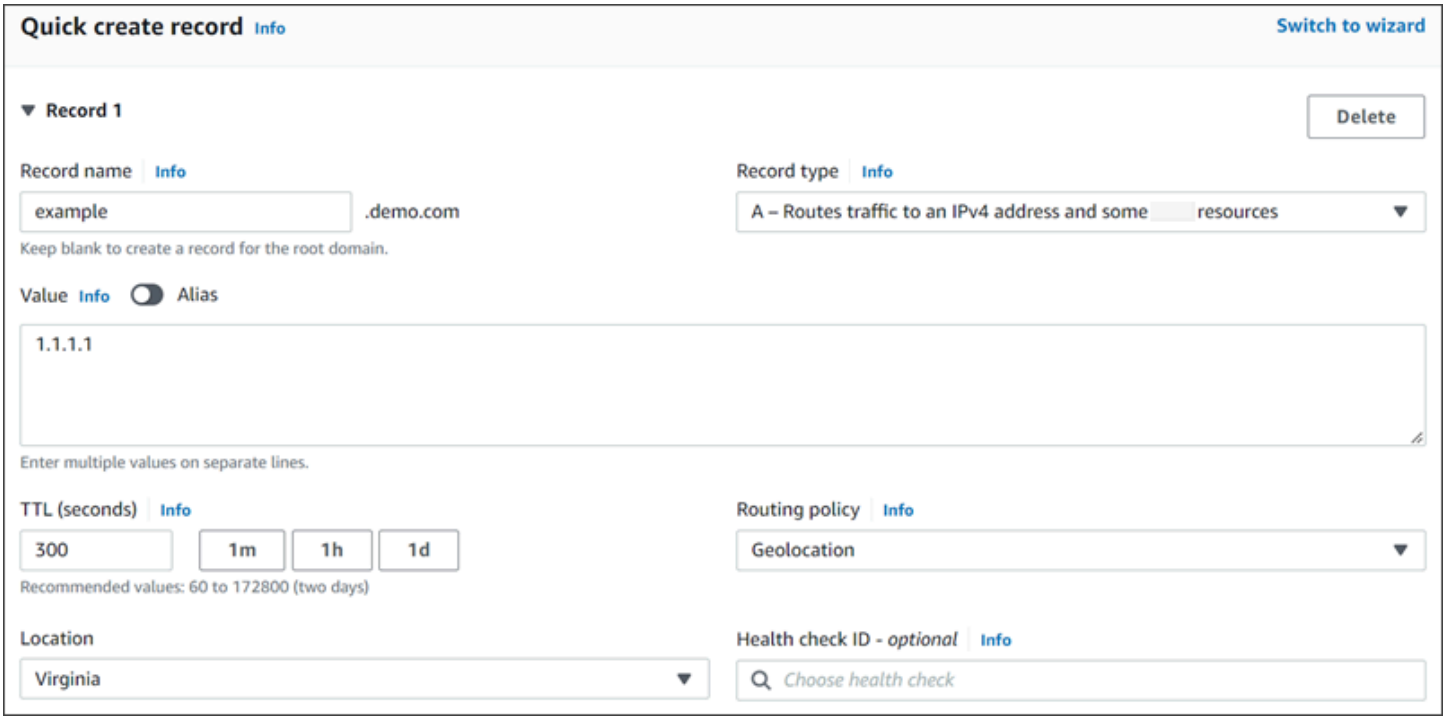
如果 DNS 查詢源自混合式網路的內部部署部分，則會將其視為源自該 VPC 所在的 AWS 區域。

如果包含運作狀態檢查，則可以建立以下項目的預設記錄：

- 未對應至地理位置的 IP 位址。
- 來自您尚未為其建立地理位置記錄之位置的 DNS 查詢。

如果 DNS 查詢區域的地理位置記錄運作狀態不佳，則會傳回預設記錄 (如果該記錄運作狀態良好)。

在下圖的範例組態中，會將來自 us-east-1 AWS 區域 (維吉尼亞) 的 DNS 查詢路由至 1.1.1.1 端點。



地理鄰近路由

地理位置鄰近性路由讓 Amazon Route 53 根據您的使用者和資源的地理位置將流量路由到您的資源。它將流量路由到可用的最接近的資源。您也可以指定值，選擇將更多的流量或更少的流量路由至指定資源，稱為偏差。對於其流量會路由至資源的地理區域，偏差會擴大或縮小該地理區域的大小。

為您的資源建立地理位置鄰近性規則，並為每個規則指定下列其中一個值：

- 如果您正在使用AWS資源，請指定您在其中建立資源的AWS 區域或本機區域群組。
- 如果您使用非 AWS 資源，請指定資源的經緯度。

若要使用 AWS Local Zones，您必須先啟用它們。如需詳細資訊，請參閱《AWS Local Zones 使用者指南》中的本機區域入門。

若要了解 AWS 區域 和 Local Zone 之間的差異，請參閱《Amazon EC2 使用者指南》中的區域 (Region) 和區域 (Zone)。

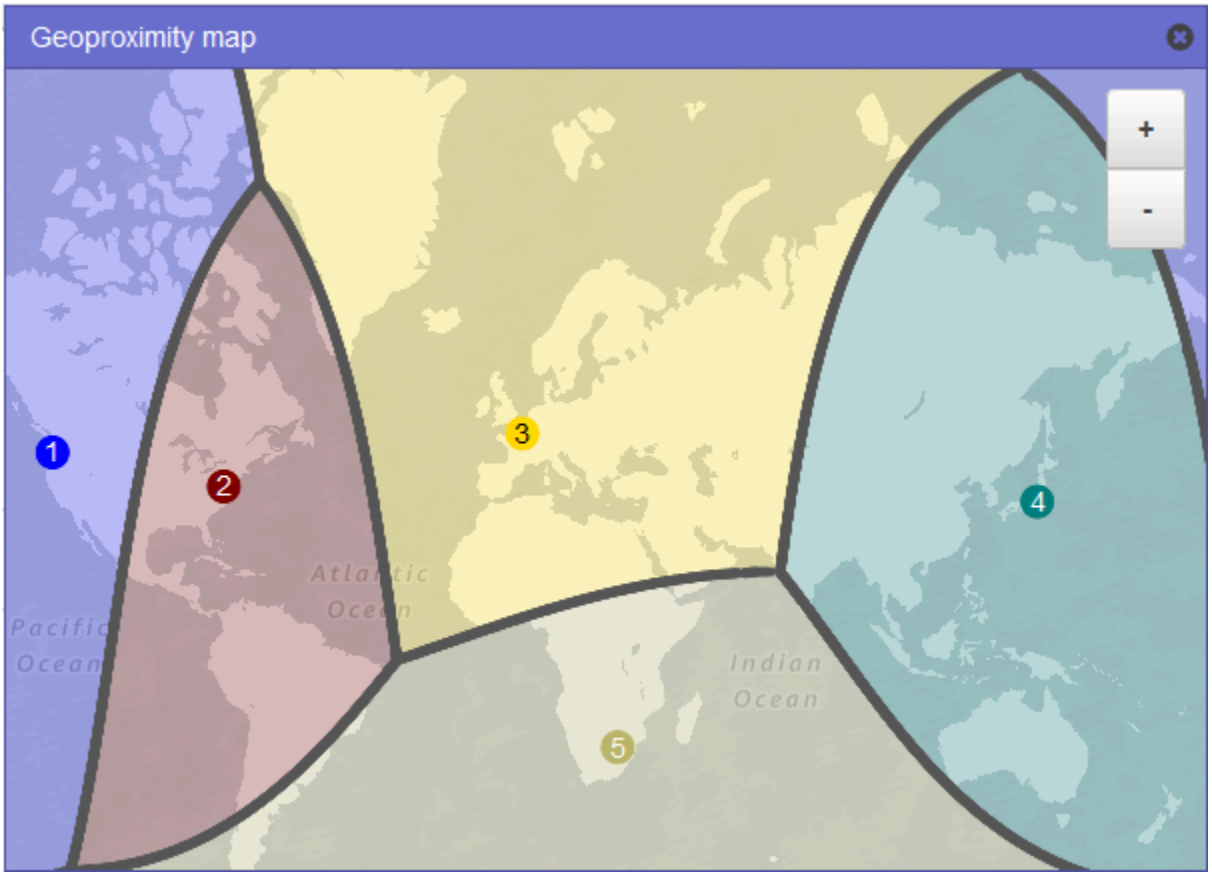
若要選擇性地變更 Route 53 從中將流量路由到資源的地理區域大小，請為偏差指定適用的值：

- 若要擴大 Route 53 從中將流量路由到資源的地理區域大小，請為偏差指定介於 1 到 99 之間的正整數。Route 53 縮小相鄰區域的大小。

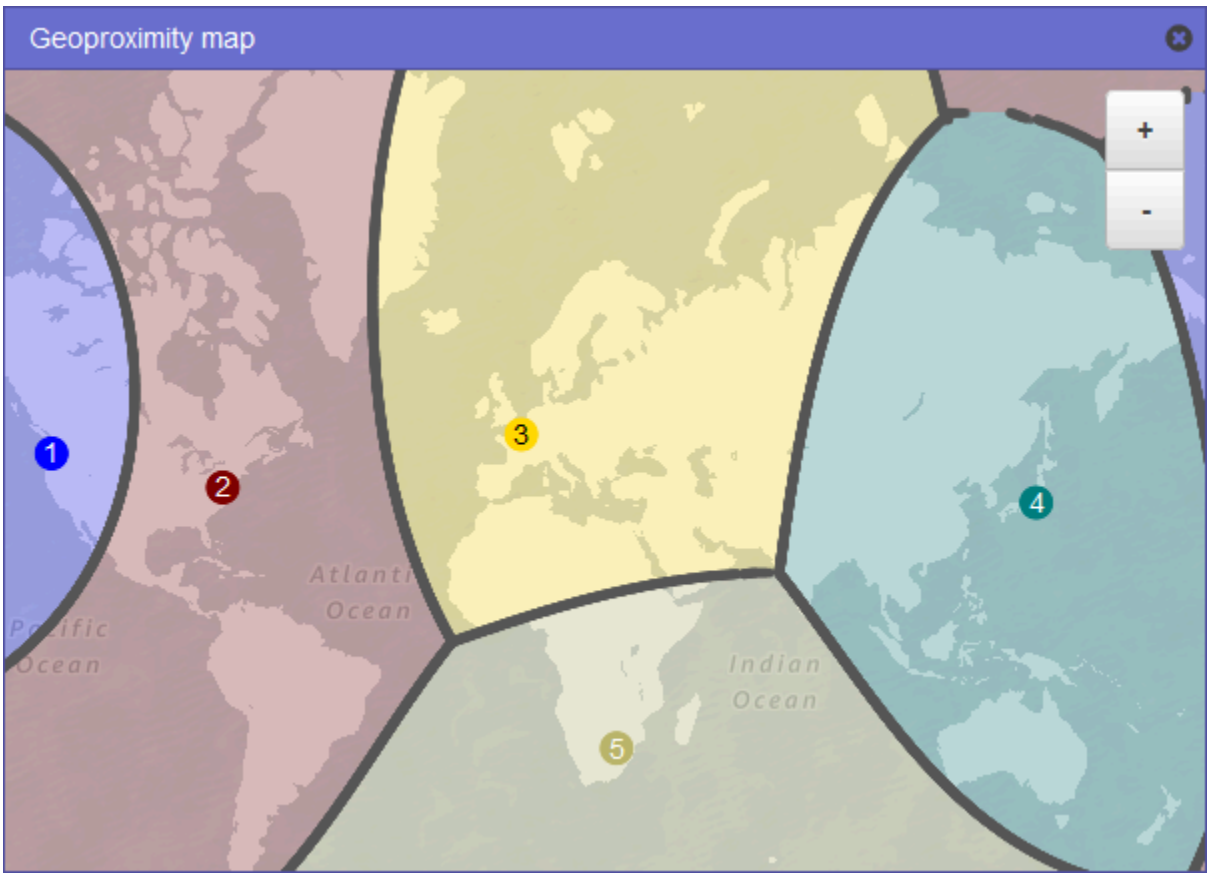
- 若要縮小 Route 53 從中將流量路由到資源的地理區域大小，請為偏差指定介於 -1 到 -99 之間的負整數。Route 53 擴大相鄰區域的大小。

下圖顯示四個 AWS 區域 (編號 1 到 4)，以及在南非約翰尼斯堡由緯度和經度指定的位置 (5)。

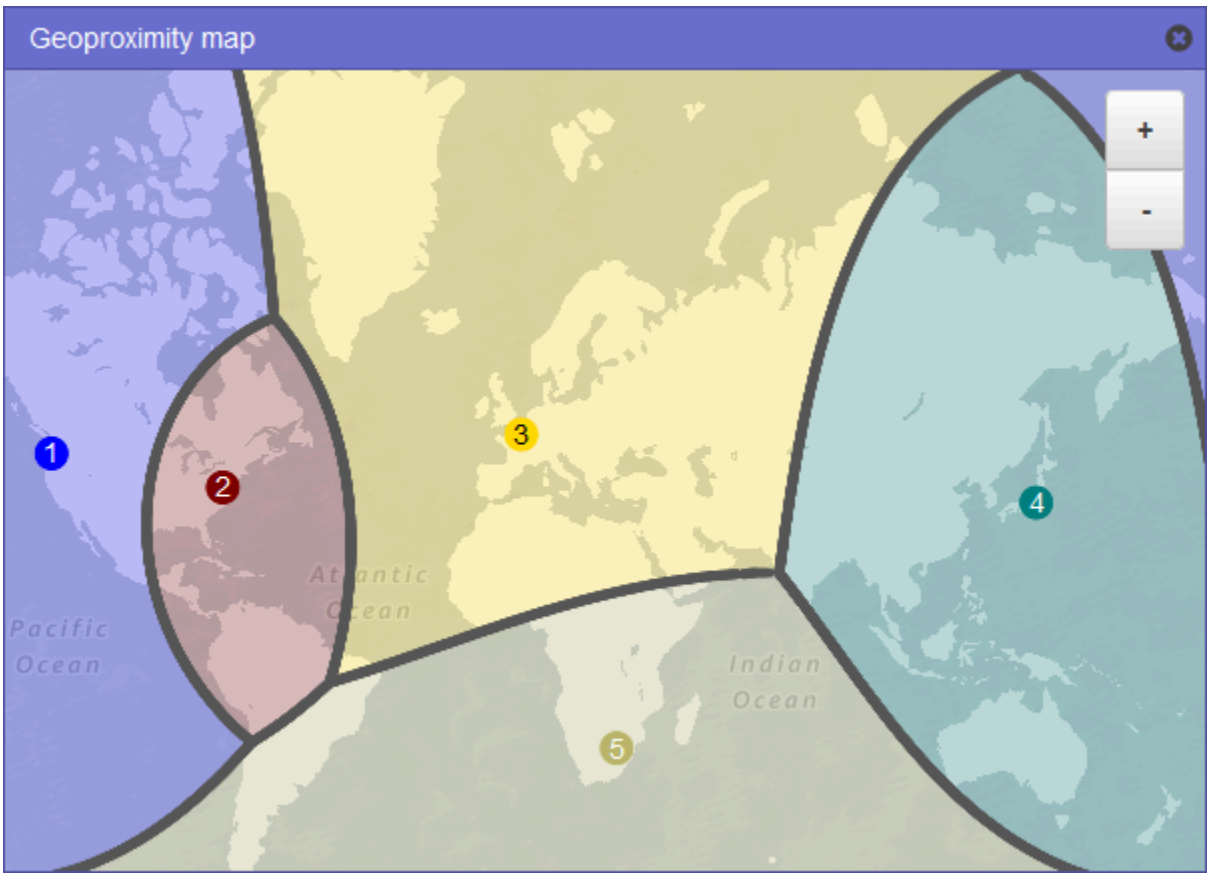
> **Note**
>
> 這些地圖僅適用於交通流量。



下列地圖顯示如果您為美國東部 (維吉尼亞北部) 區域新增 +25 偏差會發生什麼情況 (地圖上的編號 2)。流量會從比之前較大部分的北美洲地區、南美洲的所有地區，路由至該區域中的資源。



下列地圖顯示如果您將美國東部 (維吉尼亞北部) 區域的偏差變更為 -25 時會發生什麼情況。量會從比之前較小部分的北美洲和南美洲地區，路由至該區域中的資源，並會將較多流量路由至相鄰區域 1、3 和 5 的資源。



變更資源的偏差產生的影響，取決於多種因素，包括下列項目：

- 您擁有的資源數目。
- 資源彼此之間的距離。
- 您在地理區域之間的邊界區域附近擁有的使用者數目。例如，假設您在 AWS 區域 美國東部 (維吉尼亞北部) 和美國西部 (奧勒岡) 擁有資源，並且您在美國德州達拉斯、奧斯丁和聖安東尼奧有許多使用者。這些城市在您的資源之間大約是等距，因此對偏差的小幅變更，都可能導致從某個 AWS 區域的資源到另一個區域的資源流量大幅擺動。

我們建議您以較小的增量來變更偏差，以防止由於流量的意外擺動而導致您的資源負擔過重。

如需詳細資訊，請參閱 Amazon Route 53 如何使用 EDNS0 判斷使用者的位置。

Amazon Route 53 如何使用偏差來路由流量

以下是 Amazon Route 53 用來決定如何路由流量的公式：

偏差

```
Biased distance = actual distance * [1 - (bias/100)]
```

當偏差的值為正數，Route 53 會認為 DNS 查詢的來源和您在地理位置鄰近性記錄中指定的資源 (如 AWS 區域 中的 EC2 執行個體) 比實際距離更接近。例如，假設您有以下的地理位置鄰近性記錄：

- Web 伺服器 A 的記錄，它具有正偏差 50
- Web 伺服器 B 的記錄，它沒有偏差

當地理位置鄰近性記錄具有正偏差 50 時，Route 53 會將查詢的來源與該記錄的資源之間的距離減半。然後 Route 53 會計算哪個資源更接近查詢的來源。假設 Web 伺服器 A 與查詢的來源相距 150 公里，而 Web 伺服器 B 與查詢的來源相距 100 公里。如果這兩個記錄都沒有偏差，Route 53 會將查詢路由到 Web 伺服器 B，因為它更接近。不過，因為 Web 伺服器 A 的記錄具有正偏差 50，所以 Route 53 會認為 Web 伺服器 A 與查詢的來源相距 75 公里。因此，Route 53 會將查詢路由到 Web 伺服器 A。

以下是針對正偏差 50 的計算：

```
Bias = 50
Biased distance = actual distance * [1 - (bias/100)]

Biased distance = 150 kilometers * [1 - (50/100)]
Biased distance = 150 kilometers * (1 - .50)
Biased distance = 150 kilometers * (.50)
Biased distance = 75 kilometers
```

以延遲為基礎的路由

如果您的應用程式託管在多個 AWS 區域 中，您可以透過從延遲最低的 AWS 區域 處理使用者的請求來幫助使用者提高效能。

> **Note**
>
> 使用者和資源之間延遲的相關資料，完全以使用者和 AWS 資料中心之間的流量為基準。如果您不使用 AWS 區域 中的資源，則使用者和資源之間的實際延遲可能和 AWS 延遲資料有很大的差異。即使您的資源與 AWS 區域 位於同一個城市，也是如此。

若要使用以延遲為基礎的路由，您可以為多個 AWS 區域 中的資源建立延遲記錄。當 Route 53 收到網域或子網域 (example.com 或 acme.example.com) 的 DNS 查詢時，它會判斷您為哪些 AWS 區域 建立延遲記錄、哪個區域能夠為使用者提供最低延遲，然後選擇該區域的延遲記錄。Route 53 使用所選記錄的值 (例如 Web 伺服器的 IP 地址) 進行回應。

例如，假設您在美國西部 (奧勒岡) 區域與亞太區域 (新加坡) 區域都有 Elastic Load Balancing 負載平衡器。您為每個負載平衡器建立延遲記錄。當位於倫敦的使用者在瀏覽器中輸入您的網域名稱時，將出現以下情況：

1. DNS 會將查詢路由至 Route 53 名稱伺服器。
2. Route 53 參照其有關倫敦與新加坡區域以及倫敦與奧勒岡州區域之間延遲的資料。
3. 如果倫敦與奧勒岡州區域之間的延遲較低，Route 53 會使用位於奧勒岡州的負載平衡器的 IP 地址回應查詢。如果倫敦與新加坡區域之間的延遲較低，Route 53 會使用位於新加坡的負載平衡器的 IP 地址回應查詢。

由於網路連線和路由的變化，網際網路上主機之間的延遲可能會隨著時間改變。以延遲為基礎的路由是根據在一段時間進行的延遲測量，這些測量會反映上述變化。這週路由到奧勒岡州區域的請求，下週可能會被路由到新加坡區域。

> **Note**
>
> 當瀏覽器或其他檢視器使用支援 EDNS0 edns-client-subnet 延伸功能的 DNS 解析器時，DNS 解析程式會將 Route 53 傳送為使用者 IP 位址的截斷版本。如果您設定 Latency Based Routing，Route 53 在將流量路由到您的資源時會考慮此值。如需詳細資訊，請參閱 Amazon Route 53 如何使用 EDNS0 判斷使用者的位置。

您可以在私有託管區域中使用延遲路由政策。

如需在使用延遲路由政策來建立記錄時指定值的資訊，請參閱下列主題：

- 延遲記錄的專用值
- 延遲別名記錄的專用值
- 所有路由政策的常見值
- 所有路由政策的別名記錄常見值

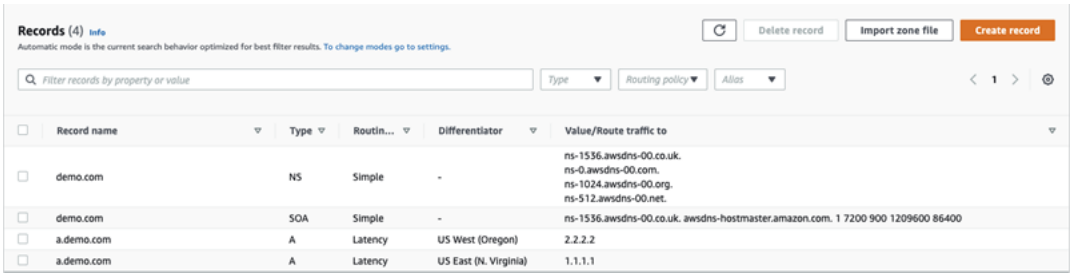
私有託管區域中以延遲為基礎的路由

對於私有託管區域，Route 53 會使用位於相同 AWS 區域 的端點，或是在距離上最接近查詢源自之 VPC 的 AWS 區域 的端點回應 DNS 查詢。

> **Note**
>
> 如果您將輸出端點轉送到輸入端點，則記錄將根據輸入端點所在的位置進行解析，而非輸出端點。

如果包含運作狀態檢查，且對查詢來源為最低延遲的記錄運作狀態不佳，則會傳回下一個最低延遲且運作狀態良好的端點。

在下圖的範例組態中，會將來自 us-east-1 AWS 區域 或與其最接近的 DNS 查詢路由至 1.1.1.1 端點。會將來自 us-west-2 或與其最接近的 DNS 查詢路由至 2.2.2.2 端點。



以 IP 為基礎的路由

藉助 Amazon Route 53 中以 IP 為基礎的路由功能，您可以利用對網路、應用程式和用戶端的了解來微調 DNS 路由，從而為最終使用者做出最佳 DNS 路由決策。以 IP 為基礎的路由讓您能夠透過以使用者 IP 到端點映射的形式將資料上傳到 Route 53，進行精細控制，從而最佳化效能或降低網路成本。

地理位置和以延遲為基礎的路由依賴於 Route 53 收集並保持更新的資料。這種方法適用於大多數客戶，但以 IP 為基礎的路由為您提供了額外的功能，讓您能夠根據自己對客戶群的了解來最佳化路由。例如，全球視訊內容供應商可能希望從特定網際網路服務供應商 (ISP) 路由最終使用者。

以下是以 IP 為基礎的路由的一些常用案例：

- 您希望將最終使用者從某些 ISP 路由到特定端點，以最佳化網絡傳輸成本或效能。
- 您希望根據您對用戶端實體位置的了解，向現有 Route 53 路由類型 (例如地理位置路由) 添加覆寫。

管理 IP 範圍並將其與資源記錄集關聯 (RRSet)

對於 IPv4，您可以使用 1 到 24 位元 (含) 長度之間的 CIDR 區塊，而對於 IPv6，您可以使用 1 到 48 位元 (含) 長度之間的 CIDR 區塊。若要定義零位元 CIDR 區塊 (0.0.0.0/0 或 ::/0)，請使用預設 ("*") 位置。

對於 CIDR 超過 CIDR 集合中指定長度的 DNS 查詢，Route 53 會將其與較短的 CIDR 進行比對。例如，如果您指定 2001:0DB8::/32 做為 CIDR 集合中的 CIDR 區塊，而查詢源自於 2001:0DB8:0000:1234::/48，則將會相符。另一方面，如果您在 CIDR 集合中指定 2001:0DB8:0000:1234::/48，而查詢源自於 2001:0DB8::/32，則將不會相符，Route 53 將以預設 ("*") 位置的記錄回答。

您可以將 CIDR 區塊 (或 IP 範圍) 集組合成 CIDR 位置，然後將這些位置組合成稱為 CIDR 集合的可重複使用實體：

CIDR 區塊

以 CIDR 表示法表示的 IP 範圍，例如 192.0.2.0/24 或 2001:DB8::/32。

CIDR 位置

具名的 CIDR 區塊清單。例如， example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 二零零一::: /32]。CIDR 位置清單中的區塊不必相鄰或在相同的範圍內。

單個位置可以同時具有 IPv4 和 IPv6 區塊，並且此位置可分別與 A 和 AAAA 記錄集相關聯。

根據慣例，位置名稱通常是一個位置，但也可以是任何字串，例如 Company-A。

CIDR 集合

具名的位置集合。例如，我的集合 = [example-isp-seattle， example-isp-tokyo]。

以 IP 為基礎的路由資源記錄集參考集合中的某個位置，並且同一記錄集名稱和類型的所有資源記錄集必須參考同一集合。例如，如果您在兩個區域中建立網站，並希望根據來源 IP 地址將 DNS 查詢從兩個不同 CIDR 位置引導至特定網站，則必須將這兩個位置列在同一 CIDR 集合中。

您也可以使用 AWS RAM 跨 AWS 帳戶分享這些集合。當您進行更新 (例如編輯某個集合中的一個 IP 範圍) 時，更新會自動套用於與該集合關聯的所有記錄集。

您無法在私有託管區域中使用以 IP 為基礎的路由政策。

如需在使用以 IP 為基礎的路由政策來建立記錄時指定值的資訊，請參閱下列主題：

- 特定於以 IP 為基礎記錄的值
- 特定於以 IP 為基礎的別名記錄的值

- 所有路由政策的常見值
- 所有路由政策的別名記錄常見值

主題

- 使用 CIDR 位置和區塊建立 CIDR 集合
- 設定 CIDR 位置和區塊
- 刪除 CIDR 集合
- 從地理位置路由轉變為以 IP 為基礎的路由

使用 CIDR 位置和區塊建立 CIDR 集合

首先建立一個 CIDR 集合，然後將 CIDR 區塊和位置添加到其中。

使用 Route 53 主控台建立 CIDR 集合

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 IP-based routing (以 IP 為基礎的路由)，然後選擇 CIDR collections (CIDR 集合)。
3. 選擇 Create CIDR collection (建立 CIDR 集合)。
4. 在 Create CIDR collection (建立 CIDR 集合) 窗格中的 Details (詳細資訊) 下，輸入集合的名稱。
5. 選擇 Create collection (建立集合) 以建立空集合。

   - 或 -

   在建立 CIDR 位置區段中，於 CIDR 位置方塊中輸入 CIDR 位置的名稱。位置名稱可以是任何識別字串，例如 **`company 1`** 或 **`Seattle`**。不必是實際的地理位置。

   > **Important**
   > CIDR 位置名稱的長度上限為 16 個字元。

   在 CIDR 區塊方塊中輸入 CIDR 區塊，每行一個。這些地址可以是 IPv4 或 IPv6 地址，範圍從 /0 到 /24 (對於 IPv4) 和 /0 到 /48 的地址 (對於 IPv6)。

6. 輸入 CIDR 區塊後，選擇 Create CIDR collection (建立 CIDR 集合)，或 Add another location (新增另一個位置) 以繼續輸入位置和 CIDR 區塊。您可以為每個集合輸入多個 CIDR 位置。
7. 輸入 CIDR 位置後，選擇 Create CIDR collection (建立 CIDR 集合)。

設定 CIDR 位置和區塊

使用 Route 53 主控台設定 CIDR 位置

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 IP-based routing (以 IP 為基礎的路由)、CIDR collections (CIDR 集合)，然後，在 CIDR collections (CIDR 集合) 區段中，按一下 Collection name (集合名稱) 清單中指向某個 CIDR 集合的連結。

   在 CIDR locations (CIDR 位置) 頁面上，可以建立 CIDR 位置、刪除位置或編輯位置及其區塊。

   - 若要建立位置，選擇 Create CIDR location (建立 CIDR 位置)。
   - 在 Create CIDR location (建立 CIDR 位置) 窗格中，輸入位置的名稱、與該位置關聯的 CIDR 區塊，然後選擇 Create (建立)。
   - 若要檢視 CIDR 位置及其中的區塊，選擇某個位置旁邊的選項按鈕，以在位置窗格中顯示其名稱和 CIDR 區塊。

     在此窗格中，您還可以選擇編輯以更新該位置或其 CIDR 區塊的名稱。完成編輯後，選擇 Save (儲存)。
   - 若要刪除某個 CIDR 位置及其中的區塊，選擇待刪除位置旁的選項按鈕，然後選擇 Delete (刪除)。若要確認刪除，在文字輸入欄位中輸入位置名稱，然後選擇 Delete (刪除)。

     > **Important**
     >
     > 刪除 CIDR 位置的操作無法復原。如果您有任何與該位置關聯的 DNS 記錄，則您的網域可能無法連線。

刪除 CIDR 集合

使用 Route 53 主控台刪除 CIDR 集合、其位置和區塊

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 IP-based routing (以 IP 為基礎的路由)，然後選擇 CIDR collections (CIDR 集合)。
3. 在 CIDR collections (CIDR 集合) 區段中，按一下您要刪除的集合的連結名稱。
4. 在 CIDR locations (CIDR 位置) 頁面上，依次選擇各個位置，然後選擇 Delete (刪除)，在對話方塊中輸入其名稱，再選擇 Delete (刪除)。您必須刪除一個 CIDR 集合中的每一個位置，才能刪除該集合。
5. 刪除完所有 CIDR 位置後，在 CIDR locations (CIDR 位置)頁面，選擇待刪除之集合旁邊的選項按鈕，然後選擇 Delete (刪除)。

從地理位置路由轉變為以 IP 為基礎的路由

如果您使用的是地理位置或地理位置鄰近性路由政策，並且您看到特定用戶端總是被路由到非最佳的端點 (根據其實體位置或網絡拓撲得知)，則可以透過使用以 IP 為基礎的路由，更好地定位這些用戶端的公有 IP 範圍。

下表包含一個現有地理位置路由的地理位置組態範例，我們將針對加利佛尼亞 IP 範圍進行微調。

記錄集名稱	路由政策和原始伺服器	應用程式端點的 IP 地址
example。com	地理位置路由 (美國)	198.51.100.1
example。com	地理位置路由 (歐洲)	198.51.100.2

若要覆寫來自加利佛尼亞的 IP 範圍以轉到新的應用程式端點，首先使用新的記錄集名稱重新建立地理位置路由。

記錄集名稱	路由政策和原始伺服器	應用程式端點的 IP 地址
geo.example.com	地理位置路由 (美國)	198.51.100.1

記錄集名稱	路由政策和原始伺服器	應用程式端點的 IP 地址
geo.example.com	地理位置路由 (歐洲)	198.51.100.2

然後，建立以 IP 為基礎的路由記錄以及指向您最近重新建立的地理位置路由記錄集的預設記錄。

記錄集 名稱	路由政策和原始伺服器	應用程式端點的 IP 地址
example。com	以 IP 為基礎的路由 (預設)	要成為預設 geo.example.com 應用程式端點的別名記錄。例如 198.51.100.1 。
example。com	以 IP 為基礎的路由 (加利佛尼亞 IP 範圍)	198.51.100.3

多值回答路由

多值回答路由可讓您設定 Amazon Route 53 傳回多個值 (例如 Web 伺服器的 IP 地址)，以回應 DNS 查詢。您可以為幾乎任意記錄指定多個值，但多值回答路由也可讓您檢查每個資源的運作狀態，以便 Route 53 只傳回正常資源的值。雖然它不能取代負載平衡器，但由於其具備傳回多個可進行運作狀態檢查的 IP 地址的能力，您可以將它與 DNS 配合使用，以提高可用性和負載平衡。

若要將流量以近乎隨機的方式路由到多個資源 (例如 Web 伺服器)，您可以為每個資源建立一個多值回答記錄，並選擇性地將 Route 53 運作狀態檢查關聯至每個記錄。Route 53 最多使用八個正常記錄來回應每個 DNS 查詢，並向不同的 DNS 解析程式提供不同的回應。如果 Web 伺服器在解析程式快取回應後變得不可用，用戶端軟體可以嘗試回應中提供的其他 IP 地址。

注意下列事項：

- 如果您將運作狀態檢查與多值回答記錄建立關聯，Route 53 只會在運作狀態檢查為正常運作時，使用對應 IP 地址來回應 DNS 查詢。
- 如不建立運作狀態檢查與多值回答記錄的關聯，Route 53 一律將記錄視為良好狀態。
- 如果您有八個以下正常運作的記錄，Route 53 會使用所有正常記錄回應所有 DNS 查詢。
- 當所有記錄都狀況不良，Route 53 會使用最多八個狀況不良的記錄來回應 DNS 查詢。

您可以在私有託管區域中使用多值答案路由政策。

如需在使用多值回答路由政策來建立記錄時指定值的資訊，請參閱 多值回答記錄的專用值 和 所有路由政策的常見值。

加權路由

加權路由可讓您將多個資源與單一網域名稱 (example.com) 或子網域名稱 (acme.example.com) 關聯，然後選擇多少流量路由到每個資源。這可用於各種用途，包括負載平衡和測試新版本的軟體。

若要設定加權路由，您可以為每個資源建立同名和同類型的記錄。您為每個記錄指派相對權數，該值對應於您要傳送到每個資源的流量規模。Amazon Route 53 會根據指派給記錄的權重 (佔該群組中所有記錄總權重的比例) 將流量傳送到資源：

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

例如，如果您想要將一小部分的流量傳送到一個資源，並將其餘流量傳送到另一個資源，則可以指定權重 1 和 255。權數為 1 的資源會取得 1/256 的流量 (1/(1+255))，另一個資源會取得 255/256 的流量 (255/(1+255))。您可以透過變更權重逐步變更負載平衡。如果您想要停止傳送流量到資源，可以將該記錄的權重變更為 0。

如需在使用加權路由政策來建立記錄時指定值的資訊，請參閱下列主題：

- 加權記錄的專用值
- 加權別名記錄的專用值
- 所有路由政策的常見值
- 所有路由政策的別名記錄常見值

您可以在私有託管區域中使用加權路由政策。

運作狀態檢查和加權路由

如果您在加權記錄群組中新增所有記錄的運作狀態檢查，但您為某些記錄設定非零權重，而為其他記錄設定零權重，則運作狀態檢查的運作方式與所有記錄都是非零權重相同，除了以下例外：

- Route 53 最初只考量非零加權記錄 (如果有)。
- 如果權重大於 0 的所有記錄都是狀況不良，Route 53 會考慮零加權記錄。

下表詳細說明 0 權重記錄包括運作狀態檢查時的行為：

	第 1 筆記錄	第 2 筆記錄	第 3 筆記錄
Weight	1	1	0
包括運作狀態檢查？	是	是	是
運作狀態檢查狀態	狀況不良	狀況不良	狀態良好
DNS 查詢已回答？	否	否	是
運作狀態檢查狀態	狀況不良	狀況不良	狀況不良
DNS query answered?	是	是	否
運作狀態檢查狀態	狀況不良	狀態良好	狀況不良
DNS 查詢已回答？	否	是	否
運作狀態檢查狀態	狀態良好	狀態良好	狀況不良
DNS 查詢已回答？	是	是	否
運作狀態檢查狀態	狀態良好	狀態良好	狀態良好
DNS 查詢已回答？	是	是	否

下表詳細說明 0 權重記錄不括含運作狀態檢查時的行為：

	第 1 筆記錄	第 2 筆記錄	第 3 筆記錄
Weight	1	1	0
包括運作狀態檢查？	是	是	否
運作狀態檢查狀態	狀態良好	狀態良好	N/A
DNS query answered?	Yes	是	No
運作狀態檢查狀態	狀況不良	狀況不良	N/A
DNS 查詢已回答？	否	否	是
運作狀態檢查狀態	狀況不良	狀態良好	不適用
DNS query answered?	否	是	否

Amazon Route 53 如何使用 EDNS0 判斷使用者的位置

為了提高地理位置、地理鄰近度、IP 型和延遲路由的準確性，Amazon Route 53 支援 EDNS0 的 edns-client-subnet 延伸。(EDNS0 將多個選用延伸新增至 DNS 通訊協定。) edns-client-subnet 只有當 DNS 解析器支援路由 53 時才能使用：

- 當瀏覽器或其他檢視器使用不支援的 DNS 解析器時 edns-client-subnet，Route 53 會使用 DNS 解析器的來源 IP 位址來估算使用者的位置，並以解析器位置的 DNS 記錄回應地理位置查詢。
- 當瀏覽器或其他檢視器使用支援的 DNS 解析器時 edns-client-subnet，DNS 解析器會將 Route 53 傳送截斷版本的使用者 IP 位址。Route 53 根據該截斷的 IP 地址而不是 DNS 解析程式的來源 IP 地址來判斷使用者的位置；這通常能夠更準確地估計使用者的位置。然後，Route 53 使用使用者位置的 DNS 記錄來回應地理位置查詢。

- EDNS0 不適用於私有託管區域。對於私有託管區域，Route 53 使用來自私有託管區域所在的 AWS 區域 中的 Route 53 Resolvers 的資料，做出地理位置和延遲路由決策。

如需有關的詳細資訊 edns-client-subnet，請參閱 DNS 要求中的 EDNS 用戶端子網路 RFC、用戶端子網路。

選擇別名或非別名記錄

Amazon Route 53 別名記錄為 DNS 功能提供 Route 53 特定延伸。別名記錄可讓您將流量路由到選定的AWS資源，例如 CloudFront 分發和 Amazon S3 儲存貯體。也可讓您將流量從託管區域中的某個記錄路由至另一個記錄。

與 CNAME 記錄不同，您可以在 DNS 命名空間的頂端節點 (也稱為 Zone Apex) 上建立別名記錄。例如，如果您註冊 DNS 名稱 example.com，Zone Apex 就是 example.com。您不能為 example.com 建立 CNAME 記錄，但可以為會將流量路由至 www.example.com 的 example.com 建立別名記錄 (只要 www.example.com 的記錄類型並非 CNMAE 類型)。

當 Route 53 收到別名記錄的 DNS 查詢時，Route 53 會以適用於該資源的值來回應：

- Amazon API Gateway 自訂區域 API 或邊緣最佳化 API – Route 53 會使用 API 的一或多個 IP 地址來回應。
- Amazon VPC 介面端點 – Route 53 會使用介面端點的一或多個 IP 地址來回應。
- 發 CloudFront 佈 — Route 53 會針對可提供內容的CloudFront 邊緣伺服器的一或多個 IP 位址進行回應。
- Elastic Beanstalk 環境 – Route 53 會使用環境的一或多個 IP 地址來回應。
- Elastic Load Balancing 負載平衡器：Route 53 會使用負載平衡器的一個或多個 IP 地址來回應。這包括 Application Load Balancer、Classic Load Balancer 和 Network Load Balancer。
- AWS Global Accelerator 加速器：Route 53 會使用加速器的 IP 地址來回應。
- 設定為靜態網站的 Amazon S3 儲存貯體 – Route 53 使用 Amazon S3 儲存貯體的一個 IP 地址回應每個請求。
- 相同託管區域中的其他相同類型的 Route 53 記錄 - Route 53 會將查詢視為如同針對別名記錄所參考的記錄來回應 (請參閱 別名和 CNAME 記錄的比較)。
- AWS AppSync 網域名稱 – Route 53 會使用界面端點的一個或多個 IP 地址來回應。

當您使用別名記錄將流量路由至 AWS 資源時，Route 53 會自動辨識資源的變更。例如，假設 example.com 的別名記錄指向位於 lb1-1234.us-east-2.elb.amazonaws.com 的 Elastic Load Balancing

負載平衡器。如果負載平衡器的 IP 地址變更，Route 53 會使用新的 IP 地址，自動開始回應 DNS 查詢。

如果別名記錄指向 AWS 資源，您無法設定存留時間 (TTL)；Route 53 會使用資源的預設 TTL。如果別名記錄指向相同託管區域中的另一個記錄，Route 53 會使用該別名記錄指向的記錄的 TTL。如需「Elastic Load Balancing」目前的 TTL 值的詳細資訊，請前往 Elastic Load Balancing 使用指南中的要求路由並搜尋「ttl」。

如需如何使用 Route 53 主控台建立記錄的資訊，請參閱 使用 Amazon Route 53 主控台來建立記錄。如需為別名記錄指定值的詳細資訊，請參閱您在建立或編輯 Amazon Route 53 記錄指定的值中適用的主題：

- 簡單別名記錄的專用值
- 加權別名記錄的專用值
- 延遲別名記錄的專用值
- 容錯移轉別名記錄的專用值
- 地理位置別名記錄的專用值
- 地理鄰近別名記錄的特定值
- 所有路由政策的別名記錄常見值

別名和 CNAME 記錄的比較

別名記錄與 CNAME 記錄類似，但有一些重要的差異。下列清單比較別名記錄和 CNAME 記錄。

您可將查詢重新引導到下列資源

別名記錄

別名記錄只能將查詢重新引導到選取的 AWS 資源，例如：

- Amazon S3 儲存貯體
- CloudFront 分佈
- 同一個 Route 53 託管區域中的另一個記錄

例如，您可以建立名為 acme.example.com 的別名記錄，將查詢重新引導到也名為 acme.example.com 的 Amazon S3 儲存貯體。您也可以建立 acme.example.com 別名記錄，將查詢重新引導到 example.com 託管區域中名為 zenith.example.com 的記錄。

CNAME 記錄

CNAME 記錄可以將 DNS 查詢重新引導到任何 DNS 記錄。例如，您可以建立 CNAME 記錄，將來自 acme.example.com 的查詢重新引導到 zenith.example.com 或 acme.example.org。對於您將查詢重新引導到的網域，您不需要使用 Route 53 作為 DNS 服務。

建立與網域具有相同名稱的記錄 (Zone Apex 的記錄)

別名記錄

在大多數組態中，您可以建立與託管區域 (Zone Apex) 同名的別名記錄。但如果您想要將來自 Zone Apex (例如 example.com) 的查詢，重新引導到相同託管區域中類型為 CNAME 的記錄 (例如 zenith.example.com)，則是例外。別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

CNAME 記錄

您無法建立與託管區域 (Zone Apex) 同名的 CNAME 記錄。對於網域名稱的託管區域 (example.com) 和子網域的託管區域 (zenith.example.com)，都是如此。

DNS 查詢的定價

別名記錄

Route 53 不收取針對 AWS 資源進行別名查詢的費用。如需詳細資訊，請參閱 Amazon Route 53 定價。

CNAME 記錄

Route 53 針對 CNAME 查詢收取費用。

> **Note**
>
> 如果您建立重新引導到 Route 53 託管區域 (同一個託管區域或另一個託管區域) 中另一個記錄名稱的 CNAME 記錄，每個 DNS 查詢都會變更為兩個查詢：
>
> - Route 53 會以您要重新引導的目標記錄名稱回應第一個 DNS 查詢。
> - 接著，DNS 解析器必須為第一個回應中的記錄提交另一個查詢，以取得有關要將流量導向到哪個位置的資訊，例如 Web 伺服器的 IP 地址。
>
> 如果 CNAME 記錄重新引導到使用另一個 DNS 服務託管的記錄名稱，Route 53 收取一個查詢的費用。另一個 DNS 服務可能會針對第二個查詢收取費用。

DNS 查詢中指定的記錄類型

別名記錄

只在當別名記錄的名稱 (例如 acme.example.com) 和別名記錄的類型 (例如 A 或 AAAA) 符合 DNS 查詢中的名稱和類型時，Route 53 才會回應 DNS 查詢。

CNAME 記錄

無論 DNS 查詢中指定的記錄類型為何 (例如 A 或 AAAA)，CNAME 記錄都會重新引導記錄名稱的 DNS 查詢。

dig 或 nslookup 查詢中的記錄列出方式

別名記錄

為回應 dig 或 nslookup 查詢，別名記錄會列為您在建立記錄時指定的記錄類型 (例如 A 或 AAAA) (您指定的別名記錄的記錄類型取決於接收路由流量的資源。例如，若要將流量路由到 S3 儲存貯體，則為該類型指定 A)。僅能在 Route 53 主控台中，或在回應程式設計請求 (例如 AWS CLI `list-resource-record-sets` 命令) 時看到的別名屬性。

CNAME 記錄

CNAME 記錄會列為 CNAME 記錄，以回應 dig 或 nslookup 查詢。

支援的 DNS 記錄類型

Amazon Route 53 支援本節列出的 DNS 記錄類型。每個記錄類型還包含範例，說明當您使用 API 存取 Route 53 時如何設定 `Value` 元素的格式。

> **Note**
>
> 針對包括網域名稱的記錄類型，請輸入完整網域名稱，例如 www.example.com。結尾的點號為選用；Route 53 會假設網域名稱是完整的。這表示 Route 53 會將 www.example.com (無結尾點號) 和 www.example.com. (有結尾點號) 視為相同。

Route 53 提供 DNS 功能的延伸，又稱為別名記錄。類似於 CNAME 記錄，別名記錄可讓您將流量路由至所選的 AWS 資源，例如 CloudFront 分發和 Amazon S3 儲存貯體。如需詳細資訊 (包含別名與 CNAME 記錄的比較)，請參閱 選擇別名或非別名記錄。

主題

- A 記錄類型
- AAAA 記錄類型
- CAA 記錄類型
- CNAME 記錄類型
- DS 記錄類型
- MX 記錄類型
- NAPTR 記錄類型
- NS 記錄類型
- PTR 記錄類型
- SOA 記錄類型
- SPF 記錄類型
- SRV 記錄類型
- TXT 記錄類型

A 記錄類型

您可以使用格式為點號十進位格式之 IPv4 位址的 A 記錄，將流量路由傳送到像是 Web 伺服器的資源。

Amazon Route 53 主控台的範例

```
192.0.2.1
```

Route 53 API 的範例

```
<Value>192.0.2.1</Value>
```

AAAA 記錄類型

您可以使用格式為點號十六進位格式之 IPv6 位址的 AAAA 記錄，將流量路由傳送到像是 Web 伺服器的資源。

Amazon Route 53 主控台的範例

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Route 53 API 的範例

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

CAA 記錄類型

CAA 記錄會指定允許哪種憑證授權單位 (CA) 為網域或子網域發出憑證。建立 CAA 記錄有助於防止錯誤的 CA 為您的網域發出憑證。CAA 記錄不能替代由您的憑證授權單位指定的安全要求，例如驗證您是網域擁有者的要求。

您可以使用 CAA 記錄來指定以下內容：

- 哪些憑證授權機構 (CA) 可以發出 SSL/TLS 憑證 (如果有)
- 當 CA 發出網域或子網域的憑證時要聯絡的電子郵件地址或 URL

當您將 CAA 記錄新增到託管區域，可以指定以空格分隔的三個設定：

```
flags tag "value"
```

請注意有關 CAA 記錄的以下事項：

- `tag` 的值僅可包含 A-Z、a-z 和 0-9 字元。
- 永遠用引號 ("") 括住 `value`。
- 某些 CA 允許或需要其他 `value` 的值。以名稱值組形式指定其他值，並以分號 (;) 分隔，例如：

  ```
  0 issue "ca.example.net; account=123456"
  ```
- 如果 CA 收到對子網域 (例如 www.example.com) 的憑證請求，而且如果該子網域沒有 CAA 記錄，CA 提交對父系網域 (例如 example.com) 的 CAA 記錄的 DNS 查詢。如果父系網域的記錄存在，而且如果憑證請求有效，CA 會為子網域發出憑證。
- 我們建議您向 CA 諮詢，以判斷要為 CAA 記錄指定哪些值。
- 您無法建立具有相同名稱的 CAA 記錄與 CNAME 記錄，因為 DNS 名稱不允許 CNAME 記錄和任何其他記錄的類型使用相同名稱。

主題

- 授權 CA 為網域或子網域發出憑證

- 授權 CA 為網域或子網域發出萬用字元憑證
- 防止任何 CA 為網域或子網域發出憑證
- 要求任何 CA 在收到無效憑證請求時聯絡您
- 使用 CA 支援的另一個設定
- 範例

授權 CA 為網域或子網域發出憑證

若要授權 CA 為網域或子網域發出憑證，請建立一個與網域或子網域同名的記錄，並指定以下設定：

- 標記 - `0`
- 標籤 - `issue`
- 值 – 您授權為網域或子網域發出憑證的 CA 代碼

例如，假設您想要授權 ca.example.net 為 example.com 發出憑證。您使用以下設定，為 example.com 建立 CAA 記錄：

```
0 issue "ca.example.net"
```

如需有關如何授權 AWS Certificate Manager 發出憑證的詳細資訊，請參閱 AWS Certificate Manager 使用者指南中的設定 CAA 記錄。

授權 CA 為網域或子網域發出萬用字元憑證

若要授權 CA 為網域或子網域發出萬用字元憑證，請建立一個與網域或子網域同名的記錄，並指定以下設定。萬用字元憑證適用於網域或子網域及其子網域。

- 標記 - `0`
- 標籤 - `issuewild`
- 值 – 您授權為網域或子網域及其子網域發出憑證的 CA 代碼

例如，假設您想要授權 ca.example.net 為 example.com 發出萬用字元憑證 (適用於 example.com 及其所有子網域)。您使用以下設定，為 example.com 建立 CAA 記錄：

```
0 issuewild "ca.example.net"
```

當您要授權 CA 為網域或子網域發出萬用字元憑證，請建立一個與網域或子網域同名的記錄，並指定以下設定。萬用字元憑證適用於網域或子網域及其子網域。

防止任何 CA 為網域或子網域發出憑證

若要防止任何 CA 為網域或子網域發出萬用字元憑證，請建立一個與網域或子網域同名的記錄，並指定以下設定：

- 標記 - `0`
- 標籤 - `issue`
- 值 - `";"`

例如，假設您不希望任何 CA 為 example.com 發出憑證。您使用以下設定，為 example.com 建立 CAA 記錄：

```
0 issue ";"
```

如果您不需要任何 CA 為 example.com 或其子網域發出憑證，可以使用以下設定，為 example.com 建立 CAA 記錄：

```
0 issuewild ";"
```

> **Note**
>
> 如果您為 example.com 建立 CAA 記錄並指定下列兩個值，使用值 ca.example.net 的 CA 可以為 example.com 發出憑證：
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

要求任何 CA 在收到無效憑證請求時聯絡您

如果您希望收到無效憑證請求的任何 CA 聯絡您，請指定以下設定：

- 標記 - `0`
- 標籤 - `iodef`
- 值 – 當 CA 收到無效憑證請求時，您希望 CA 通知的 URL 或電子郵件地址。使用適用的格式：

```
"mailto:email-address"

"http://URL"

"https://URL"
```

例如，如果您希望收到無效憑證請求的任何 CA 傳送電子郵件到 admin@example.com，使用以下設定建立 CAA 記錄：

```
0 iodef "mailto:admin@example.com"
```

使用 CA 支援的另一個設定

如果您的 CA 支援未在 CAA 記錄的 RFC 中定義的功能，請指定以下設定：

- 標記 – 128 (如果 CA 不支援指定的功能，此值可防止 CA 發出憑證。)
- 標籤 – 您授權 CA 使用的標籤
- 值 – 與標籤值對應的值

例如，假設您的 CA 在收到無效憑證請求時支援傳送簡訊。(據我們所知，沒有任何一個 CA 支援此選項。) 記錄的設定可能如下：

```
128 exampletag "15555551212"
```

範例

Route 53 主控台的範例

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Route 53 API 的範例

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

CNAME 記錄類型

CNAME 記錄會將目前記錄的名稱 (例如 acme.example.com) 的 DNS 查詢對應到另一個網域 (例如 example.com 或 example.net)，或另一個子網域 (acme.example.com 或 zenith.example.org)。

> **Important**
>
> DNS 通訊協定不允許您為 DNS 命名空間的頂端節點 (也稱為 Zone Apex) 建立 CNAME 記錄。例如，如果您註冊 DNS 名稱 example.com，Zone Apex 就是 example.com。您不能為 example.com 建立 CNAME 記錄，但可以為 www.example.com、newproduct.example.com 等建立 CNAME 記錄。
>
> 此外，如果您為子網域建立 CNAME 記錄，則無法建立為該子網域任何其他記錄。例如，如果您為 www.example.com 建立 CNAME，則無法建立其 Name (名稱) 欄位值是 www.example.com 的任何其他記錄。

Amazon Route 53 也支援別名記錄，可讓您將查詢路由至選定 AWS 資源 (例如 CloudFront 分發和 Amazon S3 儲存貯體)。別名在某些方面與 CNAME 記錄類型類似；不過，您可以針對 Zone Apex 建立別名。如需更多詳細資訊，請參閱 選擇別名或非別名記錄。

Route 53 主控台的範例

```
hostname.example.com
```

Route 53 API 的範例

```
<Value>hostname.example.com</Value>
```

DS 記錄類型

委派簽署人 (DS) 記錄是指委派子網域地區的地區金鑰。當您設定 DNSSEC 簽署時，如果已建立信任鏈，則可能會建立 DS 記錄。如需在 Route 53 中設定 DNSS EC 的相關資訊，請參閱 在 Amazon Route 53 中設定 DNSSEC 簽署。

前三個值是代表金鑰標籤、演算法與摘要類型的十進位值。第四個值是地區金鑰的摘要。如需 DS 記錄格式的詳細資訊，請參閱 RFC 4034。

Route 53 主控台的範例

```
123 4 5 1234567890abcdef1234567890absdef
```

Route 53 API 的範例

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

MX 記錄類型

MX 記錄會指定郵件伺服器的名稱，且如果您有兩個或多個郵件伺服器，則會同時指定優先順序。MX 記錄的每個值會包含兩個值：優先順序和網域名稱。

優先順序

代表電子郵件伺服器優先順序的整數。如果只指定一個伺服器，優先順序可以是介於 0 到 65535 之間的任何整數。如果指定多個伺服器，為優先順序指定的值指出哪個是您希望電子郵件第一個路由到的電子郵件伺服器，然後第二個，以此類推。含最低優先順序值的伺服器優先。例如，如果您有兩個電子郵件伺服器，而且為優先順序指定值 10 和 20，電子郵件永遠會移至優先順序 10 的伺服器 (除非伺服器不可用)。如果指定值 10 和 10，電子郵件會大致相等地路由到兩個伺服器。

網域名稱

電子郵件伺服器的網域名稱。指定 A 或 AAAA 記錄的名稱 (如 mail.example.com)。在 RFC 2181 的 DNS 規格釐清中，第 10.3 節禁止指定網域名稱值的 CNAME 記錄名稱。(RFC 提到的「別名」表示 CNAME 記錄，而非 Route 53 別名記錄。)

Amazon Route 53 主控台的範例

```
10 mail.example.com
```

Route 53 API 的範例

```
<Value>10 mail.example.com</Value>
```

NAPTR 記錄類型

名稱授權單位指標 (NAPTR) 是一種記錄類型，供動態委派探索系統 (DDDS) 應用程式用來將一個值轉換為另一個值，或將一個值取代為另一個值。例如，一個常見用途是將電話號碼轉換為 SIP URI。

NAPTR 記錄的 `Value` 元素包含六個以空格分隔的值：

順序

當您指定一個以上的記錄，您希望 DDDS 應用程式評估記錄的順序。有效值：0-65535。

Preference

指定兩個或更多具有相同 Order (順序) 的記錄時，您對這些記錄的順序偏好設定會納入評估。例如，如果兩個記錄的 Order (順序) 為 1，DDDS 應用程式會先評估具有較低 Preference (偏好設定) 的記錄。有效值：0-65535。

Flags

DDDS 應用程式特定的設定。RFC 3404 中目前定義的值是大寫字母和小寫字母"A"、"P"、"S" 和 "U"，以及空字串 ""。用引號括住 Flags (標記)。

服務

DDDS 應用程式特定的設定。用引號括住 Service (服務)。

如需詳細資訊，請參閱適用的 RFC：

- URI DDDS 應用程式 – https://tools.ietf.org/html/rfc3404#section-4.4
- S-NAPTR DDDS 應用程式 – https://tools.ietf.org/html/rfc3958#section-6.5
- U-NAPTR DDDS 應用程式 – https://tools.ietf.org/html/rfc4848#section-4.5

Regexp

規則運算式，DDDS 應用程式用來將輸入值轉換為輸出值。例如，IP 電話系統可使用規則運算式，將使用者輸入的電話號碼轉換為 SIP URI。用引號括住 Regexp。為 Regexp 指定值，或者為 Replacement (取代) 指定值，但不要同時為這兩者指定值。

規則運算式可以包含下列任何可列印的 ASCII 字元：

- a-z
- 0-9
- - (連字號)
- (空格)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- " (引號)。若要將常值引號包含在字串中，請在它前面加上 \ 字元：\"。
- \ (反斜線)。若要將反斜線包含在字串中，請在它前面加上 \ 字元：\\。

以八進位格式指定所有其他值，例如國際化網域名稱。

如需 Regexp 語法，請參閱 RFC 3402 第 3.2 節替代表達式語法

Replacement

您需要 DDDS 應用程式對其提交 DNS 查詢的下一個網域名稱的完整網域名稱 (FQDN)。DDDS 應用程式會用您為 Replacement (取代) 指定的值 (如果有) 取代輸入值。為 Regexp 指定值，或者為 Replacement (取代) 指定值，但不要同時為這兩者指定值。如果您為 Regexp 指定值，請為 Replacement 指定一個點 (.)。

網域名稱可以包含 a-z、0-9 和 - (連字號)。

如需有關 DDDS 應用程式和 NAPTR 記錄的詳細資訊，請參閱以下 RFC：

- RFC 3401
- RFC 3402
- RFC 3403
- RFC 3404

Amazon Route 53 主控台的範例

```
100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .
100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .
100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .
```

Route 53 API 的範例

```
<ResourceRecord>
   <Value>100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .</Value>
   <Value>100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .</
Value>
   <Value>100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .</Value>
</ResourceRecord>
```

NS 記錄類型

NS 記錄會識別託管區域的名稱伺服器。注意下列事項：

- NS 記錄最常用於控制網域如何進行網際網路流量路由。若要使用託管區域中的記錄來路由某網域的流量，您可以將網域註冊設定更新成使用預設 NS 記錄中的四個名稱伺服器。(這是與託管區域具有相同名稱的 NS 記錄)。
- 您可以為子網域 (acme.example.com) 建立個別的託管區域，並使用該託管區域來路由子網域及其子網域 (subdomain.acme.example.com) 的網際網路流量。您可以設定此組態，即所謂的「將子網域的責任委派給託管區域」；設定步驟是在根網域的託管區域中建立另一筆 NS 記錄 (example.com)。如需更多詳細資訊，請參閱 路由傳送子網域的流量。
- 您也可以使用 NS 記錄來設定白標籤名稱伺服器。如需更多詳細資訊，請參閱 設定白標籤名稱伺服器。

如需 NS 記錄的詳細資訊，請參閱 Amazon Route 53 為公有託管區域建立的 NS 和 SOA 記錄。

Amazon Route 53 主控台的範例

```
ns-1.example.com
```

Route 53 API 的範例

```
<Value>ns-1.example.com</Value>
```

PTR 記錄類型

PTR 記錄會將 IP 位址對應至對應的網域名稱。

Amazon Route 53 主控台的範例

```
hostname.example.com
```

Route 53 API 的範例

```
<Value>hostname.example.com</Value>
```

SOA 記錄類型

起始授權 (SOA) 記錄提供有關網域和對應 Amazon Route 53 託管區域的資訊。如需有關 SOA 記錄中欄位的資訊，請參閱 Amazon Route 53 為公有託管區域建立的 NS 和 SOA 記錄。

Route 53 主控台的範例

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Route 53 API 的範例

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

SPF 記錄類型

SPF 記錄原先用於驗證電子郵件訊息寄件者的身分。不過，不再建議您建立類型是 SPF 記錄的記錄。RFC 7208 在電子郵件中授權網域使用的寄件者政策架構 (SPF) 第 1 版已更新為 "...[I]ts existence and mechanism defined in [RFC4408] have led to some interoperability issues. Accordingly, its use is no longer appropriate for SPF version 1; implementations are not to use it." (在 [RFC4408] 中定義的其存在和機制已導致一些互通性問題。因此，它已不再適合 SPF 版本 1；實作不應再使用它。) 請參閱 RFC 7208 的第 14.1 節 SPF DNS 記錄類型。

建議您建立包含適用值的 TXT 記錄，而不是 SPF 記錄。如需有效值的詳細資訊，請參閱 Wikipedia 文章寄件者政策架構。

Amazon Route 53 主控台的範例

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Route 53 API 的範例

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

SRV 記錄類型

SRV 記錄 `Value` 元素包含四個以空格分隔的值。前三個值是代表優先順序、權重和連接埠的十進位值。第四個值是網域名稱。SRV 記錄用於存取服務，例如電子郵件或通訊服務。如需 SRV 記錄格式的資訊，請參閱您要連線的服務文件。

Amazon Route 53 主控台的範例

```
10 5 80 hostname.example.com
```

Route 53 API 的範例

```
<Value>10 5 80 hostname.example.com</Value>
```

TXT 記錄類型

TXT 記錄包含一或多個用雙引號 (") 括住的字串。使用簡便路由政策時，請將網域 (example.com) 或子網域 (www.example.com) 的所有值包含在相同 TXT 記錄中。

主題

- 輸入 TXT 記錄值
- TXT 記錄值中的特殊字元
- TXT 記錄值中的大寫和小寫
- 範例

輸入 TXT 記錄值

單一字串最多可以包含 255 個字元，包括下列字元：

- a-z
- A-Z
- 0-9
- 空格
- - (連字號)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

如果您需要輸入超過 255 個字元的值，請將該值分割為 255 個字元以下的字串，然後以雙引號 (") 括住每個字串。在主控台中，在同一行上列出所有字串：

```
"String 1" "String 2" "String 3"
```

對於 API，將所有字串包含在同一 Value 元素中：

```
<Value>"String 1" "String 2" "String 3"</Value>
```

TXT 記錄中值的最大長度是 4,000 個字元。

每行輸入一個 TXT 值，即可輸入多個值。

TXT 記錄值中的特殊字元

如果您的 TXT 記錄包含下列任何字元，則必須使用 \#######格式的逸出碼來指定字元：

- 八進位字元 000 到 040 (0 至 32 十進位，0x00 到 0x20 十六進位)
- 八進位字元 177 到 377 (127 至 255 十進位，0x7F 到 0xFF 十六進位)

例如，如果您的 TXT 記錄的值是 "exämple.com"，則指定 "ex\344mple.com"。

如需 ASCII 字元和八進位碼之間的對應，請在網際網路上搜尋「ascii 八進位碼」。一項有用的參考是 ASCII 程式碼 – 延伸 ASCII 表格。

若要將引號 (") 包含在字串中，請在引號前面放置反斜線 (\) 字元：\"。

TXT 記錄值中的大寫和小寫

大小寫會保留，因此 "Ab" 和 "aB" 是不同的值。

範例

Amazon Route 53 主控台的範例

在不同的行放置每個值：

```
"This string includes \"quotation marks\"."
"The last character in this string is an accented e specified in octal format: \351"
"v=spf1 ip4:192.168.0.1/16 -all"
```

Route 53 API 的範例

在不同的 Value 元素中放置每個值：

```
<Value>"This string includes \"quotation marks\"."</Value>
<Value>"The last character in this string is an accented e specified in octal format:
 \351"</Value>
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

使用 Amazon Route 53 主控台來建立記錄

下列程序說明如何使用 Amazon Route 53 主控台來建立記錄。如需如何使用路由 53 API 建立記錄的相關資訊，請參閱 Amazon 路線 53 API 參考ChangeResourceRecordSets中的。

> **Note**
>
> 若要為複雜路由組態建立記錄，您也可以使用流量流程視覺化編輯器，並將組態儲存為流量政策。然後，您可以將流量政策與相同託管區域或多個託管區域中的一或多個網域名稱 (例如 example.com) 或子網域名稱 (如 www.example.com) 關聯。此外，如果新組態執行不如預期，您可以復原更新。如需詳細資訊，請參閱 使用流量流程來路由 DNS 流量。

使用 Route 53 主控台建立靜態路由

1. 如果您不要建立別名記錄，請移至步驟 2。

   如果您要建立別名記錄，以將 DNS 流量路由至 Elastic Load Balancing 負載平衡器之外或其他 Route 53 記錄的 AWS 資源，也請前往步驟 2。

   如果您要建立將流量路由至 Elastic Load Balancing 負載平衡器的別名記錄，而且如果您使用不同的帳戶建立託管區域與負載平衡器，請執行 取得 Elastic Load Balancing 負載平衡器的 DNS 名稱 程序以取得負載平衡器的 DNS 名稱。
2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 如果您的網域已經有託管區域，請跳到步驟 5。如果您的網域尚未有託管區域，請執行適用的程序來建立託管區域：

   - 若要將網際網路流量路由到您的資源 (例如 Amazon S3 儲存貯體或 Amazon EC2 執行個體)，請參閱 建立公有託管區域。
   - 如要路由 VPC 中的流量，請參閱 建立私有託管區域。
5. 在 Hosted Zones (託管區域) 頁面上，選擇您要建立記錄的託管區域名稱。
6. 選擇建立記錄。
7. 選擇並定義適用的路由政策和值。如需詳細資訊，請參閱要建立的記錄類型的相關主題：

   - 所有路由政策的常見值
   - 所有路由政策的別名記錄常見值
   - 簡單記錄的專用值
   - 簡單別名記錄的專用值
   - 容錯移轉記錄的專用值

- 容錯移轉別名記錄的專用值
- 地理位置記錄的專用值
- 地理位置別名記錄的專用值
- 地理鄰近度記錄的特定值
- 地理鄰近別名記錄的特定值
- 延遲記錄的專用值
- 延遲別名記錄的專用值
- 特定於以 IP 為基礎記錄的值
- 特定於以 IP 為基礎的別名記錄的值
- 多值回答記錄的專用值
- 加權記錄的專用值
- 加權別名記錄的專用值

8. 選擇建立記錄。

> **Note**
>
> 新記錄需要一些時間傳播到 Route 53 DNS 伺服器。目前，驗證變更是否已傳播的唯一方法是使用 GetChangeAPI 動作。變更通常會在 60 秒內傳播至所有 Route 53 名稱伺服器。

9. 如果您要建立多個記錄，請重複步驟 7 到 8。

取得 Elastic Load Balancing 負載平衡器的 DNS 名稱

1. 使用用來建立 Classic Load Balancer、Application Load Balancer 或 Network Load Balancer (您要為其建立別名記錄) 的 AWS 帳戶登入 AWS Management Console。
2. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
3. 在導覽窗格中，選擇 Load Balancers (負載平衡器)。
4. 在負載平衡器清單，選取您要為其建立別名記錄的負載平衡器。
5. 在 Description (描述) 標籤上，取得 DNS name (DNS 名稱) 的值。
6. 如果您要為其他 Elastic Load Balancing 負載平衡器建立別名記錄，請重複步驟 4 和 5。
7. 登出 AWS Management Console。
8. 使用您用來建立 Route 53 託管區域的 AWS 帳戶，再次登入 AWS Management Console。

9. 回到使用 Amazon Route 53 主控台來建立記錄程序的步驟 3。

資源記錄集許可

資源記錄集許可使用身分識別與存取管理 (IAM) 政策條件，可讓您為 Route 53 主控台上的動作或使用 ChangeResourceRecordSetsAPI 設定精細許可。

所謂的資源記錄集，就是具有相同名稱和類型 (及類別，但絕大多數用途所用的類別一律都是 IN 或 Internet) 的多個資源記錄，但它們內含的資料不同。例如，如果您選擇地理位置路由，則可能會有多個 A 或 AAAA 記錄指向相同網域的不同端點。所有的 A 或 AAAA 記錄會合併成一個資源記錄集。如需有關 DNS 術語的詳細資訊，請參閱 RFC 7719。

透過 IAM 政策條件、`route53:ChangeResourceRecordSetsNormalizedRecordNames`、`route53:ChangeResourceRecordSetsRecordTypes` 以及 `route53:ChangeResourceRecordSetsActions` 可以將細微的管理權限授予任何其他 AWS 帳戶的其他 AWS 使用者。這種方式可讓您授予以下許可權限給某人：

- 單一的資源記錄集。
- 特定 DNS 記錄類型的所有資源記錄集。
- 名稱包含特定字串的資源記錄集。
- 使用 ChangeResourceRecordSetsAPI 或 Route 53 主控台時，執行任何或所有`CREATE | UPSERT | DELETE` 動作。

您也可以建立將所有 Route 53 政策條件合併在一起的存取許可權限。例如，您可以授予某人修改 marketing-example.com 的 A 記錄資料的權限，但不允許該使用者刪除任何記錄。

如需資源記錄集許可權限的詳細資訊，請參閱使用 IAM 政策條件進行精細定義存取控制，以便管理資源記錄集。

如需了解如何驗證 AWS 使用者，請參閱使用身分驗證，如需了解如何控制 Route 53 資源的存取行為，請參閱存取控制。

您在建立或編輯 Amazon Route 53 記錄指定的值

在使用 Amazon Route 53 主控台建立記錄時，您指定的值取決於您要使用的路由政策，以及您是否要建立將流量路由到 AWS 資源的別名記錄

主題

- 所有路由政策的常見值
- 所有路由政策的別名記錄常見值
- 簡單記錄的專用值
- 簡單別名記錄的專用值
- 容錯移轉記錄的專用值
- 容錯移轉別名記錄的專用值
- 地理位置記錄的專用值
- 地理位置別名記錄的專用值
- 地理鄰近度記錄的特定值
- 地理鄰近別名記錄的特定值
- 延遲記錄的專用值
- 延遲別名記錄的專用值
- 特定於以 IP 為基礎記錄的值
- 特定於以 IP 為基礎的別名記錄的值
- 多值回答記錄的專用值
- 加權記錄的專用值
- 加權別名記錄的專用值

所有路由政策的常見值

這些是您在建立或編輯 Amazon Route 53 記錄時指定的常見值。所有路由政策都會使用這些值。

主題

- 記錄名稱
- 值/將流量路由到
- TTL (秒)

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Name (名稱) 欄位中輸入值 (例如 @ 符號)。

CNAME 記錄

如果您要建立的記錄具有 Record type (記錄類型) 的 CNAME 值，則記錄的名稱不能與託管區域的名稱相同。

特殊字元

如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。

萬用字元

您可以在名稱中使用星號 (*) 字元。DNS 會根據 * 字元出現在名稱中的位置，將其視為萬用字元或 * 字元 (ASCII 42)。如需更多詳細資訊，請參閱 在託管區域和記錄的名稱中使用星號 (*)。

> **Important**
>
> 您不能將 * 萬用字元用於具有 NS 類型的資源記錄集。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

A – IPv4 地址

IPv4 格式的 IP 地址，例如 192.0.2.235。

AAAA - IPv6 地址

IPv6 格式的 IP 地址，例如 2001:0db8:85a3:0:0:8a2e:0370:7334。

CAA - 憑證授權機構授權

三個以空格分隔的值，其控制哪些憑證授權機構可以發出 Record name (記錄名稱) 所指定網域或子網域的憑證或萬用字元憑證。您可以使用 CAA 記錄來指定以下內容：

- 哪些憑證授權機構 (CA) 可以發出 SSL/TLS 憑證 (如果有)
- 當 CA 發出網域或子網域的憑證時要聯絡的電子郵件地址或 URL

CNAME – 正式名稱

完全合格的網域名稱 (例如，www.example.com)，您想要 Route 53 傳回以回應此記錄的 DNS 查詢。行尾點號為選用，Route 53 會假設網域名稱是完整的。這表示 Route 53 會將 www.example.com (無結尾點號) 和 www.example.com. (有結尾點號) 視為相同。

MX - 郵件交換

優先順序與指定郵件伺服器的網域名稱，例如 10 mailserver.example.com。行尾點號視為選用。

NAPTR - 命名授權指標

六個以空格分隔的設定，動態委派探索系統 (Dynamic Delegation Discovery System，DDDS) 應用程式可使用這些設定來將一個值轉換為另一個值，或將一個值取代成另一個值。如需更多詳細資訊，請參閱 NAPTR 記錄類型。

PTR - 指標

您要 Route 53 傳回的網域名稱。

NS - 名稱伺服器

名稱伺服器的網域名稱，例如 ns1.example.com。

> **Note**
>
> 您只能使用簡單路由政策來指定 NS 記錄。

SPF - 寄件者政策架構

SPF 記錄是以引號括住，例如 "v=spf1 ip4:192.168.0.1/16-all"。不建議使用 SPF 記錄。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

SRV - 服務定位器

SRV 記錄。SRV 記錄用於存取服務，例如電子郵件或通訊服務。如需 SRV 記錄格式的資訊，請參閱您要連線的服務文件。行尾點號為選用。

SRV 記錄的格式為：

[priority] [weight] [port] [server host name] ([優先順序] [權重] [連接埠] [伺服器主機名稱])

例如：

1 10 5269 xmpp-server.example.com。

TXT - 文字

文字記錄。請以引號括住文字，例如 "Sample Text Entry"。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

所有路由政策的別名記錄常見值

這些是您在建立或編輯 Amazon Route 53 記錄時指定的常見別名值。所有路由政策都會使用這些值。

主題

- 記錄名稱
- 值/將流量路由到

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Name (名稱) 欄位中輸入值 (例如 @ 符號)。

CNAME 記錄

如果您要建立的記錄具有 Type (類型) 的 CNAME 值，則記錄的名稱不能與託管區域的名稱相同。

CloudFront 分佈和 Amazon S3 儲存貯體的別名

您指定的值部分取決於您路由流量的目標 AWS 資源：

- CloudFront 分佈 – 您的分佈必須包含符合記錄名稱的替代網域名稱。例如，如果記錄名稱為 acme.example.com，您的 CloudFront 分佈必須包含 acme.example.com 做為其中一個替代網域名稱。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的使用備用網域名稱 (CNAME)。
- Amazon S3 儲存貯體 - 記錄的名稱必須符合您 Amazon S3 儲存貯體的名稱。例如，如果您的儲存貯體名稱為 acme.example.com，此記錄名稱也必須包含 acme.example.com。

  此外，您必須設定儲存貯體處理網站託管。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的「為網站託管設定儲存貯體」。

特殊字元

如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。

萬用字元

您可以在名稱中使用星號 (*) 字元。DNS 會根據 * 字元出現在名稱中的位置，將其視為萬用字元或 * 字元 (ASCII 42)。如需更多詳細資訊，請參閱 在託管區域和記錄的名稱中使用星號 (*)。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

Important

如果您用相同的 AWS 帳戶建立託管區域以及路由流量的資源，而且您的資源沒有出現在 Endpoint (端點) 清單中，請查看以下項目：

- 確認您已為 Record type (記錄類型) 選擇了支援的值。您路由流量的資源有特定支援的值。例如，若要將流量路由到 S3 儲存貯體，則必須為 Record type (記錄類型) 選擇 A - IPv4 地址。
- 確認該帳戶具有能夠列出可用資源的 IAM 許可。例如，如果要讓 CloudFront 分佈出現在 Endpoint (端點) 清單中，帳戶必須具有執行以下動作的許可：`cloudfront:ListDistributions`。

  如需 IAM 政策範例，請參閱 使用 Amazon Route 53 主控台所需的許可。

如果您使用不同的 AWS 帳戶建立託管區域與資源，Endpoint (端點) 清單將不會顯示出您的資源。請參閱有關您的資源類型的以下文件，以判斷應該在 Endpoint (端點) 中輸入何值。

API Gateway 自訂區域 API 和最佳化邊緣 API

針對 API Gateway 自訂區域 API 和最佳化邊緣 API，請執行下列任何一項：

- 如果您使用相同的帳戶來建立 Route 53 託管區域與您的 API – 請選擇 Endpoint (端點)，然後從清單中選擇 API。如果您有許多 API，您可以輸入 API 端點的前幾個字元來篩選清單。

> **Note**
>
> 您要建立的記錄名稱必須符合您 API 的自訂網域名稱，例如 api.example.com。

- 若您使用了不同的帳戶來建立您的 Route 53 託管區域和您的 API – 請輸入 API 的 API 端點，例如 api.example.com。

  如果您使用了 AWS 帳戶來建立目前的託管區域，並使用不同的帳戶來建立 API，則 API 不會出現在 Endpoints (端點) 清單中的 API Gateway API 下方。

  如果您使用一個帳戶來建立目前的託管區域，並使用一個或多個不同的帳戶來建立您所有的 API，則 Endpoint (端點) 清單在 API Gateway API 下顯示 No targets available (沒有可用的目標)。如需更多詳細資訊，請參閱 使用網域名稱將流量路由到 Amazon API Gateway API。

CloudFront 分佈

若是 CloudFront 分佈，請執行下列其中一項操作：

- 如果您使用相同的帳戶來建立 Route 53 託管區域與 CloudFront 分佈 – 請選擇 Endpoint (端點)，然後從清單中選擇分佈。如果您有許多分佈，您可以輸入分佈之網域名稱的前幾個字元來篩選清單。

  如果您的分佈未出現在清單中，請注意下列情況：

  - 此記錄名稱必須符合分佈的替代網域名稱。
  - 如果您只將一個替代網域名稱新增至分佈，則可能需要 15 分鐘的時間讓變更傳播至所有 CloudFront 節點。在變更傳播完成之前，Route 53 不會知道新的替代網域名稱。
- 如果您使用不同的帳戶來建立 Route 53 託管區域與分佈 – 請輸入分佈的 CloudFront 網域名稱，例如 d111111abcdef8.cloudfront.net。

  如果您使用一個 AWS 帳戶來建立目前的託管區域，並使用不同的帳戶來建立分佈，則分佈不會出現在 Endpoints (端點) 清單中。

  如果您使用一個帳戶來建如果您使用一個帳戶來建立目前的託管區域，並使用一個或多個不同的帳戶來建立您所有的分佈，則 Endpoint (端點) 清單在 CloudFront distributions (CloudFront 分佈) 下顯示 No targets available (沒有可用的目標)。

> **Important**
>
> 請勿將查詢路由至尚未傳播至所有節點的 CloudFront 分佈，否則使用者將無法存取適用的內容。

您的 CloudFront 分佈必須包含符合記錄名稱的備用網域名稱。例如，如果記錄名稱為 acme.example.com，您的 CloudFront 分佈必須包含 acme.example.com 做為其中一個替代網域名稱。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的使用備用網域名稱 (CNAME)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Record type (記錄類型) 值為 A - IPv4 地址，另一個記錄則具有值 AAAA - IPv6 地址。如需更多詳細資訊，請參閱 使用您的網域名稱將流量路由到 Amazon CloudFront 分發。

具有區域化子網域的 Elastic Beanstalk 環境

如果 Elastic Beanstalk 環境的網域名稱包含您部署環境的區域，您可以建立別名記錄將流量路由至該環境。例如，網域名稱 `my-environment.us-west-2.elasticbeanstalk.com` 是區域化網域名稱。

> **Important**
>
> 若環境是在 2016 年初以前所建立，網域名稱不會包含區域。若要將流量路由至這些環境，您必須建立 CNAME 記錄而非別名記錄。請注意，您無法為根網域名稱建立 CNAME 記錄。例如，如果您的網域名稱是 example.com，您可以建立將 acme.example.com 流量路由至您 Elastic Beanstalk 環境的記錄，但無法建立將 example.com 流量路由至您 Elastic Beanstalk 環境的記錄。

若是具有區域化子網域的 Elastic Beanstalk 環境，請執行下列其中一項操作：

- 如果您使用相同的帳戶來建立 Route 53 託管區域與 Elastic Beanstalk 環境 – 請選擇 Endpoint (端點)，然後從清單中選擇環境。如果您有許多環境，您可以輸入環境之正式名稱記錄 (CNAME) 屬性的前幾個字元來篩選清單。
- 如果您使用不同的帳戶來建立 Route 53 託管區域與 Elastic Beanstalk 環境 - 輸入 Elastic Beanstalk 環境的 CNAME 屬性。

如需更多詳細資訊，請參閱 將流量路由到 AWS Elastic Beanstalk 環境。

ELB 負載平衡器

若是 ELB 負載平衡器，請執行下列其中一個動作：

- 如果您使用相同的帳戶來建立 Route 53 託管區域與負載平衡器 – 請選擇 Endpoint (端點)，然後從清單中選擇負載平衡器。如果您有許多負載平衡器，您可以輸入 DNS 名稱的前幾個字元來篩選清單。
- 如果您使用不同的帳戶來建立 Route 53 託管區域與負載平衡器 – 請輸入您在 取得 Elastic Load Balancing 負載平衡器的 DNS 名稱 程序中所取得的值。

  如果您使用一個 AWS 帳戶來建立目前的託管區域，並使用不同的帳戶來建立負載平衡器，則負載平衡器不會出現在 Endpoints (端點) 清單中。

  如果您使用一個帳戶來建立目前的託管區域，並使用一個或多個不同的帳戶來建立所有負載平衡器，則 Endpoints (端點)清單在 Elastic Load Balancer 下顯示 No targets available (沒有可用的目標)。

針對來自不同帳戶的應用程式和 Classic Load Balancer，主控台會在其開頭加上 dualstack.。當用戶端 (例如 web 瀏覽器) 要求您網域名稱 (example.com) 或子網域名稱 (www.example.com) 的 IP 地址時，用戶端可以要求 IPv4 地址 (A 記錄)、IPv6 地址 (AAAA 記錄) 或 IPv4 與 IPv6 地址 (以不同的要求)。dualstack. 指定可讓 Route 53 根據用戶端要求的 IP 地址格式，以您負載平衡器的適當 IP 地址來回應。

如需更多詳細資訊，請參閱 將流量路由到 ELB 負載平衡器。

AWS Global Accelerator 加速器

對於 AWS Global Accelerator 加速器，請輸入加速器的 DNS 名稱 您可以輸入您使用現有 AWS 帳戶或其他 AWS 帳戶所建立的加速器 DNS 名稱

Amazon S3 儲存貯體

若是設定為網站端點的 Amazon S3 儲存貯體，請執行下列其中一項操作：

- 如果您使用相同的帳戶來建立 Route 53 託管區域與 Amazon S3 儲存貯體 – 請選擇 Endpoint (端點) ，然後從清單中選擇儲存貯體。如果您有許多儲存貯體，您可以輸入 DNS 名稱的前幾個字元來篩選清單。

  Endpoint (端點) 的值會變更為您儲存貯體的 Amazon S3 網站端點。
- 如果您使用不同的帳戶來建立 Route 53 託管區域與 Amazon S3 儲存貯體 – 請輸入您建立 S3 儲存貯體的區域名稱。使用出現在 Amazon Web Services 一般參考 中 Amazon S3 網站端點資料表內網站端點欄中的值。

如果您使用目前帳戶以外的 AWS 帳戶來建立 Amazon S3 儲存貯體，該儲存貯體不會出現在 Endpoints (端點) 清單中。

您必須設定儲存貯體處理網站託管。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的「為網站託管設定儲存貯體」。

記錄名稱必須符合您的 Amazon S3 儲存貯體名稱。例如，如果您的 Amazon S3 儲存貯體名稱為 acme.example.com，此記錄名稱也必須包含 acme.example.com。

在加權別名、延遲別名、容錯移轉別名或地理位置別名記錄群組中，您只能建立一個記錄將查詢路由至 Amazon S3 儲存貯體，因為記錄名稱必須符合儲存貯體名稱，而且儲存貯體名稱必須為全域唯一。

Amazon VPC 介面端點

針對 Amazon VPC 介面端點，請執行下列其中一項：

- 如果您使用相同的帳戶來建立 Route 53 託管區域與介面端點 – 請選擇 Endpoint (端點)，然後從清單中選擇環境。如果您有許多介面端點，您可以輸入 DNS 主機名稱的前幾個字元來篩選清單。
- 如果您使用不同的帳戶建立 Route 53 託管區域和介面端點 – 請輸入介面端點的 DNS 主機名稱，例如 vpce-123456789abcdef01-example-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com。

  如果您使用了 AWS 帳戶來建立目前的託管區域，並使用不同的帳戶來建立介面端點，則介面端點不會出現在 Endpoint (端點) 清單的 VPC endpoints (VPC 端點) 下方。

  如果您使用一個帳戶來建立目前的託管區域，並使用一個或多個不同的帳戶來建立所有的介面端點，則 Endpoint (端點) 清單會在 VPC endpoints (VPC 端點) 下顯示 No targets available (沒有可用的目標)。

  如需更多詳細資訊，請參閱 使用網域名稱將流量路由到 Amazon Virtual Private Cloud 介面端點。

此託管區域中的記錄

針對此託管區域中的記錄，選擇 Endpoint (端點)，然後選擇適用的記錄。如果您有許多記錄，您可以輸入名稱的前幾個字元來篩選清單。

如果託管區域只包含預設 NS 與 SOA 記錄，Endpoints (端點) 清單會顯示 No Targets Available (沒有可用的目標)。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法選擇 Record type (記錄類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

簡單記錄的專用值

在建立簡單記錄時，指定下列值。

主題

- 路由政策
- 記錄名稱
- 值/將流量路由到
- 記錄類型
- TTL (秒)

路由政策

選擇 Simple routing (簡便路由)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Name (名稱) 欄位中輸入值 (例如 @ 符號)。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權

- CNAME – 正式名稱
- MX - 郵件交換
- NAPTR - 名稱授權指標
- NS - 名稱伺服器

  名稱伺服器的網域名稱，例如 ns1.example.com。

  > **Note**
  >
  > 您只能使用簡單路由政策來指定 NS 記錄。

- PTR - 指標
- SPF - 寄件者政策架構
- SRV - 服務定位器
- TXT - 文字

如需上述值的詳細資訊，請參"值/將流量路由到"的常見值。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

根據您想要 Route 53 回應 DNS 查詢的方式，選取 Record type (記錄類型) 的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

簡單別名記錄的專用值

在建立別名記錄時，指定下列值。如需更多詳細資訊，請參閱 選擇別名或非別名記錄。

> **Note**
>
> 如果您在 AWS GovCloud (US) Region 中使用 Route 53，此功能有一些限制。如需詳細資訊，請參閱《AWS GovCloud (US) 使用者指南》中的 Amazon Route 53 頁面。

主題

- 路由政策
- 記錄名稱
- 值/將流量路由到
- 記錄類型
- 評估目標運作狀態

路由政策

選擇 Simple routing (簡便路由)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Name (名稱) 欄位中輸入值 (例如 @ 符號)。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需哪些 AWS 資源可供您設定目標的資訊，請參閱"值/將流量路由到"的別名記錄的常見值。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

請根據您路由流量的目標 AWS 資源來選取適用的值：

API Gateway 自訂區域 API 和最佳化邊緣 API

選取 A - IPv4 address (A - IPv4 地址)。

Amazon VPC 介面端點

選取 A - IPv4 address (A - IPv4 地址)。

CloudFront 分佈

選取 A - IPv4 address (A - IPv4 地址)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Type (類型) 值為 A - IPv4 地址，另一個記錄的值則為 AAAA - IPv6 地址。

具有區域化子網域的 Elastic Beanstalk 環境

選取 A - IPv4 address (A - IPv4 地址)

ELB 負載平衡器

選取 A - IPv4 address (A - IPv4 地址) 或 AAAA - IPv6 address (AAAA - IPv6 地址)

Amazon S3 儲存貯體

選取 A - IPv4 address (A - IPv4 地址)

此託管區域中的其他記錄

選取您要建立別名的記錄類型。支援 NS 與 SOA 以外的所有類型。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法將流量路由到 Type (類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

評估目標運作狀態

當 Routing policy (路由政策) 的值是 Simple (簡便) 時，您可以選擇 No (否) 或預設的 Yes (是)，因為 Evaluate target health (評估目標運作狀態) 對 Simple (簡便) 路由沒有效果。如果您只有一個具有指定名稱和類型的記錄，則無論資源運作狀態是否健康，Route 53 都會使用該記錄中的值來回應 DNS 查詢。

容錯移轉記錄的專用值

在建立容錯移轉記錄時，指定下列值。

> **Note**
>
> 如需在私有託管區域中建立容錯移轉記錄的資訊，請參閱 在私有託管區域中設定容錯移轉。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- TTL (秒)
- 值/將流量路由到
- 容錯移轉記錄類型
- 運作狀態檢查
- 記錄 ID

路由政策

選擇 Failover (容錯移轉)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為容錯移轉記錄群組中的兩個記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

為主要與次要容錯移轉記錄選取相同的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權
- CNAME – 正式名稱
- MX - 郵件交換
- NAPTR - 名稱授權指標
- PTR - 指標
- SPF - 寄件者政策架構
- SRV - 服務定位器

- TXT - 文字

如需上述值的詳細資訊，請參"值/將流量路由到"的常見值。

容錯移轉記錄類型

選擇適用於此記錄的值。若要讓容錯移轉正常運作，您必須建立一個主要容錯移轉記錄與一個次要容錯移轉記錄。

您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非容錯移轉記錄作為容錯移轉記錄。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate Target Health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態，如果建立 Domain Name (網域名稱) 的值與記錄名稱符合的運作狀態檢查，然後將運作狀態檢查與這些記錄關聯，運作狀態檢查結果將會無法預測。

記錄 ID

輸入可唯一識別主要與次要記錄的值。

容錯移轉別名記錄的專用值

在建立容錯移轉別名記錄時，指定下列值。

如需詳細資訊，請參閱以下主題：

- 如需在私有託管區域中建立容錯移轉記錄的資訊，請參閱 在私有託管區域中設定容錯移轉。
- 如需別名記錄的資訊，請參閱 選擇別名或非別名記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- 值/將流量路由到
- 容錯移轉記錄類型
- 運作狀態檢查
- 評估目標運作狀態
- 記錄 ID

路由政策

選擇 Failover (容錯移轉)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為容錯移轉記錄群組中的兩個記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

根據您路由流量的目標 AWS 資源來選取適用的值。為主要與次要容錯移轉記錄選取相同的值：

API Gateway 自訂區域 API 和最佳化邊緣 API

選取 A - IPv4 address (A - IPv4 地址)。

Amazon VPC 介面端點

選取 A - IPv4 address (A - IPv4 地址)。

CloudFront 分佈

選取 A - IPv4 address (A - IPv4 地址)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Type (類型) 值為 A - IPv4 地址，另一個記錄的值則為 AAAA - IPv6 地址。

具有區域化子網域的 Elastic Beanstalk 環境

選取 A - IPv4 address (A - IPv4 地址)

ELB 負載平衡器

選取 A - IPv4 address (A - IPv4 地址) 或 AAAA - IPv6 address (AAAA - IPv6 地址)

Amazon S3 儲存貯體

選取 A - IPv4 address (A - IPv4 地址)

此託管區域中的其他記錄

選取您要建立別名的記錄類型。支援 NS 與 SOA 以外的所有類型。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法將流量路由到 Type (類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需哪些 AWS 資源可供您設定目標的資訊，請參閱"值/將流量路由到"的別名記錄的常見值。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

> **Note**
>
> 當您建立主要與次要容錯移轉記錄時，您可以選擇性地建立一個容錯移轉與一個容錯移轉別名記錄，這兩個記錄具有相同的 Name (名稱) 與 Record type (記錄類型) 值。如果您混合容錯移轉記錄與容錯移轉別名記錄，任一記錄都可以是主要記錄。

容錯移轉記錄類型

選擇適用於此記錄的值。若要讓容錯移轉正常運作，您必須建立一個主要容錯移轉記錄與一個次要容錯移轉記錄。

您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非容錯移轉記錄作為容錯移轉記錄。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate Target Health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參

考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態，如果建立 Domain Name (網域名稱) 的值與記錄名稱符合的運作狀態檢查，然後將運作狀態檢查與這些記錄關聯，運作狀態檢查結果將會無法預測。

評估目標運作狀態

如果您想讓 Route 53 藉由檢查 Endpoint (端點) 所指定資源的運作狀態來判斷是否使用此記錄回應 DNS 查詢，則選擇 Yes (是)

注意下列事項：

API Gateway 自訂區域 API 和最佳化邊緣 API

當端點是 API Gateway 自訂區域 API 或邊緣最佳化 API 時，將 Evaluate target health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

CloudFront 分佈

當別名目標是 CloudFront 分佈時，您無法將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)。

具有區域化子網域的 Elastic Beanstalk 環境

如果您在 Endpoint (端點) 中指定 Elastic Beanstalk 環境，而此環境包含 ELB 負載平衡器，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。(如果環境包含多個 Amazon EC2 執行個體，就會自動包含 ELB 負載平衡器)。如果您將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)，而且沒有運作狀態良好的 Amazon EC2 執行個體，或負載平衡器本身即運作狀態不良，則 Route 53 會將查詢路由至其他運作狀態良好的可用資源 (如有)。

如果環境包含單一 Amazon EC2 執行個體，則沒有特殊需求。

ELB 負載平衡器

運作狀態檢查行為取決於負載平衡器的類型：

- Classic Load Balancers – 如果您在 Endpoint (端點) 中指定 ELB Classic Load Balancer，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。如果您將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，而且沒有運作狀態良好的 EC2 執行個體或負載平衡器本身運作狀態不良，Route 53 會將查詢路由至其他資源。
- Application Load Balancer 與 Network Load Balancer – 如果您指定 ELB Application Load Balancer 或 Network Load Balancer，並將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，Route 53 會根據與負載平衡器相關聯之目標群組的運作狀態，將查詢路由至負載平衡器：
  - 包含目標的目標群組必須至少包含一個運作狀態良好的目標，Application Load Balancer 或 Network Load Balancer 才會視為運作狀態良好。若有任何目標群組只包含運作狀態不良的目標，負載平衡器會被視為運作狀態不良，而且 Route 53 會將查詢路由至其他資源。
  - 不含任何已註冊目標的目標群組會被視為運作狀態不良。

> **Note**
>
> 當您建立負載平衡器時，您可以設定 Elastic Load Balancing 運作狀態檢查的設定，它們不是 Route 53 運作狀態檢查，但會執行類似的功能。不要建立向 ELB 負載平衡器註冊之 EC2 執行個體的 Route 53 運作狀態檢查。

S3 儲存貯體

當端點為 S3 儲存貯體時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

Amazon VPC 介面端點

當端點是 Amazon VPC 介面端點時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

相同託管區域中的其他記錄

如果您在 Endpoint (端點) 中指定的 AWS 資源是一筆記錄或一組記錄 (例如一組加權記錄)，但不是其他別名記錄，建議您建立運作狀態檢查與端點中所有記錄的關聯性。如需更多詳細資訊，請參閱當您忽略運作狀態檢查時會發生什麼情況？。

記錄 ID

輸入可唯一識別主要與次要記錄的值。

地理位置記錄的專用值

在建立地理位置記錄時，指定下列值。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- TTL (秒)
- 值/將流量路由到
- 位置
- 美國各州
- 運作狀態檢查
- 記錄 ID

路由政策

選擇 Geolocation (地理位置)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Name (名稱) 欄位中輸入值 (例如 @ 符號)。

為地理位置記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

為地理位置記錄群組中的所有記錄選取相同的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權
- CNAME – 正式名稱
- MX - 郵件交換
- NAPTR - 名稱授權指標
- PTR - 指標
- SPF - 寄件者政策架構
- SRV - 服務定位器
- TXT - 文字

如需上述值的詳細資訊，請參"值/將流量路由到"的常見值。

位置

當您設定 Route 53 根據查詢來源位置來回應 DNS 查詢時，請選取要讓 Route 53 使用此記錄中設定回應的洲別或國家。如果您想要 Route 53 回應美國境內個別州的 DNS 查詢，請從 Location (位置) 清單中選取 United States (美國)，然後從 Sublocation (子位置) 群組下選擇相應的州。

對於私有託管區域，請選擇最接近您的資源所在的 AWS 區域的大洲、國家/地區或細分區域。例如，如果您的資源位於 us-east-1，則可以指定北美、美國或維吉尼亞。

> **Important**
>
> 我們建議您建立一個 Location (位置) 值為 Default (預設) 的地理位置記錄。這會涵蓋您尚未建立記錄的地理位置，以及 Route 53 無法識別位置的 IP 地址。配置預設位置時，將國家代碼設為星號 "*"。

您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非地理位置記錄作為地理位置記錄。

如需更多詳細資訊，請參閱 地理位置路由。

以下是 Amazon Route 53 與每個洲別關聯的國家/地區。國家/地區代碼來自 ISO 3166。如需詳細資訊，請參閱 Wikipedia 文章 ISO 3166-1 alpha-2：

非洲 (AF)

AO、BF、BI、BJ、BW、CD、CF、CG、CI、CM、CV、DJ、DZ、EG、ER、ET、GA、GH、GM、GN

南極洲 (AN)

AQ、GS、TF

亞洲 (AS)

AE、AF、AM、AZ、BD、BH、BN、BT、CC、CN、GE、HK、ID、IL、IN、IO、IQ、IR、JO、JP、KG

歐洲 (EU)

AD、AL、AT、AX、BA、BE、BG、BY、CH、CY、CZ、DE、DK、EE、ES、FI、FO、FR、GB、GG、

北美洲 (NA)

AG、AI、AW、BB、BL、BM、BQ、BS、BZ、CA、CR、CU、CW、DM、DO、GD、GL、GP、GT、H

大洋洲 (OC)

AS、AU、CK、FJ、FM、GU、KI、MH、MP、NC、NF、NR、NU、NZ、PF、PG、PN、PW、SB、TK

南美洲 (SA)

AR、BO、BR、CL、CO、EC、FK、GF、GY、PE、PY、SR、UY、VE

> **Note**
>
> Route 53 不支援建立下列國家的地理位置記錄：布威島 (BV)、聖誕群島 (CX)、西撒哈拉 (EH)，以及赫德島及麥克唐納群島 (HM)。沒有這些國家的 IP 地址相關資料可用。

美國各州

當您設定 Route 53 根據查詢來自的美國州別來回應 DNS 查詢時，請從 U.S. states (美國各州) 清單中選取該州。美國領土 (例如波多黎各) 會列為 Location (位置) 清單中的國家。

> **Important**
>
> 某些 IP 地址與美國相關聯，但未與個別州相關聯。如果您建立美國所有州的記錄，建議您也建立美國記錄，以路由這些未關聯之 IP 地址的查詢。如果您未建立美國記錄，Route 53 會使用預設地理位置記錄 (如果已建立) 中的設定或「沒有回應」，回應來自未與美國關聯之 IP 地址的 DNS 查詢。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate Target Health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態，如果建立 Domain Name (網域名稱) 的值與記錄名稱符合的運作狀態檢查，然後將運作狀態檢查與這些記錄關聯，運作狀態檢查結果將會無法預測。

針對地理位置記錄，如果端點運作狀態不良，Route 53 會尋找更大關聯地理區域的記錄。例如，假設您有美國某州、美國、北美洲與所有位置 (Location (位置) 為 Default (預設)) 的記錄。如果州記錄的端點運作狀態不良，Route 53 會依序檢查美國、北美洲與所有位置的記錄，直到找到具有運作狀態良好端點的記錄。如果所有適用記錄的運行狀況都不佳 (包括所有位置記錄)，則 Route 53 會使用最小地理區域的記錄值回應 DNS 查詢。

記錄 ID

輸入地理位置記錄群組中可唯一識別這個記錄的值。

地理位置別名記錄的專用值

在建立地理位置別名記錄時，指定下列值。

如需更多詳細資訊，請參閱 選擇別名或非別名記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- 值/將流量路由到
- 位置
- 美國各州
- 運作狀態檢查
- 評估目標運作狀態
- 記錄 ID

路由政策

選擇 Geolocation (地理位置)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為地理位置記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

根據您路由流量的目標 AWS 資源來選取適用的值。為地理位置記錄群組中的所有記錄選取相同的值：

API Gateway 自訂區域 API 和最佳化邊緣 API

選取 A - IPv4 address (A - IPv4 地址)。

Amazon VPC 介面端點

選取 A - IPv4 address (A - IPv4 地址)。

CloudFront 分佈

選取 A - IPv4 address (A - IPv4 地址)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Record type (記錄類型) 值為 A - IPv4 地址，另一個記錄則具有值 AAAA - IPv6 地址。

具有區域化子網域的 Elastic Beanstalk 環境

選取 A - IPv4 address (A - IPv4 地址)

ELB 負載平衡器

選取 A - IPv4 address (A - IPv4 地址) 或 AAAA - IPv6 address (AAAA - IPv6 地址)

Amazon S3 儲存貯體

選取 A - IPv4 address (A - IPv4 地址)

此託管區域中的其他記錄

選取您要建立別名的記錄類型。支援 NS 與 SOA 以外的所有類型。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法將流量路由到 Type (類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需哪些 AWS 資源可供您設定目標的資訊，請參閱 值/將流量路由到。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

位置

當您設定 Route 53 根據查詢來源位置來回應 DNS 查詢時，請選取要讓 Route 53 使用此記錄中設定回應的洲別或國家。如果您想要 Route 53 回應美國境內個別州的 DNS 查詢，請從 Location (位置) 清單中選取 United States (美國)，然後從 U.S. states (美國各州) 清單中選擇相應的州。

對於私有託管區域，請選擇最接近您的資源所在的 AWS 區域的大洲、國家/地區或細分區域。例如，如果您的資源位於 us-east-1，則可以指定北美、美國或維吉尼亞。

> **Important**
>
> 我們建議您建立一個 Location (位置) 值為 Default (預設) 的地理位置記錄。這會涵蓋您尚未建立記錄的地理位置，以及 Route 53 無法識別位置的 IP 地址。配置預設位置時，將國家代碼設為星號 "*"。

您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非地理位置記錄作為地理位置記錄。

如需更多詳細資訊，請參閱 地理位置路由。

以下是 Amazon Route 53 與每個洲別關聯的國家/地區。國家/地區代碼來自 ISO 3166。如需詳細資訊，請參閱 Wikipedia 文章 ISO 3166-1 alpha-2：

非洲 (AF)

AO、BF、BI、BJ、BW、CD、CF、CG、CI、CM、CV、DJ、DZ、EG、ER、ET、GA、GH、GM、GN

南極洲 (AN)

AQ、GS、TF

亞洲 (AS)

AE、AF、AM、AZ、BD、BH、BN、BT、CC、CN、GE、HK、ID、IL、IN、IO、IQ、IR、JO、JP、KG

歐洲 (EU)

AD、AL、AT、AX、BA、BE、BG、BY、CH、CY、CZ、DE、DK、EE、ES、FI、FO、FR、GB、GG、

北美洲 (NA)

AG、AI、AW、BB、BL、BM、BQ、BS、BZ、CA、CR、CU、CW、DM、DO、GD、GL、GP、GT、H

大洋洲 (OC)

AS、AU、CK、FJ、FM、GU、KI、MH、MP、NC、NF、NR、NU、NZ、PF、PG、PN、PW、SB、TK

南美洲 (SA)

AR、BO、BR、CL、CO、EC、FK、GF、GY、PE、PY、SR、UY、VE

> **Note**
>
> Route 53 不支援建立下列國家的地理位置記錄：布威島 (BV)、聖誕群島 (CX)、西撒哈拉 (EH)，以及赫德島及麥克唐納群島 (HM)。沒有這些國家的 IP 地址相關資料可用。

美國各州

當您設定 Route 53 根據查詢來自的美國州別來回應 DNS 查詢時，請從 U.S. states (美國各州) 清單中選取該州。美國領土 (例如波多黎各) 會列為 Location (位置) 清單中的國家。

> **Important**
>
> 某些 IP 地址與美國相關聯，但未與個別州相關聯。如果您建立美國所有州的記錄，建議您也建立美國記錄，以路由這些未關聯之 IP 地址的查詢。如果您未建立美國記錄，Route 53 會使用預設地理位置記錄 (如果已建立) 中的設定或「沒有回應」，回應來自未與美國關聯之 IP 地址的 DNS 查詢。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate target health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

針對地理位置記錄，如果端點運作狀態不良，Route 53 會尋找更大關聯地理區域的記錄。例如，假設您有美國某州、美國、北美洲與所有位置 (Location (位置) 為 Default (預設)) 的記錄。如果州記錄的端點運作狀態不良，Route 53 會依序檢查美國、北美洲與所有位置的記錄，直到找到具有運作狀態良好端點的記錄。如果所有適用記錄的運行狀況都不佳 (包括所有位置記錄)，則 Route 53 會使用最小地理區域的記錄值回應 DNS 查詢。

評估目標運作狀態

如果您想讓 Route 53 藉由檢查 Endpoint (端點) 所指定資源的運作狀態來判斷是否使用此記錄回應 DNS 查詢，則選擇 Yes (是)

注意下列事項：

API Gateway 自訂區域 API 和最佳化邊緣 API

當端點是 API Gateway 自訂區域 API 或邊緣最佳化 API 時，將 Evaluate target health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

CloudFront 分佈

當別名目標是 CloudFront 分佈時，您無法將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)。

具有區域化子網域的 Elastic Beanstalk 環境

如果您在 Endpoint (端點) 中指定 Elastic Beanstalk 環境，而此環境包含 ELB 負載平衡器，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。(如果環境包含多個 Amazon EC2 執行個體，就會自動包含 ELB 負載平衡器)。如果您將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)，而且沒有運作狀態良好的 Amazon EC2 執行個體，或負載平衡器本身即運作狀態不良，則 Route 53 會將查詢路由至其他運作狀態良好的可用資源 (如有)。

如果環境包含單一 Amazon EC2 執行個體，則沒有特殊需求。

ELB 負載平衡器

運作狀態檢查行為取決於負載平衡器的類型：

- Classic Load Balancers – 如果您在 Endpoint (端點) 中指定 ELB Classic Load Balancer，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。如果您將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，而且沒有運作狀態良好的 EC2 執行個體或負載平衡器本身運作狀態不良，Route 53 會將查詢路由至其他資源。
- Application Load Balancer 與 Network Load Balancer – 如果您指定 ELB Application Load Balancer 或 Network Load Balancer，並將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，Route 53 會根據與負載平衡器相關聯之目標群組的運作狀態，將查詢路由至負載平衡器：
  - 每個包含目標的目標群組必須至少包含一個運作狀態良好的目標，Application Load Balancer 或 Network Load Balancer 才會視為運作狀態良好。若有任何目標群組只包含運作狀態不良的目標，負載平衡器會被視為運作狀態不良，而且 Route 53 會將查詢路由至其他資源。
  - 不含任何已註冊目標的目標群組會被視為運作狀態不良。

> **Note**
>
> 當您建立負載平衡器時，您可以設定 Elastic Load Balancing 運作狀態檢查的設定，它們不是 Route 53 運作狀態檢查，但會執行類似的功能。不要建立向 ELB 負載平衡器註冊之 EC2 執行個體的 Route 53 運作狀態檢查。

S3 儲存貯體

當端點為 S3 儲存貯體時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

Amazon VPC 介面端點

當端點是 Amazon VPC 介面端點時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

相同託管區域中的其他記錄

如果您在 Endpoint (端點) 中指定的 AWS 資源是一筆記錄或一組記錄 (例如一組加權記錄)，但不是其他別名記錄，建議您建立運作狀態檢查與端點中所有記錄的關聯性。如需更多詳細資訊，請參閱當您忽略運作狀態檢查時會發生什麼情況？。

記錄 ID

輸入地理位置記錄群組中可唯一識別這個記錄的值。

地理鄰近度記錄的特定值

建立地理鄰近度記錄時，請指定下列值。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- TTL (秒)
- 值/將流量路由到
- 端點位置
- 偏差
- 運作狀態檢查
- 記錄 ID

路由政策

選擇地理鄰近度。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Name (名稱) 欄位中輸入值 (例如 @ 符號)。

為地理鄰近記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需詳細資訊，請參閱 支援的 DNS 記錄類型。

為地理鄰近記錄群組中的所有記錄選取相同的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權
- CNAME – 正式名稱
- MX - 郵件交換
- NAPTR - 名稱授權指標
- PTR - 指標
- SPF - 寄件者政策架構
- SRV - 服務定位器
- TXT - 文字

如需上述值的詳細資訊，請參"值/將流量路由到"的常見值。

端點位置

您可以使用下列其中一項指定資源端點位置：

自訂座標

指定地質圖面區域的經度和緯度。

AWS 區域

從「位置」清單中選擇可用的「區域」。

如需區域的詳細資訊，請參閱AWS全域基礎結構。

AWS本地區域群組

從「位置」清單中選擇可用的「本機區域群組」。

如需有關 Local Zones 的詳細資訊，請參閱 L ocal Zones 使用指南中的可用 L AWS ocal Zones。本地區域群組通常是沒有結束字元的本地區域。例如，如果「本地區域`us-east-1-bue-1a`」是「本地區域群組」`us-east-1-bue-1`。

您也可以使用 describe-availability-zonesCLI 命令來識別特定本機 Local Zones 群組：

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

此命令會傳回:`"GroupName": "us-west-2-den-1"`，指定本機區域`us-west-2-den-1a`屬於本機區域群組`us-west-2-den-1`。

您無法建立與地理鄰近記錄具有相同值的「記錄名稱」和「記錄類型」的非地理鄰近記錄。

您也無法建立兩個 geo鄰近度資源記錄集來為相同記錄名稱/記錄類型指定相同位置。

偏差

偏見可以擴展或縮小 Route 53 將流量路由到資源的地理區域。積極的偏見擴大了該區域，負偏差使其縮小。如需詳細資訊，請參閱 Amazon Route 53 如何使用偏差來路由流量。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、地理鄰近別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以針對「評估目標 Health 全狀況」選取「是」。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態，如果建立 Domain Name (網域名稱) 的值與記錄名稱符合的運作狀態檢查，然後將運作狀態檢查與這些記錄關聯，運作狀態檢查結果將會無法預測。

對於地理鄰近度記錄，如果端點狀態不良，Route 53 會尋找仍然健康的最接近端點。

記錄 ID

輸入唯一識別地理鄰近記錄群組中此記錄的值。

地理鄰近別名記錄的特定值

建立地理鄰近別名記錄時，請指定下列值。

如需詳細資訊，請參閱 選擇別名或非別名記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- 值/將流量路由到
- 端點位置
- 偏差
- 運作狀態檢查
- 評估目標運作狀態
- 記錄 ID

路由政策

選擇地理鄰近度。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為地理鄰近記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需詳細資訊，請參閱 支援的 DNS 記錄類型。

根據您路由流量的目標 AWS 資源來選取適用的值。為地理鄰近記錄群組中的所有記錄選取相同的值：

API Gateway 自訂區域 API 和最佳化邊緣 API

選取 A - IPv4 address (A - IPv4 地址)。

Amazon VPC 介面端點

選取 A - IPv4 address (A - IPv4 地址)。

CloudFront 分佈

選取 A - IPv4 address (A - IPv4 地址)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Record type (記錄類型) 值為 A - IPv4 地址，另一個記錄則具有值 AAAA - IPv6 地址。

具有區域化子網域的 Elastic Beanstalk 環境

選取 A - IPv4 address (A - IPv4 地址)

ELB 負載平衡器

選取 A - IPv4 address (A - IPv4 地址) 或 AAAA - IPv6 address (AAAA - IPv6 地址)

Amazon S3 儲存貯體

選取 A - IPv4 address (A - IPv4 地址)

此託管區域中的其他記錄

選取您要建立別名的記錄類型。支援 NS 與 SOA 以外的所有類型。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法將流量路由到 Type (類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需哪些 AWS 資源可供您設定目標的資訊，請參閱 值/將流量路由到。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

端點位置

您可以使用下列其中一項指定資源端點位置：

自訂座標

指定地質圖面區域的經度和緯度。

AWS 區域

從「位置」清單中選擇可用的「區域」。

如需區域的詳細資訊，請參閱AWS全域基礎結構。

AWS本地區域群組

從「位置」清單中選擇可用的「本地區域」。

如需有關 Local Zones 的詳細資訊，請參閱 L ocal Zones 使用指南中的可用 L AWS ocal Zones。本地區域群組通常是沒有結束字元的本地區域。例如，如果「本地區域`us-east-1-bue-1a`」是「本地區域群組」`us-east-1-bue-1`。

您也可以使用 describe-availability-zonesCLI 命令來識別特定本機 Local Zones 群組：

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

此命令會傳回:`"GroupName": "us-west-2-den-1"`，指定本機區域`us-west-2-den-1a`屬於本機區域群組`us-west-2-den-1`。

您無法建立與地理鄰近記錄具有相同值的「記錄名稱」和「記錄類型」的非地理鄰近記錄。

您也無法建立兩個地理鄰近資源記錄集，這些記錄集會為相同的記錄名稱和記錄類型指定相同位置。

如需詳細資訊，請參閱 available-local-zones .html

偏差

偏見可以擴展或縮小 Route 53 將流量路由到資源的地理區域。積極的偏見擴大了該區域，負偏差使其縮小。如需詳細資訊，請參閱 Amazon Route 53 如何使用偏差來路由流量。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、地理鄰近別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，選取 [是]。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

對於地理鄰近度記錄，如果端點狀態不良，Route 53 會尋找仍然健康的最接近端點。

評估目標運作狀態

如果您想讓 Route 53 藉由檢查 Endpoint (端點) 所指定資源的運作狀態來判斷是否使用此記錄回應 DNS 查詢，則選擇 Yes (是)

注意下列事項：

API Gateway 自訂區域 API 和最佳化邊緣 API

當端點是 API Gateway 自訂區域 API 或邊緣最佳化 API 時，將 Evaluate target health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

CloudFront 分佈

當端點為 CloudFront 發佈時，您無法將評估目標健全狀況設定為是。

具有區域化子網域的 Elastic Beanstalk 環境

如果您在 Endpoint (端點) 中指定 Elastic Beanstalk 環境，而此環境包含 ELB 負載平衡器，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。(如果環境包含多個 Amazon EC2 執行個體，就會自動包含 ELB 負載平衡器)。如果您將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)，而且沒有運作狀態良好的 Amazon EC2 執行個體，或負載平衡器本身即運作狀態不良，則 Route 53 會將查詢路由至其他運作狀態良好的可用資源 (如有)。

如果環境包含單一 Amazon EC2 執行個體，則沒有特殊需求。

ELB 負載平衡器

運作狀態檢查行為取決於負載平衡器的類型：

- Classic Load Balancers – 如果您在 Endpoint (端點) 中指定 ELB Classic Load Balancer，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。如果您將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，而且沒有運作狀態良好的 EC2 執行個體或負載平衡器本身運作狀態不良，Route 53 會將查詢路由至其他資源。
- Application Load Balancer 與 Network Load Balancer – 如果您指定 ELB Application Load Balancer 或 Network Load Balancer，並將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，Route 53 會根據與負載平衡器相關聯之目標群組的運作狀態，將查詢路由至負載平衡器：
  - 每個包含目標的目標群組必須至少包含一個運作狀態良好的目標，Application Load Balancer 或 Network Load Balancer 才會視為運作狀態良好。若有任何目標群組只包含運作狀態不良的目標，負載平衡器會被視為運作狀態不良，而且 Route 53 會將查詢路由至其他資源。

- 不含任何已註冊目標的目標群組會被視為運作狀態不良。

> **Note**
>
> 當您建立負載平衡器時，您可以設定 Elastic Load Balancing 運作狀態檢查的設定，它們不是 Route 53 運作狀態檢查，但會執行類似的功能。不要建立向 ELB 負載平衡器註冊之 EC2 執行個體的 Route 53 運作狀態檢查。

S3 儲存貯體

當端點為 S3 儲存貯體時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

Amazon VPC 介面端點

當端點是 Amazon VPC 介面端點時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

相同託管區域中的其他記錄

如果您在 Endpoint (端點) 中指定的 AWS 資源是一筆記錄或一組記錄 (例如一組加權記錄)，但不是其他別名記錄，建議您建立運作狀態檢查與端點中所有記錄的關聯性。如需詳細資訊，請參閱 當您忽略運作狀態檢查時會發生什麼情況？。

記錄 ID

輸入唯一識別地理鄰近記錄群組中此記錄的值。

延遲記錄的專用值

在建立延遲記錄時，指定下列值。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- TTL (秒)
- 值/將流量路由到
- 區域
- 運作狀態檢查
- 記錄 ID

路由政策

選擇 Latency (延遲)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為延遲記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

根據您想要 Route 53 回應 DNS 查詢的方式，選取 Type (類型) 的值。

為延遲記錄群組中的所有記錄選取相同的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權
- CNAME – 正式名稱
- MX - 郵件交換
- NAPTR - 名稱授權指標
- PTR - 指標
- SPF - 寄件者政策架構
- SRV - 服務定位器
- TXT - 文字

如需上述值的詳細資訊，請參"值/將流量路由到"的常見值。

區域

您在此記錄中指定之資源所在的 Amazon EC2 區域。Route 53 會根據您已指定的其他值來建議 Amazon EC2 區域。這同樣適用於私有託管區域。不建議變更此值。

注意下列事項：

- 每個 Amazon EC2 區域只能建立一個延遲記錄。
- 並非所有 Amazon EC2 區域都需要建立延遲記錄。Route 53 會從您建立延遲記錄的區域之間選擇具有最佳延遲的區域。
- 您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非延遲記錄作為延遲記錄。
- 如果您建立以區域 cn-north-1 為標籤的記錄，Route 53 一律會使用此記錄回應來自中國境內的查詢，而不論延遲為何。

如需使用延遲記錄的詳細資訊，請參閱 以延遲為基礎的路由。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate target health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

記錄 ID

輸入延遲記錄群組中可唯一識別這個記錄的值。

延遲別名記錄的專用值

在建立延遲別名記錄時，指定下列值。

如需更多詳細資訊，請參閱 選擇別名或非別名記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- 值/將流量路由到
- 區域
- 運作狀態檢查
- 評估目標運作狀態
- 記錄 ID

路由政策

選擇 Latency (延遲)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為延遲記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

請根據您路由流量的目標 AWS 資源來選取適用的值：

API Gateway 自訂區域 API 和最佳化邊緣 API

選取 A - IPv4 address (A - IPv4 地址)。

Amazon VPC 介面端點

選取 A - IPv4 address (A - IPv4 地址)。

CloudFront 分佈

選取 A - IPv4 address (A - IPv4 地址)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Record type (記錄類型) 值為 A - IPv4 地址，另一個記錄則具有值 AAAA - IPv6 地址。

具有區域化子網域的 Elastic Beanstalk 環境

選取 A - IPv4 address (A - IPv4 地址)

ELB 負載平衡器

選取 A - IPv4 address (A - IPv4 地址) 或 AAAA - IPv6 address (AAAA - IPv6 地址)

Amazon S3 儲存貯體

選取 A - IPv4 address (A - IPv4 地址)

此託管區域中的其他記錄

選取您要建立別名的記錄類型。支援 NS 與 SOA 以外的所有類型。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法將流量路由到 Type (類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

為延遲記錄群組中的所有記錄選取相同的值。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需哪些 AWS 資源可供您設定目標的資訊，請參閱"值/將流量路由到"的別名記錄的常見值。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

區域

您在此記錄中指定之資源所在的 Amazon EC2 區域。Route 53 會根據您已指定的其他值來建議 Amazon EC2 區域。這同樣適用於私有託管區域。不建議變更此值。

注意下列事項：

- 每個 Amazon EC2 區域只能建立一個延遲記錄。
- 並非所有 Amazon EC2 區域都需要建立延遲記錄。Route 53 會從您建立延遲記錄的區域之間選擇具有最佳延遲的區域。
- 您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非延遲記錄作為延遲記錄。
- 如果您建立以區域 cn-north-1 為標籤的記錄，Route 53 一律會使用此記錄回應來自中國境內的查詢，而不論延遲為何。

如需使用延遲記錄的詳細資訊，請參閱 以延遲為基礎的路由。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate target health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參

考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態，如果建立 Domain Name (網域名稱) 的值與記錄名稱符合的運作狀態檢查，然後將運作狀態檢查與這些記錄關聯，運作狀態檢查結果將會無法預測。

評估目標運作狀態

如果您想讓 Route 53 藉由檢查 Endpoint (端點) 所指定資源的運作狀態來判斷是否使用此記錄回應 DNS 查詢，則選擇 Yes (是)

注意下列事項：

API Gateway 自訂區域 API 和最佳化邊緣 API

當端點是 API Gateway 自訂區域 API 或邊緣最佳化 API 時，將 Evaluate target health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

CloudFront 分佈

當別名目標是 CloudFront 分佈時，您無法將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)。

具有區域化子網域的 Elastic Beanstalk 環境

如果您在 Endpoint (端點) 中指定 Elastic Beanstalk 環境，而此環境包含 ELB 負載平衡器，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。(如果環境包含多個 Amazon EC2 執行個體，就會自動包含 ELB 負載平衡器)。如果您將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)，而且沒有運作狀態良好的 Amazon EC2 執行個體，或負載平衡器本身即運作狀態不良，則 Route 53 會將查詢路由至其他運作狀態良好的可用資源 (如有)。

如果環境包含單一 Amazon EC2 執行個體，則沒有特殊需求。

ELB 負載平衡器

運作狀態檢查行為取決於負載平衡器的類型：

- Classic Load Balancers – 如果您在 Endpoint (端點) 中指定 ELB Classic Load Balancer，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。如果您將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，而且沒有運作狀態良好的 EC2 執行個體或負載平衡器本身運作狀態不良，Route 53 會將查詢路由至其他資源。
- Application Load Balancer 與 Network Load Balancer – 如果您指定 ELB Application Load Balancer 或 Network Load Balancer，並將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，Route 53 會根據與負載平衡器相關聯之目標群組的運作狀態，將查詢路由至負載平衡器：
  - 每個包含目標的目標群組必須至少包含一個運作狀態良好的目標，Application Load Balancer 或 Network Load Balancer 才會視為運作狀態良好。若有任何目標群組只包含運作狀態不良的目標，負載平衡器會被視為運作狀態不良，而且 Route 53 會將查詢路由至其他資源。
  - 不含任何已註冊目標的目標群組會被視為運作狀態不良。

> **Note**
>
> 當您建立負載平衡器時，您可以設定 Elastic Load Balancing 運作狀態檢查的設定，它們不是 Route 53 運作狀態檢查，但會執行類似的功能。不要建立向 ELB 負載平衡器註冊之 EC2 執行個體的 Route 53 運作狀態檢查。

S3 儲存貯體

當端點為 S3 儲存貯體時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

Amazon VPC 介面端點

當端點是 Amazon VPC 介面端點時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

相同託管區域中的其他記錄

如果您在 Endpoint (端點) 中指定的 AWS 資源是一筆記錄或一組記錄 (例如一組加權記錄)，但不是其他別名記錄，建議您建立運作狀態檢查與端點中所有記錄的關聯性。如需更多詳細資訊，請參閱當您忽略運作狀態檢查時會發生什麼情況？。

記錄 ID

輸入延遲記錄群組中可唯一識別這個記錄的值。

特定於以 IP 為基礎記錄的值

在建立以 IP 為基礎的記錄時，指定下列值。

> **Note**
>
> 雖然允許在私有託管區域中建立以 IP 為基礎的記錄，但不支援此記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- TTL (秒)
- 值/將流量路由到
- 位置
- 運作狀態檢查
- 記錄 ID

路由政策

選擇 IP-based (以 IP 為基礎)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為以 IP 為基礎的記錄群組中的所有記錄輸入相同的名稱。

CNAME 記錄

如果您要建立的記錄具有 Record type (記錄類型) 的 CNAME 值，則記錄的名稱不能與託管區域的名稱相同。

特殊字元

如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。

萬用字元

您可以在名稱中使用星號 (*) 字元。DNS 會根據 * 字元出現在名稱中的位置，將其視為萬用字元或 * 字元 (ASCII 42)。如需更多詳細資訊，請參閱 在託管區域和記錄的名稱中使用星號 (*)。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

根據您想要 Route 53 回應 DNS 查詢的方式，選取 Type (類型) 的值。

為延遲記錄群組中的所有記錄選取相同的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權
- CNAME – 正式名稱
- MX - 郵件交換
- NAPTR - 名稱授權指標
- PTR - 指標
- SPF - 寄件者政策架構
- SRV - 服務定位器
- TXT - 文字

如需上述值的詳細資訊，請參值/將流量路由到“值/將流量路由到”的常見值。

位置

您在此記錄中指定的資源的 CIDR 位置名稱由 CIDR 位置中的 CIDR 區塊值指定。

如需使用以 IP 為基礎的記錄的詳細資訊，請參閱 以 IP 為基礎的路由。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。

- 針對別名記錄或容錯移轉別名、地理位置別名、以 IP 為基礎的別名、延遲別名或加權別名記錄群組中的記錄，您可以為 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

記錄 ID

輸入以 IP 為基礎的記錄群組中可唯一識別這個記錄的值。

特定於以 IP 為基礎的別名記錄的值

在建立以 IP 為基礎的別名記錄時，指定下列值。

> **Note**
>
> 雖然可以在私有託管區域中建立以 IP 為基礎的別名記錄，但這個做法並不受到支援。

如需更多詳細資訊，請參閱 選擇別名或非別名記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- 值/將流量路由到
- 位置
- 運作狀態檢查
- 評估目標運作狀態
- 記錄 ID

路由政策

選擇 IP-based (以 IP 為基礎)。

> **Note**
>
> 雖然可以在私有託管區域中建立以 IP 為基礎的別名記錄，但這個做法並不受到支援。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為以 IP 為基礎的記錄群組中的所有記錄輸入相同的名稱。

CNAME 記錄

如果您要建立的記錄具有 Record type (記錄類型) 的 CNAME 值，則記錄的名稱不能與託管區域的名稱相同。

CloudFront 分發和 Amazon S3 儲存貯體的別名

您指定的值部分取決於您路由流量的目標 AWS 資源：

- CloudFront 分佈 – 您的分佈必須包含符合記錄名稱的替代網域名稱。例如，如果記錄名稱為 acme.example.com，您的 CloudFront 分佈必須包含 acme.example.com 做為其中一個替代網域名稱。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的使用備用網域名稱 (CNAME)。
- Amazon S3 儲存貯體 - 記錄的名稱必須符合您 Amazon S3 儲存貯體的名稱。例如，如果您的儲存貯體名稱為 acme.example.com，此記錄名稱也必須包含 acme.example.com。

  此外，您必須設定儲存貯體處理網站託管。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的「為網站託管設定儲存貯體」。

特殊字元

如需如何指定 a-z、0-9 與 - (連字號) 以外的字元，以及如何指定國際化網域名稱的資訊，請參閱 DNS 網域名稱格式。

萬用字元

您可以在名稱中使用星號 (*) 字元。DNS 會根據 * 字元出現在名稱中的位置，將其視為萬用字元或 * 字元 (ASCII 42)。如需更多詳細資訊，請參閱 在託管區域和記錄的名稱中使用星號 (*)。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

根據您路由流量的目標 AWS 資源來選取適用的值。為以 IP 為基礎的記錄群組中的所有記錄選取相同的值：

API Gateway 自訂區域 API 和最佳化邊緣 API

選取 A - IPv4 address (A - IPv4 地址)。

Amazon VPC 介面端點

選取 A - IPv4 address (A - IPv4 地址)。

CloudFront 分佈

選取 A - IPv4 address (A - IPv4 地址)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Record type (記錄類型) 值為 A - IPv4 地址，另一個記錄則具有值 AAAA - IPv6 地址。

具有區域化子網域的 Elastic Beanstalk 環境

選取 A - IPv4 address (A - IPv4 地址)

ELB 負載平衡器

選取 A - IPv4 address (A - IPv4 地址) 或 AAAA - IPv6 address (AAAA - IPv6 地址)

Amazon S3 儲存貯體

選取 A - IPv4 address (A - IPv4 地址)

此託管區域中的其他記錄

選取您要建立別名的記錄類型。支援 NS 與 SOA 以外的所有類型。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法將流量路由到 Type (類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需哪些 AWS 資源可供您設定目標的資訊，請參閱"值/將流量路由到"的別名記錄的常見值。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

位置

當您設定 Route 53 根據查詢來源位置來回應 DNS 查詢時，請選取要讓 Route 53 使用此記錄中設定回應的 CIDR 位置。

> **Important**
>
> 我們建議您建立一個 Location (位置) 值為 Default (預設) 的以 IP 為基礎的記錄。這會涵蓋您尚未建立記錄的位置，以及 Route 53 無法識別位置的 IP 地址。

您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非以 IP 為基礎的記錄作為以 IP 為基礎的記錄。

如需更多詳細資訊，請參閱 以 IP 為基礎的路由。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、以 IP 為基礎的路由別名、延遲別名或加權別名記錄群組中的記錄，您可以為 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

對於以 IP 為基礎的別名記錄，如果某個端點運作狀態不良，Route 53 會在更大的關聯位置中尋找記錄。例如，假設您有美國某州、美國、北美洲與所有位置 (Location (位置) 為 Default (預設)) 的記錄。如果州記錄的端點運作狀態不良，Route 53 會依序檢查美國、北美洲與所有位置的記錄，直到找到具有運作狀態良好端點的記錄。如果所有適用記錄的運行狀況都不佳 (包括所有位置記錄)，則 Route 53 會使用最小地理區域的記錄值回應 DNS 查詢。

評估目標運作狀態

如果您想讓 Route 53 藉由檢查 Endpoint (端點) 所指定資源的運作狀態來判斷是否使用此記錄回應 DNS 查詢，則選擇 Yes (是)

注意下列事項：

API Gateway 自訂區域 API 和最佳化邊緣 API

當端點是 API Gateway 自訂區域 API 或邊緣最佳化 API 時，將 Evaluate target health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

CloudFront 分佈

當別名目標是 CloudFront 分佈時，您無法將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)。

具有區域化子網域的 Elastic Beanstalk 環境

如果您在 Endpoint (端點) 中指定 Elastic Beanstalk 環境，而此環境包含 ELB 負載平衡器，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。(如果環境包含多個 Amazon EC2 執行個體，就會自動包含 ELB 負載平衡器)。如果您將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)，而且沒有運作狀態良好的 Amazon EC2 執行個體，或負載平衡器本身即運作狀態不良，則 Route 53 會將查詢路由至其他運作狀態良好的可用資源 (如有)。

如果環境包含單一 Amazon EC2 執行個體，則沒有特殊需求。

ELB 負載平衡器

運作狀態檢查行為取決於負載平衡器的類型：

- Classic Load Balancers – 如果您在 Endpoint (端點) 中指定 ELB Classic Load Balancer，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。如果您將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，而且沒有運作狀態良好的 EC2 執行個體或負載平衡器本身運作狀態不良，Route 53 會將查詢路由至其他資源。
- Application Load Balancer 與 Network Load Balancer – 如果您指定 ELB Application Load Balancer 或 Network Load Balancer，並將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，Route 53 會根據與負載平衡器相關聯之目標群組的運作狀態，將查詢路由至負載平衡器：
  - 每個包含目標的目標群組必須至少包含一個運作狀態良好的目標，Application Load Balancer 或 Network Load Balancer 才會視為運作狀態良好。若有任何目標群組只包含運作狀態不良的目標，負載平衡器會被視為運作狀態不良，而且 Route 53 會將查詢路由至其他資源。
  - 不含任何已註冊目標的目標群組會被視為運作狀態不良。

> **Note**
>
> 當您建立負載平衡器時，您可以設定 Elastic Load Balancing 運作狀態檢查的設定，它們不是 Route 53 運作狀態檢查，但會執行類似的功能。不要建立向 ELB 負載平衡器註冊之 EC2 執行個體的 Route 53 運作狀態檢查。

S3 儲存貯體

當端點為 S3 儲存貯體時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

Amazon VPC 介面端點

當端點是 Amazon VPC 介面端點時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

相同託管區域中的其他記錄

如果您在 Endpoint (端點) 中指定的 AWS 資源是一筆記錄或一組記錄 (例如一組加權記錄)，但不是其他別名記錄，建議您建立運作狀態檢查與端點中所有記錄的關聯性。如需更多詳細資訊，請參閱當您忽略運作狀態檢查時會發生什麼情況？。

記錄 ID

輸入以 IP 為基礎的記錄群組中可唯一識別這個記錄的值。

多值回答記錄的專用值

在建立多值回答記錄時，指定下列值。

> **Note**
>
> 不支援建立多值回答別名記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- TTL (秒)
- 值/將流量路由到
- 運作狀態檢查
- 記錄 ID

路由政策

選取 Multivalue answer (多值回答)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為多值記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

選取 NS 或 CNAME 以外的任何值。

為多值回應記錄群組中的所有記錄選取相同的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

> **Note**
>
> 如果您建立兩個或多個具有相同名稱與類型的多值回應記錄，即表示您在使用主控台並且為 TTL 指定不同的值，則 Route 53 會將所有記錄的 TTL 值變更為您指定的最後一個值。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。如果您要輸入超過一個值，請在不同的行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權
- MX - 郵件交換
- NAPTR - 名稱授權指標
- PTR - 指標
- SPF - 寄件者政策架構

- SRV - 服務定位器
- TXT - 文字

如需上述值的詳細資訊，請參"值/將流量路由到"的常見值。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名或加權別名記錄群組中的記錄，您可以為 Evaluate target health (評估目標運作狀態) 選擇 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

記錄 ID

輸入多值回應記錄群組中可唯一識別這個記錄的值。

加權記錄的專用值

在建立加權記錄時，指定下列值。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- TTL (秒)
- 值/將流量路由到
- Weight
- 運作狀態檢查
- 記錄 ID

路由政策

選取 Weighted (加權)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Record name (記錄名稱) 欄位中輸入值 (例如 @ 符號)。

為加權記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱。

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

為加權記錄群組中的所有記錄選取相同的值。

TTL (秒)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。若您指定了較長的值 (例如，172800 秒或兩日)，您會減少 DNS 遞迴解析程式必須向 Route 53 進行的呼叫數量，以取得此記錄中最新的資訊。如此能降低延遲，並減少您的 Route 53 服務帳單。如需更多詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

不過，如果您指定了較長的 TTL 值，則您需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式在要求 Route 53 提供最新資訊之前，使用其快取中值的時間會更久。如果您要變更已在使用中的網域或子網域設定，我們建議您一開始指定較短的值 (例如 300 秒)，然後在確認新的設定正確時再提高該值。

如果您將此記錄與運作狀態檢查關聯，建議您指定 60 秒或更少的 TTL，讓用戶端可以快速回應運作狀態變更。

您必須為此加權記錄群組中的所有記錄指定相同的 TTL 值。

> **Note**
>
> 如果您建立兩個或多個具有相同名稱與類型的加權記錄，並指定不同的 TTL 值，Route 53 會將所有記錄的 TTL 值變更為您指定的最後一個值。

如果加權記錄群組包含一或多個將流量路由至 ELB 負載平衡器的加權別名記錄，建議您為具有相同名稱與類型的所有非別名加權記錄指定 60 秒的 TTL。60 秒以外的值 (負載平衡器的 TTL) 會改變您為 Weight (權重) 指定之值的效果。

值/將流量路由到

選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入適用於 Record type (記錄類型) 值的值。針對 CNAME 以外的所有類型，您可以輸入多個值。分行輸入每個值。

您可以將流量路由至，或指定下列值：

- A – IPv4 地址
- AAAA - IPv6 地址
- CAA - 憑證機構授權
- CNAME – 正式名稱
- MX - 郵件交換

- NAPTR - 名稱授權指標
- PTR - 指標
- SPF - 寄件者政策架構
- SRV - 服務定位器
- TXT - 文字

如需上述值的詳細資訊，請參"值/將流量路由到"的常見值。

Weight

此值可判斷 Route 53 使用目前記錄回應的 DNS 查詢比例。Route 53 會計算具有相同 DNS 名稱與類型組合之記錄的權重總和。然後，Route 53 會根據資源的整體權重比例來回應查詢。

您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非加權記錄作為加權記錄。

輸入介於 0 到 255 之間的整數。若要停用路由至資源，請將 Weight (權重) 設定為 0。如果您將群組中所有記錄的 Weight (權重) 都設定為 0，則會將流量路由至機率相等的所有資源。這可確保您不會意外停用加權記錄群組的路由。

將 Weight (權重) 設定為 0 的效果，不同於將運作狀態檢查與加權記錄關聯的效果。如需更多詳細資訊，請參閱 當您已設定運作狀態檢查時，Amazon Route 53 會如何選擇記錄。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。

- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate target health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

記錄 ID

輸入加權記錄群組中可唯一識別這個記錄的值。

加權別名記錄的專用值

在建立加權別名記錄時，指定下列值。如需更多詳細資訊，請參閱 選擇別名或非別名記錄。

主題

- 路由政策
- 記錄名稱
- 記錄類型
- 值/將流量路由到
- Weight
- 運作狀態檢查
- 評估目標運作狀態
- 記錄 ID

路由政策

選擇 Weighted (加權)。

記錄名稱

輸入您要路由流量的網域或子網域名稱。預設值為託管區域名稱。

> **Note**
>
> 如果您想要建立與託管區域同名的記錄，則不要在 Name (名稱) 欄位中輸入值 (例如 @ 符號)。

為加權記錄群組中的所有記錄輸入相同的名稱。

如需記錄名稱的詳細資訊，請參閱 記錄名稱

記錄類型

DNS 記錄類型。如需更多詳細資訊，請參閱 支援的 DNS 記錄類型。

請根據您路由流量的目標 AWS 資源來選取適用的值：

API Gateway 自訂區域 API 和最佳化邊緣 API

選取 A - IPv4 address (A - IPv4 地址)。

Amazon VPC 介面端點

選取 A - IPv4 address (A - IPv4 地址)。

CloudFront 分佈

選取 A - IPv4 address (A - IPv4 地址)。

如果已為分佈啟用 IPv6，請建立兩個記錄，一個記錄的 Record type (記錄類型) 值為 A - IPv4 地址，另一個記錄則具有值 AAAA - IPv6 地址。

具有區域化子網域的 Elastic Beanstalk 環境

選取 A - IPv4 address (A - IPv4 地址)

ELB 負載平衡器

選取 A - IPv4 address (A - IPv4 地址) 或 AAAA - IPv6 address (AAAA - IPv6 地址)

Amazon S3 儲存貯體

選取 A - IPv4 address (A - IPv4 地址)

此託管區域中的其他記錄

選取您要建立別名的記錄類型。支援 NS 與 SOA 以外的所有類型。

> **Note**
>
> 如果想要建立與託管區域 (也就是 Zone Apex) 同名的別名記錄，則無法將流量路由到 Type (類型) 值為 CNAME 的記錄。這是因為別名記錄必須與流量路由到的目標記錄具有相同的類型，而不支援為 Zone Apex 建立 CNAME 記錄的做法，即使對於別名記錄也是如此。

為加權記錄群組中的所有記錄選取相同的值。

值/將流量路由到

您從清單選擇的值，或在欄位中輸入的值，皆依據您將流量路由至哪個 AWS 資源而定。

如需哪些 AWS 資源可供您設定目標的資訊，請參閱"值/將流量路由到"的別名記錄的常見值。

如需如何設定 Route 53 將流量路由至特定 AWS 資源的詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

Weight

此值可判斷 Route 53 使用目前記錄回應的 DNS 查詢比例。Route 53 會計算具有相同 DNS 名稱與類型組合之記錄的權重總和。然後，Route 53 會根據資源的整體權重比例來回應查詢。

您無法建立具有相同 Record name (記錄名稱) 與 Record type (記錄類型) 值的非加權記錄作為加權記錄。

輸入介於 0 到 255 之間的整數。若要停用路由至資源，請將 Weight (權重) 設定為 0。如果您將群組中所有記錄的 Weight (權重) 都設定為 0，則會將流量路由至機率相等的所有資源。這可確保您不會意外停用加權記錄群組的路由。

將 Weight (權重) 設定為 0 的效果，不同於將運作狀態檢查與加權記錄關聯的效果。如需更多詳細資訊，請參閱 當您已設定運作狀態檢查時，Amazon Route 53 會如何選擇記錄。

運作狀態檢查

若要讓 Route 53 檢查所指定端點的運作狀態，並只在端點運作狀態良好時才使用此記錄回應 DNS 查詢，請選擇運作狀態檢查。

Route 53 不會檢查記錄中所指定端點的運作狀態，例如 Value (值) 欄位中的 IP 地址所指定的端點。當您為記錄選擇運作狀態檢查時，Route 53 會檢查您在運作狀態檢查中指定的端點運作狀態。如需 Route 53 如何判斷端點是否運作狀態良好的資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

只有在 Route 53 於兩個或多個記錄之間進行選擇以回應 DNS 查詢，而且您想要讓 Route 53 能夠部分根據運作狀態檢查的狀態來選擇時，將運作狀態檢查與記錄關聯才有用。請只在下列組態中使用運作狀態檢查：

- 您正在檢查具有相同名稱、類型和路由政策 (例如容錯移轉或加權記錄) 的一組記錄中之所有記錄運作狀態，並為所有記錄指定運駐狀態檢查 ID。如果記錄的運作狀態檢查指定運作狀態不良的端點，Route 53 會使用該記錄的值停止回應查詢。
- 針對別名記錄或容錯移轉別名、地理位置別名、延遲別名、以 IP 為基礎的別名或加權別名記錄群組中的記錄，您可以在 Evaluate target health (評估目標運作狀態) 中選取 Yes (是)。如果別名記錄參考相同託管區域中的非別名記錄，您也必須指定所參考記錄的運作狀態檢查。如果將運作狀態檢查與別名記錄關聯，並且對於 Evaluate Target Health (評估目標運作狀態) 選擇 Yes (是)，則值都必須為 true。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。

如果您的運作狀態檢查只依網域名稱指定端點，建議您建立每個端點的個別運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。對 Domain Name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄名稱 (example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

評估目標運作狀態

如果您想讓 Route 53 藉由檢查 Endpoint (端點) 所指定資源的運作狀態來判斷是否使用此記錄回應 DNS 查詢，則選擇 Yes (是)

注意下列事項：

API Gateway 自訂區域 API 和最佳化邊緣 API

當端點是 API Gateway 自訂區域 API 或邊緣最佳化 API 時，將 Evaluate target health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

CloudFront 分佈

當別名目標是 CloudFront 分佈時，您無法將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)。

具有區域化子網域的 Elastic Beanstalk 環境

如果您在 Endpoint (端點) 中指定 Elastic Beanstalk 環境，而此環境包含 ELB 負載平衡器，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。(如果環境包含多個 Amazon EC2 執行個體，就會自動包含 ELB 負載平衡器)。如果您將 Evaluate target health (評估目標運作狀態) 設為 Yes (是)，而且沒有運作狀態良好的 Amazon EC2 執行個體，或負載平衡器本身即運作狀態不良，則 Route 53 會將查詢路由至其他運作狀態良好的可用資源 (如有)。

如果環境包含單一 Amazon EC2 執行個體，則沒有特殊需求。

ELB 負載平衡器

運作狀態檢查行為取決於負載平衡器的類型：

- Classic Load Balancers – 如果您在 Endpoint (端點) 中指定 ELB Classic Load Balancer，Elastic Load Balancing 只會將查詢路由至已向負載平衡器註冊之運作狀態良好的 Amazon EC2 執行個體。如果您將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，而且沒有運作狀態良好的 EC2 執行個體或負載平衡器本身運作狀態不良，Route 53 會將查詢路由至其他資源。
- Application Load Balancer 與 Network Load Balancer – 如果您指定 ELB Application Load Balancer 或 Network Load Balancer，並將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是)，Route 53 會根據與負載平衡器相關聯之目標群組的運作狀態，將查詢路由至負載平衡器：
  - 每個包含目標的目標群組必須至少包含一個運作狀態良好的目標，Application Load Balancer 或 Network Load Balancer 才會視為運作狀態良好。若有任何目標群組只包含運作狀態不良的目標，負載平衡器會被視為運作狀態不良，而且 Route 53 會將查詢路由至其他資源。
  - 不含任何已註冊目標的目標群組會被視為運作狀態不良。

> **Note**
>
> 當您建立負載平衡器時，您可以設定 Elastic Load Balancing 運作狀態檢查的設定，它們不是 Route 53 運作狀態檢查，但會執行類似的功能。不要建立向 ELB 負載平衡器註冊之 EC2 執行個體的 Route 53 運作狀態檢查。

S3 儲存貯體

當端點為 S3 儲存貯體時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

Amazon VPC 介面端點

當端點是 Amazon VPC 介面端點時，將 Evaluate Target Health (評估目標運作狀態) 設定為 Yes (是) 沒有特殊需求。

相同託管區域中的其他記錄

如果您在 Endpoint (端點) 中指定的 AWS 資源是一筆記錄或一組記錄 (例如一組加權記錄)，但不是其他別名記錄，建議您建立運作狀態檢查與端點中所有記錄的關聯性。如需更多詳細資訊，請參閱當您忽略運作狀態檢查時會發生什麼情況？。

記錄 ID

輸入加權記錄群組中可唯一識別這個記錄的值。

透過匯入區域檔案建立記錄

如果您要從另一個 DNS 服務提供者遷移，而且您的目前 DNS 服務提供者可讓您將目前 DNS 設定匯出到區域檔案，您可以透過匯入區域檔案快速為 Amazon Route 53 託管區域建立所有記錄。

> **Note**
>
> 區域檔案使用標準格式 (稱為 BIND)，以文字格式表示記錄。如需區域檔案格式的資訊，請參閱 Wikipedia 項目區域檔案。如需更多詳細資訊，請參閱 RFC 1034 網域名稱 - 概念和設施第 3.6.1 節和 RFC 1035 網域名稱 - 實作和規格第 5 節。

如果要透過匯入區域檔案建立記錄，請注意以下事項：

- 區域檔案必須採用符合 RFC 標準的格式。
- 區域檔案中記錄的網域名稱必須符合託管區域的名稱。
- Route 53 支援 `$ORIGIN` 和 `$TTL` 關鍵字。如果區域檔案包含 `$GENERATE` 或 `$INCLUDE` 關鍵字，則匯入會失敗，Route 53 會傳回錯誤。
- 當您匯入區域檔案，Route 53 會忽略區域檔案中的 SOA 記錄。Route 53 也會忽略與託管區域名稱同名的任何 NS 記錄。
- 您最多可以匯入 1,000 個記錄。
- 如果託管區域已包含出現在區域檔案中的記錄，匯入程序會失敗，並且不會建立任何記錄。
- 建議您檢閱區域檔案的內容，確認記錄名稱包含或排除行尾點號：
  - 當區域檔案中的記錄名稱包含行尾點號 (`example.com.`)，匯入程序會將此名稱解讀為完整網域名稱，並使用該名稱建立 Route 53 記錄。
  - 當區域檔案中的記錄名稱不包含行尾點號 (`www`)，匯入程序會將該名稱與區域檔案中的網域名稱 (`example.com`) 串連起來，並使用該串連名稱 (`www.example.com`) 建立 Route 53 記錄。

  如果匯出程序不會將行尾點號新增到記錄的網域名稱，Route 53 匯入的程序會將網域名稱新增到記錄的名稱。例如，假設您要將記錄匯入到託管區域 `example.com`，而區域檔案中 MX 記錄的名稱是 `mail.example.com` (沒有行尾點號)。Route 53 匯入程序會建立名為 `mail.example.com.example.com` 的 MX 記錄。

> **Important**
>
> 對於 CNAME、MX、PTR 和 SRV 記錄，此行為也適用於包含在 RDATA 值中的網域名稱。例如，假設您有 `example.com` 的區域檔案。如果區域檔案中的 CNAME 記錄

(support，沒有行尾點號) 具有 RDATA 值 www.example.com (也沒有行尾點號)，則匯入程序會建立名為 support.example.com 的 Route 53 記錄來將流量路由至 www.example.com.example.com。匯入區域檔案之前，請先檢閱 RDATA 值和更新 (如適用)。

Route 53 不支援將記錄匯出到區域檔案。

若要透過匯入區域檔案建立記錄

1. 從目前提供網域服務的 DNS 服務提供者取得區域檔案。此程序和術語因服務提供者而異。如需有關將記錄匯出或儲存到區域檔案或 BIND 檔案的資訊，請參閱提供者的介面和文件。

   如果不清楚此程序，請詢問目前 DNS 提供者的客戶支援，以取得記錄清單或區域檔案資訊。
2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 在 Hosted Zones (託管區域) 頁面，建立新的託管區域：

   a. 選擇 Create Hosted Zone (建立託管區域)。

   b. 輸入您的網域名稱，並選擇性地輸入註解。

   c. 選擇建立。
5. 選擇 Import Zone File (匯入區域檔案)。
6. 在 Import Zone File (匯入區域檔案) 窗格中，將區域檔案的內容貼至 Zone File (區域檔案) 文字方塊中。
7. 選擇 Import (匯入)。

   > **Note**
   >
   > 根據區域檔案中的記錄數量，您可能需要等待幾分鐘，才能完成建立記錄。
8. 如果您使用網域的另一個 DNS 服務 (這很常見，如果您向另一個註冊商註冊該網域)，請將 DNS 服務遷移至 Route 53。完成該步驟後，您的註冊商會開始將 Route 53 識別為您的 DNS 服務，以回應對您網域的 DNS 查詢，且查詢會開始傳送至 Route 53 DNS 伺服器。(一般而言，在 DNS 查詢開始被路由到 Route 53 之前，會有一兩天的延遲，因為先前 DNS 服務的相關資訊在 DNS 解析程式中快取這麼長時間。) 如需詳細資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

編輯記錄

下列程序說明如何使用 Amazon Route 53 主控台來編輯記錄。如需如何使用路由 53 API 編輯記錄的相關資訊，請參閱 Amazon 路線 53 API 參考ChangeResourceRecordSets中的。

> **Note**
>
> 對記錄的變更需要一些時間傳播到 Route 53 DNS 伺服器。目前，驗證變更是否已傳播的唯一方法是使用 GetChangeAPI 動作。變更通常會在 60 秒內傳播至所有 Route 53 名稱伺服器。

若要使用 Route 53 主控台編輯記錄

1. 如果您不要編輯別名記錄，請跳至步驟 2。

   如果您要編輯將流量路由至 Elastic Load Balancing Classic Load Balancer、Application Load Balancer 或 Network Load Balancer 的別名記錄，並且如果您使用不同的帳戶建立 Route 53 託管區域與負載平衡器，請執行程序 取得 Elastic Load Balancing 負載平衡器的 DNS 名稱 以取得負載平衡器的 DNS 名稱。

   如果您要編輯任何其他 AWS 資源的別名記錄，請跳到步驟 2。
2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 在 Hosted Zones (託管區域) 頁面上，選擇包含要編輯之記錄的託管區域列。
5. 選取您要編輯的記錄所在的列，然後在 Edit record (編輯記錄) 窗格中輸入變更內容。
6. 輸入適用的值。如需詳細資訊，請參閱 您在建立或編輯 Amazon Route 53 記錄指定的值。
7. 選擇 Save changes (儲存變更)。
8. 如果您要編輯多個記錄，請重複步驟 5 到 7。

刪除記錄

下列程序說明如何使用 Route 53 主控台來刪除記錄。如需如何使用路由 53 API 刪除記錄的相關資訊，請參閱 Amazon 路線 53 API 參考ChangeResourceRecordSets中的。

> **Note**
>
> 對記錄的變更需要一些時間傳播到 Route 53 DNS 伺服器。目前，驗證變更是否已傳播的唯一方法是使用 GetChangeAPI 動作。變更通常會在 60 秒內傳播至所有 Route 53 名稱伺服器。

若要刪除記錄

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在「Hosted Zones」(託管區域) 頁面上，選擇包含要刪除之記錄的託管區域列。
3. 在記錄清單中，選擇要刪除的記錄。

   若要選取多個連續的記錄，請選擇第一列，按住 Shift 鍵，然後選擇最後一列。若要選取多個非連續的記錄，請選擇第一列，按住 Ctrl 鍵，然後選擇其餘列。

   您無法刪除 Type (類型) 為 NS 或 SOA 值的記錄。
4. 選擇刪除。
5. 選擇 Delete (刪除) 來關閉對話方塊。

列出記錄

下列程序說明如何使用 Amazon Route 53 主控台來列出託管區域中的記錄。如需有關如何使用路由 53 API 列出記錄的詳細資訊，請參閱 Amazon 路線 53 API 參考ListResourceRecordSets中的。

若要列出記錄

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 在 Hosted Zones (託管區域) 頁面上，選擇託管區域的名稱。
4. 若要變更搜尋模式，請選擇記錄表格右上角的齒輪圖示。選擇以下一項：

   - 自動

     在此模式下，該服務根據記錄數量使用篩選條件。2,000 個以內的記錄使用完整模式，2,000 個以上的記錄使用快速模式。

- 完整

  在此模式下，所有搜尋篩選條件都可使用，但搜尋效能可能會較慢。

- 快速

  在此模式下，部分進階功能不可用，但搜尋效能會更快。

若只要顯示選取的記錄，請在記錄清單上方輸入適用的搜尋條件。在自動模式下，搜尋行為取決於託管區域最多包含 2,000 個記錄還是超過 2,000 個記錄：

最多 2,000 個記錄和完整模式

- 若要顯示有特定值的記錄，請在 Search (搜尋) 欄位中輸入值，並按 Enter 鍵。例如，若要顯示以 192.0 開頭之 IP 地址的記錄，請在 Search (搜尋) 欄位中輸入值，並按 Enter 鍵。
- 若只要顯示具有相同 DNS 記錄類型的記錄，請從下拉式清單中選取 Record type (記錄類型)，然後輸入記錄類型。
- 若只要顯示別名記錄，在下拉式選單中選取 Aliase (別名)，然後輸入 **`Yes`**。
- 若只要顯示加權記錄，請在下拉式清單中選取 Routing policy (路由政策)，然後輸入 **`WEIGHTED`**。

超過 2,000 個記錄和快速模式

- 您可以僅搜尋記錄名稱，而不搜尋記錄值。您也無法根據記錄類型、別名或加權記錄來進行篩選。

  為此，請將游標放入篩選條件文字方塊中，然後依次選取屬性和記錄名稱。

- 針對具有三個標籤 (以點號分隔的三個部分) 的記錄，當您在搜尋欄位中輸入值並按 Enter 鍵時，Route 53 主控台會自動在記錄名稱右側的第三個標籤上執行萬用字元搜尋。例如，假設託管區域 example.com 包含名為 record1.example.com 一直到 record100.example.com 的 100 個記錄。(Record1 是右側第三個標籤。) 以下是當您搜尋下列值時會發生的情況：
  - record1 – Route 53 主控台會搜尋 record1*.example.com，傳回 record1.example.com、record10.example.com 一直到 record19.example.com 以及 record100.example.com。
  - record1.example.com – 如同上述範例，主控台會搜尋 record1*.example.com 並傳回相同的記錄。
  - 1 – 主控台會搜尋 1*.example.com 且不傳回任何記錄。
  - example – 主控台會搜尋 example*.example.com 且不傳回任何記錄。
  - example.com – 在此範例中，主控台不會執行萬用字元搜尋。會傳回託管區域中的所有記錄。

- 自動搜尋模式：使用此搜尋模式時，您必須先提供屬性，例如記錄名稱，才能進行搜尋。

> **Note**
>
> 如果右側第三個標籤包含一或多個連字號 (例如 `third-label.example.com`)，而且如果您搜尋緊接在連字號前第三個標籤的部分 (在此範例中即為 `third`)，Route 53 就不會傳回任何記錄。反之，擇一包括緊接在連字號前的連字號 (搜尋 `third-`) 或省略字元 (搜尋 `third`)。

- 針對具有四或多個標籤的記錄，您必須指定記錄的確切名稱。不支援萬用字元搜尋。例如，如果託管區域包含名為 label4.record1.example.com 的記錄，則只有在搜尋欄位中指定 label4.record1.example.com 時，才能找到該記錄。

使用流量流程來路由 DNS 流量

在下列情況中，管理託管區域中的相關記錄可能會是艱鉅的挑戰：

- 您有許多執行相同操作的資源，例如為相同網域提供流量的 Web 伺服器。
- 您想要使用別名記錄和 Route 53 路由政策組合 (例如延遲、備援和加權) 來建立複雜的記錄樹。

您可以一次建立一個記錄，但是在 Route 53 主控台中檢閱設定時，很難追蹤各個記錄之間的關係。流量流程大幅簡化了在大型和複雜組態中建立和維護記錄的程序。

Visual editor (視覺化編輯器)

流量流程視覺化編輯器可讓您建立複雜的記錄樹，並查看記錄之間的關係。例如，您可能會建立組態，其中延遲別名記錄參照加權記錄，而加權記錄參照多個 AWS 區域 中的資源。每個組態皆稱為流量政策。您可以視需要免費建立任意數量的流量政策。

版本控制

您可以建立多個版本的流量政策，這樣在組態變更時，就不需要從頭開始。舊版本會繼續存在，直到您刪除它們為止；每個流量政策有 1000 個版本的預設限制。您可以選擇是否要針對每個版本輸入描述。

自動建立和更新記錄

流量政策可代表數十個或甚至數百個記錄。流量流程可讓您建立流量政策記錄，以自動建立所有這些記錄。您可在樹狀結構的根目錄 (例如 example.com 或 www.example.com) 指定託管區域和記錄

名稱，而 Route 53 會在樹狀結構中自動建立所有其他記錄。根記錄 (流量政策記錄) 顯示在託管區域的記錄清單中；所有其他記錄都會隱藏。

當您建立新版流量政策時，您可以選擇性地更新您已使用舊版流量政策建立的流量政策記錄。當您更新流量政策記錄時，Route 53 會自動更新樹狀結構中的所有其他記錄。您也可以將流量政策記錄再次更新為使用舊版流量政策，以快速復原變更。

> **Note**
>
> 您可以使用流量流程來建立僅限公有託管區域中的記錄。

重複用於不同託管區域中的多個記錄

您可以使用流量政策，自動在多個公有託管區域中建立記錄。例如，如果您將相同的 Web 伺服器用於多個網域名稱，您可以使用相同的流量政策，以在 example.com、example.org 和 example.net 的託管區域中建立流量政策記錄。

Route 53 回應 DNS 查詢的方式

當用戶端針對根目錄記錄名稱 (例如 example.com 或 www.example.com) 提交查詢時，Route 53 會根據您用來建立對應流量政策記錄的流量政策中的組態來回應查詢。

地理位置鄰近性路由政策

t 使用地理鄰近路由，您可以根據資源的位置路由流量，並選擇性地將流量從一個位置的資源轉移到另一個位置的資源。如需詳細資訊，請參閱 地理鄰近路由。

流量流程的費用

每個流量政策記錄都會產生月費。如需詳細資訊，請參閱 Amazon Route 53 定價的「流量流程」一節。

為了將這些費用降至最低，您可以在託管區域中建立一或多個別名記錄 (參照該託管區域中的流量政策記錄)。例如，您可以建立 example.com 的流量政策記錄，然後建立參照流量政策記錄之 www.example.com 的別名記錄

主題

- 建立和管理流量政策
- 建立和管理政策記錄

建立和管理流量政策

主題

- 建立流量政策
- 在建立流量政策時指定的值
- 檢視顯示地理位置鄰近性設定效果的地圖
- 建立其他版本的流量政策
- 透過匯入 JSON 文件來建立流量政策
- 檢視流量政策版本和關聯的政策記錄
- 刪除流量政策版本和流量政策

建立流量政策

若要建立流量政策，請執行下列程序。

建立流量政策

1. 設計您的組態。如需複雜 DNS 路由組態的運作方式的詳細資訊，請參閱設定 DNS 備援中的建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。
2. 根據您的組態設計，建立要用於端點的運作狀態檢查。
3. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
4. 在導覽窗格中，選擇 Traffic policies (流量政策)。
5. 選擇 Create traffic policy (建立流量政策)。
6. 在 Name policy (名稱政策) 頁面，指定適用的值。如需詳細資訊，請參閱 在建立流量政策時指定的值。
7. 選擇下一步。
8. 在 Create traffic policy (建立流量政策) policy name (政策名稱) v1 頁面上，指定適用的值。如需詳細資訊，請參閱 在建立流量政策時指定的值。

   您可以透過以下方式刪除流量政策的規則、端點和分支：

   - 若要刪除規則或端點，請按一下方塊右上角的 x。

> **Important**
>
> 如果您刪除有子規則和端點的規則，Amazon Route 53 也會刪除所有子系。

- 如果將兩個規則連線至相同子規則或端點，並且您希望刪除其中一個連線，請將游標停留在要刪除的連線上，然後按一下該連線的 x。

9. 選擇 Create traffic policy (建立流量政策)。
10. 選用：在 Create policy records with traffic policy (用流量政策建立政策記錄) 頁面上，使用新的流量政策在一個託管區域中建立一或多個政策記錄。如需詳細資訊，請參閱 您在建立或更新政策記錄時指定的值。您也可以稍後在相同的託管區域或其他託管區域中建立政策記錄。

    如果您不希望現在建立政策記錄，請選擇 Skip this step (略過此步驟)，主控台會顯示您使用目前 AWS 帳戶建立的流量政策和政策記錄清單。
11. 如果您在先前步驟中指定了政策記錄的設定，請選擇 Create policy record (建立政策記錄)。

在建立流量政策時指定的值

在建立流量政策時，指定下列值。

-
-
-
-
-
-
-

政策名稱

輸入描述流量政策的名稱。這個值會顯示在主控台中的流量政策清單。流量政策的名稱在建立後無法變更。

版本

當您建立流量政策或新版本的現有政策，由 Amazon Route 53 自動指派這個值。

版本描述

輸入適用於此版本的流量政策的說明。這個值會顯示在主控台中的流量政策版本清單。

DNS 類型

使用此流量政策版本建立政策記錄時，選擇您希望 Amazon Route 53 指派給所有記錄的 DNS 類型。如需支援的類型清單，請參閱支援的 DNS 記錄類型。

> **Important**
>
> 如果您要建立新版本的現有流量政策，可以變更 DNS 類型。不過，您無法編輯政策記錄，並選擇具有不同 DNS 類型的流量政策版本 (相較於用來建立該政策記錄的流量政策版本)。例如，如果您使用 DNS type (DNS 類型) 為 A 的流量政策版本建立政策記錄，則無法編輯該政策記錄和選擇具有任何其他 DNS type (DNS 類型) 值的流量政策版本。

如果要將流量路由到以下 AWS 資源，請選擇適用的值：

- CloudFront 發佈 — 選擇 A：IPv4 格式的 IP 位址或 AAAA：IPv6 格式的 IP 位址。
- ELB Application Load Balancer：選擇 A：IPv4 格式的 IP 地址或 AAAA：IPv6 格式的 IP 地址。
- ELB Classic Load Balancer：選擇 A：IPv4 格式的 IP 地址或 AAAA：IPv6 格式的 IP 地址。
- ELB Network Load Balancer：選擇 A：IPv4 格式的 IP 地址 或 AAAA：IPv6 格式的 IP 地址。
- Elastic Beanstalk 環境：選擇 A：IPv4 格式的 IP 地址。
- 設定為網站端點的 Amazon S3 儲存貯體：選擇 A: IP address in IPv4 format (A：IPv4 格式的 IP 地址)。

連線到

根據您的組態設計，選擇適用的規則或端點。

容錯移轉規則

當您要設定主動-被動容錯移轉時，請選擇此選項，在此情況下，一個資源會在可用時接受所有流量，而另一個資源會在第一個資源不可用時接受所有流量。

如需詳細資訊，請參閱 主動-被動容錯移轉。

地理位置規則

當您希望 Amazon Route 53 根據使用者的位置來回應 DNS 查詢，請選擇此選項。

如需詳細資訊，請參閱 地理位置路由。

當您選擇 Geolocation rule (地理位置規則) 時，也請選擇發出請求的來源國家/地區或美國州別。

延遲規則

當您在多個 Amazon EC2 資料中心擁有多個執行相同功能的資源，並且您希望 Route 53 使用提供最佳延遲的資源來回應 DNS 查詢時，請選擇此選項。

當您選擇延遲規則時，也請選擇 AWS 區域。

如需詳細資訊，請參閱 以延遲為基礎的路由。

地理位置鄰近性規則

當您希望 Route 53 根據資源位置和 (選用) 指定的偏差來回應 DNS 查詢時，請選擇此選項。偏差可讓您將更多流量傳送到資源，或者從資源中移出更多流量。

當您選擇 Geoproximity rule (地理位置鄰近性規則) 時，請輸入下列值：

端點位置

請選擇適用的值：

- Custom (enter coordinates) (自訂 (輸入座標)) - 如果您的端點不是 AWS 資源，請選擇 Custom (enter coordinates) (自訂 (輸入座標))。
- AWS 區域：如果您的端點是 AWS 資源，請選擇您從中建立資源的 AWS 區域。
- AWS Local Zones：如果您的端點是 AWS 資源，請選擇您從中建立資源的 AWS Local Zones。

如果您使用 AWS Local Zones，則必須先啟用它們。如需詳細資訊，請參閱《AWS Local Zones 使用者指南》中的本機區域入門。

如需可用的 Local Zone，請參閱 AWS Local Zones locations。

若要了解 AWS 區域 和 Local Zone 之間的差異，請參閱《Amazon EC2 使用者指南》中的區域 (Region) 和區域 (Zone)。

> **Important**
>
> 單一地理位置鄰近性路由政策不能含有兩個或多個地理上位於相同都會區域內的位置。

此外，部分 AWS 區域 和當地區域彼此位置太近，例如美國西部 (奧勒岡) 和美國波特蘭，無法在相同的地理位置鄰近性路由政策中使用。如果您需要將流量路由傳送至相同都會區域內的多個位置，請改為定義會對區域中兩個不同的端點採用 50/50 加權路由規則 (WRR) 的地理位置鄰近性路由政策，以在這些端點之間平均分配流量。

座標

如果您為 Endpoint location (端點位置) 選擇 Custom (enter coordinates) (自訂 (輸入座標))，請輸入資源位置的經緯度。注意下列事項：

- 緯度代表赤道以南 (負) 或以北 (正) 的位置。有效值為 -90 度到 90 度。
- 經度代表本初子午線以西 (負) 或以東 (正) 的位置。有效值為 -180 度到 180 度。
- 您可以從一些線上地圖應用程式取得經緯度。例如，在 Google Maps，位置的 URL 指定經緯度：

  https://www.google.com/maps/@47.6086111,-122.3409953,20z
- 您最多可以輸入兩位精度小數，例如，47.63。如果指定更高精度的值，Route 53 會將該值截斷到小數點後的兩位數。對於赤道處的緯度和經度，0.01 度大約是 0.69 英里。

偏差

若要選擇性地變更 Route 53 從中將流量路由至資源的地理區域大小，請為 Bias (偏差) 指定適用的值：

- 若要擴大 Route 53 從中將流量路由到資源的地理區域大小，請為偏差指定介於 1 到 99 之間的正整數。Route 53 縮小相鄰區域的大小。
- 若要縮小 Route 53 從中將流量路由到資源的地理區域大小，請為偏差指定介於 -1 到 -99 之間的負整數。Route 53 擴大相鄰區域的大小。

> **Important**
>
> 變更 Bias (偏差) 值的效果是相對的 (根據其他資源的位置)，而不是絕對的 (根據距離)。因此，變更的效果難以預測。例如，根據資源所在的位置，將偏差從 10 變更為 15 可能意味著在紐約市大都會地區增加或減去大量流量之間的差異。我們建議您以較小的增量變更偏差並對結果進行評估，然後進行其他變更 (如果適用)。

如需詳細資訊，請參閱 地理鄰近路由。

多值回答規則

當您希望 Route 53 用隨機選擇的最多大約八個正常回答來回應 DNS 查詢時，請選擇此選項。

如需詳細資訊，請參閱 多值回答路由。

加權規則

當您具有執行相同功能的多個資源 (例如，服務相同網站的 Web 伺服器)，並希望 Route 53 按照您指定的比例 (例如，1/3 路由到一個伺服器，2/3 路由到另一個伺服器) 將流量路由到這些資源時，請選擇此選項。

當您選擇 Weighted rule (加權規則) 時，請輸入要套用至此規則的權重。

如需詳細資訊，請參閱 加權路由。

端點

選擇此選項可指定要路由 DNS 查詢的資源，例如 CloudFront 分配或 Elastic Load Balancing 負載平衡器。

現有規則

當您想要將 DNS 查詢路由到此流量政策中的現有規則時，請選擇此選項。例如，您可以建立兩個或多個地理位置規則，這些規則會將不同國家/地區的查詢路由到同一個容錯移轉規則。然後該容錯移轉規則可能會將查詢路由到兩個 Elastic Load Balancing 負載平衡器。

如果流量政策不包含任何規則，此選項不可用。

現有端點

當您想要將 DNS 查詢路由到現有端點時，請選擇此選項。例如，如果您有兩個容錯移轉規則，您可能需要兩個在容錯移轉時 (次要) 選項的 DNS 查詢路由至相同 Elastic Load Balancing 負載平衡器。

如果流量政策不包含任何端點，此選項不可用。

值類型

請選擇適用的選項：

CloudFront 分佈

如果您要將流量路由到 CloudFront 分發，請選擇此選項。只有當您為 DNS 類型選擇 A：IPv4 格式的 IP 地址或為 DNS 類型選擇 AAAA：IPv6 格式的 IP 地址時，此選項才可用。

ELB Application Load Balancer

如果要將流量路由到 Elastic Load Balancing Application Load Balancer，請選擇此選項。只有在針對 DNS type (DNS 類型) 選擇 A: IP address in IPv4 format (A：IPv4 格式的 IP 地址) 或 AAAA: IP address in IPv6 format (AAAA：IPv6 格式的 IP 地址) 時，此選項才可用。

ELB Classic Load Balancer

如果要將流量路由到 Elastic Load Balancing Classic Load Balancer，請選擇此選項。只有在針對 DNS type (DNS 類型) 選擇 A: IP address in IPv4 format (A：IPv4 格式的 IP 地址) 或 AAAA: IP address in IPv6 format (AAAA：IPv6 格式的 IP 地址) 時，此選項才可用。

ELB Network Load Balancer

如果要將流量路由到 Elastic Load Balancing Network Load Balancer，請選擇此選項。只有在針對 DNS type (DNS 類型) 選擇 A: IP address in IPv4 format (A：IPv4 格式的 IP 地址) 或 AAAA: IP address in IPv6 format (AAAA：IPv6 格式的 IP 地址) 時，此選項才可用。

Elastic Beanstalk 環境

如果要將流量路由到 Elastic Beanstalk 環境，請選擇此選項。只有在針對 DNS type (DNS 類型) 選擇 A: IP address in IPv4 format (A：IPv4 格式的 IP 地址) 時，此選項才可用。

S3 網站端點

如果要將流量路由到設定為網站端點的 Amazon S3 儲存貯體，請選擇此選項。只有在針對 DNS type (DNS 類型) 選擇 A: IP address in IPv4 format (A：IPv4 格式的 IP 地址) 時，此選項才可用。

類型 DNS 類型值

如果您希望 Route 53 使用 Value (值) 欄位的值來回應 DNS 查詢，請選擇此選項。例如，如果您在建立此流量政策時針對 DNS type (DNS 類型) 的值選擇 A，Value type (值類型) 清單中的此選項將會 Type A value (類型 A 值)。這需要您在 Value (值) 欄位中輸入 IPv4 格式的 IP 地址。Route 53 會使用 Value (值) 欄位中的 IP 地址，來回應路由至此端點的 DNS 查詢。

值

根據您針對 Value type (值類型) 選擇的選項，選擇或輸入值：

CloudFront 分佈

從與目AWS前科目相關聯的分配清單中選擇分配。 CloudFront

ELB Application Load Balancer

從與目前 AWS 帳戶關聯的負載平衡器清單中選擇 Elastic Load Balancing Application Load Balancer。

ELB Classic Load Balancer

從與目前 AWS 帳戶關聯的負載平衡器清單中選擇 Elastic Load Balancing Classic Load Balancer。

ELB Network Load Balancer

從與目前 AWS 帳戶關聯的負載平衡器清單中選擇 Elastic Load Balancing Network Load Balancer。

Elastic Beanstalk 環境

從與目前 AWS 帳戶 關聯的環境清單中選擇 Elastic Beanstalk 環境。

S3 網站端點

從與目前 AWS 帳戶建立關聯且設定為網站端點的 Amazon S3 儲存貯體清單中選擇 Amazon S3 儲存貯體。

> **Important**
>
> 當您根據此流量政策建立政策記錄時，您在此處選擇的儲存貯體必須與您在政策記錄中為 Policy record DNS name 指定的網域名稱 (如 www.example.com) 相符。如果 Value (值) 和 Policy record DNS name (政策記錄 DNS 名稱) 不相符，Amazon S3 不會回應該網域名稱的 DNS 查詢。

類型 DNS 類型值

輸入值，該值對應於您在啟動此流量政策時針對 DNS type (DNS 類型) 指定的值。例如，如果您針對 DNS type (DNS 類型) 選擇 MX，請輸入兩個值：您希望指派給郵件伺服器的優先順序，以及該郵件伺服器的網域名稱 (如 `10 sydney.mail.example.com`)。

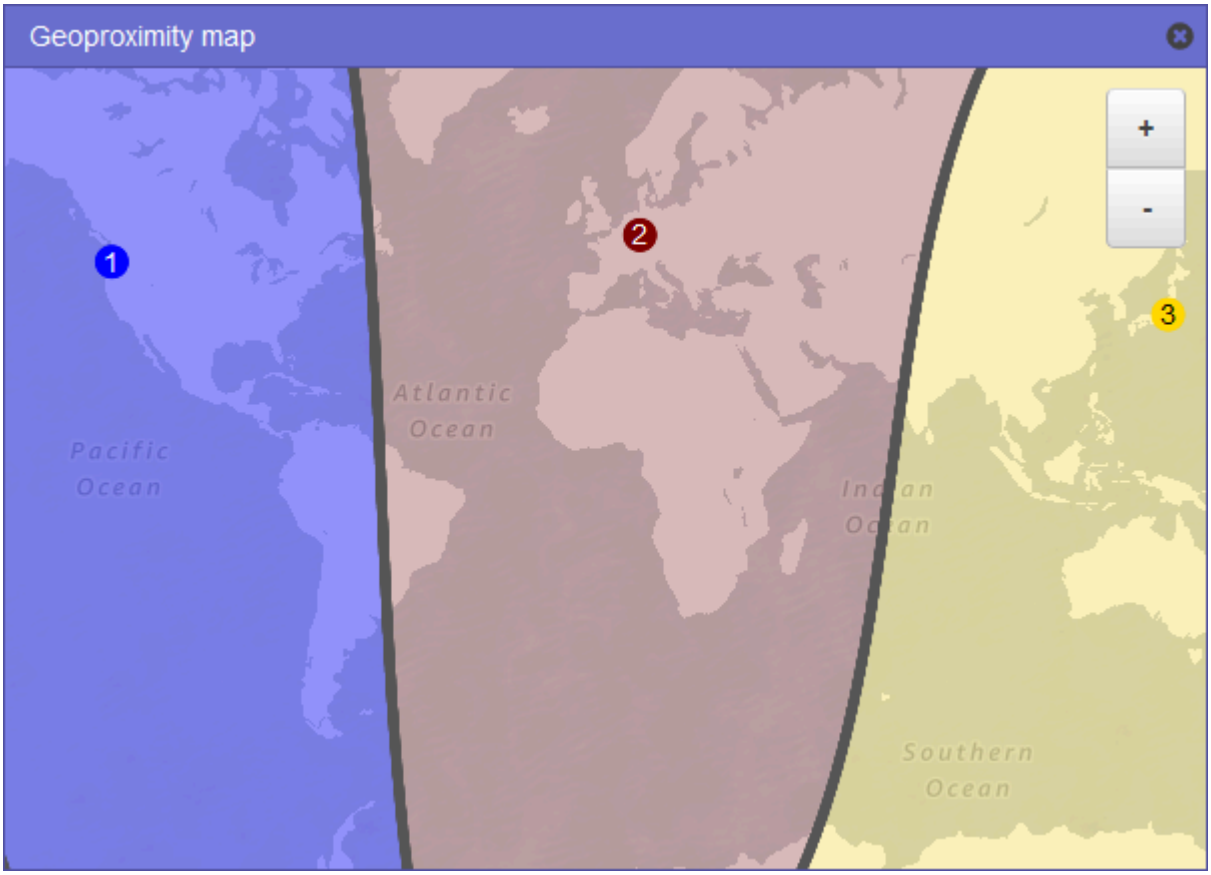
如需支援的 DNS 類型的詳細資訊，請參閱支援的 DNS 記錄類型。

檢視顯示地理位置鄰近性設定效果的地圖

地理位置鄰近性規則可讓您在 AWS 區域 或 Local Zone 指定資源的位置，以及在非 AWS 位置使用經緯度指定資源的位置。當您建立地理位置鄰近性規則時，依預設，Route 53 會將網際網路流量路由至

離使用者最近的資源。您也可以透過指定偏差 (可擴大或縮小流量從中路由至資源的地理區域大小)，選擇將較多流量或較少流量路由至資源。如需地理位置鄰近性路由的詳細資訊，請參閱地理鄰近路由。

您可以顯示地圖，來顯示出目前地理位置鄰近性設定的效果。例如，如果您在美國西部 (奧勒岡)、歐洲 (法蘭克福) 和亞太區域 (東京) 區域中擁有資源，且如果您不指定偏差，則地圖將如下所示。



若要顯示地理位置鄰近性規則的地圖，請選擇顯示地理位置鄰近性地圖旁的圖形圖示。(此圖示會顯示在規則上方。) 若要隱藏地圖，請再次選擇圖示，或選擇地圖右上角的 x。

注意下列事項：

- 地圖的精確度誤差約為 10 英里 (16 公里)。
- 當您新增、編輯或刪除區域，或是變更區域的偏差設定時，地圖會自動調整。
- 每個規則定義中的區域號碼和顏色與地圖上的號碼和顏色對應。
- 您可以放大和縮小，以查看較多或較少詳細資訊。使用地圖上的 + 和 - 按鈕、觸控板或滑鼠滾輪來變更縮放層級。
- 您可以在地圖視窗內移動地圖，以查看特定區域。使用觸控板或以滑鼠按一下並拖曳地圖。您也可以在瀏覽器視窗中移動地圖視窗。
- 如果您在政策中具有多個地理位置鄰近性規則，您一次只能查看一個規則的地圖。

建立其他版本的流量政策

當您編輯流量政策，Amazon Route 53 會自動建立另一個版本的流量政策並保留之前的版本，除非您選擇將它們刪除。新版本與您正在編輯的流量政策同名；它與原始版本的區別在於 Route 53 自動遞增的版本編號。您可以在同名的流量政策的任何現有版本的基礎上建立流量政策的新版本。

對於指定流量政策的新版本，Route 53 不會重複使用版本編號。例如，如果您建立了三個版本 MyTrafficPolicy，刪除最後兩個版本，然後建立另一個版本，則新版本為版本 4。透過保留之前的版本，Route 53 可確保當新組態不按您希望的方式來路由流量時，您可以復原到之前的組態。

若要建立新的流量政策版本，請執行下列程序。

若要建立另一個版本的流量政策

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Traffic policies (流量政策)。
3. 選擇您要建立其新版本的流量政策的名稱。
4. 在頁面頂端的 Traffic policy versions (流量政策版本) 表格中，選取要做為新流量政策版本基礎的流量政策版本核取方塊。
5. 選擇 Edit policy as new version (將政策編輯為新版本)。
6. 在 Update description (更新描述) 頁面，輸入新流量政策版本的描述。建議您指定可區別該版本與相同流量政策的其他版本的描述。當您建立新的政策記錄，您指定的值會顯示在此流量政策的可用版本清單中。
7. 選擇下一步。
8. 更新組態 (如適用)。如需詳細資訊，請參閱 在建立流量政策時指定的值。

   您可以透過以下方式刪除流量政策的規則、端點和分支：

   - 若要刪除規則或端點，請按一下方塊右上角的 x。

     > **Important**
     >
     > 如果您刪除有子規則和端點的規則，Route 53 也會刪除所有子系。

   - 如果將兩個規則連線至相同子規則或端點，並且您希望刪除其中一個連線，請將游標停留在要刪除的連線上，然後按一下該連線的 x。

9. 當您完成編輯，請選擇 Save as new version (儲存為新版本)。
10. 選用：指定設定，透過使用新的流量政策，在單一託管區域中建立一或多個政策記錄版本。如需詳細資訊，請參閱 您在建立或更新政策記錄時指定的值。您也可以稍後在相同的託管區域或其他託管區域中建立政策記錄。

    如果您不希望現在建立政策記錄，請選擇 Skip this step (略過此步驟)，主控台會顯示您使用目前 AWS 帳戶建立的流量政策和政策記錄清單。
11. 如果您在先前步驟中指定了政策記錄的設定，請選擇 Create policy record (建立政策記錄)。

透過匯入 JSON 文件來建立流量政策

您可以透過匯入 JSON 格式的文件來建立新的流量政策或新版本的現有流量政策，該文件描述要包含在流量政策中的所有端點和規則。如需有關 JSON 文件格式以及多個可複製和修改的範例的資訊，請參閱 Amazon Route 53 API 參考中的流量政策文件格式。

取得現有流量政策版本的 JSON 格式文件的最簡單方法，是使用 AWS CLI 中的 `get-traffic-policy` 命令。如需詳細資訊，請參閱 AWS CLI 命令參考中的 get-traffic-policy。

`get-traffic-policy` 命令建立的 JSON 檔案包含反斜線 (\) 作為逸出字元。匯入 JSON 檔案之前，請以 null 字元取代所有反斜線。

若要透過匯入 JSON 文件來建立流量政策

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 若要透過匯入 JSON 文件來建立新的流量政策，請執行以下步驟：
   a. 在導覽窗格中，選擇 Traffic policies (流量政策)。
   b. 選擇 Create traffic policy (建立流量政策)。
   c. 在 Name policy (名稱政策) 頁面，指定適用的值。如需詳細資訊，請參閱 在建立流量政策時指定的值。
   d. 跳至步驟 4。
3. 若要透過匯入 JSON 文件來建立新版本的現有流量政策，請執行以下步驟：
   a. 在導覽窗格中，選擇 Traffic policies (流量政策)。
   b. 選擇要做為新版本的基礎的流量政策的名稱。
   c. 在 Traffic policy versions (流量政策版本) 表格中，選取要做為新版本的基礎版本核取方塊。

d. 選擇 Edit policy as new version (將政策編輯為新版本)。
e. 在 Update description (更新描述) 頁面，輸入新版本的描述。
f. 跳至步驟 4。

4. 選擇下一步。
5. 選擇 Import traffic policy (匯入流量政策)。
6. 輸入新的流量政策、貼上範例流量政策，或貼上現有的流量政策。
7. 選擇 Import traffic policy (匯入流量政策)。

檢視流量政策版本和關聯的政策記錄

您可以檢視為流量政策建立的所有版本，以及透過使用該流量政策的每個版本建立的所有政策記錄。

若要檢視流量政策版本和關聯的政策記錄

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Traffic policies (流量政策)。
3. 選擇流量政策的名稱。
4. 頂端表格列出您建立的流量政策的所有版本。此表格包含以下資訊：

   版本編號

   您建立的流量政策的每個版本的號碼。如果您選擇版本編號，主控台會顯示該版本的組態。

   政策記錄的數目

   透過使用此流量政策版本，建立的政策記錄數目。

   DNS 類型

   建立流量政策版本時，指定的 DNS 類型。

   版本描述

   建立流量政策版本時，指定的描述。

5. 底部表格列出透過使用頂端表格中的流量政策版本所建立的所有政策記錄。此表格包含以下資訊：

   政策記錄 DNS 名稱

   您已將流量政策與之關聯的 DNS 名稱。

Status

可能的值包括以下：

已套用

Route 53 已完成建立或更新政策記錄和對應的記錄。

正在建立

Route 53 正在建立新政策記錄的記錄。

更新中

您已更新政策記錄，而且 Route 53 正在建立一組新的記錄，以取代指定 DNS 名稱的一組現有記錄。

正在刪除

Route 53 正在刪除政策記錄和關聯的記錄。

失敗

Route 53 無法建立或更新政策記錄和關聯的記錄。

已使用的版本

指示用來建立政策記錄的流量政策版本。

DNS 類型

Route 53 為此政策記錄建立的所有記錄的 DNS 類型。當您編輯政策記錄，必須指定具有相同 DNS 類型的流量政策版本 (相較於要編輯的政策記錄的 DNS 類型)。

TTL (以秒為單位)

您要 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。如果您指定較長的值 (例如 172,800 秒或兩天)，您會支付較低的 Route 53 服務費用，因為遞迴解析程式傳送請求至 Route 53 的頻率會降低。不過，需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式使用其快取中的值更久，而不是要求 Route 53 提供最新資訊。

刪除流量政策版本和流量政策

若要刪除流量政策，您必須刪除為該流量政策建立的所有版本 (包括原始版本)。此外，若要刪除流量政策版本，您必須刪除透過使用該流量政策版本所建立的所有政策記錄。

> **Important**
>
> 如果您刪除 Amazon Route 53 用來回應 DNS 查詢的政策記錄，Route 53 會停止回應對應 DNS 名稱的查詢。例如，如果 Route 53 使用 www.example.com 的政策記錄來回應 www.example.com 的 DNS 查詢，而且您刪除該政策記錄，您的使用者就無法透過使用網域名稱 www.example.com 來存取您的網站或 Web 應用程式。

若要刪除流量政策版本以及 (選用) 流量政策，請執行以下步驟：

若要刪除流量政策版本和流量政策

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Traffic policies (流量政策)。
3. 選擇要針對其刪除流量政策版本且 (選用) 要完全刪除的流量政策的名稱。
4. 如果您希望在頂端表格上刪除的流量政策版本，顯示於底部表格中的 Version used (已使用的版本) 欄，請選取底部表格中對應政策記錄的核取方塊。

   例如，如果要刪除流量政策的版本 3，但是透過使用版本 3 建立了底部表格中的政策記錄之一，請選取該政策記錄的核取方塊。
5. 選擇 Delete policy records (刪除政策記錄)。
6. 選擇底部表格的重新整理按鈕來重新整理顯示，直到刪除的政策記錄不再出現在表格中。
7. 在頂端表格，選取要刪除的流量政策版本的核取方塊。
8. 選擇 Delete version (刪除版本)。
9. 如果已刪除之前步驟中的所有流量政策版本，而且還要刪除流量政策，請選擇頂端表格的重新整理按鈕來重新整理顯示，直到表格清空為止。
10. 在導覽窗格中，選擇 Traffic policies (流量政策)。
11. 在流量政策清單，選取要刪除的流量政策的核取方塊。
12. 選擇 Delete traffic policy (刪除流量政策)。

建立和管理政策記錄

在您建立流量政策時，若要將網際網路流量路由到您指定的資源，您可以建立一或多個政策記錄。每個政策記錄皆可識別您要建立政策記錄的託管區域，以及您希望將流量路由到哪個網域或子網域名稱。例

如，如果您要路由 www.example.com 的流量，您必須指定 example.com 託管區域的託管區域 ID，而且必須指定 www.example.com 做為政策記錄 DNS 名稱。

如果您要使用相同的流量政策，路由多個網域或子網域名稱的流量，您有兩個選擇：

- 您可以為每個網域或子網域名稱建立政策記錄。
- 您可以建立一個政策記錄，然後建立參照至該政策記錄的 CNAME 或別名記錄。

例如，如果您要為 example.com、example.net 及 example.org 使用相同的流量政策，您可以執行以下步驟之一：

- 為每個網域各建立一個政策記錄。
- 為其中一個網域建立一個政策記錄，然後在其他兩個網域的託管區域中建立 CNAME 記錄。您必須在這兩個 CNAME 記錄中指定所建立政策記錄的記錄名稱。

如果您要為一個網域及其子網域 (例如 example.com 與 www.example.com) 使用相同的流量政策，您可以為其中一個名稱建立一個政策記錄，然後為另一個名稱建立別名記錄。例如，您可以為 example.com 建立一個政策記錄，然後為使用 example.com 記錄做為其別名目標的 www.example.com 建立別名記錄。

> **Note**
>
> 您建立的每個政策記錄都會產生月費。如果您要為多個網域或子網域名稱使用相同的流量政策，您可以使用 CNAME 或別名記錄以降低您的費用：
>
> - 如果您建立一個政策記錄以及一或多個參照至該政策記錄檔 CNAME 記錄，您只需支付政策記錄以及 CNAME 記錄的 DNS 查詢的費用。
> - 如果您建立一個政策記錄，並且在參照至該政策記錄檔託管區域中建立一或多個別名記錄，您只需支付政策記錄以及別名記錄的 DNS 查詢的費用。

主題

- 建立政策記錄
- 您在建立或更新政策記錄時指定的值
- 更新政策記錄
- 刪除政策記錄

建立政策記錄

若要建立政策記錄，請執行下列程序。

> **Important**
>
> 對於建立的每個政策記錄，會產生月費。如果您稍後刪除政策記錄，我們會按比例收取費用。如需詳細資訊，請參閱 Amazon Route 53 定價頁面上的「流量流程」區段。

若要建立政策記錄

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Policy records (政策記錄)。
3. 在 Policy records (政策記錄) 頁面，選擇 Create policy records (建立政策記錄)。
4. 在 Create policy records (建立政策記錄) 頁面，指定適用的值。如需詳細資訊，請參閱 您在建立或更新政策記錄時指定的值。
5. 選擇 Create policy records (建立政策記錄)。

   建立的政策記錄狀態可能需要幾分鐘時間才能顯示為已套用。
6. 如果要在其他託管區域中建立政策記錄，重複步驟 3 到 5。

> **Note**
>
> 如果政策記錄狀態為失敗，請選擇狀態旁邊的資訊按鈕，以取得有關失敗的詳細資訊。如果您需要進一步協助並想要聯絡 AWS Support，請參閱 How do I get technical support from AWS?

您在建立或更新政策記錄時指定的值

在建立或更新政策記錄時指定以下值

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name

- TTL

流量政策

選擇要將其組態用於此政策記錄的流量政策。

版本

選擇要將其組態用於此政策記錄的流量政策版本。

如果要更新現有的政策記錄，則必須選擇 DNS 類型與政策記錄的目前 DNS 類型相符的版本。例如，如果政策記錄的 DNS 類型是 A，您必須選擇 DNS 類型為 A 的版本。

託管區域

選擇託管區域，您要在該託管區域中使用指定的流量政策和版本建立政策記錄。在建立政策記錄後，即無法變更 Hosted zone (託管區域) 的值。

政策記錄 DNS 名稱

建立政策記錄時，請使用指定流量政策和版本中的組態，輸入您希望 Route 53 回應 DNS 查詢的網域名稱或子網域名稱。

若要在指定託管區域中為多個網域名稱或子網域名稱使用相同的組態，請選擇 Add another policy record (新增另一個政策記錄)，然後輸入適用的網域名稱或子網域名稱和 TTL。

在建立政策記錄後，即無法變更 Policy record DNS name (政策記錄 DNS 名稱) 的值。

TTL (以秒為單位)

輸入您希望 DNS 遞迴解析程式快取此記錄相關資訊的時間長度 (以秒為單位)。如果您指定較長的值 (例如 172800 秒或兩天)，您會支付較低的 Route 53 服務費用，因為遞迴解析程式傳送要求至 Route 53 的頻率會降低。不過，需要更長的時間才能讓記錄變更 (例如新的 IP 地址) 生效，因為遞迴解析程式使用其快取中的值更久，而不是要求 Route 53 提供最新資訊。

更新政策記錄

若要更新政策記錄，請執行下列程序。

若要更新政策記錄

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。

2. 在導覽窗格中，選擇 Policy records (政策記錄)。
3. 在 Policy records (政策記錄) 頁面，選取要更新的政策記錄核取方塊，然後選擇 Edit policy record (編輯政策記錄)。
4. 在 Edit policy record (編輯政策記錄) 頁面，指定適用的值。如需詳細資訊，請參閱 您在建立或更新政策記錄時指定的值。
5. 選擇 Edit policy record (編輯政策記錄)。

   建立的政策記錄狀態可能需要幾分鐘時間才能顯示為已套用。
6. 如果要更新其他政策記錄，重複步驟 3 到 5。

> **Note**
>
> 如果政策記錄狀態為失敗，請選擇狀態旁邊的資訊按鈕，以取得有關失敗的詳細資訊。如果您需要進一步協助並想要聯絡 AWS Support，請參閱 How do I get technical support from AWS?

刪除政策記錄

若要刪除政策記錄，請執行下列程序。

> **Important**
>
> 如果您刪除 Amazon Route 53 用來回應 DNS 查詢的政策記錄，Route 53 會停止回應對應 DNS 名稱的查詢。例如，如果 Route 53 使用 www.example.com 的政策記錄來回應 www.example.com 的 DNS 查詢，而且您刪除該政策記錄，您的使用者就無法透過使用網域名稱 www.example.com 來存取您的網站或 Web 應用程式。

若要刪除政策記錄

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Policy records (政策記錄)。
3. 在 Policy records (政策記錄) 頁面，選取要刪除的政策記錄核取方塊，然後選擇 Delete policy record (刪除政策記錄)。

   請等待數分鐘，然後重新整理頁面，以確保政策記錄從清單中消失。

在 Amazon Route 53 中設定 DNSSEC 簽署

網域名稱系統安全延伸 (DNSSEC) 簽署可讓 DNS 解析程式驗證 DNS 回答是否來自 Amazon Route 53，並且未遭到竄改。當您使用 DNSSEC 簽署時，託管區域的每個回應都會使用公有金鑰密碼編譯來簽署。

在本章中，我們將說明如何啟用 Route 53 的 DNSSEC 簽署、如何使用 key-signing keys (金鑰簽署金鑰) (KSK)，以及如何排除問題。您可以在中使用 DNSSEC 簽署， AWS Management Console 或以程式設計方式使用 API。如需有關藉助 CLI 或開發套件來使用 Route 53 的詳細資訊，請參閱 設定 Amazon Route 53。

啟用 DNSSEC 簽署之前，請注意下列事項：

- 若要協助防止區域中斷，並避免網域無法使用的問題，您必須快速處理並解決 DNSSEC 錯誤。我們強烈建議您設定警示，以便在偵測到`DNSSECInternalFailure`或`DNSSECKeySigningKeysNeedingAction`錯誤時向您發出警示。 CloudWatch 如需詳細資訊，請參閱 使用 Amazon 監控託管區域 CloudWatch。
- DNSSEC 中有兩種金鑰：金鑰簽署金鑰 (KSK) 和區域簽署金鑰 (ZSK)。在 Route 53 DNSSEC 簽署中，每個 KSK 均基於您所擁有的 AWS KMS 中的非對稱客戶受管金鑰。您必須負責 KSK 管理，其中包括在需要時輪換它。ZSK 管理由 Route 53 進行。
- 當您啟用託管區域的 DNSSEC 簽署時，Route 53 會將 TTL 限制為一週。如果您為託管區域中的記錄設定超過一週的 TTL，則不會收到錯誤。不過，Route 53 會為該記錄強制執行一週的 TTL。對於 TTL 不到一週的記錄，以及在未啟用 DNSSEC 簽章的其他託管區域中的記錄，則不會受到影響。
- 當您使用 DNSSEC 簽章時，不支援多廠商組態。如果您已設定白標籤名稱伺服器 (也稱為虛名伺服器或私有名稱伺服器)，請確定這些名稱伺服器是由單一 DNS 提供者提供。
- 某些 DNS 提供者在其授權 DNS 中不支援委派簽署人 (DS) 記錄。如果您的父區域是由不支援 DS 查詢 (未在 DS 查詢回應中設定 AA 旗標) 的 DNS 提供者託管，則當您在其子區域中啟用 DNSSEC 時，子區域將會變成無法解析。請確定您的 DNS 供應商支援 DS 記錄。
- 設定 IAM 許可，以允許區域擁有者以外的其他使用者新增或移除區域中的記錄，這樣會很有幫助。例如，區域擁有者可以新增 KSK 並啟用簽署，也可能負責金鑰輪換。不過，其他人可能負責處理該託管區域的其他記錄。如需 IAM 政策範例，請參閱 網域記錄擁有者的許可範例。

主題

- 啟用 DNSSEC 簽署並建立信任鏈
- 停用 DNSSEC 簽署
- 使用 DNSSEC 的客戶受管金鑰

- 使用金鑰簽署金鑰 (KSK)
- Route 53 中的 KMS 金鑰和 ZSK 管理
- DNSSEC 不存在於 Route 53 中的證明
- DNSSEC 簽署故障診斷

啟用 DNSSEC 簽署並建立信任鏈

遞增步驟適用於託管區域擁有者和父區域維護者。這可以是同一個人，但如果不是，區域擁有者應通知父區域維護者並與其合作。

我們建議您按照本文中的步驟簽署您的區域並將其納入信任鏈中。以下步驟會將加入 DNSSEC 的風險降至最低。

> **Note**
>
> 在開始之前，請務必先閱讀 在 Amazon Route 53 中設定 DNSSEC 簽署 中的先決條件。

啟用 DNSSEC 簽署需要執行三個步驟，如以下章節所述。

主題

- 步驟 1：準備啟用 DNSSEC 簽署
- 步驟 2：啟用 DNSSEC 簽署並建立 KSK
- 步驟 3：建立信任鏈

步驟 1：準備啟用 DNSSEC 簽署

準備步驟透過監控區域可用性並縮短啟用簽署與插入委派簽署人 (DS) 記錄之間的等待時間，協助您將加入 DNSSEC 的風險降至最低。

準備啟用 DNSSEC 簽署

1. 監控區域可用性。

   您可以監控該區域在您網域名稱中的可用性。此可協助您處理在啟用 DNSSEC 簽署後可能需要倒回步驟的任何問題。您可以藉由使用查詢日誌記錄，監控具有大部分流量的網域名稱。如需設定查詢日誌記錄的詳細資訊，請參閱 監控 Amazon Route 53。

可以透過 Shell 指令碼或透過第三方服務進行監控。但是，其不應是判斷是否需要回復的唯一信號。您也可能會因為網域名稱不可用，而得到來自客戶的反饋。

2. 降低區域的最大 TTL。

   區域的最大 TTL 是區域中最長的 TTL 記錄。在以下區域示例中，區域的最大 TTL 為 1 天 (86400 秒)。

名稱	TTL	記錄類別	記錄類型	記錄資料
example.com。	900	IN	SOA	ns1.example.com。hostmaster.example.com。2002022401 10800 1500 604800 300
example.com。	900	IN	NS	ns1.example.com。
route53.example.com。	86400	IN	TXT	**some txt record**

   降低區域的最大 TTL 將有助於縮短啟用簽署與插入委派簽署人 (DS) 記錄之間的等待時間。建議將區域的最大 TTL 降至 1 小時 (3600 秒)。如果解析器在快取簽署記錄時發生任何問題，這讓您在一個小時後即可回復。

   回復：復原 TTL 變更。

3. 降低 SOA TTL 和 SOA 最小值欄位。

   SOA 最小值欄位是 SOA 記錄資料中的最後一個欄位。在以下 SOA 記錄示例中，最小值欄位的值為 5 分鐘（300 秒）。

名稱	TTL	記錄類別	記錄類型	記錄資料
example.com。	900	IN	SOA	ns1.example.com。hostmaster.example.com。2002022401 10800 15604800 300

SOA TTL 和 SOA 最小值欄位決定解析器記住否定答案的時間長度。啟用簽署後，Route 53 名稱伺服器開始傳回用於否定答案的 NSEC 記錄。NSEC 包含解析器可能用於合成否定答案的資訊。如果因為 NSEC 資訊導致解析器對一個名稱給予否定的答案而必須回復，則只需等待 SOA TTL 和 SOA 最小值欄位中的最大值的時間後，解析器即會停止假設。

回復：復原 SOA 變更。

4. 確認 TTL 和 SOA 最小值欄位變更生效。

   用於確保GetChange到目前為止您的更改已傳播到所有 Route 53 DNS 服務器。

步驟 2：啟用 DNSSEC 簽署並建立 KSK

您可以使用 AWS CLI 或在 Route 53 控制台上啟用 DNSSEC 簽名並創建密鑰簽名密鑰（KSK）。

- CLI
- 主控台

當您提供或建立客戶受管的 KMS 金鑰時，有幾點要求需要滿足。如需詳細資訊，請參閱 使用 DNSSEC 的客戶受管金鑰。

CLI

您可以使用您已有的金鑰，或透過使用您自己的 `hostedzone_id`、`cmk_arn`、`ksk_name`，和`unique_string` 的值 (以使請求為唯一) 執行類似如下的 AWS CLI 命令以建立金鑰 ：

```
aws --region us-east-1 route53 create-key-signing-key \
   --hosted-zone-id $hostedzone_id \
   --key-management-service-arn $cmk_arn --name $ksk_name \
   --status ACTIVE \
   --caller-reference $unique_string
```

如需客戶受管金鑰的詳細資訊，請參閱 使用 DNSSEC 的客戶受管金鑰。另請參閱 CreateKeySigningKey。

若要啟用 DNSSEC 簽署，請使用您自己的值來執行類似下列的 AWS CLI 命令：hostedzone_id

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

如需詳細資訊，請參閱enable-hosted-zone-dnssec和 EnableHostedZoneDNSSEC。

Console

啟用 DNSSEC 簽署並建立 KSK

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇託管區域，然後選擇您要啟用 DNSSEC 簽署的託管區域。
3. 在 DNSSEC signing (DNSSEC 簽署) 標籤上，選擇 Enable DNSSEC signing (啟用 DNSSEC 簽署)。

   > **Note**
   >
   > 如果本部分中的選項是 Disable DNSSEC signing (停用 DNSSEC 簽署)，則表明您已完成啟用 DNSSEC 簽署的第一步。請確定您建立或已經存在 DNSSEC 託管區域的信任鏈，然後即可完成此任務。如需詳細資訊，請參閱 步驟 3：建立信任鏈。

4. 在 Key-signing key (KSK) creation (建立金鑰簽署金鑰 (KSK)) 部分中，選擇 Create new KSK (建立新的 KSK), 並在 Provide KSK name (提供 KSK 名稱) 中，輸入 Route 53 將為您建立的 KSK 的名稱。名稱僅能包含字母、數字和底線 (_)。它必須獨一無二。
5. 在 Customer managed CMK (客戶受管的 CMK) 下，請為 Route 53 選擇客戶受管的金鑰，以便在為您建立 KSK 時使用。您可以使用適用於 DNSSEC 簽署的現有客戶受管金鑰，也可以建立新的客戶受管金鑰。

當您提供或建立客戶受管的金鑰時，有幾點要求需要滿足。如需詳細資訊，請參閱 使用 DNSSEC 的客戶受管金鑰。

6. 輸入現有客戶受管金鑰的別名。如果您想要使用新的客戶受管金鑰，請輸入客戶受管金鑰的別名，Route 53 即會為您建立一個金鑰。

> **Note**
>
> 如果您選擇讓 Route 53 建立客戶受管金鑰，請注意每個客戶受管金鑰都要分別支付費用。有關更多資訊，請參閱 AWS 金鑰 Management Service 定價。

7. 選擇 Enable DNSSEC signing (啟用 DNSSEC 簽署)。

啟用區域簽署後，請完成以下步驟 (不論您是使用主控台或是 CLI)：

1. 確認區域簽署已生效。

   如果您使用 AWS CLI，您可以使用來自`EnableHostedZoneDNSSEC()`呼叫輸出的作業識別碼來執行 get-change，或確GetChange定所有 Route 53 DNS 伺服器正在簽署回應 (狀態 =`INSYNC`)。

2. 等待至少前一個區域的最大 TTL 的時間。

   等待解析器清除其快取中所有的未簽署記錄。為此，您應等待至少前一個區域的最大 TTL 的時間。在上述 `example.com` 區域中，等待時間會是 1 天。

3. 監控客戶問題報告。

   啟用區域簽署後，客戶可能會開始看到與網路裝置和解析器有關的問題。建議的監控期為 2 週。

   以下為您可能看到的問題示例：

   - 有些網路裝置可以將 DNS 回答大小限制為 512 位元組以下，這對於有些簽署回答來說太小。應重新設定這些網路裝置，以允許更大的 DNS 回答大小。
   - 有些網路裝置會對 DNS 回答進行深入檢查，並去除有些其不理解的記錄，像是用於 DNSSEC 的記錄。應重新設定這些裝置。
   - 有些客戶的解析器宣稱可以接受比其網路支援的更大的 UDP 回應。您可以測試網路能力並適當地設定解析器。如需詳細資訊，請參閱 DNS 回覆大小測試伺服器。

復原：呼叫 DisableHostedZoneDNSSEC，然後復原中的步驟。步驟 1：準備啟用 DNSSEC 簽署

步驟 3：建立信任鏈

在 Route 53 中啟用託管區域的 DNSSEC 簽署之後，建立託管區域的信任鏈，以完成 DNSSEC 簽署設定。您可以藉由在父託管區域中建立委派簽署人 (DS) 記錄來完成此任務 (使用 Route 53 提供的資訊)。視網域的註冊位置而定，您可以將記錄新增至 Route 53 或其他網域註冊商中的父託管區域。

建立信任鏈以進行 DNSSEC 簽署

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)，然後選擇您想要建立 DNSSEC 信任鏈的託管區域。您必須先啟用 DNSSEC 簽署。
3. 在 DNSSEC signing (DNSSEC 簽署) 標籤中的 DNSSEC signing (DNSSEC 簽署) 下，選擇 View information to create DS record (檢視資訊以建立 DS 記錄)。

   > **Note**
   >
   > 如果您看不到 View information to create DS record (檢視資訊以建立 DS 記錄)，則必須先啟用 DNSSEC 簽署，才能建立信任鏈。選擇 Enable DNSSEC signing (啟用 DNSSEC 簽署) 並完成 步驟 2：啟用 DNSSEC 簽署並建立 KSK 中所述的步驟，然後回到這些步驟以建立信任鏈。

4. 在 Establish a chain of trust (建立信任鏈) 下，選擇 Route 53 registrar (Route 53 註冊商) 或 Another domain registrar (其他網域註冊商)，視您的網域註冊位置而定。
5. 使用步驟 3提供的值，以為 Route 53 中的父託管區域建立 DS 記錄。如果您的網域名稱不在 Route 53 託管，請使用提供的值在網域註冊商網站上建立 DS 記錄。

   - 如果上層區域是透過 Route 53 管理的網域，請依照下列步驟執行：

     請確定您設定正確的簽署演算法 (ECDSAP256SHA256 和類型 13) 和摘要演算法 (SHA-256 和類型 2)。

     如果 Route 53 是您的註冊商，請在 Route 53 主控台中執行以下操作：

     1. 請注意 Key type (金鑰類型)、Signing algorithm (簽署演算法) 以及 Public key (公有金鑰) 值。在導覽窗格中，選擇 Registered domains (已註冊的網域)。
     2. 選取網域，然後在 DNSSEC status (DNSSEC 狀態) 旁邊，選擇 Manage keys (管理金鑰)。
     3. 在 Manage DNSSEC keys (管理 DNSSEC 金鑰) 對話方塊中，從下拉式選單中為 Route 53 registrar (Route 53 註冊商) 選擇適當的 Key type (金鑰類型) 和 Algorithm (演算法)。

4. 複製 Route 53 註冊商的 Public key (公有金鑰)。在 Manage DNSSEC keys (管理 DNSSEC 金鑰)對話方塊中，將值貼到 Public key (公有金鑰) 方塊中。
5. 選擇新增。

   Route 53 會將 DS 記錄從公有金鑰新增至父區域。例如，如果您的網域為 `example.com`，則 DS 記錄會新增至 .com DNS 區域。

- 如果上層區域託管於 Route 53 上，或是在其他註冊處管理網域，請聯絡上層區域或網域註冊擁有者，以遵循下列指示：

  為確保以下步驟順利進行，請對父區域導入一個低 DS TTL。建議將 DS TTL 設為 5 分鐘 (300 秒)，以便在需要回復變更時更快速恢復。

  - 如果您的父區域由其他註冊機構管理，請聯絡您的註冊商以導入您區域的 DS 記錄。一般來說，您將無法調整 DS 記錄的 TTL。
  - 如果您的父區域託管在 Route 53 上，請聯絡父區域擁有者，以導入您區域的 DS 記錄。

    提供 `$ds_record_value` 給父區域擁有者。您可以透過點擊主控台中的 View Information to create DS record (查看資訊以建立 DS 記錄) 並複製 DS record (DS 記錄) 欄位，或透過呼叫 GetDNSSEC API 並檢索 'DSRecord' 欄位的值，取得此資訊：

    ```
    aws --region us-east-1 route53 get-dnssec
                --hosted-zone-id $hostedzone_id
    ```

    父區域擁有者可以透過 Route 53 主控台或 CLI 插入記錄。

    - 若要使用插入 DS 記錄 AWS CLI，父區域擁有者會建立並命名 JSON 檔案，類似下列範例。父區域擁有者可能會將檔案命名為類似 `inserting_ds.json`。

      ```
      {
          "HostedZoneId": "$parent_zone_id",
          "ChangeBatch": {
              "Comment": "Inserting DS for zone $zone_name",
              "Changes": [
                  {
                      "Action": "UPSERT",
                      "ResourceRecordSet": {
                          "Name": "$zone_name",
                          "Type": "DS",
                          "TTL": 300,
                          "ResourceRecords": [
                              {
      ```

```
                            "Value": "$ds_record_value"
                        }
                    ]
                }
            }
        ]
    }
}
```

然後執行以下命令：

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- 若要使用主控台插入 DS 記錄，

  請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。

  在導覽窗格中，選擇 Hosted zones (託管區域)，即託管區域的名稱，然後選擇 Create record (建立記錄) 按鈕。請確認 Routing policy (路由政策) 選擇簡單路由。

  在 Record name (記錄名稱) 欄位中輸入與 `$zone_name` 相同的名稱，在 Record type (記錄類型) 下拉式選單中選擇 DS，然後將 `$ds_record_value` 的值輸入 Value (值) 欄位，然後選擇Create records (建立記錄)。

回復：從父區域中刪除 DS，等待 DS TTL 的時間，然後回到建立信任的步驟。如果父區域託管在 Route 53 上，則父區域擁有者可以在 JSON 檔案將 `Action` 從 `UPSERT` 變更為 `DELETE`，然後重新執上面的 CLI 示例。

6. 根據網域記錄的 TTL，等候更新傳播。

   如果父區域位於 Route 53 DNS 服務上，父區域擁有者可以透過 GetChangeAPI 確認完整傳播。

   否則，您可以定期探測 DS 記錄的父區域，之後再等待 10 分鐘，以提高 DS 記錄插入已完全傳播的概率。請注意，有些註冊商已有 DS 插入排程，例如，每天一次。

當您在父區域中導入委派簽署人 (DS) 記錄時，已取得 DS 的驗證解析器將開始驗證來自區域的回應。

為確保建立信任的步驟順利進行，請完成以下操作：

1. 查找最大 NS TTL。

有兩組與您的區域相關聯的 NS 記錄：

- 委派 NS 記錄 — 這是父區域所持有的您區域的 NS 記錄。您可以藉由執行以下 Unix 命令來查找此記錄 (如果您的區域是 example.com，則父區域是 com)：

  ```
  dig -t NS com
  ```

  選擇其中一個 NS 記錄，然後執行以下操作：

  ```
  dig @one of the NS records of your parent zone -t NS example.com
  ```

  例如：

  ```
  dig @b.gtld-servers.net. -t NS example.com
  ```

- 區域內 NS 記錄 — 這是在您區域中的 NS 記錄。您可以藉由執行以下 Unix 命令來查找此記錄：

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  例如：

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  記下兩個區域的最大 TTL。

2. 等待最大 NS TTL 的時間。

   在 DS 插入之前，解析器會收到簽署回應，但不會驗證簽章。插入 DS 記錄時，在該區域的 NS 記錄過期前，解析器都看不到該記錄。當解析器重新獲取 NS 記錄時，亦將傳回 DS 記錄。

   如果您的客戶在具有不同步時鐘的主機上執行解析器，請確保時鐘在正確時間的 1 小時以內。

   完成此步驟後，所有具有 DNSSEC 意識的解析器都將驗證您的區域。

3. 請觀察名稱解析。

   您應該觀察到，解析器在驗證您的區域方面沒有任何問題。確認您亦將客戶向您報告問題所需要的時間納入考慮。

   我們建議監控長達 2 週。

4. （選用）延長 DS 和 NS TTL。

如果對設定滿意，則可以儲存您所做的 TTL 和 SOA 變更。請注意，Route 53 將已簽署區域的 TTL 限制為 1 週。如需詳細資訊，請參閱 在 Amazon Route 53 中設定 DNSSEC 簽署。

如果您能變更 DS TTL，我們建議您將其設為 1 小時。

停用 DNSSEC 簽署

在 Route 53 中停用 DNSSEC 簽署的步驟會根據您託管區域所屬的信任鏈而有所不同。

例如，您的託管區域可能有一個具有委派簽署人 (DS) 記錄的父區域，其做為信任鏈的一部分。您的託管區域本身也可能是啟用 DNSSEC 簽署之子區域的父區域，這是信任鏈的另一個部分。請先調查並確定託管區域的完整信任鏈，然後再採取步驟停用 DNSSEC 簽署。

當您停用簽署時，必須小心復原啟用 DNSSEC 簽署之託管區域的信任鏈。若要從信任鏈中移除託管區域，您可以移除包含此託管區域之信任鏈的所有 DS 記錄。這表示您必須依序執行下列作業：

1. 針對屬於信任鏈一部分的子區域，移除此託管區域擁有的任何 DS 記錄。
2. 移除父區域的 DS 記錄。如果您擁有信任島 (父區域中沒有 DS 記錄，且此區域中沒有子區域的 DS 記錄)，則可以略過此步驟。
3. 如果您無法移除 DS 記錄，則為了從信任鏈中移除區域，請從父區域移除 NS 記錄。如需詳細資訊，請參閱 新增或變更網域的名稱伺服器和黏附記錄。

以下遞增步驟讓您能監控個別步驟的有效性，以免您的區域出現 DNS 可用性問題。

停用 DNSSEC 簽署

1. 監控區域可用性。

   您可以監控該區域在您網域名稱中的可用性。此可協助您處理在啟用 DNSSEC 簽署後可能需要倒回步驟的任何問題。您可以藉由使用查詢日誌記錄，監控具有大部分流量的網域名稱。如需設定查詢日誌記錄的詳細資訊，請參閱 監控 Amazon Route 53。

   可以透過 Shell 指令碼或透過付費服務進行監控。但是，其不應是判斷是否需要回復的唯一信號。您也可能會因為網域名稱不可用，而得到來自客戶的反饋。

2. 查找目前 DS TTL。

   您可以藉由執行以下 Unix 命令來查找 DS TTL：

```
dig -t DS example.com example.com
```

3. 查找最大 NS TTL。

   有兩組與您的區域相關聯的 NS 記錄：

   - 委派 NS 記錄 — 這是父區域所持有的您區域的 NS 記錄。您可以藉由執行以下 Unix 命令來查找此記錄：

     首先，找到父區域的 NS（如果您的區域是 example.com，則父區域是 com）：

     ```
     dig -t NS com
     ```

     選擇其中一個 NS 記錄，然後執行以下操作：

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     例如：

     ```
     dig @b.gtld-servers.net. -t NS example.com
     ```

   - 區域內 NS 記錄 — 這是在您區域中的 NS 記錄。您可以藉由執行以下 Unix 命令來查找此記錄：

     ```
     dig @one of the NS records of your zone -t NS example.com
     ```

     例如：

     ```
     dig @ns-0000.awsdns-00.co.uk. -t NS example.com
     ```

     記下兩個區域的最大 TTL。

4. 移除父區域的 DS 記錄。

   請聯絡父區域擁有者以移除 DS 記錄。

   回復：重新插入 DS 記錄，確認 DS 插入已生效，並等待最大 NS (而不是 DS) TTL 的時間，然後所有解析程式將會再次開始驗證。

5. 確認 DS 移除已生效。

   如果父區域位於 Route 53 DNS 服務上，父區域擁有者可以透過 GetChangeAPI 確認完整傳播。

   否則，您可以定期探測 DS 記錄的父區域，之後再等待 10 分鐘，以提高 DS 記錄移除已完全傳播的概率。請注意，有些註冊商已有 DS 移除排程，例如，每天一次。

6. 等待 DS TTL 的時間。

   等到所有解析器都已使其快取中的 DS 記錄過期。

7. 停用 DNSSEC 簽署並停止金鑰簽署金鑰 (KSK)。

   - CLI
   - 主控台

   CLI

   呼叫 DisableHostedZoneDNSSEC 和 API。DeactivateKeySigningKey

   例如：

   ```
   aws --region us-east-1 route53 disable-hosted-zone-dnssec \
               --hosted-zone-id $hostedzone_id

   aws --region us-east-1 route53 deactivate-key-signing-key \
               --hosted-zone-id $hostedzone_id --name $ksk_name
   ```

   Console

   停用 DNSSEC 簽署

   1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
   2. 在導覽窗格中，選擇 Hosted zones (託管區域)，然後選擇您要停用 DNSSEC 簽署的託管區域。
   3. 在 DNSSEC signing (DNSSEC 簽署) 標籤上，選擇 Disable DNSSEC signing (停用 DNSSEC 簽署)。
   4. 在 Disable DNSSEC signing (停用 DNSSEC 簽署) 頁面上，根據您要停用 DNSSEC 簽署之區域的案例，選擇下列選項之一。
      - 僅限父區域 — 此區域具有包含 DS 記錄的父區域。在此案例中，您必須移除父區域的 DS 記錄。
      - 僅限子區域 — 此區域具有一或多個子區域之信任鏈的 DS 記錄。在此案例中，您必須移除區域的 DS 記錄。

- 父區域和子區域 — 此區域同時具有一或多個子區域之信任鏈的 DS 記錄和包含 DS 記錄的父區域。對於此案例，請按順序執行下列動作：

  a. 移除區域的 DS 記錄。

  b. 移除父區域的 DS 記錄。

  如果您有信任島，則可以略過此步驟。

5. 決定您在步驟 4 中移除的每個 DS 記錄的 TTL 是多少，並確定最長的 TTL 期間已過期。
6. 選取核取方塊，確認您已按順序執行這些步驟。
7. 在欄位中鍵入 disable (停用)，如圖所示，然後選擇 Disable (停用)。

若要停止金鑰簽署金鑰 (KSK)

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)，然後選擇您要停止的金鑰簽署金鑰 (KSK)。
3. 在 Key-signing keys (KSKs) (金鑰簽署金鑰 (KSK)) 部分中，選擇要停止的 KSK，然後在 Actions (動作) 之下，選擇 Edit KSK (編輯 KSK)，將 KSK status (KSK 狀態) 設為 Inactive (非作用中)，然後選擇 Save KSK (儲存 KSK)。

復原：呼叫ActivateKeySigningKey和 EnableHostedZoneDNSSEC API。

例如：

```
aws --region us-east-1 route53 activate-key-signing-key \
            --hosted-zone-id $hostedzone_id --name $ksk_name

aws --region us-east-1 route53 enable-hosted-zone-dnssec \
            --hosted-zone-id $hostedzone_id
```

8. 確認停用區域簽署已生效。

使用來執行`EnableHostedZoneDNSSEC()`呼叫的識別碼，GetChange以確定所有 Route 53 DNS 伺服器都已停止簽署回應 (狀態 =`INSYNC`)。

9. 請觀察名稱解析。

   您應該觀察到，沒有會導致解析器驗證您區域的問題。允許 1 到 2 週以將客戶向您報告問題所需要的時間一併納入考慮。

10. (選用) 清除。

    如果您不重新啟用簽署，您可以透過清理 KSK DeleteKeySigningKey並刪除對應的客戶管理金鑰以節省成本。

使用 DNSSEC 的客戶受管金鑰

當您在 Amazon Route 53 中啟用 DNSSEC 簽署時，Route 53 會為您建立金鑰簽署金鑰 (KSK)。若要建立 KSK，Route 53 必須使用中 AWS Key Management Service 支援 DNSSEC 的客戶管理金鑰。本節說明客戶受管金鑰的詳細資料和要求，這些金鑰在您使用 DNSSEC 時很有幫助。

當您使用 DNSSEC 的客戶受管金鑰時，請謹記以下幾點：

- 與 DNSSEC 簽署一起使用的客戶受管金鑰必須位於美國東部 (維吉尼亞北部) 區域。
- 客戶受管金鑰必須是具有 ECC_NIST_P256 金鑰規格的非對稱客戶受管金鑰。這些客戶受管金鑰僅用於簽署和驗證。如需建立非對稱客戶管理金鑰的協助，請參閱 AWS Key Management Service 開發人員指南中的建立非對稱客戶管理金鑰。如需協助尋找現有客戶受管金鑰的加密組態，請參閱 AWS Key Management Service 開發人員指南中的檢視客戶受管金鑰的加密組態。
- 如果您自行建立客戶受管金鑰，以便在 Route 53 中搭配 DNSSEC 使用，則必須包含讓 Route 53 具有必要許可的特定金鑰政策陳述式。Route 53 必須能夠存取您的客戶受管金鑰，以便為您建立 KSK。如需詳細資訊，請參閱 DNSSEC 簽署需要 Route 53 客戶受管金鑰許可。
- Route 53 可以為您建立客戶管理的金鑰，以 AWS KMS 便在沒有其 AWS KMS 他權限的情況下與 DNSSEC 簽章搭配使用。但是，如果您想要在建立金鑰後對其進行編輯，則必須具有特定的許可。您必須擁有的特定許可如下：`kms:UpdateKeyDescription`、`kms:UpdateAlias` 以及 `kms:PutKeyPolicy`。
- 請注意，無論是您自己建立客戶受管金鑰，還是 Route 53 為您建立金鑰，都會針對您擁有的每個客戶受管金鑰收取個別費用。如需詳細資訊，請參閱 AWS Key Management Service 定價。

使用金鑰簽署金鑰 (KSK)

當您啟用 DNSSEC 簽署時，Route 53 會為您建立金鑰簽署金鑰 (KSK)。在 Route 53 中，每個託管區域中最多可擁有兩個 KSK。啟用 DNSSEC 簽署之後，您可以新增、移除或編輯您的 KSK。

當您使用 KSK 時，請注意下列事項：

- 在刪除 KSK 之前，您必須先編輯 KSK，將其狀態設定為 Inactive (非作用中)。
- 為託管區域啟用 DNSSEC 簽署時，Route 53 會將 TTL 限制為一週。如果您將託管區域中記錄的 TTL 設定為一週以上，則不會收到錯誤，但 Route 53 會強制執行一週的 TTL。
- 若要協助防止區域中斷，並避免網域無法使用的問題，您必須快速處理並解決 DNSSEC 錯誤。我們強烈建議您設定警示，以便在偵測到`DNSSECInternalFailure`或`DNSSECKeySigningKeysNeedingAction`錯誤時向您發出警示。 CloudWatch 如需詳細資訊，請參閱 使用 Amazon 監控託管區域 CloudWatch。
- 本節描述的 KSK 操作可讓您輪換區域的 KSK。如需詳細資訊和 step-by-step 範例，請參閱部落格文章中的 DNSSEC 金鑰輪替設定使用 Amazon Route 53 進行 DNSSEC 簽署和驗證。

若要使用中的 KSK AWS Management Console，請遵循以下各節中的指導。

新增金鑰簽署金鑰 (KSK)

當您啟用 DNSSEC 簽署時，Route 53 會為您建立金鑰簽署 (KSK)。您也可以單獨新增 KSK。在 Route 53 中，每個託管區域中最多可擁有兩個 KSK。

建立 KSK 時，您必須提供或要求 Route 53 建立客戶受管金鑰，以搭配 KSK 使用。當您提供或建立客戶受管金鑰時，有幾點要求需要滿足。如需詳細資訊，請參閱 使用 DNSSEC 的客戶受管金鑰。

請遵循下列步驟，在 AWS Management Console中新增 KSK。

新增 KSK

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)，然後選擇託管區域。
3. 在 DNSSEC 標籤上的 Key-signing keys (KSKs) (金鑰簽署金鑰 (KSK)) 中，選擇 Switch to advanced view (切換至進階檢視)，然後在 Actions (動作) 下選擇 Add KSK (新增 KSK)。
4. 在 KSK 下，輸入 Route 53 將為您建立的 KSK 名稱。名稱僅能包含字母、數字和底線 (_)。它必須獨一無二。
5. 輸入適用於 DNSSEC 簽署的客戶受管金鑰的別名，或輸入新客戶受管金鑰的別名，Route 53 將為您建立此金鑰。

> **Note**
>
> 如果您選擇讓 Route 53 建立客戶受管金鑰，請注意每個客戶受管金鑰都要分別支付費用。如需詳細資訊，請參閱 AWS Key Management Service 定價。

6. 選擇 Create KSK (建立 KSK)。

編輯金鑰簽署金鑰 (KSK)

您可以將 KSK 的狀態編輯為 Active (作用中) 或 Inactive (非作用中)。當 KSK 處於作用中狀態時，Route 53 會使用該 KSK 進行 DNSSEC 簽署。在刪除 KSK 之前，您必須先編輯 KSK，將其狀態設定為 Inactive (非作用中)。

請遵循下列步驟，在 AWS Management Console中編輯 KSK。

編輯 KSK

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)，然後選擇託管區域。
3. 在 DNSSEC signing (DNSSEC 簽署) 標籤上的 Key-signing keys (KSKs) (金鑰簽署金鑰 (KSK)) 中，選擇 Switch to advanced view (切換至進階檢視)，然後，在 Actions (動作) 下選擇 Edit KSK (編輯 KSK)。
4. 對 KSK 進行所需的更新，然後選擇 Save (儲存)。

刪除金鑰簽署金鑰 (KSK)

在刪除 KSK 之前，您必須先編輯 KSK，將其狀態設定為 Inactive (非作用中)。

您可能會刪除 KSK 的一點原因是做為例行金鑰輪換的環節之一。定期輪換密碼編譯金鑰是一種最佳實務。您的組織可能會針對輪換金鑰的頻率提供標準指引。

請依照下列步驟，在 AWS Management Console中刪除 KSK。

刪除 KSK

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

2. 在導覽窗格中，選擇 Hosted zones (託管區域)，然後選擇託管區域。
3. 在 DNSSEC 標籤上的 Key-signing keys (KSKs) (金鑰簽署金鑰 (KSK)) 中，選擇 Switch to advanced view (切換至進階檢視)，然後在 Actions (動作) 下選擇 Delete KSK (刪除 KSK)。
4. 按照指引確認刪除 KSK。

Route 53 中的 KMS 金鑰和 ZSK 管理

本節說明目前 Route 53 用於已啟用 DNSSEC 簽署的區域的做法。

> **Note**
>
> Route 53 使用以下可能會變更的規則。將來的任何變更都不會降低您區域或 Route 53 的安全狀態。

53 號幹線如何使用與您的 KSK AWS KMS 相關聯的

在 DNSSEC 中，KSK 用於生成 DNSKEY 資源紀錄集的資源紀錄簽名 (RRSIG)。All `ACTIVE` KSK 均用於生成 RRSIG。路由 53 透過呼叫關聯 KMS 金鑰上的 `Sign` AWS KMS API 來產生 RRSIG。如需詳細資訊，請參閱《AWS KMS API 指南》中的簽署。這些 RRSIG 不會計入區域的資源紀錄集限制。

RRSIG 會過期。為防止 RRSIG 過期，會每一到七天再生成一次 RRSIG 以定期對其進行重新整理。

每次呼叫以下任一項 API 時，也會重新整理 RRSIG：

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSC
- EnableHostedZoneDNSSC

每次 Route 53 執行重新整理時，我們都會生成 15 個 RRSIG 來確保未來幾天的可用性，以防相關聯的 KMS 金鑰變得無法存取。在估計 KMS 金鑰成本時，您可以假定每天定期重新整理一次。KMS 金鑰政策的意外變更，可能會讓 KMS 金鑰變得無法存取。無法存取的 KMS 金鑰會將關聯的 KSK 狀態設定為 `ACTION_NEEDED`。我們強烈建議您在偵測

到DNSSECKeySigningKeysNeedingAction錯誤時設定 CloudWatch 警示來監控此狀況，因為驗證解析器會在最後一次 RRSIG 到期後開始查詢失敗。如需詳細資訊，請參閱 使用 Amazon 監控託管區域 CloudWatch。

Route 53 如何管理您區域的 ZSK

啟用 DNSSEC 簽署的每個新託管區域均有一個 ACTIVE 區域簽署金鑰 (ZSK)。ZSK 由每個託管區域單獨生成，並為 Route 53 所有。目前的金鑰演算法是 ECDSAP256SHA256。

我們將在簽署開始後的 7-30 天內，開始對區域執行定期 ZSK 輪換。目前，Route 53 使用發佈前金鑰滾動法。如需詳細資訊，請參閱發佈前區域簽署金鑰滾動法。此方法會將另一個 ZSK 帶至該區域。輪換將每 7-30 天重複一次。

如果區域的任何 KSK 處於 ACTION_NEEDED 狀態，Route 53 將暫停 ZSK 輪換，因為 Route 53 無法重新生成 DNSKEY 資源紀錄集的 RRSIG，以考慮區域 ZSK 中的變更。情況解除後，ZSK 輪換將自動恢復。

DNSSEC 不存在於 Route 53 中的證明

> **Note**
>
> Route 53 使用以下可能會變更的規則。將來的任何變更都不會降低您區域或 Route 53 的安全狀態。

DNSSEC 有三種不存在證明：

- 記錄與查詢名稱相符的不存在證明。
- 類型與查詢名稱相符的不存在證明。
- 用於生成回應記錄的通配符記錄的不存在證明。

Route 53 使用 BL 方法實現記錄與查詢名稱相符的不存在證明。如需詳細資訊，請參閱 BL。這種方法可生成精簡表示的證明，並避免區域遍歷。

萬一存在與查詢名稱相符，但與查詢類型不相符的記錄 (例如查詢 web.example.com/AAAA，但只有 web.example.com/A 存在)，我們會傳回包含所有支援資源紀錄類型的最小 NSEC (下一次安全) 記錄。

當 Route 53 從通配符記錄合成答案時，回應將不隨附下一次安全記錄，或通配符的 NSEC 記錄。此類 NSEC 記錄用於某些實作 (通常是執行離線簽署的實作)，以防止回應中的資源紀錄簽署 (RRSIG) 被重

複用於欺騙不同的回應。Route 53 將線上簽署用於 non-DNSKEY 記錄來產生回應特定的 RRSIG，不能將這些 RRSIG 重複用於不同的回應。

DNSSEC 簽署故障診斷

本節中的資訊可協助您解決 DNSSEC 簽署的問題，包括啟用、停用及金鑰簽署金鑰 (KSK)。

啟用 DNSSEC

在開始啟用 DNSSEC 簽署之前，請務必先閱讀 在 Amazon Route 53 中設定 DNSSEC 簽署 中的先決條件。

停用 DNSSEC

為了安全地停用 DNSSEC，Route 53 會檢查目標區域是否位於信任鏈中。其會檢查目標區域的父項是否具有目標區域的任何 NS 記錄以及目標區域的 DS 記錄。如果目標區域無法公開解析，例如，在查詢 NS 和 DS 時得到 SERVFAIL 回應，Route 53 就無法判斷停用 DNSSEC 是否安全。您可以聯絡您的父區域以修正這些問題，並於稍後再重試停用 DNSSEC。

KSK 狀態為 Action needed (需採取動作)

當 Route 53 DNSSEC 失去對應的訪問權限（由於權限或`ACTION_NEEDED`刪除）時，KSK 可以將其KeySigningKey狀態更改為「需要操作」 AWS KMS key （或 AWS KMS key 狀態）。

如果 KSK 的狀態為 Action needed (需採取動作)，意味著最終其將導致使用 DNSSEC 驗證解析器的客戶端發生區域中斷，而您必須快速採取行動以防止生產區域變得無法解析。

若要修正這個問題，請確定您 KSK 作為依據的客戶受管金鑰已啟用且具有正確的許可。如需所需許可的詳細資訊，請參閱DNSSEC 簽署需要 Route 53 客戶受管金鑰許可。

修正 KSK 之後，請使用主控台或重新啟動 AWS CLI，如中步驟 2：啟用 DNSSEC 簽署並建立 KSK所述。

為了防止將 future 發生此問題，請考慮按照中的建議添加 Amazon CloudWatch 指標以跟踪 KSK 的狀態。在 Amazon Route 53 中設定 DNSSEC 簽署

KSK 狀態為 Internal failure (內部故障)

當 KSK 的狀態為內部故障（或KeySigningKey狀態）時，`INTERNAL_FAILURE`在問題解決之前，您無法使用任何其他 DNSSEC 實體。您必須採取行動，才能使用 DNSSEC 簽署，包括使用此 KSK 或您的其他 KSK。

若要修正此問題，請再試一次啟用或停用 KSK。

若要修正使用 API 時的問題，請嘗試啟用簽署 (EnableHostedZoneDNSSEC) 或停用簽署 (DisableHostedZoneDN SSEC)。

務必及時修正 Internal failure (內部故障) 問題。在修正此問題之前，除了修正 Internal failure (內部故障) 的操作之外，您無法對託管區域進行任何其他變更。

使用 AWS Cloud Map 建立記錄和運作狀態檢查

如果您希望將網際網路流量或 Amazon VPC 內的流量路由至應用程式元件或微服務，您可以使用 AWS Cloud Map 自動建立記錄並選擇建立運作狀態檢查。如需詳細資訊，請參閱 AWS Cloud Map 開發人員指南。

DNS 限制和行為

DNS 訊息傳受若干因素約束，這些因素會影響您建立和使用託管區域及記錄的方式。本節說明這些因素。

最大回應大小

為了遵守 DNS 標準，透過 UDP 傳送的回應，大小不超過 512 位元組。超過 512 位元組的回應會被截斷，解析程式必須透過 TCP 重新發出請求。如果解析程式支援 EDNS0 (如 RFC 2671 中所定義) 並向 Amazon Route 53 公告 EDNS0 選項，則 Route 53 將允許透過 UDP 發出的回應達到 4096 位元組，而且不會截斷。

授權區段處理

為使查詢成功，Route 53 會將相關託管區域的名稱伺服器 (NS) 記錄附加到 DNS 回答的授權區段。對於找不到的名稱 (NXDOMAIN 回答)，Route 53 會將相關託管區域的起始授權 (SOA) 記錄 (如 RFC 1035 中所定義) 附加到 DNS 回答的授權區段。

其他區段處理

Route 53 會將記錄附加到其他區段。如果記錄已知且合適，服務將為回答區段中引述的 MX、CNAME、NS 或 SRV 記錄的任何目標附加 A 或 AAAA 記錄。如需這些 DNS 記錄類型的詳細資訊，請參閱 支援的 DNS 記錄類型。

什麼是 Amazon Route 53 Resolver？

Amazon Route 53 Resolver 以遞迴方式回應來自公用記錄、Amazon VPC 特定 DNS 名稱和 Amazon Route 53 私有託管區域的 AWS 資源的 DNS 查詢，預設情況下可在所有 VPC 中使用。

> **Note**
>
> Amazon Route 53 Resolver 之前稱為 Amazon DNS 伺服器，但在引入解析器規則以及入站和出站端點時重新命名。如需詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的 Amazon DNS 伺服器。

Amazon VPC 將連線到 VPC+2 IP 地址的 Route 53 Resolver。此 VPC+2 地址會連線到可用區域內的 Route 53 Resolver。

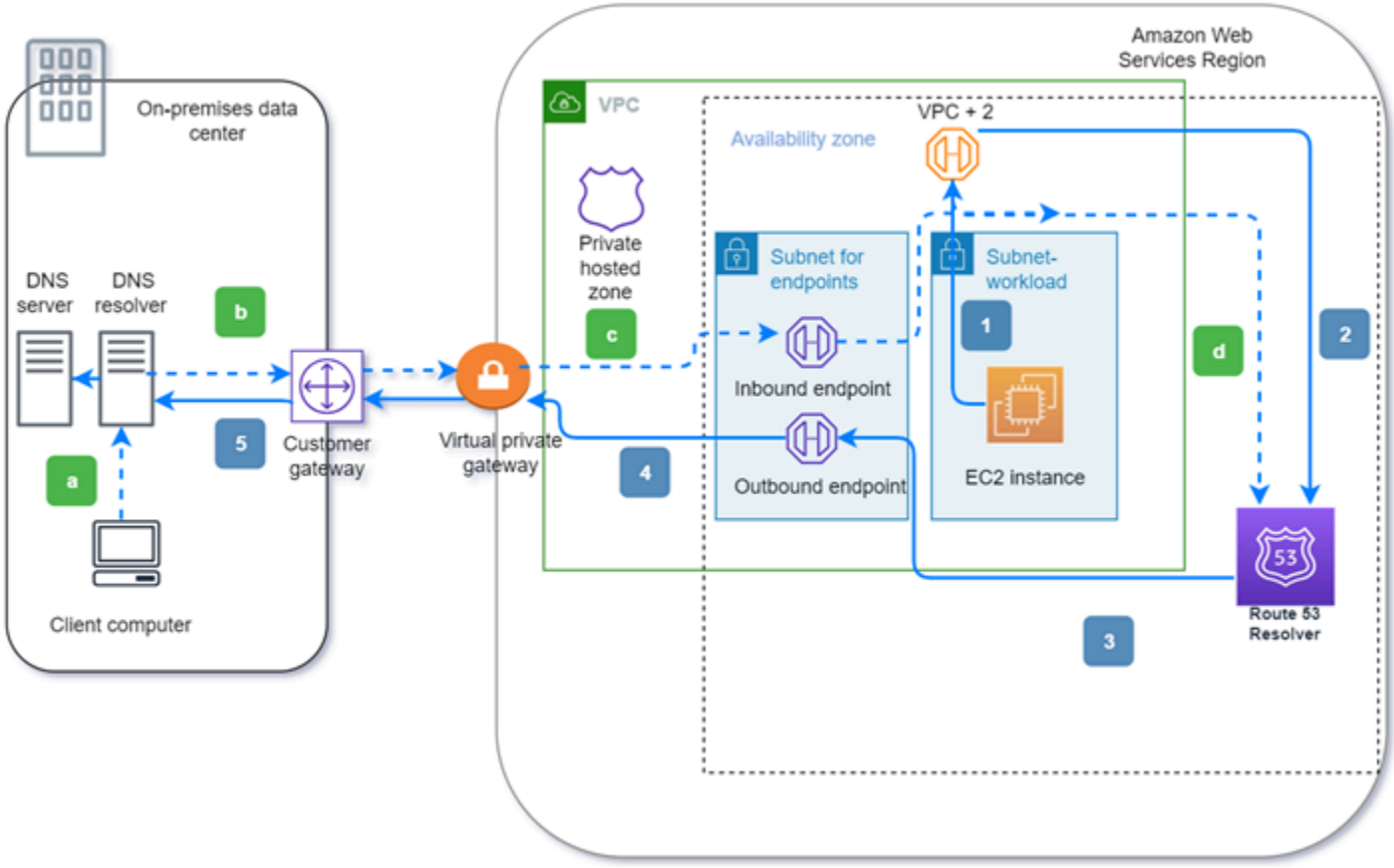
Route 53 Resolver 會自動回應下列項目的 DNS 查詢：

- EC2 執行個體的本機 VPC 網域名稱 (例如，ec2-192-0-2-44.compute-1.amazonaws.com)。
- 私有託管區域中的記錄 (例如，acme.example.com)。
- 針對公有網域名稱，Route 53 Resolver 會向網際網路上的公有名稱伺服器執行遞迴查詢。

如果您的工作負載同時利用 VPC 和內部部署資源，則還需要解析內部部署託管的 DNS 記錄。同樣地，這些內部部署資源可能需要解析託管於上的名稱 AWS。透過 Resolver 端點和條件式轉送規則，您可以解析內部部署資源與 VPC 之間的 DNS 查詢，以透過 VPN 或 Direct Connect (DX) 建立混合雲端設定。具體而言：

- 傳入 Resolver 端點允許從內部部署網路或其他 VPC 向 VPC 進行 DNS 查詢。
- 傳出 Resolver 端點允許從內部部署網路或其他 VPC 向 VPC 進行 DNS 查詢。
- Resolver 規則可讓您為每個網域名稱建立一個轉送規則，並指定要將 DNS 查詢從 VPC 轉送至內部部署 DNS 解析器的網域名稱，以及從內部部署轉送至 VPC 的網域名稱。規則會直接套用至您的 VPC，並且可以在多個帳戶之間共用。

下圖顯示具有 Resolver 端點的混合式 DNS 解析。請注意，此圖表已簡化為僅顯示一個可用區域。



此圖說明了下列步驟：

傳出 (實心箭頭 1-5)：

1. Amazon EC2 執行個體需要將 DNS 查詢解析為 internal.example.com 的網域。授權 DNS 伺服器位於內部部署資料中心。此 DNS 查詢會傳送至連線到 Route 53 Resolver 的 VPC 中的 VPC+2。
2. Route 53 Resolver 轉送規則設定為將查詢轉送至內部部署資料中心的 internal.example.com。
3. 查詢會轉送至傳出端點。
4. 輸出端點會透過 AWS 與資料中心之間的私人連線，將查詢轉送至內部部署 DNS 解析器。連線可以是 AWS Direct Connect 或 AWS Site-to-Site VPN，描繪為虛擬私有閘道。
5. 內部部署 DNS 解析器會解析 internal.example.com 的 DNS 查詢，並透過相同的路徑反向傳回 Amazon EC2 執行個體的答案。

入站（虛線箭頭 a—d）：

a. 內部部署資料中心中的用戶端必須解析網域 dev.example.com AWS 資源的 DNS 查詢。它會將查詢傳送至內部部署 DNS 解析器。

b. 內部部署 DNS 解析器具有轉送規則，可將 dev.example.com 的查詢指向傳入端點。

c. 查詢會透過私人連線 (例如 AWS Direct Connect 或 AWS Site-to-Site VPN，描繪為虛擬閘道) 抵達輸入端點。

d. 入站端點將查詢發送到 Route 53 解析器，Route 53 解析器解析 dev.example.com 的 DNS 查詢，並通過相同的路徑反向返回客戶端的答案。

主題

- 在 VPC 和您網路之間解析 DNS 查詢
- Route 53 解析器可用性和擴展
- 開始使用 Route 53 Resolver
- 將傳入 DNS 查詢轉送到您的 VPC
- 將傳出 DNS 查詢轉送到您的網路
- 管理傳入端點
- 管理傳出端點
- 管理轉送規則
- 在 Amazon Route 53 中啟用 DNSSEC 驗證

在 VPC 和您網路之間解析 DNS 查詢

此外，Resolver 包含您設定以解答內部部署環境的往返 DNS 查詢的端點。

> **Note**
>
> 不支援將私人 DNS 查詢從內部部署 DNS 伺服器轉寄至任何 VPC CIDR + 2 位址，而且這麼做可能導致結果不穩定。建議您改為使用 Resolver 傳入端點。

您也可以設定轉送規則，來整合網路上 Resolver 與 DNS 解析程式之間的 DNS 解析。您的網路可包含任何可從 VPC 連線的網路，例如以下項目：

- VPC 本身
- 另一個對等 VPC
- AWS 與連線的內部部署網路 AWS Direct Connect、VPN 或網路位址轉譯 (NAT) 閘道

開始轉送查詢前，請在連線的 VPC 中建立 Resolver 傳入及 (或) 傳出端點。這些端點提供輸入或輸出查詢的路徑：

傳入端點：您網路上的 DNS 解析程式可以透過此端點，將 DNS 查詢轉送至 Route 53 Resolver。

這可讓您的 DNS 解析器輕鬆解析 AWS 資源的網域名稱，例如 Route 53 私有託管區域中的 EC2 執行個體或記錄。如需詳細資訊，請參閱 您網路上的 DNS 解析程式如何將 DNS 查詢轉送至 Route 53 Resolver 端點。

傳出端點：Resolver 會有條件地透過此端點向您網路上的解析程式轉送查詢

若要轉送選取的查詢，您可以建立 Resolver 規則，而該規則指定您想要轉送之 DNS 查詢的網域名稱 (如 example.com)，以及您要轉送查詢至網路上哪個 DNS 解析程式的 IP 地址。如果查詢符合多項規則 (example.com、acme.example.com)，Resolver 會選擇最符合的規則 (acme.example.com)，並轉送查詢到您以該規則指定的 IP 地址。如需詳細資訊，請參閱 Route 53 Resolver 端點如何從您的 VPC 轉送 DNS 查詢到您的網路。

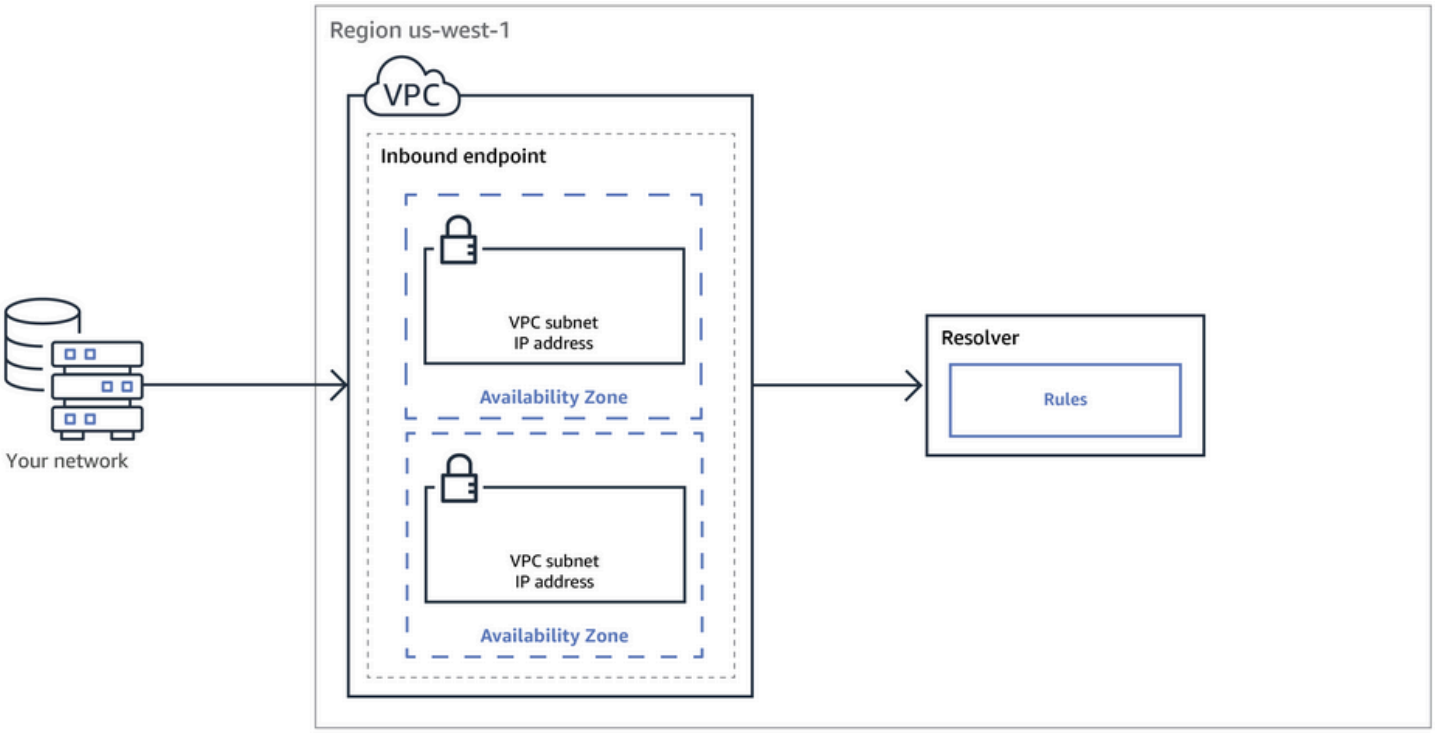
類似於 Amazon VPC，Resolver 是區域性的。在有 VPC 的每個區域中，您可以選擇將查詢從 VPC 轉送到網路 (對外查詢)、從網路轉送至 VPC (傳入查詢)，或兩者皆選。

您無法在非您擁有的 VPC 中建立 Resolver 端點。只有 VPC 擁有者可以建立 VPC 層級的資源，例如傳入端點。

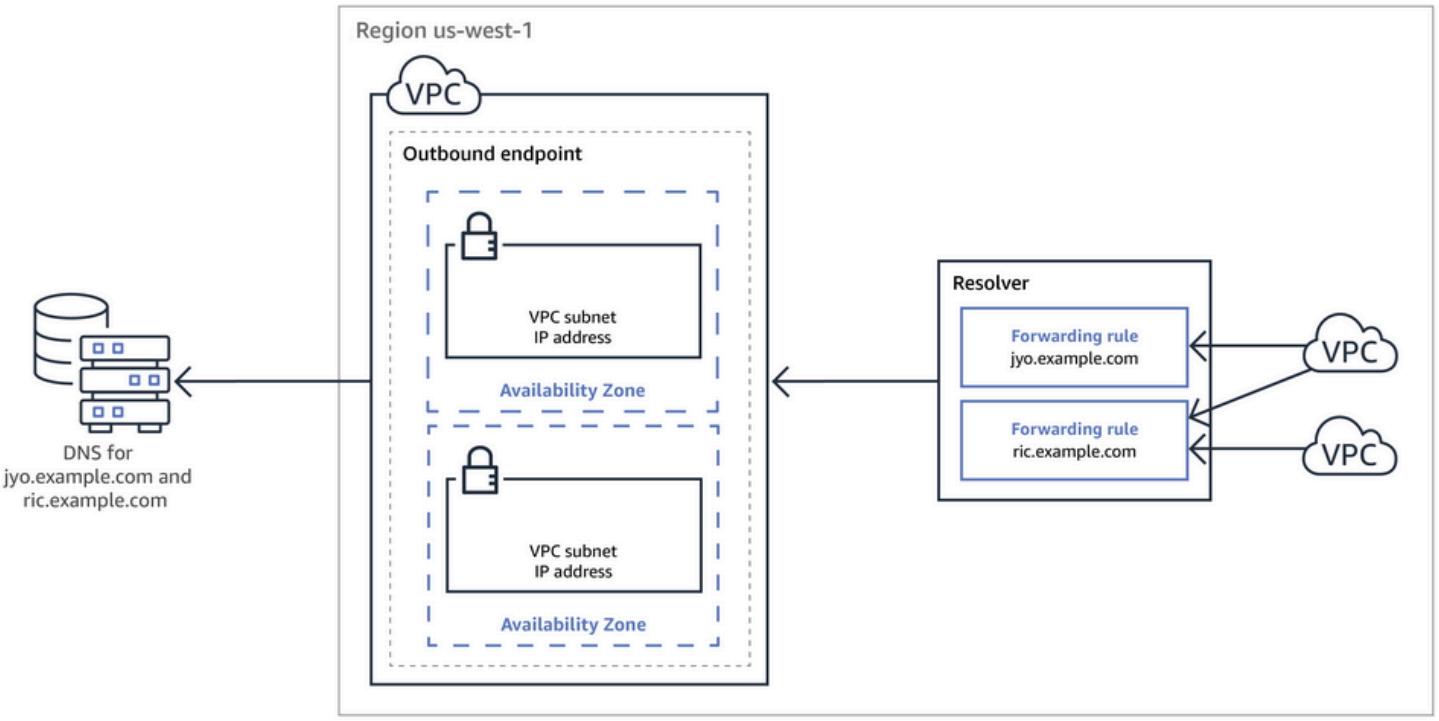
> **Note**
>
> 建立 Resolver 端點時，您無法指定執行個體租用屬性設定為 `dedicated` 的 VPC。如需詳細資訊，請參閱 。

若要使用傳入或傳出轉送，請在您的 VPC 中建立 Resolver 端點。在定義端點的過程中，您需要指定希望傳入 DNS 查詢轉送到哪些 IP 地址，或希望傳出查詢來自哪些 IP 地址。對於您指定的每個 IP 地址，Resolver 會自動建立 VPC 彈性網路介面。

下圖顯示 DNS 查詢從您網路上的 DNS 解析程式到達 Route 53 Resolver 端點的路徑。



下圖顯示 DNS 查詢從其中一個 VPC 中的 EC2 執行個體到達您網路上的 DNS 解析程式的路徑。



如需 VPC 網路介面的概觀，請參閱 Amazon VPC 使用者指南中的彈性網路介面。

主題

- 您網路上的 DNS 解析程式如何將 DNS 查詢轉送至 Route 53 Resolver 端點
- Route 53 Resolver 端點如何從您的 VPC 轉送 DNS 查詢到您的網路
- 建立傳入和傳出端點時的注意事項

您網路上的 DNS 解析程式如何將 DNS 查詢轉送至 Route 53 Resolver 端點

當您想要將 DNS 查詢從網路轉送至 AWS 區域中的 Route 53 Resolver 端點時，請執行以下步驟：

1. 您可以在 VPC 中建立 Route 53 Resolver 傳入端點，並指定您網路上的解析程式將 DNS 查詢轉送到哪些 IP 地址。

   對於您為傳入端點所指定的每個 IP 地址，Resolver 會在您建立傳入端點的 VPC 中，建立 VPC 彈性網路介面。
2. 您在網路上設定解析程式，將適用網域名稱的 DNS 查詢轉送至您在傳入端點中指定的 IP 地址。如需詳細資訊，請參閱 建立傳入和傳出端點時的注意事項。

以下是 Resolver 解析在網路上產生之 DNS 查詢的方法：

1. 您網路上的 Web 瀏覽器或其他應用程式會提交您轉送到 Resolver 的網域名稱 DNS 查詢。
2. 您網路上的解析程式會將查詢轉送至傳入端點的 IP 地址。
3. 傳入端點將查詢轉送至 Resolver。
4. Resolver 從內部或對公有名稱伺服器執行遞迴查詢，在 DNS 查詢中取得網域名稱的適用值。
5. Resolver 會將值傳回傳入端點。
6. 傳入端點將值傳回您網路上的解析程式。
7. 您網路上的解析程式將值傳回應用程式。
8. 應用程式使用 Resolver 傳回的值提交 HTTP 請求，例如，請求 Amazon S3 儲存貯體中的物件。

創建入站端點不會改變解析器的行為，它只是提供從 AWS 網絡外部位置到解析器的路徑。

Route 53 Resolver 端點如何從您的 VPC 轉送 DNS 查詢到您的網路

當您想要將 AWS 區域中一或多個 VPC 中 EC2 執行個體的 DNS 查詢轉寄至您的網路時，請執行下列步驟。

1. 在 VPC 中建立 Route 53 Resolver 傳出端點並指定多個值：

- 在前往網路解析程式途中，您希望 DNS 查詢通過的 VPC。
- 您希望 Resolver 從中轉送 DNS 查詢之 VPC 中的 IP 地址。對網路上的主機而言，這些是 DNS 查詢產生來源的 IP 地址。
- VPC 安全群組

對於您為傳出端點所指定的每個 IP 地址，Resolver 會在您指定的 VPC 中建立 Amazon VPC 彈性網路介面。如需詳細資訊，請參閱 建立傳入和傳出端點時的注意事項。

2. 您要建立一或多項規則，指定您希望 Resolver 轉送到您網路解析程式之 DNS 查詢的網域名稱。您也要指定解析程式的 IP 地址。如需詳細資訊，請參閱 使用規則來控制哪些查詢轉送到您的網路。
3. 建立每項規則與將 DNS 查詢轉送至網路之 VPC 的關聯。

主題

- 使用規則來控制哪些查詢轉送到您的網路
- Resolver 如何判斷查詢中的網域名稱是否符合任何規則
- Resolver 如何判斷將 DNS 查詢轉送至何處
- 在多個區域中使用規則
- Resolver 建立自動定義規則所針對的網域名稱

使用規則來控制哪些查詢轉送到您的網路

這些規則會控制 Route 53 Resolver 端點將哪些 DNS 查詢轉送到網路 DNS 解析程式，以及 Resolver 解答哪些查詢。

有幾種方式可以分類規則。一種方法是以規則建立者為分類依據：

- 自動定義的規則 – Resolver 會自動建立自動定義的規則，並建立這些規則與您 VPC 的關聯。這些規則大多適用於 Resolver 回答查詢的 AWS特定域名。如需詳細資訊，請參閱 Resolver 建立自動定義規則所針對的網域名稱。
- 自訂規則 – 您建立自訂規則，並建立這些規則與 VPC 的關聯。目前，您只能建立一種自訂規則，即條件式轉送規則，也稱為轉送規則。轉送規則可讓 Resolver 將 DNS 查詢從您的 VPC 轉送至網路 DNS 解析程式的 IP 地址。

  如果您為同一個網域建立轉送規則做為自動定義規則使用，Resolver 會根據轉送規則的設定，將該網域名稱的查詢轉送至網路 DNS 解析程式。

另一個方法是依據操作內容分類規則：

- 條件式轉送規則 – 當您想要將指定網域名稱的 DNS 查詢轉送到您網路的 DNS 解析程式時，建立條件式轉送規則 (也稱為轉送規則)。
- 系統規則 – 系統規則可讓 Resolver 選擇性地覆寫在轉送規則中定義的行為。當您建立系統規則時，Resolver 會解析指定子網域的 DNS 查詢，否則即由您網路的 DNS 解析程式解析。

  根據預設，轉送規則適用於網域名稱及其所有子網域。如果您想要將網域查詢轉送到網路的解析程式，但不想轉送某些子網域的查詢，您可以建立針對子網域的系統規則。例如，如果您為 example.com 建立了轉送規則，但不想轉送 acme.example.com 的查詢，您可以建立一項系統規則，並指定 acme.example.com 為網域名稱。
- 遞迴規則 – Resolver 會自動建立名為 Internet Resolver (網際網路解析程式) 的遞迴規則。對於您未建立自訂規則，而且 Resolver 也未建立自動定義規則的任何網域名稱，這個規則會使 Route 53 Resolver 成為遞迴解析程式。如需如何覆寫這種行為的資訊，請參閱本主題稍後的「將所有查詢轉送到您的網路」。

您可以建立套用至特定網域名稱 (您或大多數網 AWS 域名稱)、公用 AWS 網域名稱或所有網域名稱的自訂規則。

將特定網域名稱的查詢轉送到您的網路

若要將 example.com 等特定網域名稱的查詢轉送到您的網路，您可以建立一項規則，指定該網域名稱。您也可以指定您網路 DNS 解析程式的 IP 地址，將查詢轉送至此地址。然後，建立每項規則與將 DNS 查詢轉送至網路之 VPC 的關聯。例如，您可以分別為 example.com、example.org 和 example.net 建立規則。然後，您可以使用任何組合將規則與 AWS 區域中的 VPC 產生關聯。

將 amazonaws.com 的查詢轉送至您的網路

網域名稱 Amazonaws.com 是 EC2 執行個體和 S3 儲存貯體等資 AWS 源的公有網域名稱。如果您想要將 amazonaws.com 的查詢轉送到您的網路，請建立一項規則，指定網域名稱為 amazonaws.com，並指定規則類型為 Forward (轉送)。

> **Note**
>
> 即使您建立了 amazonaws.com 轉送規則，Resolver 也不會自動轉送某些 amazonaws.com 子網域的 DNS 查詢。如需詳細資訊，請參閱 Resolver 建立自動定義規則所針對的網域名稱。如需如何覆寫這種行為的資訊，請參閱接下來的「將所有查詢轉送到您的網路」。

將所有查詢轉送到您的網路

如果您想要將所有查詢轉送至您的網路，您可以建立一項規則，指定「.」(點) 為網域名稱，並建立規則與將所有 DNS 查詢轉送至網路之 VPC 的關聯。解析器仍然不會將所有 DNS 查詢轉發到您的網絡，因為在之外使用 DNS 解析器 AWS 會破壞某些功能。例如，某些內部 AWS 網域名稱具有無法從外部存取的內部 IP 位址範圍 AWS。如需建立「.」規則後無法將查詢轉送到您網路的網域名稱清單，請參閱 Resolver 建立自動定義規則所針對的網域名稱。

不過，您可以停用反向 DNS 的自動定義系統規則，讓「.」規則將所有反向 DNS 查詢轉送至您的網路。如需如何關閉自動定義之規則的詳細資訊，請參閱 Resolver 中反向 DNS 查詢的轉送規則。

如果您想要嘗試將所有網域名稱的 DNS 查詢轉送至您的網路，包括預設排除轉送的網域名稱，您可以建立「.」規則，然後執行下列一項操作：

- 將 VPC 的 `enableDnsHostnames` 標記設為 `false`
- 為Resolver 建立自動定義規則所針對的網域名稱列出的網域名稱建立規則

> **Important**
>
> 如果您在建立「.」規則時將所有網域名稱轉送到您的網路，包括 Resolver 排除的網域名稱，有些功能可能會停止運作。

Resolver 如何判斷查詢中的網域名稱是否符合任何規則

Route 53 Resolver 會比較 DNS 查詢中的網域名稱和與查詢產生來源 VPC 相關聯之規則中的網域名稱。在下列情況中，Resolver 認為網域名稱符合：

- 網域名稱完全相符
- 查詢中的網域名稱是規則中網域名稱的子網域

例如，如果規則中的網域名稱是 acme.example.com，Resolver 會將 DNS 查詢中的下列網域名稱視為相符：

- acme.example.com
- zenith.acme.example.com

下列網域名稱不相符：

- example。com
- nadir.example.com

如果查詢中的網域名稱符合多項規則中的網域名稱 (例如 example.com 和 www.example.com)，Resolver 會使用包含最多特定網域名稱的規則 (www.example.com) 路由傳出 DNS 查詢。

Resolver 如何判斷將 DNS 查詢轉送至何處

當在 VPC 之 EC2 執行個體上執行的應用程式提交 DNS 查詢時，Route 53 Resolver 會執行以下步驟：

1. Resolver 檢查規則中的網域名稱。

   如果查詢中的網域名稱符合規則中的網域名稱，Resolver 會將查詢轉送至您建立傳出端點時所指定的 IP 地址。然後傳出端點會將查詢轉送至您網路的解決程式 IP 地址，即您在建立規則時所指定的地址。

   如需詳細資訊，請參閱 Resolver 如何判斷查詢中的網域名稱是否符合任何規則。

2. Resolver 端點根據「.」規則中的設定轉送 DNS 查詢。

   如果查詢中的網域名稱不符合任何其他規則中的網域名稱，Resolver 會根據自動定義之「.」(點) 規則中的設定轉送查詢。點規則適用於所有網域名稱，但私人託管區域中的某些 AWS 內部網域名稱和記錄名稱除外。如果查詢中的網域名稱不符合您自訂轉送規則中的任何名稱，此規則可讓 Resolver 將 DNS 查詢轉送至公有的名稱伺服器。如果您想要將所有查詢轉送到網路上的 DNS 解析器，則可以建立自訂轉送規則，指定網域名稱為「.」，指定類型為 Forwarding (轉送)，並指定這些解析程式的 IP 地址。

3. Resolver 會將回應傳回至提交查詢的應用程式。

在多個區域中使用規則

Route 53 解析器是一種地區服務，因此您在一個 AWS 區域中創建的對象僅在該區域中可用。若要在多個區域中使用相同的規則，您必須在每個區域中建立該規則。

建立規則的 AWS 帳戶可以與其他 AWS 帳號共用規則。如需詳細資訊，請參閱 與其他 AWS 帳戶共享解析器規則並使用共享規則。

Resolver 建立自動定義規則所針對的網域名稱

Resolver 會自動建立自動定義的系統規則，其中會定義如何解析所選網域的查詢：

- 針對私有託管區域和 Amazon EC2 特定網域名稱 (如 compute.amazonaws.com 和 compute.internal)，自動定義規則可確保您的私有託管區域和 EC2 執行個體繼續解析，前提是您為較少的特定域名 (如「.」(點) 或「com」) 建立條件轉送規則。
- 針對公開預留網域名稱 (如 localhost 和 10.in-addr.arpa)，DNS 最佳實務建議在本機解答查詢，不要將查詢轉送到公有名稱伺服器。請參閱 RFC 6303，本機服務 DNS 區域。

> **Note**
>
> 如果為「.」(點) 或「com」建立條件式轉送規則，建議您也為 amazonaws.com 建立系統規則。(系統規則可讓 Resolver 在本機解析特定網域和子網域的 DNS 查詢。) 建立此系統規則可提升效能、減少轉送至您網路的查詢數量，以及降低 Resolver 費用。

如果您想要覆寫自動定義的規則，則可以為相同的網域名稱建立條件式轉送規則。

您也可以停用某些自動定義的規則。如需詳細資訊，請參閱 Resolver 中反向 DNS 查詢的轉送規則。

Resolver 會建立下列自動定義的規則。

私有託管區域的規則

針對已與 VPC 建立關聯的每個私有託管區域，Resolver 會建立規則，並建立它與 VPC 的關聯。如果您建立該私有託管區域與多個 VPC 的關聯，則 Resolver 會建立該規則與多個相同 VPC 的關聯。

此規則的類型為 Forward (轉送)。

各種 AWS 內部網域名稱的規則

在本節中，所有內部網域名稱的規則類型都是 Forward (轉送)。Resolver 會將這些網域名稱的 DNS 查詢轉送至 VPC 的授權名稱伺服器。

> **Note**
>
> 當您將 VPC 的 `enableDnsHostnames` 標記設定為 `true` 時，Resolver 會建立大部分這些規則。即使您未使用 Resolver 端點，Resolver 也會建立規則。

當您將 VPC 的 enableDnsHostnames 標記設定為 true 時，Resolver 會建立下列自動定義規則，並建立其與 VPC 的關聯：

- ####.compute.internal，例如，eu-west-1.compute.internal。us-east-1 區域不使用此網域名稱。
- ####. #算。 amazon-domain-name例如，歐盟西部-1. 計算. 亞馬遜網站或 CN-北 1. 計算機. us-east-1 區域不使用此網域名稱。
- ec2.internal。僅 us-east-1 區域使用此網域名稱。
- compute-1.internal。僅 us-east-1 區域使用此網域名稱。
- compute-1.amazonaws.com。僅 us-east-1 區域使用此網域名稱。

當您將 VPC 的 enableDnsHostnames 標記設定為 true 時，以下是 Resolver 建立之規則的反向 DNS 查詢的自動定義規則。

- 10.in-addr.arpa
- 16.172.in-addr.arpa 到 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- VPC 的各個 CIDR 範圍的規則。例如，如果 VPC 的 CIDR 範圍為 10.0.0.0/23，Resolver 將會建立以下規則：
  - 0.0.10.in-addr-arpa
  - 1.0.10.in-addr-arpa

當您將 VPC 的 enableDnsHostnames 標記設定為 true 時，也會建立以下 localhost 相關網域的自動定義規則，及其與 VPC 的關聯：

- localhost
- localdomain
- 127.in-addr.arpa
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa

當您透過傳輸閘道或 VPC 對等互連連接兩個 VPC 並啟用 DNS 支援時，Resolver 會建立下列自動定義規則，並建立其與 VPC 的關聯：

- 對等 VPC 的 IP 地址範圍反向 DNS 查詢，例如，0.192.in-addr.arpa

如果將 IPv4 CIDR 區塊新增至 VPC，Resolver 會為新的 IP 地址範圍新增自動定義規則。

- 如果其他 VPC 位在另一個區域，則以下網域名稱：
  - *####*.compute.internal。us-east-1 區域不使用此網域名稱。
  - *####. #*算。 *amazon-domain-name*。us-east-1 區域不使用此網域名稱。
  - ec2.internal。僅 us-east-1 區域使用此網域名稱。
  - compute-1.amazonaws.com。僅 us-east-1 區域使用此網域名稱。

所有其他網域的規則

Resolver 建立的「.」(點) 規則適用本主題前文中未指定的所有網域名稱。「.」規則都有 Recursive (遞迴) 類型，這表示規則可讓 Resolver 做為遞迴解析程式使用。

建立傳入和傳出端點時的注意事項

在 AWS 區域中建立輸入和輸出解析器端點之前，請考慮下列問題。

主題

- 每個 區域中的傳入和傳出端點數量
- 針對傳入和傳出端點使用相同的 VPC
- 傳入端點和私有託管區域
- VPC 對等互連
- 共用子網路中的 IP 位址
- 在您的網路和您建立端點的 VPC 之間的連線
- 當您共用規則時，您也會共用傳出端點
- 選擇端點的協定
- 在為專用執行個體租戶設定的 VPC 中使用 Resolver

每個 區域中的傳入和傳出端點數量

當您想要將 AWS 區域中 VPC 的 DNS 與網路的 DNS 整合時，通常需要一個解析器輸入端點 (適用於轉寄至 VPC 的 DNS 查詢) 和一個輸出端點 (用於從 VPC 轉寄到網路的查詢)。您可以建立多個傳入端點和多個傳出端點，但一個傳入或傳出端點就足夠處理每一相應方向的 DNS 查詢。注意下列事項：

- 對於每個 Resolver 端點，您需要指定位於不同可用區域的兩個或更多個 IP 地址。端點中的每個 IP 地址每秒可以處理大量的 DNS 查詢。(如需了解端點中每個 IP 地址每秒的查詢次數的目前上限，請

參閱 Route 53 Resolver 的配額。) 如果您需要 Resolver 來處理更多的查詢，您可以將多個 IP 地址新增到現有的端點，而不是新增其他端點。

- Resolver 定價是根據端點中的 IP 地址數量和該端點處理的 DNS 查詢數量。每個端點包含至少兩個 IP 地址。如需 Resolver 定價的詳細資訊，請參閱 Amazon Route 53 定價。
- 每個規則指定 DNS 查詢轉送自哪個傳出端點。如果您在 AWS 區域中建立多個傳出端點，並且想要將部分或全部 Resolver 規則與每個 VPC 建立關聯，您需要建立這些規則的多個副本。

針對傳入和傳出端點使用相同的 VPC

您可以在相同 VPC 中或相同區域中的不同 VPC 中建立傳入和傳出端點。

如需詳細資訊，請參閱 Amazon Route 53 的最佳實務。

傳入端點和私有託管區域

如果您希望 Resolver 使用私有託管區域中的記錄來解析傳入 DNS 查詢，請將私有託管區域與您建立傳入端點的 VPC 建立關聯。如需有關將私有託管區域與 VPC 建立關聯的詳細資訊，請參閱 使用私有託管區域。

VPC 對等互連

無論您選擇的 VPC 是否與其他 VPC 對等，您都可以將 AWS 區域中的任何 VPC 用於輸入端點或輸出端點。如需詳細資訊，請參閱 Amazon Virtual Private Cloud VPC 對等互連。

共用子網路中的 IP 位址

當您建立傳入或傳出端點時，只有在目前帳戶建立 VPC 時，才能在共用子網路中指定 IP 地址。如果另一個帳戶建立 VPC 並與您的帳戶共用 VPC 中的子網路，則您無法在該子網路中指定 IP 地址。如需共用子網路的詳細資訊，請參閱 Amazon VPC 使用者指南中的使用共用 VPC。

在您的網路和您建立端點的 VPC 之間的連線

在您的網路和您建立端點的 VPC 之間，您必須有以下其中一個連線：

- 傳入端點 – 您必須在網路和每個建立了傳入端點的 VPC 間設定 AWS Direct Connect 連線或 VPN 連接。
- 傳出端點 – 在您的網路和您建立傳出端點的每個 VPC 之間，您必須設定 AWS Direct Connect 連線、VPN 連接或網路位址轉譯 (NAT) 閘道。

當您共用規則時，您也會共用傳出端點

當您建立規則時，您需要指定傳出端點，供 Resolver 用來將 DNS 查詢轉送到您的網路。如果您與其他 AWS 帳戶共用規則，也會間接共用您在規則中指定的輸出端點。如果您使用多個 AWS 帳戶在一個 AWS 區域中建立 VPC，則可以執行下列動作：

- 在該區域中建立一個傳出端點。
- 使用一個 AWS 帳戶建立規則。
- 與區域中建立 VPC 的所有 AWS 帳戶共用規則。

這可讓您使用區域中的一個輸出端點，將多個 VPC 的 DNS 查詢轉寄至您的網路，即使 VPC 是使用不同 AWS 的帳戶建立的。

選擇端點的協定

端點協定確定如何將資料傳輸至傳入端點以及從傳出端點傳輸資料。不需要加密 VPC 流量的 DNS 查詢，因為網路上的每個封包流程都根據規則個別授權，以在傳輸和交付之前驗證正確的來源和目的地。未同時經傳輸和接收實體明確授權，資訊在實體之間任意傳遞的可能性極小。如果封包路由至目的地時沒有與其相符的規則，則此封包會捨棄。如需詳細資訊，請參閱 VPC 功能。

可用的通訊協定包括：

- Do53：透過連接埠 53 的 DNS。透過使用 Route 53 Resolver 轉送資料，而無需額外加密。雖然外部各方無法讀取數據，但可以在 AWS 網絡中查看。使用 UDP 或 TCP 傳送封包。Do53 主要用於 Amazon VPC 內部和之間的流量。
- DoH：透過加密的 HTTPS 工作階段傳輸資料。DoH 新增了額外的安全層級，未經授權的使用者無法解密資料，並且除預期收件人之外的任何人都無法讀取資料。
- DoH-FIPS：透過符合 FIPS 140-2 密碼編譯標準的加密 HTTPS 工作階段傳輸資料。僅支援傳入端點。如需詳細資訊，請參閱 FIPS PUB 140-2。

對於傳入端點，您可以按如下方式套用協定：

- Do53 和 DOH 組合。
- Do53 和 DoH-FIPS 組合。
- 單獨 Do53。
- 單獨 DoH。

- 單獨 DoH-FIPS。
- 無，視為 Do53。

對於傳出端點，您可以按如下方式套用協定：

- Do53 和 DOH 組合。
- 單獨 Do53。
- 單獨 DoH。
- 無，視為 Do53。

另請參閱 當您建立或編輯傳入端點時所指定的值 和 當您建立或編輯傳出端點時所指定的值。

在為專用執行個體租戶設定的 VPC 中使用 Resolver

建立 Resolver 端點時，您無法指定執行個體租用屬性設定為 `dedicated` 的 VPC。Resolver 不會在單一租戶硬體上執行。

您可以繼續使用 Resolver 解析源自於 VPC 的 DNS 查詢。至少建立一個執行個體租用屬性設為 `default` 的 VPC ，並在建立傳入和傳出端點時指定該 VPC。

當您建立轉送規則時，可以將其與任何 VPC 建立關聯，無論該執行個體租用屬性的設定為何。

Route 53 解析器可用性和擴展

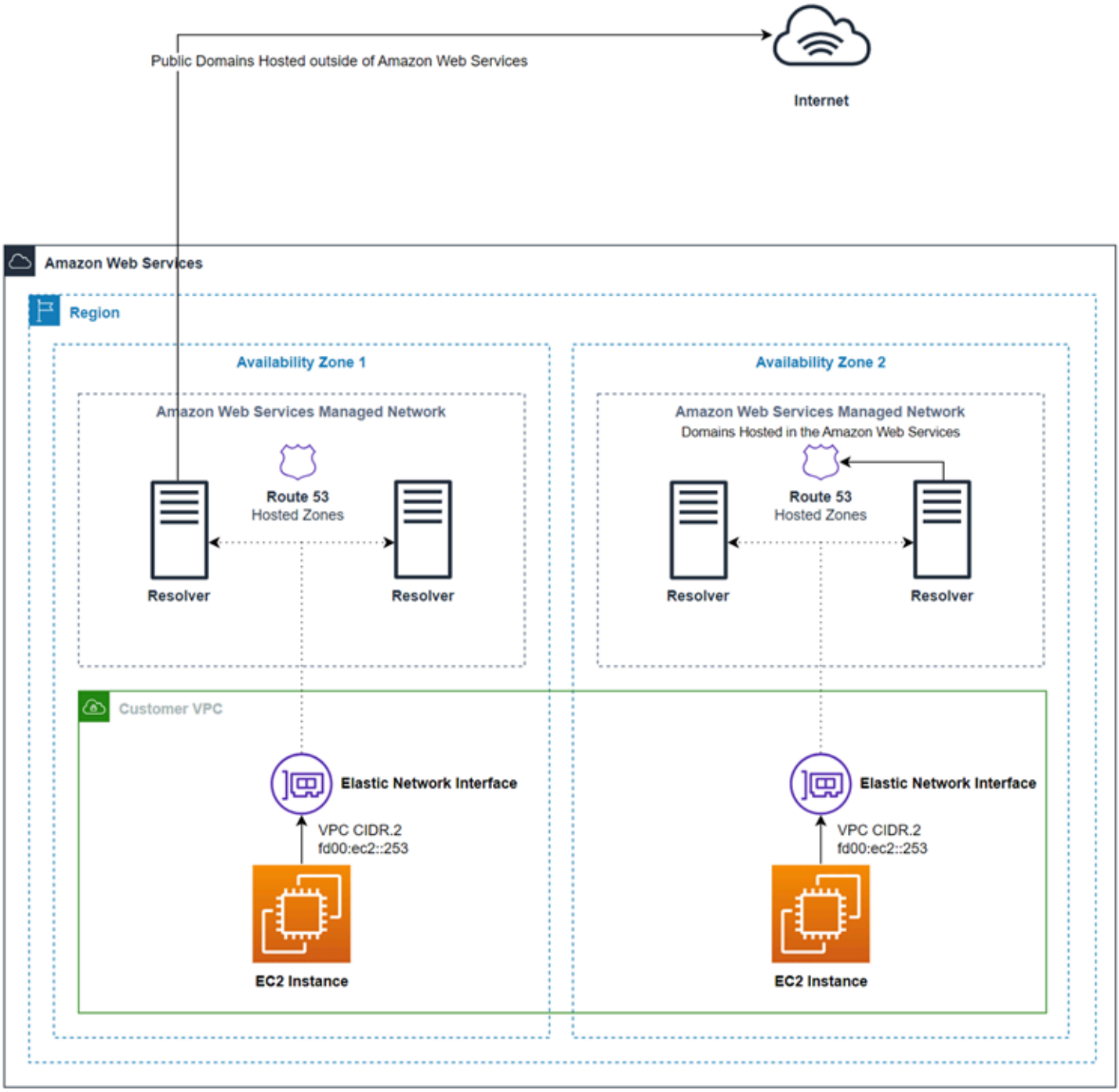
Amazon Route 53 Resolver在 Amazon VPC CIDR + 2 地址和 fd00:ec2:: 253 上執行，預設情況下可在所有 VPC 中使用，並以遞迴方式回應公用記錄的 DNS 查詢、Amazon 虛擬私人雲端專用 DNS 名稱和路由 53 私有託管區域。Route 53 解析器有兩個高可用性元件，對使用者而言是透明的：Nitro 解析器服務和區域解析器叢集。Nitro 解析器服務是一項服務，它在 Nitro 執行個體上的 Nitro 卡中執行，以及在舊一代執行個體的 Dom0 中執行，並在主機伺服器上本機消耗位址至 Route 53 解析器的封包。如需詳細資訊，請參閱 AWS Nitro 系統的安全性設計。

Nitro Resolver 服務帶有本機快取，可回應執行個體在短時間內執行的重複查詢，藉此協助減少延遲。當 Nitro Resolver 服務收到沒有快取回答的查詢時，它會將查詢轉送至 Zonal 解析器叢集，這是一個高可用性的解析器叢集，通常位於與執行個體相同的可用區域中。當上游名稱伺服器或路徑中的其他元件處理查詢時，Nitro Resolver 服務通常能夠透明地處理這些失敗，而不會影響執行個體上執行的工作負載。此外，如果解析器從域名服務器遇到查詢超時，拒絕的連接或 SERVFAILS，則它可能會以超出

存留時間（TTL）值的緩存答案進行響應，以提高可用性。Nitro Resolver 服務與區域解析器叢集之間的查詢僅限於客戶 VPC 以外的嚴密控制網路，客戶無法存取此網路，並受到嚴格的安全控制。透過處理 Nitro 解析器服務與 VPC 以外的區域解析器叢集之間的查詢，可防止客戶在其 VPC 內攔截 DNS 查詢。目的地為外部伺服器命名的查詢 AWS 將遍歷公用網際網路，這些網際網路源自屬於區域解析器叢集的公用 IP 位址。我們目前不支援 EDNS0-Client 子網路屬性，這表示所有傳送至公用 DNS 名稱伺服器的查詢都不包含原始客戶 IP 位址的相關資訊。

Nitro 解析器服務是執行個體上連結本機服務的一部分。連結本機服務包括 Route 53 解析器、Amazon 時間服務 (NTP)、執行個體中繼資料服務 (IMDS) 和 Windows 授權服務 (適用於 Windows 執行個體)。這些服務會隨著您在 VPC 中建立的每個 elastic network interface 進行擴充，每個網路介面允許每秒 1024 個封包 (PPS) 傳送至連結本機服務。超過此限制的封包會遭到拒絕。您可以從 ethtool 傳回的`linklocal_allowance_exceeded`值判斷您是否已超過此限制。如需有關 ethtool 的詳細資訊，請參閱 Amazon EC2 使用者指南中的監控 Amazon EC2 執行個體的網路效能。「CloudWatch代理程式」也可以向測 CloudWatch 量結果報告此測量結果。由於 Route 53 解析器是針對每個網路介面實作，因此當您在更多可用區域中新增更多執行個體時，它會擴展並變得更加可靠。每個 VPC 的查詢數目沒有彙總限制，因此 Route 53 解析器可以在 VPC 的範圍內進行擴展，而這本質上是根據網路位址使用量 (NAU) 而定。如需詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的 VPC 網路地址用量。

下圖顯示 Route 53 解析器如何解析可用區域內解析 DNS 查詢的概觀。



開始使用 Route 53 Resolver

包含精靈的 Route 53 Resolver 主控台會引導您完成以下步驟以開始使用 Resolver：

- 建立端點：傳入、傳出或兩者。
- 對於傳出端點，建立一或多個轉送規則，其會針對您要路由 DNS 查詢到網路來指定網域名稱。

- 如果您建立傳出端點，請選擇您想要與規則建立關聯的 VPC。

使用精靈設定 Route 53 Resolver

1. 登入 AWS Management Console 並開啟解析程式主控台，網址為 https://console.aws.amazon.com/route53resolver/。
2. 在 Welcome to Route 53 Resolver (歡迎來到 Route 53 Resolver) 頁面中，選擇 Configure endpoints (設定端點)。
3. 在導覽列上，選擇您要建立解析程式端點的區域。
4. 在 Basic configuration (基本組態) 下，選擇您希望轉送 DNS 查詢的方向：
   - Inbound and outbound (傳入和傳出)：精靈會引導您完成設定，讓您將 DNS 查詢從您網路的解析程式轉送至 VPC 中的 Resolver，並將指定的查詢 (例如 example.com 或 example.net) 從 VPC 轉送至您網路的解析程式。
   - Inbound only (僅傳入)：精靈會引導您完成設定，讓您將 DNS 查詢從您網路的解析程式轉送至 VPC 中的 Resolver。
   - Outbound only (僅傳出)：精靈會引導您完成設定，讓您將指定的查詢從 VPC 轉送至您網路的解析程式。
5. 選擇下一步。
6. 如果您選擇 Inbound and outbound (傳入和傳出) 或 Inbound only (僅傳入)，請輸入適當的值以設定傳入端點。然後繼續執行步驟 7。如需詳細資訊，請參閱 當您建立或編輯傳入端點時所指定的值。

   如果選擇 Outbound only (僅傳出)，請跳到步驟 7。
7. 輸入適當的值以設定傳出端點。如需詳細資訊，請參閱 當您建立或編輯傳出端點時所指定的值。
8. 如果您選擇 Inbound and outbound (傳入和傳出) 或 Outbound only (僅傳出)，請輸入適當的值以建立規則。如需詳細資訊，請參閱 當您建立或編輯規則時所指定的值。
9. 在 Review and create (檢閱和建立) 頁面中，確認您在前幾頁指定的設定值是正確的。如有必要，請針對適用的部分選擇 Edit (編輯)，並且更新設定。當您滿意設定時，請選擇 Submit (提交)。

   > **Note**
   >
   > 建立傳出端點需要幾分鐘。在第一個傳出端點建立完成前，您無法建立另一個。

10. 如要建立多項規則，請參閱 管理轉送規則。

11. 您已建立傳入端點，請在您的網路上設定 DNS 解析程式，將適當的 DNS 查詢轉送至您傳入端點的 IP 地址。如需詳細資訊，請參閱 DNS 應用程式文件。

將傳入 DNS 查詢轉送到您的 VPC

若要將 DNS 查詢從您的網路轉送到 Resolver，請建立傳入端點。傳入端點會指定您希望網路上的 DNS 解析器將 DNS 查詢轉送到哪些 IP 地址 (從可用的 IP 地址範圍到您的 VPC)。這些 IP 地址不是公有 IP 地址，因此對於每個輸入端點，您需要使用連接或 VPN 連接將 VPC AWS Direct Connect 連接到網絡。

主題

- 設定傳入轉送
- 當您建立或編輯傳入端點時所指定的值

設定傳入轉送

若要建立傳入端點，請執行下列程序。

建立傳入端點

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Inbound endpoints (傳入端點)。
3. 在導覽列上，選擇您要建立傳入端點的區域。
4. 選擇 Create inbound endpoint (建立傳入端點)。
5. 輸入適用的值。如需詳細資訊，請參閱 當您建立或編輯傳入端點時所指定的值。
6. 選擇 Create (建立)。
7. 在您的網路上設定 DNS 解析程式，將適當的 DNS 查詢轉送至您傳入端點的 IP 地址。如需詳細資訊，請參閱 DNS 應用程式文件。

當您建立或編輯傳入端點時所指定的值

當您建立或編輯傳入端點時，請指定下列值：

Outpost ID

如果要在 AWS Outposts VPC 上為解析器建立端點，則此為 ID。 AWS Outposts

Endpoint name (端點名稱)

易記的名稱可讓您在儀表板中輕鬆找出傳入端點。

區域名稱區域中的 VPC

所有來自您網路的傳入 DNS 查詢，都會通過此 VPC 前往 Resolver。

此端點的安全群組

您想用來控制存取此 VPC 之一或多個安全群組的 ID。您指定的安全群組必須包含一或多個傳入規則。傳入規則必須允許連接埠 53 上的 TCP 和 UDP 存取權限。您無法在建立端點之後變更此值。

某些安全群組規則會導致追蹤您的連線，而輸入端點每個 IP 位址每秒的總查詢最高可低至 1500 次。若要避免安全性群組造成的連線追蹤，請參閱未追蹤的連線。

> **Note**
>
> 若要新增多個安全性群組，請使用 AWS CLI 指令`create-resolver-endpoint`。如需詳細資訊，請參閱 create-resolver-endpoint

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 安全群組規則。

端點類型

端點類型可為 IPv4、IPv6 或雙堆疊 IP 地址。對於雙堆疊端點，端點將同時具有 IPv4 和 IPv6 地址，網路上的 DNS 解析程式可將 DNS 查詢轉送至此類地址。

> **Note**
>
> 基於安全理由，我們拒絕從公共互聯網接入所有雙堆棧和 IPv6 IP 地址的 IPv6 流量。

IP 地址

您希望您網路上的 DNS 解析程式將 DNS 查詢轉送到這些 IP 地址。我們需要您至少指定兩個 IP 地址以供備援使用。注意下列事項：

多個可用區域

建議您至少在兩個可用區域中指定 IP 地址。您可以在那些或其他可用區域選擇性指定其他 IP 地址。

IP 地址和 Amazon VPC 彈性網路介面

針對您指定的可用區域、子網路和 IP 地址的各種組合，Resolver 會建立 Amazon VPC 彈性網路介面。如需了解端點中每個 IP 地址每秒的 DNS 查詢次數的目前上限，請參閱 Route 53 Resolver 的配額。如需每個彈性網路介面的定價的相關資訊，請參閱 Amazon Route 53 定價頁面上的「Amazon Route 53」。

> **Note**
>
> Resolver 端點具有私有 IP 地址。這些 IP 位址在端點的生命週期中不會變更。

針對每個 IP 地址，指定以下值。每個 IP 地址都必須位在您指定之 VPC 的可用區域內，您的 VPC 是在 VPC in the region-name Region (區域名稱區域中的 VPC) 中指定。

可用區域

您希望 DNS 查詢通往 VPC 途中所經過的可用區域。您指定的可用區域必須設定子網路。

子網路

包含要指派給解析器端點 ENI 之 IP 位址的子網路。這些是您將發送 DNS 查詢的地址。子網路必須有可用的 IP 地址。

子網路 IP 地址必須符合端點類型。

IP 地址

您想要將 DNS 查詢轉送到此 IP 地址。

選擇要讓 Resolver 從指定之子網路的可用 IP 地址當中為您選擇 IP 地址，還是您想要自己指定 IP 地址。

如果您選擇自行指定 IP 位址，請輸入 IPv4 或 IPv6 位址，或同時輸入兩者。

通訊協定

端點協定確定如何將資料傳輸至傳入端點。根據所需的安全層級，選擇協定。

- Do53： (預設值) 透過使用 Route 53 Resolver 轉送資料，而無需額外加密。雖然外部各方無法讀取資料，但可以在 AWS 網路內檢視資料。
- DoH：透過加密的 HTTPS 工作階段傳輸資料。DoH 新增了額外的安全層級，未經授權的使用者無法解密資料，並且除預期收件人之外的任何人都無法讀取資料。
- DoH-FIPS：透過符合 FIPS 140-2 密碼編譯標準的加密 HTTPS 工作階段傳輸資料。僅支援傳入端點。如需詳細資訊，請參閱 FIPS PUB 140-2。

對於傳入端點，您可以按如下方式套用協定：

- Do53 和 DOH 組合。
- Do53 和 DoH-FIPS 組合。
- 單獨 Do53。
- 單獨 DoH。
- 單獨 DoH-FIPS。
- 無，視為 Do53。

> **Important**
>
> 您無法將傳入端點的協定直接從僅 Do53 變更為僅 DoH 或 DoH-FIPS。這是為了防止依賴 Do53 的傳入流量突然中斷。若要將協定從 Do53 變更為 DoH 或 DoH-FIPS，您必須先同時啟用 Do53 和 DoH，或同時啟用 Do53 和 DoH-FIPS，以確保所有傳入流量都已使用 DoH 協定或 DoH-FIPS 傳輸，然後移除 Do53。

標籤

指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

將傳出 DNS 查詢轉送到您的網路

若要將一或多個 VPC 中的 Amazon EC2 執行個體上所產生的 DNS 查詢轉送到您的網路，請建立傳出端點和一項或多項規則：

傳出端點

若要將 DNS 查詢從 VPC 轉送到網路，請建立傳出端點。傳出端點會指定查詢的來源 IP 地址。您從 VPC 可用的 IP 地址範圍選擇的這些 IP 地址並非公有 IP 地址。也就是說，針對每個傳出端

點，您都需要使用 AWS Direct Connect 連線、VPN 連線或網路位址轉譯 (NAT) 閘道來將 VPC 連接到網路。請注意，您可以在相同的區域為多個 VPC 使用同一個傳出端點，或者也可以建立多個傳出端點。如果您希望輸出端點使用 DNS64，您可以使用 Amazon Virtual Private Cloud 啟用 DNS64。如需更多詳細資訊，請參閱《Amazon VPC 使用者指南》中的「DNS64 和 NAT64」。

解析器隨機選擇 Route 53 解析器規則中的目標 IP，並且沒有偏好選擇特定目標 IP 而不是另一個。如果目標 IP 不響應轉發的 DNS 請求，解析器將重試到另一個 IP。當所有定義的 IP 位址都可用時，會跨目標 IP 位址使用循環配置資源。

規則

若要指定您想要轉送到您網路上 DNS 解析程式之查詢的網域名稱，您可以建立一或多項規則。每項規則指定一個網域名稱。然後，將規則與您要轉送查詢至網路的 VPC 建立關聯。

如需詳細資訊，請參閱下列主題：

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules

設定傳出轉送

要設定 Resolver 將 VPC 中產生的 DNS 查詢轉送到您的網路的，請執行以下程序。

> **Important**
>
> 在建立傳出端點後，您必須建立一或多項規則，並將它們與一或多個 VPC 相關聯。規則指定您想要轉送到您網路的 DNS 查詢的網域名稱。

建立傳出端點

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Outbound endpoints (傳出端點)。
3. 在導覽列上，選擇您要建立傳出端點的區域。
4. 選擇 Create outbound endpoint (建立傳出端點)。
5. 輸入適用的值。如需詳細資訊，請參閱 當您建立或編輯傳出端點時所指定的值。
6. 選擇 Create (建立)。

> **Note**
>
> 建立傳出端點需要幾分鐘。在第一個傳出端點建立完成前，您無法建立另一個。

7. 建立一或多項規則，指定您想要轉送到您網路的 DNS 查詢網域名稱。如需詳細資訊，請參閱下一程序。

若要建立一或多項轉送規則，請執行以下程序。

建立轉送規則並建立規則與一或多個 VPC 的關聯

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇規則。
3. 在導覽列上，選擇您建立規則的區域。
4. 選擇建立規則。
5. 輸入適用的值。如需詳細資訊，請參閱 當您建立或編輯規則時所指定的值。
6. 選擇 Save (儲存)。
7. 若要新增另一個規則，請重複步驟 4 至 6。

當您建立或編輯傳出端點時所指定的值

當您建立或編輯傳出端點時，請指定下列值：

Outpost ID

如果要在 AWS Outposts VPC 上為解析器建立端點，則此為 ID。 AWS Outposts

Endpoint name (端點名稱)

易記的名稱可讓您在儀表板中輕鬆找出傳出端點。

區域名稱區域中的 VPC

所有傳出的 DNS 查詢會流經此 VPC 前往您的網路。

此端點的安全群組

您想用來控制存取此 VPC 之一或多個安全群組的 ID。您指定的安全群組必須包含一或多項傳出規則。傳出規則必須允許您網路 DNS 查詢連接埠上的 TCP 和 UDP 存取。您無法在建立端點之後變更此值。

某些安全群組規則會導致追蹤您的連線，並可能影響從輸出端點到目標名稱伺服器的每秒查詢次數上限。若要避免安全性群組造成的連線追蹤，請參閱未追蹤的連線。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 安全群組規則。

端點類型

端點類型可為 IPv4、IPv6 或雙堆疊 IP 地址。對於雙堆疊端點，端點將同時具有 IPv4 和 IPv6 地址，網路上的 DNS 解析程式可將 DNS 查詢轉送至此類地址。

> **Note**
>
> 出於安全理由，我們拒絕所有雙堆棧和 IPv6 IP 地址的 IPv6 流量直接訪問公共互聯網。

IP 地址

在前往您網路的解析程式途中，您希望 Resolver 將 DNS 查詢轉送至您 VPC 中的這個 IP 地址。這些不是您網路的 DNS 解析程式的 IP 地址；當您建立規則與一或多個 VPC 相關聯時，您會指定解析程式 IP 地址。我們需要您至少指定兩個 IP 地址以供備援使用。

> **Note**
>
> Resolver 端點具有私有 IP 地址。這些 IP 位址在端點的生命週期中不會變更。

注意下列事項：

多個可用區域

建議您至少在兩個可用區域中指定 IP 地址。您可以在那些或其他可用區域選擇性指定其他 IP 地址。

IP 地址和 Amazon VPC 彈性網路介面

針對您指定的可用區域、子網路和 IP 地址的各種組合，Resolver 會建立 Amazon VPC 彈性網路介面。如需了解端點中每個 IP 地址每秒的 DNS 查詢次數的目前上限，請參閱 Route 53

Resolver 的配額。如需每個彈性網路介面的定價的相關資訊，請參閱 Amazon Route 53 定價頁面上的「Amazon Route 53」。

IP 地址的順序

您可以依任何順序指定 IP 地址。轉送 DNS 查詢時，Resolver 不會根據 IP 地址列出的順序選擇 IP 地址。

針對每個 IP 地址，指定以下值。每個 IP 地址都必須位在您指定之 VPC 的可用區域內，您的 VPC 是在 VPC in the region-name Region (區域名稱區域中的 VPC) 中指定。

可用區域

您希望 DNS 查詢通往您網路途中所經過的可用區域。您指定的可用區域必須設定子網路。

子網路

該子網路包含您希望在通往您的網路途中發出 DNS 查詢的 IP 地址。子網路必須有可用的 IP 地址。

子網路 IP 地址必須符合端點類型。

IP 地址

您希望在通往您的網路途中發出 DNS 查詢的 IP 地址。

選擇要讓 Resolver 從指定之子網路的可用 IP 地址當中為您選擇 IP 地址，還是您想要自己指定 IP 地址。

如果您選擇自行指定 IP 位址，請輸入 IPv4 或 IPv6 位址，或同時輸入兩者。

通訊協定

端點協定確定如何從傳出端點傳輸資料。根據所需的安全層級，選擇協定。

- Do53： (預設值) 透過使用 Route 53 Resolver 轉送資料，而無需額外加密。雖然外部各方無法讀取資料，但可以在 AWS 網路內檢視資料。
- DoH：透過加密的 HTTPS 工作階段傳輸資料。DoH 新增了額外的安全層級，未經授權的使用者無法解密資料，並且除預期收件人之外的任何人都無法讀取資料。

對於傳出端點，您可以按如下方式套用協定：

- Do53 和 DOH 組合。
- 單獨 Do53。

- 單獨 DoH。
- 無，視為 Do53。

標籤

指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

當您建立或編輯規則時所指定的值

當您建立或編輯轉送規則時，請指定下列值：

規則名稱

易記的名稱可讓您在儀表板中輕鬆找出規則。

規則類型

請選擇適用的值：

- Forward (轉送) – 當您想要將指定網域名稱的 DNS 查詢轉送到您網路上的解析程式時，請選擇此選項。
- System (系統) – 當您希望 Resolver 選擇性地覆寫轉送規則中定義的行為時，請選擇此選項。當您建立系統規則時，Resolver 會解析指定子網域的 DNS 查詢，否則即由您網路的 DNS 解析程式解析。

根據預設，轉送規則適用於網域名稱及其所有子網域。如果您想要將網域查詢轉送到網路的解析程式，但不想轉送某些子網域的查詢，您可以建立針對子網域的系統規則。例如，如果您為 example.com 建立了轉送規則，但不想轉送 acme.example.com 的查詢，您可以建立一項系統規則，並指定 acme.example.com 為網域名稱。

使用此規則的 VPC

使用此規則轉送指定網域名稱或名稱之 DNS 查詢的 VPC。您可以套用規則至任意數量的 VPC。

網域名稱

此網域名稱的 DNS 查詢會轉送到您在 Target IP addresses (目標 IP 地址) 中指定的 IP 地址。如需詳細資訊，請參閱 Resolver 如何判斷查詢中的網域名稱是否符合任何規則。

傳出端點

Resolver 透過您在此處指定的傳出端點將 DNS 查詢轉送到您在目標 IP 地址中指定的 IP 地址。

目標 IP 地址

當 DNS 查詢符合您在 Domain name (網域名稱) 指定的名稱時，傳出端點會將查詢轉送到您在這裡指定的 IP 地址。這些通常是您網路 DNS 解析程式的 IP 地址。

目標 IP 地址僅在 Rule type (規則類型) 值是 Forward (轉送) 時才可用。

指定 IPv4 或 IPv6 地址，以及要用於端點的協定。

標籤

指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

這些是用於組織 AWS 帳單的標籤。 AWS Billing and Cost Management 如需有關使用成本配置標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

管理傳入端點

若要管理傳入端點，請執行適用的程序。

主題

- 檢視和編輯傳入端點
- 檢視傳入端點的狀態
- 刪除傳入端點

檢視和編輯傳入端點

若要檢視及編輯傳入端點的設定，請執行下列程序。

檢視及編輯傳入端點的設定

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Inbound endpoints (傳入端點)。
3. 在導覽列上，選擇您建立傳入端點的區域。
4. 選擇您想要檢視設定或想要編輯的端點選項。

5. 選擇 View details (檢視詳細資訊) 或 Edit (編輯)。

   如需傳入端點值的資訊，請參閱當您建立或編輯傳入端點時所指定的值。

6. 如果您選擇 Edit (編輯)，請輸入適合的值，然後選擇 Save (儲存)。

檢視傳入端點的狀態

若要檢視傳入端點的狀態，請執行下列程序。

檢視傳入端點的狀態

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Inbound endpoints (傳入端點)。
3. 在導覽列上，選擇您建立傳入端點的區域。Status (狀態) 欄包含以下其中一個值：

   正在建立

   Resolver 正在為此端點建立和設定一或多個 Amazon VPC 網路介面。

   可運作

   此端點的 Amazon VPC 網路介面已正確設定，而且能夠在您的網路和 Resolver 之間傳送傳入或傳出 DNS 查詢。

   更新中

   Resolver 正在建立或取消一或多個網路介面與此端點的關聯。

   自動復原

   Resolver 正在嘗試復原與此端點相關聯的一或多個網路介面。在復原過程中，由於每個 IP 地址 (每個網路介面) 的 DNS 查詢次數有所限制，端點會以有限容量運作。如需目前的限制，請參閱 Route 53 Resolver 的配額。

   需採取動作

   此端點運作狀態不佳，Resolver 無法自動復原它。若要解決該問題，建議您檢查與端點相關聯的每個 IP 地址。對於每個無法使用的 IP 地址，請新增另一個 IP 地址，然後刪除無法使用的 IP 地址。(一個端點一定要包含至少兩個 IP 地址)。狀態為 Action needed (需採取動作) 可能有各式各樣的原因。以下是兩個常見的原因：

   - 已使用 Amazon VPC 刪除與端點相關聯的一或多個網路介面。

- 由於一些已超出 Resolver 所能控制的原因，而無法建立網路介面。

正在刪除

Resolver 正在刪除此端點和相關聯的網路介面。

刪除傳入端點

若要刪除傳入端點，請執行下列程序。

> **Important**
> 如果刪除傳入端點，您網路的 DNS 查詢即不再轉送到您於端點中指定之 VPC 中的 Resolver。

刪除傳入端點

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Inbound endpoints (傳入端點)。
3. 在導覽列上，選擇您建立傳入端點的區域。
4. 選擇您要刪除的端點選項。
5. 選擇 刪除。
6. 若要確認您要刪除該端點，請輸入端點名稱，然後選擇 Submit (提交)。

管理傳出端點

若要管理傳出端點，請執行適用的程序。

主題

- 檢視和編輯傳出端點
- 檢視輸出端點的狀態
- 刪除傳出端點

檢視和編輯傳出端點

若要檢視及編輯傳出端點的設定，請執行下列程序。

檢視及編輯傳出端點的設定

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Outbound endpoints (傳出端點)。
3. 在導覽列上，選擇您建立傳出端點的區域。
4. 選擇您想要檢視設定或想要編輯的端點選項。
5. 選擇 View details (檢視詳細資訊) 或 Edit (編輯)。

   如需傳出端點值的資訊，請參閱 當您建立或編輯傳出端點時所指定的值。
6. 如果您選擇 Edit (編輯)，請輸入適合的值，然後選擇 Save (儲存)。

檢視輸出端點的狀態

若要檢視傳出端點的狀態，請執行下列程序。

檢視傳出端點的狀態

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Outbound endpoints (傳出端點)。
3. 在導覽列上，選擇您建立傳出端點的區域。Status (狀態) 欄包含以下其中一個值：

   正在建立

   Resolver 正在為此端點建立和設定一或多個 Amazon VPC 網路介面。

   可運作

   此端點的 Amazon VPC 網路介面已正確設定，而且能夠在您的網路和 Resolver 之間傳送傳入或傳出 DNS 查詢。

   更新中

   Resolver 正在建立或取消一或多個網路介面與此端點的關聯。

自動復原

Resolver 正在嘗試復原與此端點相關聯的一或多個網路介面。在復原過程中，由於每個 IP 地址 (每個網路介面) 的 DNS 查詢次數有所限制，端點會以有限容量運作。如需目前的限制，請參閱 Route 53 Resolver 的配額。

需採取動作

此端點運作狀態不佳，Resolver 無法自動復原它。若要解決該問題，建議您檢查與端點相關聯的每個 IP 地址。對於每個無法使用用的 IP 地址，請新增另一個 IP 地址，然後刪除無法使用的 IP 地址。(一個端點一定要包含至少兩個 IP 地址)。狀態為 Action needed (需採取動作) 可能有各式各樣的原因。以下是兩個常見的原因：

- 已使用 Amazon VPC 刪除與端點相關聯的一或多個網路介面。
- 由於一些已超出 Resolver 所能控制的原因，而無法建立網路介面。

正在刪除

Resolver 正在刪除此端點和相關聯的網路介面。

刪除傳出端點

在刪除端點之前，您必須先刪除與 VPC 相關聯的任何規則。

若要刪除傳出端點，請執行下列程序。

> **Important**
>
> 如果您刪除傳出端點，則針對指定已刪除傳出端點的那些規則，Resolver 會停止將 DNS 查詢從您的 VPC 轉送到您的網路。

刪除傳出端點

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Outbound endpoints (傳出端點)。
3. 在導覽列上，選擇您建立傳出端點的區域。
4. 選擇您要刪除的端點選項。
5. 選擇 刪除。

6. 若要確認您要刪除該端點，請輸入端點名稱，然後選擇 Submit (提交)。

管理轉送規則

如果您希望 Resolver 將指定網域名稱的查詢轉送到您的網路，您可以針對每個網域名稱建立一項轉送規則，並指定要轉送查詢的網域名稱。

主題

- 檢視和編輯轉送規則
- 建立轉送規則
- 新增反向查詢的規則
- 建立轉送規則與 VPC 的關聯
- 取消轉送規則與 VPC 的關聯
- 與其他 AWS 帳戶共享解析器規則並使用共享規則
- 刪除轉送規則
- Resolver 中反向 DNS 查詢的轉送規則

檢視和編輯轉送規則

若要檢視及編輯轉送規則設定，請執行下列程序。

檢視和編輯轉送規則設定

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇規則。
3. 在導覽列上，選擇您建立規則的區域。
4. 選擇您想要檢視設定或想要編輯的規則選項。
5. 選擇 View details (檢視詳細資訊) 或 Edit (編輯)。

   如需轉送規則值的資訊，請參閱當您建立或編輯規則時所指定的值。
6. 如果您選擇 Edit (編輯)，請輸入適合的值，然後選擇 Save (儲存)。

建立轉送規則

若要建立一或多項轉送規則，請執行以下程序。

建立轉送規則並建立規則與一或多個 VPC 的關聯

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇規則。
3. 在導覽列上，選擇您建立規則的區域。
4. 選擇建立規則。
5. 輸入適用的值。如需詳細資訊，請參閱 當您建立或編輯規則時所指定的值。
6. 選擇 Save (儲存)。
7. 若要新增另一個規則，請重複步驟 4 至 6。

新增反向查詢的規則

如果您需要控制 VPC 中的反向查詢，則可以將規則新增至傳出解析程式端點。

建立反向查詢規則

1. 依照上一個程序中的步驟進行，直到執行至步驟 5。
2. 當您指定規則時，請輸入 PTR 記錄您想要使用反向查詢轉送規則的一個或多個 IP 地址。

   例如，若您需要轉送查詢 10.0.0.0/23 範圍內的地址，請輸入兩個規則：

   - 0.0.10.in-addr-arpa
   - 1.0.10.in-addr-arpa

   這些子網路中的任何 IP 地址都會參考為這些 PTR 記錄的子網域 — 例如，10.0.1.161 的反向查詢地址為 161.1.0.10.in-addr.arpa，也就是 1.0.10.in-addra.arpa 的子網域。
3. 指定要轉送這些查詢的目標伺服器。
4. 將這些規則新增至傳送解析程式端點。

請注意，為 VPC 開啟 enableDNSHostNames 會自動新增 PTR 記錄。請參閱 什麼是 Amazon Route 53 Resolver？。只有當您想要明確指定 IP 範圍的解析程式時，才需要先前的程序 — 例如，將查詢轉送至 Active Directory 伺服器時。

建立轉送規則與 VPC 的關聯

建立轉送規則後，您必須建立規則與一或多個 VPC 的關聯。這些規則只有在與 VPC 相關聯後才有效。當您建立規則與 VPC 的關聯時，Resolver 即開始將規則中指定之網域名稱的 DNS 查詢轉送到您在規則中指定的 DNS 解析程式。查詢會通過您在建立規則時所指定的傳出端點。

建立轉送規則與一或多個 VPC 的關聯

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇規則。
3. 在導覽列上，選擇您建立規則的區域。
4. 選擇您想與一或多個 VPC 建立關聯的規則名稱。
5. 選擇 Associate VPC (關聯 VPC)。
6. 在 VPCs that use this rule (使用此規則的 VPC) 下，選擇想與規則關聯的 VPC。
7. 選擇新增。

取消轉送規則與 VPC 的關聯

下列情況可以取消轉送規則與 VPC 的關聯：

- 針對產生自此 VPC 的 DNS 查詢，您希望 Resolver 停止將規則中指定之網域名稱的查詢轉送到您的網路。
- 您要刪除轉送規則。如果規則目前與一或多個 VPC 相關聯，您必須先取消規則與所有 VPC 的關聯，才能刪除規則。

如果您想要取消轉送規則與一或多個 VPC 的關聯，請執行下列程序。

取消轉送規則與 VPC 的關聯

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

2. 在導覽窗格中，選擇規則。
3. 在導覽列上，選擇您建立規則的區域。
4. 選擇您想要與一或多個 VPC 取消關聯的規則名稱。
5. 選擇您想要與規則取消關聯的 VPC 選項。
6. 選擇取消關聯。
7. 輸入 disassociate 以確認。
8. 選擇提交。

與其他 AWS 帳戶共享解析器規則並使用共享規則

您可以與其 AWS 他帳戶共用您使用一個 AWS 帳戶建立的解析器規則。若要共用規則，Route 53 解析程式主控台會與 Res AWS ource Access Manager 整合。如需 Resource Access Manager 的詳細資訊，請參閱 Resource Access Manager 使用者指南。

注意下列事項：

建立共享規則與 VPC 的關聯

如果其他 AWS 帳戶與您的帳戶共用了一或多個規則，您可以使規則與 VPC 產生關聯，方式與您建立的規則與 VPC 相關聯。如需詳細資訊，請參閱 建立轉送規則與 VPC 的關聯。

刪除或停止共享規則

如果您與其他帳戶共享規則，然後刪除或停止共享該規則，而且如果該規則與一或多個 VPC 相關聯，則 Route 53 Resolver 會根據剩餘的規則開始處理這些 VPC 的 DNS 查詢。此行為和您取消規則與 VPC 的關聯一樣。

如果將規則共用至組織單位 (OU)，且 OU 中的帳戶移至不同的 OU，則會刪除共用規則與帳戶中任何 VPC 之間的所有關聯。

規則和關聯的數目上限

當帳戶建立規則並與一或多個其他帳戶共用時，每個 AWS 區域的規則數目上限會套用至建立該規則的帳戶。

當共享規則的帳戶建立此規則與一或多個 VPC 的關聯時，每個區域規則與 VPC 間關聯數的上限即適用於共享此規則的帳戶。

如需目前的 Resolver 配額，請參閱 Route 53 Resolver 的配額。

許可

若要與其他 AWS 帳號共用規則，您必須擁有使用該PutResolverRulePolicy動作的權限。

規則共用的 AWS 帳戶限制

共用規則的帳戶無法變更或刪除規則。

標記

只有建立規則的帳戶可以新增、刪除或檢視規則的標籤。

若要檢視規則目前的共用狀態 (包括共用帳戶的帳戶或共用規則的帳戶)，以及與其他帳戶共用規則，請執行以下程序。

檢視共用狀態和與其他 AWS 帳戶共用規則

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇規則。
3. 在導覽列上，選擇您建立規則的區域。

   Sharing status (共用狀態) 欄顯示規則目前的共享狀態，它們是目前帳戶建立的規則或與目前帳戶共用的規則：

   - 未共用：目前 AWS 帳戶已建立規則，且該規則不會與任何其他帳戶共用。
   - Shared by me (由我共用)：目前的帳戶建立了規則，且與一或多個帳戶共用。
   - Shared with me (與我共用)：另一個帳戶建立了規則，且與目前的帳戶共用。
4. 選擇您想要顯示共用資訊的規則名稱，或您想要與其他帳戶共用的規則名稱。

   在 Rule: ***rule name*** (規則：規則名稱) 頁面中，Owner (擁有者) 下的值會顯示建立規則的帳戶 ID。除非 Sharing status (共用狀態) 的值為 Shared with me (與我共用)，否則即為目前的帳戶。若是如此，Owner (擁有者) 即為建立了規則，且與目前帳戶共用規則的帳戶。
5. 選擇 Share (共用) 以檢視更多資訊，或與其他帳戶共用規則。Resource Access Manager 主控台會顯示一個頁面，視 Sharing status (共用狀態) 的值而定：

   - Not shared (不共用)：顯示 Create resource share (建立資源共用) 頁面。如需如何與其他帳戶、OU 或組織共用規則的資訊，請跳到步驟 6。
   - Shared by me (由我共用)：Shared resources (共用的資源) 頁面會顯示目前帳戶所擁有的規則和其他資源，以及與其他帳戶共用的規則和資源。

- Shared with me (與我共用)：Shared resources (共用的資源) 頁面會顯示其他帳戶所擁有的規則和其他資源，以及與目前帳戶共用的規則和資源。

6. 若要與其他 AWS 帳戶、OU 或組織共用規則，請指定下列值。

> **Note**
>
> 您無法更新共用設定。如果您想要變更以下任一設定，您必須重新共用使用新設定的規則，然後移除舊的共用設定。

描述

輸入有助於您記憶為何共享規則的簡短描述。

資源

選擇您要共享之規則的核取方塊。

主體

輸入 AWS 帳號、OU 名稱或組織名稱。

標籤

指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

這些是用於組織 AWS 帳單的標籤；您也可以將標籤用於其他用途。 AWS Billing and Cost Management 如需有關使用成本配置標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

刪除轉送規則

若要刪除轉送規則，請執行以下程序。

注意下列事項：

- 如果轉送規則與任何 VPC 相關聯，您必須先取消規則與該 VPC 的關聯，才能刪除規則。如需詳細資訊，請參閱 取消轉送規則與 VPC 的關聯。
- 您無法刪除預設的網際網路解析程式規則，其 Type (類型) 值為 Recursive (遞迴)。對於您未建立自訂規則，而且 Resolver 也未建立自動定義規則的任何網域名稱，這個規則會使 Route 53 Resolver

成為遞迴解析程式。如需如何分類規則的詳細資訊，請參閱使用規則來控制哪些查詢轉送到您的網路。

刪除轉送規則

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇規則。
3. 在導覽列上，選擇您建立規則的區域。
4. 選擇您要刪除的規則選項。
5. 選擇 刪除。
6. 若要確認您要刪除該規則，請輸入規則名稱，然後選擇 Submit (提交)。

Resolver 中反向 DNS 查詢的轉送規則

當 `enableDnsHostnames` 和 `enableDnsSupport` 為來自 Amazon VPC 的 Virtual Private Cloud (VPC) 設定為 `true` 時，Resolver 會自動為反向 DNS 查詢建立自動定義的系統規則。如需這些設定的詳細資訊，請參閱《Amazon VPC 開發人員指南》中的「VPC 中的 DNS 屬性」。

反向 DNS 查詢的轉送規則對於 SSH 或 Active Directory 等服務特別有用，這些服務可以選擇透過對客戶嘗試連線到資源的 IP 地址執行反向 DNS 查詢來驗證使用者。如需自動定義之系統規則的詳細資訊，請參閱 Resolver 建立自動定義規則所針對的網域名稱。

您可以關閉這些規則並修改所有反向 DNS 查詢，讓這些查詢可轉送至您的內部部署名稱伺服器以進行解析。

關閉自動規則之後，請建立規則，視需要將查詢轉送至您的內部部署資源。如需有關如何管理轉送規則的詳細資訊，請參閱 管理轉送規則。

若要關閉自動定義規則

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格的 Resolver 下，選擇 VPCs，然後選擇 VPC ID。
3. 在 Autodefined rules for reverse DNS resolution (反向 DNS 解析的自動定義規則) 下，取消選取核取方塊。如果核取方塊已經取消選取，您可以選取它來開啟自動定義的反向 DNS 解析。

如需相關的 API，請參閱 Resolver 組態 API。

在 Amazon Route 53 中啟用 DNSSEC 驗證

當您在 Amazon Route 53 中針對 Virtual Private Cloud (VPC) 啟用 DNSSEC 驗證時，會以密碼編譯方式檢查 DNSSEC 簽章，以確保回應未遭竄改。您可以在 VPC 詳細資料頁面上啟用 DNSSEC 驗證。

DNSSEC 驗證會在執行遞迴 DNS 解析時，由 Route 53 Resolver 套用至公用簽署名稱。

不過，如果 Route 53 Resolver 正在轉送至另一個 DNS 解析程式，而該解析程式正在執行遞迴 DNS 解析，那麼也必須套用 DNSSEC 驗證。

> **Important**
>
> 啟用 DNSSEC 驗證可能會影響來自 VPC 中 AWS 資源的公有 DNS 記錄的 DNS 解析，這可能會導致中斷。請注意，啟用或停用 DNSSEC 驗證需要幾分鐘的時間。

> **Note**
>
> 此時， Amazon Route 53 Resolver 在您的 VPC (又名 AmazonProvided DNS) 中會忽略 DNS 查詢中的 DO (DNSSEC 確定) EDNS 標頭位元和 CD (檢查停用) 位元。如果您已設定 DNSSEC，這意味著雖然 Route 53 Resolver 確實已執行 DNSSEC 驗證，但它並未返回 DNSSEC 記錄，也未在回應中設定 AD 位元。因此，Route 53 Resolver 當前不支援執行自己的 DNSSEC 驗證。如果您需要這樣做，則需要執行自己的遞迴 DNS 解析。

啟用 VPC 的 DNSSEC 驗證

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中的 Resolver 下，選擇 VPC。
3. 在 DNSSEC 驗證下方，選取核取方塊。如果已選取核取方塊，您可以取消選取此核取方塊以停用 DNSSEC 驗證。

   請注意，啟用或停用 DNSSEC 驗證需要幾分鐘的時間。

將網際網路流量路由到您的 AWS 資源

您可以使用 Amazon Route 53 將流量路由到各種 AWS 資源。

- 使用網域名稱將流量路由到 Amazon API Gateway API
- 使用您的網域名稱將流量路由到 Amazon CloudFront 分發
- 將流量路由到 Amazon EC2 執行個體
- 將流量路由到 AWS App Runner 服務
- 將流量路由到 AWS Elastic Beanstalk 環境
- 將流量路由到 ELB 負載平衡器
- 將流量路由到 Amazon S3 儲存貯體中託管的網站
- 使用網域名稱將流量路由到 Amazon Virtual Private Cloud 介面端點
- 將流量路由到 Amazon WorkMail
- 將流量路由到其他 AWS 資源
- 使用 AWS CloudFormation 建立 Amazon Route 53 和 Amazon Route 53 Resolver 資源

使用網域名稱將流量路由到 Amazon API Gateway API

您可以使用 Amazon API Gateway 來建立、發佈、維護、監控 API，並保護其安全。除了 AWS 雲端中所存放的資料，您還可以建立可存取 AWS 服務或其他 Web 服務的 API。

無論您是否已建立區域 API Gateway 端點或邊緣最佳化 API Gateway 端點，用來將網域流量路由到 API Gateway API 的方法都是相同的。

- 區域 API 端點：您建立將流量路由到區域 API 端點的 Route 53 別名記錄。
- 邊緣最佳化 API 端點：您會建立將流量路由到邊緣最佳化 API 的 Route 53 別名記錄。這會導致流量路由至與邊緣最佳化 API 相關聯的 CloudFront 發佈。

別名記錄是與 CNAME 記錄類似的 DNS 的 Route 53 延伸。如需別名和 CNAME 記錄的比較，請參閱選擇別名或非別名記錄。

> **Note**
>
> 對於 API Gateway API 或其他 AWS 資源的別名查詢，Route 53 不收取費用。

主題

- 必要條件
- 設定 Route 53 將流量路由到 API Gateway 端點

必要條件

若要開始使用，您需要滿足以下條件：

- API Gateway API 具有自訂網域名稱 (如 api.example.com)，且符合您要建立的 Route 53 記錄名稱。

  如需詳細資訊，請參閱下列主題：

  - 《Amazon API Gateway 開發人員指南》中的「設定 HTTP API 的自訂網域名稱」
  - 《Amazon API Gateway 開發人員指南》中的「設定 REST API 的自訂網域名稱」
  - 在 Amazon API 閘道開發人員指南中為 WebSocket API 設定自訂網域名稱。
- 註冊的網域名稱。您可以使用 Amazon Route 53 做為網域註冊商，也可以使用不同的註冊商。
- Route 53 做為網域的 DNS 服務。如果您使用 Route 53 註冊網域名稱，我們會將 Route 53 自動設定為網域的 DNS 服務。

  如需使用 Route 53 做為您網域 DNS 服務提供者的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

設定 Route 53 將流量路由到 API Gateway 端點

若要設定 Route 53 將流量路由到 API Gateway 端點，請執行下列程序。

若要將流量路由到 API Gateway 端點

1. 如果您已使用相同的帳戶建立 Route 53 託管區域和端點，請跳到步驟 2。

   如果您使用不同的帳戶建立託管區域和端點，請取得您要使用的自訂網域名稱的目標網域名稱：

   a. 登入 AWS Management Console 並在 https://console.aws.amazon.com/apigateway/ 開啟 API Gateway 主控台。
   b. 在導覽窗格中，選擇 Custom domain names (自訂網域名稱)。
   c. 選擇您要使用的自訂網域名稱，並取得 API Gateway domain name (API Gateway 網域名稱) 的值。

2. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 選擇託管區域的名稱，該託管區域具有要用來將流量路由到 API 的網域名稱。
5. 選擇建立記錄。
6. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入要將流量路由到 API 所使用的網域名稱。

   您要路由流量的目的地 API 必須具有自訂網域名稱 (如 api.example.com)，且符合 Route 53 記錄的名稱。

   別名

   如果您是使用 Quick create (快速建立) 記錄建立方法，請開啟 Alias (別名)。

   值/將流量路由到

   選擇 Alias to API Gateway API (API Gateway API 的別名)，然後選擇端點所來自的區域。

   指定 Endpoint (端點) 值的方式，取決於您是否使用相同的 AWS 帳戶或不同帳戶來建立託管區域和 API：

   - 相同帳戶 – 目標網域名稱的清單僅包含具有自訂網域名稱，且該名稱與您為 Record name (記錄名稱) 指定的值相符的 API。請選擇適用的值。
   - 不同帳戶 – 輸入您在此程序的步驟 1 中取得的值。

   記錄類型

   選擇 A – IPv4 地址。

   評估目標運作狀態

   為了控制 DNS 備援功能，請設定自訂運作狀態檢查。如需範例，請參閱《API Gateway 使用者指南》中的設定 DNS 備援的自訂運作狀態檢查。
7. 選擇建立記錄。

變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當傳播完成，您就可以使用在此程序中建立的別名記錄的名稱，將流量路由到 API。

使用您的網域名稱將流量路由到 Amazon CloudFront 分發

您可以使用 Amazon CloudFront（內AWS容交付網絡（CDN）作為加快 Web 內容交付速度的一種方法。 CloudFront 可以使用全球節點網路，提供您的整個網站，包括動態、靜態、串流和互動式內容。請求您內容的使用者會自動路由到可為其提供最低延遲的邊緣節點。

> **Note**
>
> 您可以將流量路由到僅適用於公有託管區域的 CloudFront 發佈。

若要用 CloudFront 來發佈您的網站內容，請建立分發並為其指定設定。例如，指定您要 CloudFront 從中取得內容的 Amazon S3 儲存貯體或 HTTP 伺服器、是否只希望選定的使用者能夠存取您的內容，以及是否希望使用者使用 HTTPS。

當您建立分發時， CloudFront 會將網域名稱指派給該分發，例如d111111abcdef8.cloudfront.net。您可以在內容的 URL 中使用此網域名稱，例如：

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

或者，您可以在 URL 中使用自己的網域名稱，例如：

```
http://example.com/logo.jpg
```

請遵循 Amazon CloudFront 開發人員指南中的步驟，在 CloudFront分發中的檔案 URL 中使用您自己的網域名稱，而不是指 CloudFront 派給分發的網域名稱。如需使用您自己的網域名稱搭配 CloudFront 發佈的詳細資訊，請參閱透過新增替代網域名稱 (CNames) 使用自訂 URL。

當您將 Route 53 網域名稱與分發搭 CloudFront 配使用時，請使用 Amazon Route 53 建立指向您的 CloudFront 分佈的別名記錄。別名記錄是 DNS 的 Route 53 延伸。別名記錄與 CNAME 記錄類似，但您可以同時為根網域 (如 example.com) 和子網域 (如 www.example.com) 建立別名記錄。(只可以為子網域建立 CNAME 記錄。) 當 Route 53 收到與別名記錄的名稱和類型均相符的 DNS 查詢時，Route 53 會使用與分佈關聯的網域名稱來回應。

> **Note**
>
> Route 53 對於 CloudFront 發行版或其他AWS資源的別名查詢不收取費用。

必要條件

若要開始使用，您需要滿足以下條件：

1. 註冊的網域名稱。您可以使用 Amazon Route 53 做為網域註冊商，也可以使用不同的註冊商。
2. Route 53 做為網域的 DNS 服務。如果您使用 Route 53 註冊網域名稱，我們會將 Route 53 自動設定為網域的 DNS 服務。

   如需使用 Route 53 做為您網域 DNS 服務提供者的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。
3. 請求公開憑證，以便 Amazon CloudFront 分發需要 HTTPS。如需詳細資訊，請參閱《AWS Certificate Manager 使用者指南》中 AWS Certificate Manager 的 步驟 2：請求公有憑證 和 DNS 驗證。
4. 一個 CloudFront 分佈。分發必須包含一個替代域名，該域名與您要用於 URL 的域名相匹配，而不是分配給分配 CloudFront 給分配的域名。

   例如，如果希望內容的 URL 包含網域名稱 example.com，分佈的 Alternate Domain Name (替代網域名稱) 欄位就必須包含 example.com。

   如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的下列文件：

   - 建立分佈的任務清單
   - 使用 CloudFront 主控台建立或更新分佈

設定 Amazon 路由 53 以將流量路由到分 CloudFront 發

若要設定 Amazon Route 53 以將流量路由到 CloudFront 分發，請按照下列步驟操作。如需將您自己的網域名稱與分發搭 CloudFront 配使用的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的透過新增替代網域名稱 (CNames) 來使用自訂 URL。

> **Note**
>
> 變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當變更傳播時，您可以使用您在此程序中建立的別名記錄名稱，將流量路由到您的 CloudFront 發佈。

若要將流量路由到 CloudFront 分佈

1. 獲取分配 CloudFront 給您的分發的域名，並確定是否啟用 IPv6：

   a. 登入AWS Management Console並開啟 CloudFront 主控台，位於https://console.aws.amazon.com/cloudfront/v4/home。

   b. 在 ID 欄中，選取您要將流量路由到的分佈連結名稱 (非核取方塊)。

   c. 在 General (一般) 索引標籤上，取得 Distribution Domain Name (分佈網域名稱) 欄位的值。

   d. 在 General (一般) 索引標籤的 Settings (設定) 區段中，選擇 edit (編輯) 並捲動以檢查 IPv6 欄位，查看該發行版是否已啟用 IPv6。如果已啟用 IPv6，您將需要為分佈建立兩個別名記錄，一個用於將 IPv4 流量路由到分佈，一個用於路由 IPv6 流量。選擇取消。

      如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中您在建立或更新分發時指定的值主題中的啟用 IPv6。

2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 針對您要用來將流量路由到您的 CloudFront 分發的網域，選擇託管區域的連結名稱。
5. 選擇建立記錄。

   您可以使用精靈來建立記錄，或選擇 Switch to quick create (切換至快速建立)。

6. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入您要用來將流量路由到您的 CloudFront 分發的網域名稱。預設值為託管區域名稱。

例如，如果託管區域的名稱是 example.com，而您想要使用 acme.example.com 將流量路由到您的分佈，請輸入 acme。

別名

如果您是使用 Quick create (快速建立) 記錄建立方法，請開啟 Alias (別名)。

> **Important**
> 您必須建立「別名」記錄，才能使 CloudFront 發佈工作。

值/將流量路由到

選擇 CloudFront 分配的別名。根據預設，選擇 us-east-1 區域。選擇在創建分發時分配 CloudFront 給分發的域名。這是您在步驟 1 中取得的值。

記錄類型

選擇 A – IPv4 地址。

如果已為分佈啟用 IPv6，而且您要建立第二個記錄，請選擇 AAAA - IPv6 address (AAAA - IPv6 地址)。

評估目標運作狀態

接受預設值 No (否)。

7. 選擇建立記錄。
8. 如果已為分佈啟用 IPv6，請重複步驟 5 到 7。對除了記錄類型欄位以外的其餘欄位指定相同設定，如步驟 6 中所說明。

將流量路由到 Amazon EC2 執行個體

Amazon EC2 在 AWS 雲端中提供可擴展的運算容量。您可以使用預先設定的範本 (Amazon Machine Image，即 AMI) 來啟動 EC2 虛擬運算環境 (執行個體)。當您啟動 EC2 執行個體時，EC2 會自動安裝作業系統 (Linux 或 Microsoft Windows) 和包含在 AMI 中的其他軟體，例如 Web 伺服器或資料庫軟體。

如果您在 EC2 執行個體上託管網站或執行 Web 應用程式，可以使用 Amazon Route 53 將網域 (例如 example.com) 的流量路由到您的伺服器。

必要條件

若要開始使用，您需要滿足以下條件：

- Amazon EC2 執行個體。如需啟動 EC2 執行個體的資訊，請參閱下列文件：
  - Linux - 請參閱 Amazon EC2 Linux 執行個體使用者指南中的 Amazon EC2 Linux 執行個體入門。
  - Microsoft Windows - 請參閱 Amazon EC2 Windows 執行個體使用者指南中的 Amazon EC2 Windows 執行個體入門。

  > **Important**
  >
  > 我們建議您也建立彈性 IP 地址，並將其與您的 EC2 執行個體關聯。彈性 IP 地址可確保您的 Amazon EC2 執行個體的 IP 地址永遠不會變更。如需有關定價的資訊，請參閱彈性 IP 地址定價。

- 註冊的網域名稱。您可以使用 Amazon Route 53 做為網域註冊商，也可以使用不同的註冊商。
- Route 53 做為網域的 DNS 服務。如果您使用 Route 53 註冊網域名稱，我們會將 Route 53 自動設定為網域的 DNS 服務。

  如需使用 Route 53 做為您網域 DNS 服務提供者的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

設定 Amazon Route 53 將流量路由到 Amazon EC2 執行個體

若要設定 Amazon Route 53 將流量路由到 EC2 執行個體，請執行下列程序。

若要將流量路由到 Amazon EC2 執行個體

1. 取得 Amazon EC2 執行個體的 IP 地址：
   a. 請登入 AWS Management Console，並在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
   b. 在主控台右上角的區域清單中，選擇您啟動執行個體所在的區域。
   c. 在導覽窗格中，選擇執行個體。
   d. 在表格中，選擇您要將流量路由到的執行個體。
   e. 在底部窗格的 Description (描述) 標籤上，取得 Elastic IPs (彈性 IP) 的值。

如未建立彈性 IP 與執行個體的關聯，請取得 IPv4 Public IP (IPv4 公有 IP) 的值。

2. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 選擇符合要路由流量之網域名稱的託管區域名稱。
5. 選擇建立記錄。
6. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入要將流量路由到 EC2 執行個體所使用的網域名稱。預設值為託管區域名稱。

   例如，如果託管區域的名稱是 example.com，而您想要使用 acme.example.com 將流量路由到您的 EC2 執行個體，請輸入 acme。

   值/將流量路由到

   選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)。輸入您在步驟 1 中取得的 IP 地址。

   記錄類型

   選擇 A – IPv4 地址。

   TTL (秒)

   接受預設值 300。
7. 選擇建立記錄。

變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當傳播完成，您就可以使用在此程序中建立的記錄的名稱，將流量路由到 EC2 執行個體。

> **Important**
>
> 如果您釋放彈性 IP，請務必同時刪除指向它的 DNS 記錄。如果不這樣做，您會取得一個懸置的 DNS 記錄，可以由未經授權的使用者接管。

將流量路由到 AWS App Runner 服務

AWS App Runner 是一種全受管服務，可讓開發人員輕鬆地大規模部署容器化 Web 應用程式和 API，而且不需要先前的基礎架構經驗。從您的原始碼或容器映像開始。App Runner 會自動建置及部署 Web 應用程式，透過加密來負載平衡流量，擴展以滿足您的流量需求，並使您的服務能夠輕鬆與在私有 Amazon VPC 中執行的其他 AWS 服務和應用程式進行通訊。使用 App Runner，而不考慮使用伺服器或擴展，您會有更多時間專注於您的應用程式。如需詳細資訊，請參閱 AWS App Runner 開發人員指南中的什麼是 AWS App Runner。

> **Important**
>
> Amazon Route 53 目前支援 2022 年 8 月 1 日之後所建立 AWS App Runner 服務的別名記錄。

若要將網域流量路由到 App Runner 服務，請使用 Amazon Route 53 建立指向 App Runner 服務的別名記錄。別名記錄是 DNS 的 Route 53 延伸。別名記錄與 CNAME 記錄類似，唯一例外是您可以同時為根網域 (如 example.com) 和子網域 (如 www.example.com，http://www.example.com/) 建立別名記錄。僅可為子網域建立 CNAME 記錄。

> **Note**
>
> 對於針對 App Runner 服務或其他 AWS 資源的別名查詢，Route 53 不收取費用。

必要條件

若要開始使用，您需要滿足以下條件：

- App Runner 服務。如需建立 App Runner 服務的相關資訊，請參閱開始使用 App Runner。
- 註冊的網域名稱。您可以使用 Amazon Route 53 做為網域註冊商，也可以使用不同的註冊商。
- Route 53 做為網域的 DNS 服務。如果您使用 Route 53 註冊網域名稱，我們會將 Route 53 自動設定為網域的 DNS 服務。

  如需使用 Route 53 做為您網域 DNS 服務提供者的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。
- 將自訂網域關聯到 App Runner 服務。如需詳細資訊，請參閱管理 App Runner 的自訂網域名稱。

- 設定 App Runner 傳回給您 Route 53 託管區域的憑證驗證記錄，以啟動網域驗證程序。如需詳細資訊，請參閱《AWS Certificate Manager 使用者指南》中 AWS Certificate Manager 的 DNS 驗證。

設定 Amazon Route 53 將流量路由到 App Runner 服務

若要設定 Amazon Route 53 將流量路由到 App Runner 服務，請執行下列程序。

若要將流量路由到 App Runner 服務

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇符合要路由流量之網域名稱的託管區域名稱。
4. 選擇建立記錄。
5. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入要將流量路由到 App Runner 服務所使用的網域名稱。預設值為託管區域名稱。

   例如，如果託管區域的名稱是 example.com，而您想要使用 acme.example.com 將流量路由到 App Runner 服務，請輸入 acme。

   值/將流量路由到

   選擇 App Runner 服務的別名，然後選擇 AWS 區域。選擇您要將流量路由到的環境的網域名稱。

   記錄類型

   接受預設值 A – IPv4 address (A – IPv4 地址)。

   評估目標運作狀態

   接受預設值 Yes (是)。
6. 選擇建立記錄。

   變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當傳播完成時，您就可以使用在此程序中所建立別名記錄的名稱，將流量路由到 App Runner 服務。

將流量路由到 AWS Elastic Beanstalk 環境

如果您使用 AWS Elastic Beanstalk 在 AWS 雲端中部署和管理應用程式，可以使用 Amazon Route 53 將網域 (例如 example.com) 的 DNS 流量路由到新的或現有 Elastic Beanstalk 環境。

若要將 DNS 流量路由到 Elastic Beanstalk 環境，請參閱下列主題中的程序。

> **Note**
>
> 這些程序假設您已使用 Route 53 做為網域的 DNS 服務。如果您使用的是另一項 DNS 服務，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務 以取得使用 Route 53 做為您網域 DNS 服務提供者的資訊。

主題

- 將應用程式部署至 Elastic Beanstalk 環境
- 取得 Elastic Beanstalk 環境的網域名稱
- 建立將流量路由到 Elastic Beanstalk 環境的 Amazon Route 53 記錄

將應用程式部署至 Elastic Beanstalk 環境

如果您已經有要將流量路由到的 Elastic Beanstalk 環境，請跳到 取得 Elastic Beanstalk 環境的網域名稱。

若要建立應用程式並將其部署至 Elastic Beanstalk 環境

- 如需建立應用程式並將其部署到 Elastic Beanstalk 環境的詳細資訊，請參閱 AWS Elastic Beanstalk 開發人員指南中的開始使用 Elastic Beanstalk。

取得 Elastic Beanstalk 環境的網域名稱

如果您已經了解 Elastic Beanstalk 環境的網域名稱，請跳到建立將流量路由到 Elastic Beanstalk 環境的 Amazon Route 53 記錄。

若要取得 Elastic Beanstalk 環境的網域名稱

1. 登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/elasticbeanstalk/ 的 Elastic Beanstalk 主控台。

2. 在應用程式清單中，尋找您要將流量路由到的應用程式，並取得 URL 的值。如果您看不見應用程式清單，請選擇導覽窗格中的 Applications (應用程式)。

   如需有關 URL 的詳細資訊，請參閱《Elastic Beanstalk 開發人員指南》中的 Elastic Beanstalk 環境的網域名稱。

建立將流量路由到 Elastic Beanstalk 環境的 Amazon Route 53 記錄

Amazon Route 53 記錄包含用於控制如何將流量路由到 Elastic Beanstalk 環境的設定。您可以建立「CNAME 記錄」或「別名記錄」，這取決於環境的網域名稱是否包含環境部署所在的區域 (例如，us-east-2)。新環境會在網域名稱中包含區域；2016 年年初之前建立的環境則不包含區域。如需 CNAME 和別名記錄的比較，請參閱選擇別名或非別名記錄。

如果網域名稱不包含區域

您必須建立「CNAME 記錄」。但是，由於 DNS 規定的限制，您只能為子網域建立 CNAME 記錄，而不能為根網域名稱建立 CNAME 記錄。例如，如果您的網域名稱是 example.com，您可以建立將 acme.example.com 流量路由至您 Elastic Beanstalk 環境的記錄，但無法建立將 example.com 流量路由至您 Elastic Beanstalk 環境的記錄。

請參閱若要建立 CNAME 記錄將流量路由到 Elastic Beanstalk 環境程序。

如果網域名稱包含區域

您可以建立別名記錄。別名記錄專屬於 Route 53，與 CNAME 記錄相比有兩個重要優勢：

- 您可以為根網域名稱或子網域建立別名記錄。例如，如果網域名稱為 example.com，則可以建立能夠將對 example.com 或 acme.example.com 的請求路由到 Elastic Beanstalk 環境的記錄。
- 對於使用別名記錄來路由流量的請求，Route 53 不收取費用。

請參閱若要建立 Amazon Route 53 別名記錄，將流量路由到 Elastic Beanstalk 環境程序。

若要建立 CNAME 記錄將流量路由到 Elastic Beanstalk 環境

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇要用於將流量路由到 Elastic Beanstalk 環境的託管區域名稱。
4. 選擇建立記錄。

5. 選擇切換以快速建立
6. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入將流量路由到 Elastic Beanstalk 環境所使用的網域名稱。預設值為託管區域名稱。

   例如，如果託管區域的名稱是 example.com，而您想要使用 acme.example.com 將流量路由到您的環境，請輸入 acme。

   > **Important**
   >
   > 您無法建立與託管區域同名的 CNAME 記錄。

   別名

   如果您是使用 Quick create (快速建立) 記錄建立方法，請開啟 Alias (別名)。

   值/將流量路由到

   選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定) 並輸入您在執行主題 取得 Elastic Beanstalk 環境的網域名稱 中的程序時取得的值。如果您使用不同的帳戶來建立 Route 53 託管區域與 Elastic Beanstalk 環境， 則輸入 Elastic Beanstalk 環境的 CNAME 屬性。

   記錄類型

   選擇 CNAME。

   TTL (秒)

   接受預設值 300。
7. 選擇建立記錄。

   變更通常會在 60 秒內傳播至所有 Route 53 伺服器。

若要建立 Amazon Route 53 別名記錄，將流量路由到 Elastic Beanstalk 環境

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇要用於將流量路由到 Elastic Beanstalk 環境的託管區域名稱。
4. 選擇建立記錄。
5. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入將流量路由到 Elastic Beanstalk 環境所使用的網域名稱。預設值為託管區域名稱。

   例如，如果託管區域的名稱是 example.com，而您想要使用 acme.example.com 將流量路由到您的環境，請輸入 acme。

   值/將流量路由到

   選擇 Alias to Elastic Beanstalk environment (Elastic Beanstalk 環境的別名)，然後選擇端點所來自的區域。選擇您要將流量路由到的環境的網域名稱。這是您在執行取得 Elastic Beanstalk 環境的網域名稱主題中的程序時取得的值。

   如果您使用不同的帳戶來建立 Route 53 託管區域與 Elastic Beanstalk 環境，請輸入 Elastic Beanstalk 環境的 CNAME 屬性。

   記錄類型

   接受預設值 A – IPv4 address (A - IPv4 地址)。

   評估目標運作狀態

   接受預設值 Yes (是)。
6. 選擇建立記錄。

變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當傳播完成，您就可以使用在此程序中建立的別名記錄的名稱，將流量路由到 Elastic Beanstalk 環境。

將流量路由到 ELB 負載平衡器

如果您在多個 Amazon EC2 執行個體上託管網站，可以使用 Elastic Load Balancing (ELB) 負載平衡器在執行個體之間分配網站流量。當網站的流量隨時間發生變化時，ELB 服務會自動擴展負載平衡器。負載平衡器還會監控其註冊執行個體的運作狀況，而且只將網域流量路由到正常運作的執行個體。

若要將網域流量路由到 ELB 負載平衡器，請使用 Amazon Route 53 建立指向負載平衡器的別名記錄。別名記錄是 DNS 的 Route 53 延伸。別名記錄與 CNAME 記錄類似，但您可以同時為根網域 (如 example.com) 和子網域 (如 www.example.com) 建立別名記錄。(只可以為子網域建立 CNAME 記錄。)

> **Note**
>
> 對於針對 ELB 負載平衡器或其他 AWS 資源的別名查詢，Route 53 不收取費用。

必要條件

若要開始使用，您需要滿足以下條件：

- ELB 負載平衡器。您可以使用 ELB Classic Load Balancer、Application Load Balancer 或 Network Load Balancer。如需建立負載平衡器的詳細資訊，請參閱 Elastic Load Balancing 使用者指南中的 Elastic Load Balancing 入門。

  為負載平衡器命名，以便稍後能夠想起其用途。您在建立負載平衡器時指定的名稱，是您在 Route 53 主控台中建立別名記錄時將選擇的名稱。
- 註冊的網域名稱。您可以使用 Route 53 做為網域註冊商，也可以使用不同的註冊商。
- Route 53 做為網域的 DNS 服務。如果您使用 Route 53 註冊網域名稱，我們會將 Route 53 自動設定為網域的 DNS 服務。

  如需使用 Route 53 做為您網域 DNS 服務提供者的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

設定 Amazon Route 53 將流量路由到 ELB 負載平衡器

若要設定 Amazon Route 53 將流量路由到 ELB 負載平衡器，請執行下列程序。

若要將流量路由到 ELB 負載平衡器

1. 如果您建立的 Route 53 託管區域和 ELB 負載平衡器使用相同的帳戶，請跳到步驟 2。

   如果您建立的託管區域和 ELB 負載平衡器使用不同的帳戶，請執行程序 取得 Elastic Load Balancing 負載平衡器的 DNS 名稱 以取得負載平衡器的 DNS 名稱。
2. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 選擇託管區域的名稱，該託管區域具有要用來將流量路由到負載平衡器的網域名稱。
5. 選擇建立記錄。
6. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入將流量路由到 ELB 負載平衡器所使用的網域或子網域名稱。預設值為託管區域名稱。

   例如，如果託管區域的名稱是 example.com，而您想要使用 acme.example.com 將流量路由到您的負載平衡器，請輸入 acme。

   別名

   如果您是使用 Quick create (快速建立) 記錄建立方法，請開啟 Alias (別名)。

   值/將流量路由到

   選擇 Alias to Application and Classic Load Balancer (Applcation Load Balancer 和 Classic Load Balancer 的別名) 或 Alias to Network Load Balancer (Network Load Balancer 的別名)，然後選擇端點所來自的區域。

   如果您建立的託管區域和 ELB 負載平衡器使用相同的 AWS 帳戶，請選擇您在建立負載平衡器時指派給其的名稱。

   如果使用不同的帳戶來建立託管區域與 ELB 負載平衡器，請輸入您在此程序的步驟 1 中取得的值。

> **Note**
>
> 僅針對來自相同 AWS 帳戶的 Application Load Balancer 和 Classic Load Balancer，控制台會在其 DNS 名稱開頭加上 dualstack.。當用戶端 (例如 web 瀏覽器) 要求您網域名稱 (example.com) 或子網域名稱 (www.example.com) 的 IP 地址時，用戶端可以要求 IPv4 地址 (A 記錄)、IPv6 地址 (AAAA 記錄) 或 IPv4 與 IPv6 地址 (以不同的要求，IPv4 優先)。dualstack. 指定可讓 Route 53 根據用戶端要求的 IP 地址格式，以您負載平衡器的適當 IP 地址來回應。針對來自不同帳戶的 Application Load Balancer 和 Classic Load Balancer，您需要在其開頭加上 dualstack.。

記錄類型

選擇 A – IPv4 地址。

評估目標運作狀態

如果您希望 Route 53 根據資源的運作狀態來路由流量，請選擇 Yes (是)。如需檢查資源運作狀態的詳細資訊，請參閱 建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。

7. 選擇建立記錄。

變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當傳播完成，您就可以使用在此程序中建立的別名記錄的名稱，將流量路由到負載平衡器。

將流量路由到 Amazon S3 儲存貯體中託管的網站

Amazon Simple Storage Service (Amazon S3) 提供安全、耐用、高可擴展性的雲端儲存空間。您可以設定 S3 儲存貯體來託管包括網頁和用戶端指令碼的靜態網站。(S3 不支援伺服器端指令碼。)

若要將網域流量路由到 S3 儲存貯體，請使用 Amazon Route 53 建立指向儲存貯體的別名記錄。別名記錄是 DNS 的 Route 53 延伸。別名記錄與 CNAME 記錄類似，唯一例外是您可以同時為根網域 (如 example.com) 和子網域 (如 www.example.com) 建立別名記錄。只可以為子網域建立 CNAME 記錄。

> **Note**
>
> 對於針對 S3 儲存貯體或其他 AWS 資源的別名查詢，Route 53 不收取費用。

必要條件

在開始使用之前，您需要滿足以下條件。如果您剛開始使用 Amazon Route 53 或 S3，請參閱 Amazon Route 53 入門，該文件會引導您完成整個程序，包括註冊網域名稱，以及建立和設定 S3 儲存貯體。

- 即為設定用來託管靜態網站的 S3 儲存貯體。

  如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的「為網站託管設定儲存貯體」。

  > **Important**
  >
  > 儲存貯體必須與您的網域或子網域同名。例如，如果您想要使用子網域 acme.example.com，儲存貯體的名稱必須是 acme.example.com。

  您可以將網域及其子網域 (例如 example.com 與 www.example.com) 的流量路由到單一儲存貯體。為網域和每個子網域建立儲存貯體，並將除了其中一個儲存貯體以外的所有儲存貯體設定為將流量重新引導至剩餘的儲存貯體。如需詳細資訊，請參閱 Amazon Route 53 入門。

  > **Note**
  >
  > 設定為網站端點的 S3 儲存貯體不支援 SSL/TLS，所以您需要將流量路由到 CloudFront 分佈並使用 S3 儲存貯體做為分佈的原始伺服器。
  > 如需有關如何建立 CloudFront 分發的指示，請參閱CloudFront 使用者指南中的建立 CloudFront 分發和設定替代網域名稱和 HTTPS 使用您的網域名稱將流量路由到 Amazon CloudFront 分發。

- 註冊的網域名稱。您可以使用 Route 53 做為網域註冊商，也可以使用不同的註冊商。
- Route 53 做為網域的 DNS 服務。如果您使用 Route 53 註冊網域名稱，我們會將 Route 53 自動設定為網域的 DNS 服務。

  如需使用 Route 53 做為您網域 DNS 服務提供者的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

設定 Amazon Route 53 將流量路由到 S3 儲存貯體

若要設定 Amazon Route 53 將流量路由到設定用來託管靜態網站的 S3 儲存貯體，請執行下列程序。

若要將流量路由到 S3 儲存貯體

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇託管區域的名稱，該託管區域具有要用來將流量路由到 S3 儲存貯體的網域名稱。
4. 選擇建立記錄。
5. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入要將流量路由到 S3 儲存貯體所使用的網域名稱。預設值為託管區域名稱。

   例如，如果託管區域的名稱是 example.com，而您想要使用 acme.example.com 將流量路由到您的儲存貯體，請輸入 acme。

   別名

   如果您是使用 Quick create (快速建立) 記錄建立方法，請開啟 Alias (別名)。

   值/將流量路由到

   選擇 Alias to S3 website endpoint (S3 網站端點的別名)，然後選擇端點所來自的區域。

   選擇與您為記錄名稱指定的值同名的儲存貯體。

   只有當儲存貯體符合下列要求時，該清單才會包含儲存貯體：

   - 儲存貯體與您建立的記錄同名。
   - 儲存貯體設定為網站端點。
   - 儲存貯體是由目前的 AWS 帳戶所建立。

     如果您使用不同的 AWS 帳戶建立儲存貯體，請輸入您 S3 儲存貯體建立所在的區域名稱。如需了解區域名稱的正確格式，請參閱 Amazon Web Services 一般參考 中的 Amazon S3 網站端點資料表中的網站端點欄。

   記錄類型

   選擇 A – IPv4 地址。

評估目標運作狀態

接受預設值 Yes (是)。

6. 選擇建立記錄。

變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當傳播完成，您就可以使用在此程序中建立的別名記錄的名稱，將流量路由到 S3 儲存貯體。

使用網域名稱將流量路由到 Amazon Virtual Private Cloud 介面端點

您可以使AWS PrivateLink 用 Amazon 虛擬私有雲端 (Amazon VPC) 界面端點存取特定服務。這些服務包含部分 AWS 服務、其他 AWS 客戶和合作夥伴在其專屬 VPC 中託管的服務，以及支援的 AWS Marketplace 合作夥伴服務。

若要將網域流量路由到介面端點，請使用 Amazon Route 53 建立別名記錄。別名記錄是 DNS 的 Route 53 延伸。別名記錄與 CNAME 記錄類似，但您可以同時為根網域 (如 example.com) 和子網域 (如 www.example.com) 建立別名記錄。只可以為子網域建立 CNAME 記錄。

> **Note**
>
> 對於介面端點或其他 AWS 資源的別名查詢，Route 53 不收取費用。

主題

- 必要條件
- 設定 Amazon Route 53 將流量路由到 Amazon VPC 介面端點。

必要條件

若要開始使用，您需要滿足以下條件：

- Amazon VPC 介面端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的介面 VPC 端點 (AWS PrivateLink)。
- 註冊的網域名稱。您可以使用 Amazon Route 53 做為網域註冊商，也可以使用不同的註冊商。
- Route 53 做為網域的 DNS 服務。如果您使用 Route 53 註冊網域名稱，我們會將 Route 53 自動設定為網域的 DNS 服務。

如需使用 Route 53 做為您網域 DNS 服務提供者的資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

設定 Amazon Route 53 將流量路由到 Amazon VPC 介面端點。

若要設定 Amazon Route 53 將流量路由到 Amazon VPC 介面端點，請執行下列程序。

將流量路由到 Amazon VPC 介面端點

1. 如果您已使用相同的帳戶建立 Route 53 託管區域和 Amazon VPC 端點，請跳到步驟 2。

   如果您使用不同的帳戶建立託管區域和介面端點，請取得介面端點的服務名稱：

   a. 登入 AWS Management Console，並在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
   b. 在導覽窗格中選擇 Endpoints (端點)。
   c. 在右側窗格中，選擇您要將網際網路流量路由至該處的端點。
   d. 在底部窗格中，取得 DNS 名稱的值，例如 vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com。
2. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 選擇託管區域的名稱，該託管區域具有要用來將流量路由到介面端點的網域名稱。
5. 選擇建立記錄。
6. 指定下列值：

   路由政策

   請選擇適用的路由政策。如需詳細資訊，請參閱 選擇路由政策。

   記錄名稱

   輸入要將流量路由到 Amazon VPC 介面端點所使用的網域名稱。

   別名

   如果您是使用 Quick create (快速建立) 記錄建立方法，請開啟 Alias (別名)。

值/將流量路由到

選擇 Alias to VPC endpoint (VPC 端點的別名)，然後選擇端點所來自的區域。

指定 Endpoints (端點) 值的方式，取決於您是否使用相同的 AWS 帳戶或不同帳戶來建立託管區域和介面端點：

- 相同帳戶 - 選擇清單並找到類別 Amazon VPC 端點。然後選擇您要將網際網路流量路由至該處的介面端點之 DNS 名稱。
- 不同帳戶 – 輸入您在此程序的步驟 1 中取得的值。

記錄類型

選擇 A – IPv4 地址。

評估目標運作狀態

接受預設值 Yes (是)。

7. 選擇建立記錄。

變更通常會在 60 秒內傳播至所有 Route 53 伺服器。當傳播完成，您就可以使用在此程序中建立的別名記錄的名稱，將流量路由到介面端點。

將流量路由到 Amazon WorkMail

您可以使用 Route 53 將流量路由到您的 Amazon WorkMail 電子郵件網域。您的路線 53 託管區域的名稱（例如 example.com）必須與 Amazon WorkMail 域的名稱相匹配。

> **Note**
>
> 您只能針對公有託管區 WorkMail 域將流量路由到 Amazon 網域。

若要將流量路由到 Amazon WorkMail，請執行以下四個程序。

將 Amazon 路線 53 配置為您的 DNS 服務，並添加 Amazon 組 WorkMail 織和電子郵件域

1. 如果您未註冊要用於電子郵件地址 (如 john@example.com) 的網域名稱，請立即註冊網域，以便了解網域是否可用。如需詳細資訊，請參閱 註冊新網域。

如果 Amazon 路由 53 不是您添加到 Amazon 的電子郵件域的 DNS 服務 WorkMail，請將該域的 DNS 服務遷移到路由 53。如需詳細資訊，請參閱 將 Amazon Route 53 設定為現有網域的 DNS 服務。

2. 新增 Amazon 組 WorkMail 織和電子郵件網域。如需詳細資訊，請參閱 Amazon WorkMail 管理員指南中的新使用者入門。

要創建一個路線 53 TXT 記錄 Amazon WorkMail

1. 在 Amazon WorkMail 主控台的導覽窗格中，選擇「網域」。
2. 選擇要用於將流量路由到 Amazon 的電子郵件域名，例如 example.com。 WorkMail
3. 開啟另一個瀏覽器標籤，並開啟 Route 53 主控台。
4. 在 Route 53 主控台中，執行以下操作：
   a. 在導覽窗格中，選擇 Hosted zones (託管區域)。
   b. 選擇您要用於 Amazon WorkMail 電子郵件網域的託管區域名稱。
5. 在 Amazon 主 WorkMail 控台的「步驟 1：驗證網域擁有權」區段中，移至「主機名稱」欄，然後複製電子郵件網域名稱前面的部分值。

   舉例來說，如果您的 Amazon WorkMail 電子郵件網域名稱是例子 .com，而主機名稱的值為例子，請複製。
6. 在 Route 53 主控台中，執行以下操作：
   a. 選擇 Create record (建立記錄)，然後選擇 Simple routing (簡便路由)。
   b. 對於 Record name (名稱)，貼上您在步驟 5 中複製的值。
   c. 對於 Record type (記錄類型)，選擇 TXT – Text (TXT – 文字)。
7. 在 Amazon WorkMail 主控台中，對於 TXT 記錄，複製「值」欄的值，包括引號。
8. 在 Route 53 主控台中，執行以下操作：
   a. 針對 Value/Route traffic to (值/路由流量至)，選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)，然後貼入在步驟 7 中複製的值。

      不要變更任何其他設定。
   b. 選擇建立。

為 Amazon 創建路線 53 MX 記錄 WorkMail

1. 在 Amazon WorkMail 主控台的「步驟 2：完成網域設定」區段中，移至記錄類型為 MX 的列，然後複製「值」欄的值。
2. 在 Route 53 主控台中，執行以下操作：
   a. 選擇建立記錄。
   b. 對於 Value/Route traffic to (值/路由流量至)，選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)，然後貼入在步驟 1 中複製的值。
   c. 對於 Record type (記錄類型)，選擇 MX – Mail Exchange (MX - 郵件交換)。

      不要變更任何其他設定。
   d. 選擇建立記錄。

為 Amazon 創建四條路線 53 CNAME 記錄 WorkMail

1. 在 Amazon WorkMail 主控台的「步驟 2：完成網域設定」區段中，移至記錄類型為 CNAME 的第一列。在 Hostname (主機名稱) 欄中，複製您電子郵件網域名稱前面的值部分。

   例如，如果您的 Amazon WorkMail 電子郵件網域是 example.com，且主機名稱的值是自動探索 .example.com，請複製自動探索。
2. 在 Route 53 主控台中，執行以下操作：
   a. 選擇建立記錄。
   b. 針對 Record name (記錄名稱)，貼上您在步驟 1 中複製的值。
   c. 在 Record type (記錄類型) 中，選擇 CNAME - Canonical Name (CNAME - 正式名稱記錄)。
3. 在 Amazon WorkMail 主控台的記錄類型為 CNAME 的第一列中，複製「值」欄的值。
4. 在 Route 53 主控台中，執行以下操作：
   a. 針對 Value/Route traffic to (值/路由流量至)，選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)，然後貼入在步驟 3 中複製的值。

      不要變更任何其他設定。
   b. 選擇建立記錄。
5. 針對 Amazon WorkMail 主控台中列出的剩餘 CNAME 記錄重複步驟 1 到 4。

將流量路由到其他 AWS 資源

以下清單包含其他指南中如何使用 Route 53 將流量路由到這些服務的指引相關主題。

- 《AWS Cloud Map 使用者指南》中的使用 AWS Cloud Map。
- 《AWS App Runner 開發人員指南》中的管理自訂網域。
- 《AWS Transfer Family 使用者指南》中的作為 DNS 提供者使用 Route 53。
- 使用 Route 53 將網域指向 Amazon Lightsail 執行個體。

建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援

Amazon Route 53 運作狀態檢查監控 Web 應用程式、Web 伺服器和其他資源的運作狀態和效能。您建立的每個運作狀態檢查可監控下列其中一項：

- 指定之資源 (例如 Web 伺服器) 的運作狀態。
- 其他運作狀態檢查的狀態。
- Amazon CloudWatch 警報的狀態。
- 此外，透過 Amazon Route 53 Application Recovery Controller，您可以使用 DNS 容錯移轉記錄來設定路由控制運作狀態檢查，以管理應用程式的流量容錯移轉。如需進一步了解，請參閱 Amazon Route 53 Application Recovery Controller 開發人員指南。

如需這些類型的運作狀態檢查的概觀，請參閱 Amazon Route 53 運作狀態檢查的類型。如需有關建立運作狀態檢查的資訊，請參閱 建立和更新運作狀態檢查。

在建立運作狀態檢查之後，您可以取得運作狀態檢查的狀態，當狀態變更時收到通知，以及設定 DNS 備援：

取得運作狀態檢查和通知

您可以在 Route 53 主控台檢視運作狀態檢查的目前狀態及最新狀態。您也可以透過其中一個 AWS SDK、、或 Route 53 API，以程式設計方 AWS Command Line Interface式處理健康狀態檢查。AWS Tools for Windows PowerShell

如果您希望在運作狀態檢查狀態變更時收到通知，可以為每次運作狀態檢查設定 Amazon CloudWatch 警示。

如需有關檢視運作狀態檢查狀態和接收通知的資訊，請參閱 監控運作狀態檢查狀態和取得通知。

設定 DNS 備援

如果您有多個執行相同功能的資源，可以設定 DNS 備援，以便 Route 53 將流量從狀況不良的資源路由到正常的資源。例如，如果您有兩個 Web 伺服器，其中一個 Web 伺服器狀況不良，Route 53 就會將流量路由到另一個 Web 伺服器。如需詳細資訊，請參閱 設定 DNS 備援。

主題

- Amazon Route 53 運作狀態檢查的類型

- Amazon Route 53 決定運作狀態檢查是否良好的方式
- 建立、更新和刪除運作狀態檢查
- 監控運作狀態檢查狀態和取得通知
- 設定 DNS 備援
- 命名和標記運作狀態檢查
- 運作狀態檢查與早於 2012-12-12 的 Amazon Route 53 API 版本搭配使用

Amazon Route 53 運作狀態檢查的類型

您可以建立下列 Amazon Route 53 運作狀態檢查類型：

監控端點的運作狀態檢查

您可以設定運作狀態檢查來監控依 IP 地址或網域名稱指定的端點。Route 53 會以您指定的定期間隔，透過網際網路向您的應用程式、伺服器或其他資源提交自動請求，以驗證其連線能力、可用性和功能。或者，您也可以設定運作狀態檢查來發出類似於使用者發出的請求，例如請求特定 URL 的網頁。

監控其他運作狀態檢查的運作狀態檢查 (計算的運作狀態檢查)

您可以建立運作狀態檢查，以監控 Route 53 將其他運作狀態檢查視為正常或狀況不良。在以下情況，這種運作狀態檢查非常有用：您有多個執行相同功能的資源 (例如多個 Web 伺服器)，而您的主要疑慮是最小資源數量是否正常。您可以為每個資源建立運作狀態檢查，而不為這些運作狀態檢查設定通知。然後，您可以建立運作狀態檢查，以監控其他運作狀態檢查的狀態，而且只在可用的 Web 資源低於指定的閾值時通知您。

監控 CloudWatch 警示的 Health 狀態檢查

您可以建立監控 CloudWatch 指標狀態的 CloudWatch 警示，例如 Amazon DynamoDB 資料庫的節流讀取事件數目，或視為狀態良好的 Elastic Load Balancing 主機數目。建立警示後，您可以建立健康狀態檢查，以監控警 CloudWatch 示的相同資料串流。

為了提高恢復能力和可用性，Route 53 不會等待 CloudWatch警報進入ALARM狀態。健康狀態檢查的狀態會根據資料串流和 CloudWatch 警示中的條件，從狀況良好變更為不健全狀況。

Route 53 支援具有以下功能的 CloudWatch 警報：

- 標準解析指標。不支援高解析指標。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的高解析度指標。

- 統計資料：平均值、最小值、最大值、總和和 SampleCount。不支援擴充統計資料。
- 健康狀態檢查只能監控與健康狀態檢查相同 AWS 帳戶中存在的 CloudWatch 警示。

Amazon Route 53 Application Recovery Controller

Amazon Route 53 Application Recovery Controller 可讓您深入瞭解應用程式和資源是否已準備好進行復原，並協助您管理和協調容錯移轉。Route 53 ARC 中的運作狀態檢查與路由控制相關聯，這是簡單的開啟/關閉切換。您可以使用容錯移轉 DNS 記錄來設定每個路由控制運作狀態檢查。然後，您可以簡單地更新 Route 53 ARC 中的路由控制項，以重新路由傳送流量並容錯移轉您的應用程式，例如跨可用區域或 AWS-區域。如需詳細資訊，請參閱 Amazon Route 53 Application Recovery Controller 開發人員指南。

若要進一步了解整備檢查，請參閱 Route 53 ARC 中的整備檢查。若要進一步了解路由控制，請參閱《Route 53 ARC 開發人員指南》中的 Route 53 ARC 中的路由控制。

Amazon Route 53 決定運作狀態檢查是否良好的方式

Amazon Route 53 會依據運作狀態檢查的類型，使用適當方法，來判斷運作狀態檢查是否正常運作。

主題

- Route 53 如何判斷監控端點的運作狀態檢查的狀態
- Route 53 如何判斷監控其他運作狀態檢查的檢查狀態
- Route 53 如何判斷監控 CloudWatch 警示的健康狀態檢查狀態

Route 53 如何判斷監控端點的運作狀態檢查的狀態

Route 53 在全球的多個位置都有運作狀態檢查程式。當您建立運作狀態檢查以監控端點時，運作狀態檢查程式即會開始傳送請求到您指定的端點，以判斷端點是否正常運作。您可以選擇您希望 Route 53 使用的位置，亦可指定間隔檢查為每隔 10 秒或每隔 30 秒。請注意，在不同資料中心的 Route 53 運作狀態檢查程式不會彼此協調，所以無論您選擇多久的間隔，有時會看到每秒多個請求，接著幾秒鐘完全沒有運作狀態檢查的情況。

每個運作狀態檢查程式都會根據下列兩個值來評估端點的運作狀態：

- 回應時間。資源在回應運作狀態檢查請求時，可能基於各種原因會很慢或無法回應。例如，資源已關閉來進行維護、正遭受分散式拒絕服務 (DDoS) 攻擊，或網路中斷。
- 端點是否回應您指定的幾次連續運作狀態檢查 (故障閾值)

Route 53 可彙總運作狀態檢查程式的資料，並判斷端點是否正常運作：

- 如果超過 18% 的運作狀態檢查程式回報端點正常運作，Route 53 即會將其視為正常運作。
- 如果 18% 以下的運作狀態檢查程式回報端點正常運作，Route 53 會將其視為狀況不良。

選擇 18% 這個值的原因，是為了確保多個區域中的運作狀態檢查程式都能將端點視為正常運作。這可以防止端點僅因為網路狀況將其從某些運作狀態檢查位置中隔離出來，就被視為狀況不良。在未來版本中，這個值可能會變更。

個別運作狀態檢查程式會依據下列運作狀態檢查的類型，使用適當回應時間，來判斷端點是否正常運作：

- HTTP 和 HTTPS 運作狀態檢查 – Route 53 必須能夠在四秒內與端點建立 TCP 連線。此外，端點必須在連線後兩秒內以 2xx 或 3xx 的 HTTP 狀態碼回應。

  > **Note**
  >
  > HTTPS 運作狀態檢查不會驗證 SSL/TLS 憑證，因此如果憑證無效或過期，檢查並不會失敗。

- TCP 運作狀態檢查 – Route 53 必須能夠在十秒內與端點建立 TCP 連線。
- 使用字串比對的 HTTP 和 HTTPS 運作狀態檢查 – 如同 HTTP 和 HTTPS 運作狀態檢查，Route 53 必須能夠在四秒內與端點建立 TCP 連線，而且端點必須在連線後兩秒內以 2xx 或 3xx 的 HTTP 狀態碼回應。

  Route 53 運作狀態檢查在收到 HTTP 狀態碼之後，必須在接下來的兩秒內收到來自端點的回應本文。Route 53 在回應本文中搜尋指定的字串。字串必須在回應本文的前 5,120 個位元組中完全顯示，否則端點的運作狀態檢查會失敗。如果您使用的是 Route 53 主控台，請在 Search String (搜尋字串) 欄位中指定字串。如果您使用的是 Route 53 API，請在建立運作狀態檢查時於 `SearchString` 元素中指定字串。

若是用來監控端點的運作狀態檢查 (除了 TCP 運作狀態檢查以外)，如果來自端點的回應包含任何標頭，則標頭必須使用 RFC7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, section 3.2, "Header Fields" 中定義的格式。

Route 53 將新的運作狀態檢查視為良好，直到有足夠的資料可判斷實際運作狀態為良好或不佳。如果您選擇選擇反轉運作狀態檢查的狀態，Route 53 會將新的運作狀態檢查視為不佳，直到有足夠的資料。

Route 53 如何判斷監控其他運作狀態檢查的檢查狀態

運作狀態檢查可以監控其他運作狀態檢查的狀態；這類運作狀態檢查稱為計算的運作狀態檢查。實際執行監控的運作狀態檢查是「父系運作狀態檢查」，而受監控的運作狀態檢查則為「子級運作狀態檢查」。一個父系運作狀態檢查可以監控最多 255 個子級運作狀態檢查的運作狀態。以下是監控的運作方式：

- Route 53 會加總視為正常運作的子級運作狀態檢查數量。
- Route 53 會比較該數字與必須正常運作的子級運作狀態檢查數目 (父系運作狀態檢查的狀態才會被視為正常)。

如需詳細資訊，請參閱 您在建立或更新運作狀態檢查時指定的值 中的 監控其他運作狀態檢查 (計算的運作狀態檢查)。

Route 53 將新的運作狀態檢查視為良好，直到有足夠的資料可判斷實際運作狀態為良好或不佳。如果您選擇選擇反轉運作狀態檢查的狀態，Route 53 會將新的運作狀態檢查視為不佳，直到有足夠的資料。

Route 53 如何判斷監控 CloudWatch 警示的健康狀態檢查狀態

當您建立以 CloudWatch 警示為基礎的健全狀況檢查時，Route 53 會監視資料串流中的對應警示，而不是監視警示狀態。如果資料串流指出警示狀態為 OK (正常)，運作狀態檢查會被視為正常運作。如果資料串流指出警示狀態為 Alarm (警示)，運作狀態檢查會被視為狀況不良。如果資料串流提供的資訊不足，無法判斷警示狀態，則運作狀態檢查的狀態取決於 Health check status (運作狀態檢查狀態) 的設定：正常、狀況不良或上次已知狀態。(在 Route 53 API 中，此設定為 `InsufficientDataHealthStatus`。)

Route 53 不支援跨帳戶 CloudWatch 警報。

> **Note**
>
> 由於 Route 53 健康狀態檢查會監控 CloudWatch 資料串流而非CloudWatch 警示狀態，因此您無法使用 CloudWatch SetAlarmStateAPI 作業強制變更健全狀況檢查的狀態。

Route 53 將新的運作狀態檢查視為良好，直到有足夠的資料可判斷實際運作狀態為良好或不佳。如果您選擇選擇反轉運作狀態檢查的狀態，Route 53 會將新的運作狀態檢查視為不佳， 直到有足夠的資料。

建立、更新和刪除運作狀態檢查

以下主題中的程序說明如何建立、更新和刪除 Route 53 運作狀態檢查。

> **Important**
>
> 如果您要更新或刪除與記錄關聯的運作狀態檢查，請先檢閱當已設定 DNS 備援時，更新或刪除運作狀態檢查中的任務，然後再繼續。

主題

- 建立和更新運作狀態檢查
- 您在建立或更新運作狀態檢查時指定的值
- 當您建立運作狀態檢查時 Amazon Route 53 顯示的值
- 變更 CloudWatch 警示設定時更新健全狀況檢查 (僅監控 CloudWatch警示的健全狀況檢查)
- 刪除運作狀態檢查
- 當已設定 DNS 備援時，更新或刪除運作狀態檢查
- 為 Amazon Route 53 運作狀態檢查設定路由器和防火牆規則

建立和更新運作狀態檢查

下列程序說明如何使用 Route 53 主控台建立和更新運作狀態檢查。

建立或更新運作狀態檢查 (主控台)

1. 如果要更新的運作狀態檢查已與記錄建立關聯，請執行 當已設定 DNS 備援時，更新或刪除運作狀態檢查 中的建議任務。
2. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
3. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
4. 如果要更新現有的運作狀態檢查，請選取運作狀態檢查，然後選擇 Edit Health Check (編輯運作狀態檢查)。

   如果要建立運作狀態檢查，請選擇 Create Health Check (建立運作狀態檢查)。如需每個設定的詳細資訊，請將滑鼠指標移至標籤上，以查看其工具提示。

5. 輸入適用的值。請注意，某些值在您建立運作狀態檢查之後無法變更。如需詳細資訊，請參閱 [您在建立或更新運作狀態檢查時指定的值]。
6. 選擇 Create Health Check (建立運作狀態檢查)。

> **Note**
>
> Route 53 將新的運作狀態檢查視為良好，直到有足夠的資料可判斷實際運作狀態為良好或不佳。如果您選擇選擇反轉運作狀態檢查的狀態，Route 53 會將新的運作狀態檢查視為不佳， 直到有足夠的資料。

7. 將運作狀態檢查與一或多個 Route 53 記錄關聯。如需有關建立和更新記錄的詳細資訊，請參閱 [處理記錄]。

您在建立或更新運作狀態檢查時指定的值

在建立或更新運作狀態檢查時，指定適用的值。請注意，在建立運作狀態檢查之後，無法變更某些值。

主題

- 監控端點
- 監控其他運作狀態檢查 (計算的運作狀態檢查)
- 監控 CloudWatch 警示
- 進階組態 (僅限 "Monitor an endpoint")
- 在運作狀態檢查失敗時收到通知

名稱

選用但建議使用：要指派給運作狀態檢查的名稱。如果您指定 Name (名稱) 的值，則 Route 53 會將標籤新增至運作狀態檢查，再將 Name (名稱) 值指派給標籤鍵，並將您指定的值指派給標籤值。Name (名稱) 標籤的值會出現在 Route 53 主控台的運作狀態檢查清單，讓您輕鬆地區分各個運作狀態檢查。

如需標記和運作狀態檢查的詳細資訊，請參閱 [命名和標記運作狀態檢查]。

要監控的內容

您希望此運作狀態檢查監控端點或其他運作狀態檢查的狀態：

- Endpoint (端點) – Route 53 會監控您所指定端點的運作狀態。您可以透過提供網域名稱或 IP 地址和連接埠來指定端點。

> **Note**
>
> 如果指定非AWS 端點，則需支付額外費用。如需詳細資訊，包括 AWS 端點的定義，請參閱 Route 53 定價頁面上的「運作狀態檢查」。

- Status of other health checks (calculated health check) (其他運作狀態檢查的狀態 (計算的運作狀態檢查)) – Route 53 會根據您指定的其他運作狀態檢查的狀態，判斷此運作狀態檢查是否正常。您也可以指定需要有多少正常的運作狀態檢查，此運作狀態檢查才會被視為正常。
- CloudWatch 警示資料串流狀態 — Route 53 藉由監控資料串流中的 CloudWatch 警示，判斷此健康狀態檢查是否健全狀況。

監控端點

如果您希望此運作狀態檢查監控端點，請指定以下值：

- Specify endpoint by
- Protocol
- IP address
- Host name
- Port
- Domain name
- Path

Specify endpoint by

您想要使用 IP 地址或使用網域名稱來指定端點。

建立運作狀態檢查之後，即無法變更 Specify endpoint by (指定端點方式) 的值。

通訊協定

您想要 Route 53 用來檢查端點運作狀態的方法：

- HTTP - Route 53 會嘗試建立 TCP 連線。如果成功，Route 53 會提交 HTTP 請求並等待 2xx 或 3xx 的 HTTP 狀態碼。
- HTTPS - Route 53 會嘗試建立 TCP 連線。如果成功，Route 53 會提交 HTTPS 請求並等待 2xx 或 3xx 的 HTTP 狀態碼。

> **Important**
>
> 如果您選擇 HTTPS，則端點必須支援 TLS 1.0 版。

如果您選擇 HTTPS 做為 Protocol (通訊協定) 的值，會產生額外費用。如需詳細資訊，請參閱 Route 53 定價。

- TCP - Route 53 會嘗試建立 TCP 連線。

如需詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

建立運作狀態檢查之後，即無法變更 Protocol (通訊協定) 的值。

IP address (僅限 "Specify endpoint by IP address")

如果您選擇 Specify endpoint by IP address (指定端點方式 - IP 地址)，此值為您希望 Route 53 執行運作狀態檢查之端點的 IPv4 或 IPv6 地址。

Route 53 無法檢查 IP 地址位於本機、私有、不可路由或多點傳送範圍內之端點的運作狀態。如需無法建立運作狀態檢查之 IP 地址的詳細資訊，請參閱以下文件：

- RFC 5735, Special Use IPv4 Addresses (RFC 5735 - 特殊用途 IPv4 地址)
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space (RFC 6598，預留的 IANA IPv4 前綴，用於共用地址空間)。
- RFC 5156, Special-Use IPv6 Addresses (RFC 5156 - 特殊用途 IPv6 地址)

如果端點是 Amazon EC2 執行個體，建議您建立彈性 IP 地址、建立它與您 EC2 執行個體的關聯，並指定此彈性 IP 地址。這可確保您的執行個體的 IP 地址永遠不會變更。如需詳細資訊，請參閱適用於 Linux 執行個體的 Amazon EC2 使用者指南中的 彈性 IP 地址 (EIP)。

如果您刪除 Amazon EC2 執行個體，請確保也刪除了與 EIP 相關聯的運作狀態檢查。如需詳細資訊，請參閱 適用於運作狀態檢查的彈性 IP 地址的最佳實務。

> **Note**
>
> 如果指定非AWS 端點，則需支付額外費用。如需詳細資訊，包括 AWS 端點的定義，請參閱 Route 53 定價頁面上的「運作狀態檢查」。

Host name (僅限 "Specify endpoint by IP address"，僅限 HTTP 和 HTTPS 通訊協定)

您希望 Route 53 在 HTTP 和 HTTPS 運作狀態檢查的 `Host` 標頭中傳遞的值。通常是您希望 Route 53 執行運作狀態檢查之網站的完整 DNS 名稱。以下是 Route 53 在檢查端點的運作狀態時建構 `Host` 標頭的方式：

- 如果您為 Port (連接埠) 指定值 **`80`** 並為 Protocol (通訊協定) 指定 HTTP，Route 53 會向端點傳遞 `Host` 標頭，其中包含 Host name (主機名稱) 的值。
- 如果您為 Port (連接埠) 指定值 **`443`** 並為 Protocol (通訊協定) 指定 HTTPS，Route 53 會向端點傳遞 `Host` 標頭，其中包含 Host name (主機名稱) 的值。
- 如果您為 Port (連接埠) 指定其他值並為 Protocol (通訊協定) 指定 HTTP 或 HTTPS，Route 53 會向端點傳遞 `Host` 標頭，其中包含 *`Host name`*:*`Port`* 值。

如果您選擇依 IP 地址指定端點，而且未指定 Host name (主機名稱) 的值，Route 53 在上述每個案例中會取代 `Host` 標頭中的 IP address (IP 地址) 的值。

Port

您希望 Route 53 執行運作狀態檢查之端點的連接埠。

Domain name (僅限 "Specify endpoint by domain name"，所有通訊協定)

您希望 Route 53 執行運作狀態檢查之端點的網域名稱 (example.com) 或子網域名稱 (backend.example.com) (如果您選擇 Specify endpoint by domain name (依網域名稱指定端點)。

如果您選擇依網域名稱指定端點，Route 53 會以您在 Request interval (請求間隔) 中指定的間隔傳送 DNS 查詢，以解析您在 Domain name (網域名稱) 中指定的網域名稱。然後，Route 53 會使用 DNS 傳回的 IP 地址，檢查端點的運作狀態。

> **Note**
>
> 如果您依網域名稱指定端點，Route 53 僅使用 IPv4 傳送運作狀態檢查至該端點。如果 Domain name (網域名稱) 中指定的網域名稱沒有 A 類型的記錄，運作狀態檢查會失敗，並顯示 DNS resolution failed (DNS 解析失敗) 錯誤。

如果您想要檢查容錯移轉、地理位置、地理位置鄰近性、延遲、多值或加權記錄的運作狀態，而且您選擇依網域名稱指定端點，我們建議您為每個端點建立單獨的運作狀態檢查。例如，針對每個提供內容給 www.example.com 的 HTTP 伺服器，建立運作狀態檢查。針對 Domain name (網域名稱) 的值，指定伺服器的網域名稱 (例如 us-east-2-www.example.com)，而非記錄的名稱 (www.example.com)。

> **Important**
>
> 在這個組態中，如果您建立 Domain name (網域名稱) 的值與記錄名稱相符的運作狀態檢查，然後將運作狀態檢查與這些記錄建立關聯，運作狀態檢查結果將會無法預測。

此外，如果 Protocol (通訊協定) 的值是 HTTP 或 HTTPS，Route 53 會在 `Host` 標頭中傳遞 Domain name (網域名稱) 的值，如之前這個清單中的 Host name (主機名稱) 所述。如果 Protocol (通訊協定) 的值是 TCP，則 Route 53 不會傳遞 `Host` 標頭。

> **Note**
>
> 如果指定非AWS 端點，則需支付額外費用。如需詳細資訊，包括 AWS 端點的定義，請參閱 Route 53 定價頁面上的「運作狀態檢查」。

Path (僅限 HTTP 和 HTTPS 通訊協定)

您希望 Route 53 在執行運作狀態檢查時請求的路徑。此路徑可以是任何值，例如檔案 `2xx` (當端點正常時，端點會傳回 HTTP 狀態碼 `3xx` 或 `/docs/route53-health-check.html`)。您也可以包含查詢字串參數，例如 `/welcome.html?language=jp&login=y`。如果您未包含正斜線 (/) 字元，Route 53 會自動新增一個正斜線。

監控其他運作狀態檢查 (計算的運作狀態檢查)

如果您希望此運作狀態檢查監控其他運作狀態檢查的狀態，請指定下列值：

- Health checks to monitor
- Report healthy when
- Invert health check status
- Disabled

Health checks to monitor

您希望 Route 53 監控的運作狀態檢查，以判斷此運作狀態檢查的運作狀態。

您最多可以新增 256 個運作狀態檢查至 Health checks to monitor (要監控的運作狀態檢查)。若要從清單中移除運作狀態檢查，請選擇該運作狀態檢查反白項目右側的 x。

> **Note**
>
> 您無法設定計算的運作狀態檢查來監控其他計算的運作狀態檢查的運作狀態。

如果您停用計算的運作狀態檢查所監控之運作狀態檢查，則 Route 53 會在計算確認計算的運作狀態檢查是否正常時，將停用的運作狀態檢查視為正常運作。如果您希望將停用的運作狀態檢查視為狀況不良，請選擇 Invert health check status (反轉運作狀態檢查狀態) 核取方塊。

Report healthy when

您希望 Route 53 執行用來決定此運作狀態檢查是否正常的計算：

- Report healthy when at least x of y selected health checks are healthy (當至少 x 個 (共 y 個) 選定運作狀態檢查是正常時，報告狀態正常) – 當新增至 Health checks to monitor (要監控的運作狀態檢查) 中指定數目的運作狀態檢查都是正常時，Route 53 會將此運作狀態檢查視為正常。注意下列事項：
  - 如果您指定的數字大於 Health checks to monitor (要監控的運作狀態檢查) 中的運作狀態檢查數目，Route 53 一律會將此運作狀態檢查視為狀況不良。
  - 如果您指定 0，Route 53 一律將此運作狀態檢查視為正常。
- Report healthy when all health checks are healthy (AND) (當所有運作狀態檢查都是正常時，報告狀態正常 (AND)) – 只有在新增至 Health checks to monitor (要監控的運作狀態檢查) 中的所有運作狀態檢查都是正常時，Route 53 才會將此運作狀態檢查視為正常。
- Report healthy when one or more health checks are healthy (OR) (當一個或多個運作狀態檢查是正常時，報告狀態正常 (OR)) – 當新增至 Health checks to monitor (要監控的運作狀態檢查) 中的運作狀態檢查至少有一項是正常時，Route 53 就會將此運作狀態檢查視為正常。

Invert health check status

選擇是否要 Route 53 反轉運作狀態檢查的狀態。如果您選擇此選項，Route 53 會將狀態正常的運作狀態檢查視為狀況不良，反之亦然。

Disabled

讓 Route 53 停止執行運作狀態檢查。當您停用運作狀態檢查時，Route 53 會停止彙總參考的運作狀態檢查之狀態。

在您停用運作狀態檢查之後，Route 53 會將參考的運作狀態檢查之狀態視為一律正常。如果您已設定 DNS 備援，Route 53 會持續將流量路由到對應的資源。如果您要停止將流量路由到資源，請變更 Invert health check status 的值。

> **Note**
>
> 在停用運作狀態檢查時，仍會產生運作狀態檢查的費用。

監控 CloudWatch 警示

如果您希望此健康狀態檢查監視警示的 CloudWatch 警示狀態，請指定下列值：

- CloudWatch alarm
- Health check status
- Invert health check status
- Disabled

CloudWatch 警報

選擇您希望 Route 53 用來判斷此健康狀態檢查是否健康狀況的 CloudWatch 警示。 CloudWatch 警示必須與健康狀態檢查 AWS 帳戶 相同。

> **Note**
>
> Route 53 支援具有以下功能的 CloudWatch 警報：
>
> - 標準解析指標。不支援高解析指標。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的高解析度指標。
> - 統計資料：`Average`、`Minimum`、`Maximum`、`Sum` 和 `SampleCount`。不支援擴充統計資料。
> - Route 53 不支援「N 中的 M」警示。如需詳細資訊，請參閱 Amazon CloudWatch 指南中的評估警示。
>
> Route 53 不支援使用度量數學來查詢多個 CloudWatch 量度的警示。

如果您要建立警示，請執行以下步驟：

1. 選擇 建立。 CloudWatch 主控台會出現在新的瀏覽器索引標籤中。
2. 輸入適用的值。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立或編輯 CloudWatch 警示。

3. 返回至 Route 53 主控台顯示的瀏覽器索引標籤。
4. 選擇CloudWatch鬧鐘清單旁的重新整理按鈕。
5. 從清單中選擇新的警示。

> **Important**
>
> 如果您在建立健康狀態檢查後變更 CloudWatch 警示的設定，則必須更新健全狀況檢查。如需詳細資訊，請參閱 變更 CloudWatch 警示設定時更新健全狀況檢查 (僅監控 CloudWatch 警示的健全狀況檢查)。

Health check status

當資料不足以判斷您選擇的警示狀態時，選擇健全狀況檢查的狀態 (狀況良好、狀況不良或上次 CloudWatch 已知狀態)。CloudWatch如果您選擇使用上次已知狀態，Route 53 會使用上次 CloudWatch 擁有足夠資料來判斷警示狀態的健全狀況檢查狀態。對於沒有上次已知狀態的新運作狀態檢查，運作狀態檢查的預設狀態是正常。

當 CloudWatch 測量結果的資料串流短暫無法使用時，Health 全狀況檢查狀態的值會提供暫時狀態。Route 53 會監控 CloudWatch 指標的資料串流，而非對應警示的狀態。) 如果指標經常或長時間 (超過幾小時) 無法使用，我們建議您不要使用上一個已知狀態。

Invert health check status

選擇是否要 Route 53 反轉運作狀態檢查的狀態。如果您選擇此選項，Route 53 會將狀態正常的運作狀態檢查視為狀況不良，反之亦然。

Disabled

讓 Route 53 停止執行運作狀態檢查。停用健康狀態檢查時，Route 53 會停止監視對應的 CloudWatch指標。

在您停用運作狀態檢查之後，Route 53 會將參考的運作狀態檢查之狀態視為一律正常。如果您已設定 DNS 備援，Route 53 會持續將流量路由到對應的資源。如果您要停止將流量路由到資源，請變更 Invert health check status 的值。

> **Note**
>
> 在停用運作狀態檢查時，仍會產生運作狀態檢查的費用。

進階組態 (僅限 "Monitor an endpoint")

如果您選擇監控端點的選項，還可以指定以下設定：

- Request interval
- Failure threshold
- String matching
- Search string
- Latency graphs
- Enable SNI
- Health checker regions
- Invert health check status
- Disabled

Request interval

每個 Route 53 運作狀態檢查程式從端點獲得回應的時間，與傳送下一個運作狀態檢查請求的時間之間的秒數。如果您選擇的間隔為 30 秒，在全球資料中心的每個 Route 53 運作狀態檢查程式會每隔 30 秒向端點傳送一次運作狀態檢查請求。平均來說，端點大約每隔兩秒會收到一次運作狀態檢查請求。如果您選擇的間隔為 10 秒，端點每秒會收到多次請求。

請注意，在不同資料中心的 Route 53 運作狀態檢查程式不會彼此協調，所以無論您選擇多久的間隔，有時會看到每秒多個請求，接著幾秒鐘完全沒有運作狀態檢查的情況。

建立運作狀態檢查之後，即無法變更 Request interval (請求間隔) 的值。

> **Note**
>
> 如果您選擇 Fast (10 seconds) (快速 (10 秒)) 做為 Request interval (請求間隔) 的值，會產生額外費用。如需詳細資訊，請參閱 Route 53 定價。

Failure threshold

端點必須通過或失敗的連續運作狀態檢查數目，才會讓 Route 53 將該端點的目前狀態從狀況不良變更為正常，或反之。如需詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

String matching (僅限 HTTP 和 HTTPS)

您是否希望 Route 53 透過提交 HTTP 或 HTTPS 請求至端點，然後在回應本文中搜尋指定的字串，來判斷端點的運作狀態。如果回應本文包含您在 Search string (搜尋字串) 中指定的值，Route 53 會將端點視為正常。如果未包含，或是端點未回應，Route 53 會將端點視為狀況不良。搜尋字串必須完全顯示在回應本文的前 5,120 個位元組中。

建立運作狀態檢查之後，即無法變更 String matching (字串比對) 的值。

> **Note**
>
> 如果您選擇 Yes (是) 做為 String matching (字串比對) 的值，會產生額外費用。如需詳細資訊，請參閱 Route 53 定價。

運作狀態檢查程式如何處理壓縮的回應

如果端點是傳回壓縮回應的 Web 伺服器，Route 53 運作狀態檢查程式只有在 Web 伺服器使用該檢查程式支援的壓縮演算法壓縮回應時，才會先解壓縮回應，再檢查指定的搜尋字串。運作狀態檢查程式支援下列壓縮演算法：

- Gzip
- Deflate

如果使用另一個演算法壓縮回應，運作狀態檢查程式就無法在搜尋字串之前解壓縮回應。在這種情況下，搜尋幾乎總是會失敗，而 Route 53 會將端點視為狀態不良

字串比對 (只有當 String matching (字串比對) 啟用時)

您希望 Route 53 在端點的回應本文中搜尋的字串。長度上限為 255 個字元。

Route 53 在回應本文中搜尋 Search string (搜尋字串) 時會考慮大小寫。

Latency graphs

選擇是否要 Route 53 測量多個 AWS 區域中健康狀態檢查程式與您的端點之間的延遲。如果您選擇此選項， CloudWatch 延遲圖表會顯示在 Route 53 主控台中 [Health 檢查] 頁面的 [延遲] 索引標籤上。如果 Route 53 運作狀態檢查程式無法連線至端點，Route 53 就無法顯示該端點的延遲圖形。

建立運作狀態檢查之後，即無法變更 Latency measurements (延遲測量) 的值。

> **Note**
>
> 如果您設定 Route 53 來測量運作狀態檢查程式和端點之間的延遲，會產生額外費用。如需詳細資訊，請參閱 Route 53 定價。

Enable SNI (僅限 HTTPS)

指定您是否希望 Route 53 在 TLS 交涉期間透過 `client_hello` 訊息將主機名稱傳送至端點。這允許端點使用適用的 SSL/TLS 憑證來回應 HTTPS 請求。

有些端點要求 HTTPS 請求必須在 `client_hello` 訊息中包含主機名稱。如果未啟用 SNI，運作狀態檢查的狀態將是 `SSL alert handshake_failure`。運作狀態檢查也可能因為其他原因而具有該狀態。如果 SNI 已啟用，仍發生此錯誤，請檢查端點的 SSL/TLS 組態並確認憑證是有效的。

請注意以下要求：

- 端點必須支援 SNI。
- 端點的 SSL/TLS 憑證在 `Common Name` 欄位中必須包含網域名稱，在`Subject Alternative Names` 欄位中包含其他幾個網域名稱。憑證的其中一個網域名稱必須符合您在 Host name (主機名稱) 中指定的值。

Health checker regions

選擇您希望 Route 53 透過使用建議區域中的運作狀態檢查程式還是使用指定區域中的運作狀態檢查程式，來檢查端點的運作狀態。

如果您更新運作狀態檢查來移除已執行運作狀態檢查的區域，Route 53 會持續從該區域執行檢查，時間長達一小時。這可確保一些運作狀態檢查程式一定在檢查端點 (例如，如果您將三個區域換成四個不同的區域)。

如果您選擇 Customize (自訂)，請選擇區域的 x 將其移除。按一下清單底部的空白處，可將區域新增回清單。您必須至少指定三個區域。

Invert health check status

選擇是否要 Route 53 反轉運作狀態檢查的狀態。如果您選擇此選項，Route 53 會將狀態正常的運作狀態檢查視為狀況不良，反之亦然。例如，如果您設定字串比對，而端點傳回指定的值，您可能希望 Route 53 將運作狀態檢查視為狀況不良。如需執行字串比對的運作狀態檢查詳細資訊，請參閱 String matching。

Disabled

讓 Route 53 停止執行運作狀態檢查。當您停用運作狀態檢查時，Route 53 會停止嘗試與端點建立 TCP 連線。

在您停用運作狀態檢查之後，Route 53 會將參考的運作狀態檢查之狀態視為一律正常。如果您已設定 DNS 備援，Route 53 會持續將流量路由到對應的資源。如果您要停止將流量路由到資源，請變更 Invert health check status 的值。

> **Note**
>
> 在停用運作狀態檢查時，仍會產生運作狀態檢查的費用。

在運作狀態檢查失敗時收到通知

使用以下選項來設定運作狀態檢查失敗時的電子郵件通知：

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

Create alarm (只有當建立運作狀態檢查時)

指定是否要建立預設 CloudWatch 鬧鐘。如果選擇是，則會在此端點的狀態變更為狀態不良時，CloudWatch 傳送 Amazon SNS 通知給您，而 Route 53 認為端點運作狀態不良一分鐘。

> **Note**
>
> 如果您想 CloudWatch 要在狀態變回正常狀態時傳送另一個 Amazon SNS 通知給您，可以在建立運作狀態檢查後建立另一個警示。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立 Amazon CloudWatch 警示。

如果您要為現有的運作狀態檢查建立警示，或要在 Route 53 將端點視為狀況不良的時間多於或少於一分鐘 (預設值) 時接收通知，請選取 No (否)，並在建立運作狀態檢查之後新增警示。如需詳細資訊，請參閱 使用 CloudWatch 監控運作狀態檢查。

Send notification to (只有當建立警示時)

指定要 CloudWatch 將通知傳送至現有 Amazon SNS 主題還是要傳送給新主題：

- Existing SNS topic (現有的 SNS 主題) – 從清單中選取主題名稱。該主題必須位於美國東部 (維吉尼亞北部)區域。
- New SNS topic (新的 SNS 主題) – 在 Topic name (主題名稱) 中輸入主題名稱，並在 Recipients (收件人) 中輸入您要對其傳送通知的電子郵件地址。使用逗號 (,)、分號 (;) 或空格分隔多個地址。

  Route 53 將在美國東部 (維吉尼亞北部) 區域建立主題。

Topic name (只有當建立新的 SNS 主題時)

如果指定 New SNS Topic (新的 SNS 主題)，請輸入新主題的名稱。

Recipient email addresses (只有當建立新的 SNS 主題時)

如果指定 New SNS topic (新的 SNS 主題)，請輸入要對其傳送通知的電子郵件地址。使用逗號 (,)、分號 (;) 或空格分隔多個名稱。

當您建立運作狀態檢查時 Amazon Route 53 顯示的值

Create Health Check (建立運作狀態檢查) 頁面會根據您輸入的值顯示以下值：

URL

Route 53 在執行運作狀態檢查時傳送請求的目標完整 URL (適用於 HTTP 或 HTTPS 運作狀態檢查) 或 IP 地址和連接埠 (適用於 TCP 運作狀態檢查)。

Health Check Type

根據您為此運作狀態檢查指定的設定，這可以是 Basic (基本) 或 Basic + additional options (基本 + 其他選項)。如需其他選項的定價資訊，請參閱 Route 53 定價。

變更 CloudWatch 警示設定時更新健全狀況檢查 (僅監控 CloudWatch警示的健全狀況檢查)

如果您建立 Route 53 健康狀態檢查來監控資料串流是否有 CloudWatch 警示，然後更新 CloudWatch 警示中的設定，Route 53 不會自動更新健全狀況檢查中的警示設定。如果您希望運作狀態檢查開始使用新的警示設定，則需要更新運作狀態檢查。

> **Note**
>
> 若要透過編寫程式的方式更新運作狀態檢查，您可以使用 UpdateHealthCheck API。只需指定`AlarmIdentifier`和的當前值`Region`，Route 53 將從中獲取最新設置 CloudWatch。如需詳細資訊，請UpdateHealthCheck參閱 Amazon 路線 53 API 參考中的。

使用新的 CloudWatch 警示設定（主控台）更新健康狀態檢查

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
3. 選取要更新的運作狀態檢查的核取方塊。
4. 選擇 Edit health check (編輯運作狀態檢查)。

   附註說明健全狀況檢查的 CloudWatch 警示已變更。Details (詳細資訊) 欄位會顯示新的警示設定。
5. 選擇儲存。

刪除運作狀態檢查

若要刪除運作狀態檢查，請執行下列程序。

> **Note**
>
> 如果您正在使用 AWS Cloud Map 且設定 AWS Cloud Map 為在註冊執行個體時建立 Route 53 健康狀態檢查，則無法使用 Route 53 主控台刪除健康狀態檢查。當您取消註冊執行個體時，系統會自動刪除運作狀態檢查。可能會有幾個小時的延遲，之後運作狀態檢查才不再出現在 Route 53 主控台中。

刪除運作狀態檢查 (主控台)

1. 如果要刪除與記錄關聯的運作狀態檢查，請執行 當已設定 DNS 備援時，更新或刪除運作狀態檢查 中的建議任務。
2. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

3. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
4. 在右窗格中，選取要刪除的運作狀態檢查。
5. 選擇 Delete Health Check (刪除運作狀態檢查)。
6. 請選擇 Yes, Delete (是，刪除)，確認刪除。

當已設定 DNS 備援時，更新或刪除運作狀態檢查

當您想要更新或刪除與運作狀態檢查關聯的記錄，或要變更有相關運作狀態檢查的記錄，您必須考慮變更對 DNS 查詢路由和 DNS 備援組態有何影響。

> **Important**
>
> 即使運作狀態檢查與一或多個記錄相關聯，Route 53 也不會阻止您刪除運作狀態檢查。如果您刪除運作狀態檢查，但未更新相關聯的記錄，系統就無法預測運作狀態檢查的未來狀態，亦有可能變更。這將會影響 DNS 備援組態的 DNS 查詢路由。

若要更新或刪除已經與記錄關聯的運作狀態檢查，我們建議您執行以下任務：

1. 識別與運作狀態檢查相關的記錄。為了識別與運作狀態檢查關聯的記錄，您必須執行下列其中一項：
   - 使用 Route 53 主控台，檢閱每個託管區域中的記錄。如需詳細資訊，請參閱 列出記錄。
   - 在每個託管區域執行 `ListResourceRecordSets` API 動作，並檢閱回應。如需詳細資訊，請ListResourceRecordSets參閱 Amazon 路線 53 API 參考中的。
2. 評估因更新或刪除運作狀態檢查，或因更新記錄，所導致的行為變更。根據該評估，判斷要進行哪些變更。

   如需詳細資訊，請參閱 當您忽略運作狀態檢查時會發生什麼情況？
3. 適時地變更運作狀態檢查和記錄。如需詳細資訊，請參閱下列主題：
   - 建立和更新運作狀態檢查
   - 編輯記錄
4. 刪除不再使用的運作狀態檢查 (如果有)。如需詳細資訊，請參閱 刪除運作狀態檢查。

為 Amazon Route 53 運作狀態檢查設定路由器和防火牆規則

當 Route 53 檢查端點的運作狀態時，會將 HTTP、HTTPS 或 TCP 請求傳送給您在建立運作狀態檢查時指定的 IP 地址和連接埠。若要讓運作狀態檢查成功，您的路由器和防火牆規則必須允許來自 Route 53 運作狀態檢查程式所使用 IP 地址的傳入流量。

如需 Route 53 健全狀況檢查程式的目前 IP 位址清單、Route 53 名稱伺服器及其他 AWS 服務的相關資訊，請參閱Amazon Route 53 伺服器的 IP 地址範圍。

在 Amazon EC2 中，安全群組會作為防火牆。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的 Amazon EC2 安全群組。若要將安全群組設定為允許 Route 53 運作狀態檢查，您可以允許來自每個 IP 地址範圍的輸入流量，或使用 AWS-managed 前置詞清單。

若要使用 AWS-managed 前置詞清單，請修改您的安全群組以允許來自 `com.amazonaws.<region>.route53-healthchecks` Amazon EC2 執行個體或資源 AWS 區域的傳入流量。`<region>` 如果您使用 Route 53 運作狀態檢查來檢查 IPv6 端點，您也應該允許來自 `com.amazonaws.<region>.ipv6.route53-healthchecks` 的傳入流量。

如需有關 AWS-managed 前置詞清單的詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 AWS受管前置詞清單。

> **Important**
>
> 當您將 IP 位址新增至允許的 IP 位址清單時，請針對您建立健全狀態檢查時指定的每個 AWS 區域，新增 CIDR 範圍內的所有 IP 位址，以及全域 CIDR 範圍。您可能會看到運作狀態檢查請求只來自區域中的一個 IP 地址。不過，該 IP 地址可能隨時改變為該區域的另一個 IP 地址。如果您想要確定同時包含目前和較舊的運作狀態檢查程式 IP 地址，請將所有 /26 和 /18 IP 地址範圍新增至允許清單。如需完整清單，請參閱 AWS 一般參考 中的 AWS IP 地址範圍。當您將 AWS-managed 前綴列表添加到輸入安全組時，它會自動添加所有必要的範圍。

監控運作狀態檢查狀態和取得通知

可在 Amazon Route 53 主控台上監控運作狀態檢查的狀態。您也可以設定 CloudWatch 警示，並在運作狀態檢查的狀態變更時取得自動通知。

主題

- 檢視運作狀態檢查狀態和運作狀態檢查失敗的原因
- 監控運作狀態檢查程式和端點之間的延遲

- 使用 CloudWatch 監控運作狀態檢查

檢視運作狀態檢查狀態和運作狀態檢查失敗的原因

在 Route 53 主控台中，您可以檢視 Route 53 運作狀態檢查程式回報的運作狀態檢查狀態 (正常運作或狀況不良)。對於計算的運作狀態檢查以外的所有運作狀態檢查，您也可以檢視上次運作狀態檢查失敗的原因，例如，運作狀態檢查程式無法與端點建立連線。

若要檢視運作狀態檢查的狀態和上次失敗原因 (主控台)

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
3. 如需所有運作狀態檢查的狀態概觀 (正常或狀況不良)，請檢視 Status (狀態) 欄。如需更多詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。
4. 對於計算的運作狀態檢查以外的所有運作狀態檢查，您可以檢視正在檢查指定端點的運作狀態之 Route 53 運作狀態檢查程式的狀態。選取運作狀態檢查。
5. 在底部窗格中，選擇 Health Checkers (運作狀態檢查程式) 標籤。

   > **Note**
   >
   > 新的運作狀態檢查必須先傳播到 Route 53 運作狀態檢查程式，運作狀態檢查狀態和上次失敗原因才會出現於 Status (狀態) 欄。傳播完成之前，該欄中的訊息會指出沒有狀態。

6. 選擇您要檢視運作狀態檢查的最新狀態，或檢視上次失敗的日期和時間和失敗原因。Status (狀態) 標籤上的表格包含下列值：

   Health checker IP (運作狀態檢查程式)

   執行運作狀態檢查的 Route 53 運作狀態檢查程式的 IP 地址。

   Last checked (上次檢查時間)

   運作狀態檢查的日期和時間，或上次失敗的日期和時間，取決於您在 Status (狀態) 標籤上方選取的選項。

   狀態

   運作狀態檢查的目前狀態，或上次運作狀態檢查失敗的原因，取決於您在 Status(狀態) 標籤上方選取的選項。

監控運作狀態檢查程式和端點之間的延遲

當建立運作狀態檢查時，如果您選擇監控端點的狀態 (而不是其他運作狀態檢查的狀態)，並選擇 Latency graphs (延遲圖形) 選項，則您可以在 Route 53 主控台的 CloudWatch 圖表上檢視下列值：

- Route 53 運作狀態檢查程式與端點建立 TCP 連線所花的平均時間 (毫秒)
- Route 53 運作狀態檢查程式接收回應 HTTP 或 HTTPS 請求的第一個位元組所花的平均時間 (毫秒)
- Route 53 運作狀態檢查程式完成 SSL/TLS 交握所花的平均時間 (毫秒)。

> **Note**
>
> 您無法為現有的運作狀態檢查啟用延遲監控。

> **Important**
>
> 運作狀態檢查程式會在 16 個備援可用區域上執行。有時候可能因部署、更新、維護等原因而無法使用可用區域。運作狀態檢查系統的設計是為了解決這個問題，而不會造成任何客戶影響。

若要檢視 Route 53 運作狀態檢查程式和端點之間的延遲 (主控台)

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
3. 選取適用運作狀態檢查的對應列。您只能檢視用來監控端點狀態並已啟用 Latency graphs (延遲圖形) 選項之運作狀態檢查的延遲資料。
4. 在底部窗格中，選擇 Latency (延遲) 標籤。
5. 選擇要顯示延遲圖形的時間範圍和地理區域。

   圖形會顯示指定時間範圍的狀態：

   TCP connection time (TCP 連線時間) (僅限 HTTP 和 TCP)

   選定地理區域中的 Route 53 運作狀態檢查程式與端點建立 TCP 連線所花的平均時間 (毫秒)。

Time to first byte (至第一個位元組的時間) (僅限 HTTP 和 HTTPS)

選定地理區域中的 Route 53 運作狀態檢查程式接收回應 HTTP 或 HTTPS 請求的第一個位元組所花的平均時間 (毫秒)。

Time to complete SSL handshake (完成 SSL 交握的時間) (僅限 HTTPS)

所選地理區域中的 Route 53 運作狀態檢查程式，完成 SSL/TLS 交握所花的平均時間 (毫秒)。

> **Note**
>
> 如果您選取一個以上的運作狀態檢查，則圖形會為每個運作狀態檢查顯示不同的色彩標示的列。

6. 若要檢視較大的圖形，並指定不同的設定，請按一下圖形。您可以變更以下設定：

統計數字

變更 CloudWatch 對資料執行的計算。

時間範圍

顯示不同期間 (例如，隔夜或上週) 的運作狀態檢查的狀態。

Period

變更圖形中資料點之間的間隔。

注意下列事項：

- 如果您剛建立運作狀態檢查，則您可能需要等待幾分鐘，資料才會顯示在圖形中，運作狀態檢查指標出現在可用的指標清單中。
- 圖形不會自動自我重新整理。若要更新顯示，請選擇重新整理 ( ) 圖示。
- 如果運作狀態檢查因故失敗 (例如連線逾時)，Route 53 便無法測量延遲，而且圖形在受影響的期間將會缺少延遲資料。

使用 CloudWatch 監控運作狀態檢查

Route 53 運作狀態檢查與 CloudWatch 指標整合，以便您執行下列作業：

- 驗證運作狀態檢查已適當設定。
- 檢閱運作狀態檢查在指定期間內的狀態。
- 設定 CloudWatch 在運作狀態檢查的狀態為狀況不良時傳送 Amazon SNS 提醒。請注意，在運作狀態檢查失敗後，可能需要幾分鐘才會收到相關的 SNS 通知。

如需更多詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

- 若要檢視運作狀態檢查的狀態 (主控台)
- 若要在運作狀態檢查狀態為狀況不良時收到 Amazon SNS 通知 (主控台)
- 檢視 CloudWatch 警示狀態和編輯 Amazon Route 53 的警示 (主控台)
- 若要在 CloudWatch 主控台檢視 Route 53 指標

若要檢視運作狀態檢查的狀態 (主控台)

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
3. 選擇適用運作狀態檢查的對應列。
4. 在底部窗格中，選擇 Monitoring (監控) 標籤。

   兩個圖形以一分鐘間隔顯示過去一小時的狀態：

   運作狀態檢查狀態

   此圖表顯示端點運作狀態的 Route 53 評估。1表示運作狀態良好，0表示運作狀態不佳。

   回報端點正常運作的運作狀態檢查程式 (%)

   針對僅監控端點的運作狀態檢查，圖表會顯示將所選端點視為正常運作的 Route 53 運作狀態檢查程式百分比。

   運作狀態檢查停用時，將無法使用此指標。

正常運作的子運作狀態檢查數目

僅適用於計算的運作狀態檢查，圖形會顯示正常運作的子運作狀態檢查數目。

> **Note**
>
> 如果您選取一個以上的運作狀態檢查，則圖形會為每個運作狀態檢查顯示不同的色彩標示的列。

5. 若要檢視較大的圖形，並指定不同的設定，請按一下圖形。您可以變更以下設定：

   統計數字

   變更 CloudWatch 對資料執行的計算。

   時間範圍

   顯示不同期間 (例如，隔夜或上週) 的運作狀態檢查的狀態。

   Period

   變更圖形中資料點之間的間隔。

   注意下列事項：

   - 如果您剛建立運作狀態檢查，則您可能需要等待幾分鐘，資料才會顯示在圖形中，運作狀態檢查指標出現在可用的指標清單中。
   - 圖形不會自動自我重新整理。若要更新顯示，請選擇重新整理 ( ) 圖示。

若要在運作狀態檢查狀態為狀況不良時收到 Amazon SNS 通知 (主控台)

1. 在 Route 53 主控台的導覽窗格中，選擇 Health Checks (運作狀態檢查)。
2. 選擇適用運作狀態檢查的對應列。
3. 在底部窗格中，選擇 Alarms (警示) 標籤。

   資料表會列出您已為此運作狀態檢查建立的警示。
4. 選擇 Create Alarm (建立警示)。

5. 指定下列值：

Alarm name (警示名稱)

輸入您希望 Route 53 顯示在 Alarms (警示) 標籤上的 Name (名稱) 欄中的名稱。

Alarm description (警示說明)

(選用) 輸入警示的說明。此值會顯示於 CloudWatch 主控台。

Send notification (傳送通知)

選擇此運作狀態檢查的狀態觸發警示時是否要 Route 53 傳送通知給您。

Notification target (通知目標) (只有在 "Send notification" 為 "Yes")

如果您希望 CloudWatch 傳送通知到現有的 SNS 主題，請從清單中選擇主題。

如果您希望 CloudWatch 傳送通知，但不傳送至現有的 SNS 主題，請執行下列其中一項操作：

- 如果您希望 CloudWatch 傳送電子郵件通知 – 選擇 New SNS topic (新的 SNS 主題) 並繼續此程序。
- 如果您希望 CloudWatch 以另一種方法來傳送通知 – 開啟新的瀏覽器標籤、前往 Amazon SNS 主控台，並建立新主題。然後返回 Route 53 主控台，從 Notification target (通知目標) 清單選擇新主題的名稱，並繼續此程序。

Topic name (只有當您選擇建立新的 Amazon SNS 主題)

輸入新 Amazon SNS 主題的名稱。

Recipient email addresses (只有當您選擇建立新的 Amazon SNS 主題時)

輸入在運作狀態檢查觸發警示時您希望 Route 53 傳送 SNS 通知的電子郵件地址。

Alarm target (警示目標)

選擇您希望 Route 53 針對此運作狀態檢查評估的值：

- Health check status (運作狀態檢查狀態) – Route 53 運作狀態檢查程式回報運作狀態檢查正常運作或狀況不良
- Health checkers that report the endpoint healthy (%) (回報端點正常運作的運作狀態檢查程式 (%)) (僅監控端點的運作狀態檢查) – 回報運作狀態檢查為正常運作的 Route 53 運作狀態檢查程式百分比

- Number of healthy child health checks (正常運作的子運作狀態檢查數目) (僅限計算的運作狀態檢查) – 在計算運作狀態檢查中，回報運作狀態檢查為正常運作狀態的子運作狀態檢查數目
- TCP connection time (TCP 連線時間) (僅限 HTTP 和 TCP 運作狀態檢查) - Route 53 運作狀態檢查程式與端點建立 TCP 連線所花費的時間 (毫秒)
- Time to complete SSL handshake (完成 TLS 交握的時間) (僅限 HTTPS 運作狀態檢查) – Route 53 運作狀態檢查程式完成 SSL/TLS 交握所花的時間 (毫秒)
- Time to first byte (至第一個位元組的時間) (僅限 HTTP 和 HTTPS 運作狀態檢查) – Route 53 運作狀態檢查程式接收回應 HTTP 或 HTTPS 請求的第一個位元組所花費的時間 (毫秒)

Alarm target (警示目標)

對於以延遲為基礎的警示目標 (TCP connection time (TCP 連線時間)、Time to complete SSL handshake (完成 SSL 交握的時間)、Time to first byte (第一個位元組的時間))，選擇您希望 CloudWatch 為特定區域或所有區域 (Global (全球)) 的 Route 53 運作狀態檢查程式來計算延遲。

請注意，如果您選擇區域，Route 53 每分鐘只測量延遲兩次，而且取樣數目會比選擇所有區域時更小。因此，更可能會出現異常值。為避免假性警示通知，我們建議您指定更多的連續期間，在這些連續期間運作狀態檢查必須失敗，CloudWatch 才會傳送通知給您。

Fulfill condition (履行條件)

使用下列設定來判斷 CloudWatch 何時應該觸發警示。

Alarm target (警示目標)	建議的條件	描述
運作狀態檢查狀態	Minimum (最小值) < 1	當端點為狀況不良時，Route 53 運作狀態檢查程式會回報。

Alarm target (警示目標)	建議的條件	描述
回報端點正常運作的運作狀態檢查程式 (%)	Average (平均值) < 「所需的百分比」	僅監控端點的運作狀態檢查 – 當回報狀態為正常運作的運作狀態檢查程式小於 18% 時，Route 53 會將運作狀態檢查的狀態視為狀況不良。請勿為此指標選擇 Sample Count (範本計數)，因為隨著 Route 53 新增更多運作狀態檢查區域，範本計數的範圍可能會變更。Average (平均值) 將始終正確表示回報運作狀態檢查程式的百分比。
正常運作的子運作狀態檢查數目	Minimum (最小值) < 「正常運作的子運作狀態檢查所需數目」	Minimum (最小值) 統計數字傳回最保守值並代表最壞情況。
TCP connection time (TCP 連線時間)	Average (平均值) > 「所需時間 (毫秒)」	Average (平均值) 比其他統計資料更為一致。
Time to complete SSL handshake (完成 SSL 交握的時間)	Average (平均值) > 「所需時間 (毫秒)」	Average (平均值) 比其他統計資料更為一致。
Time to first byte (至第一個位元組的時間)	Average (平均值) > 「所需時間 (毫秒)」	Average (平均值) 比其他統計資料更為一致。

至少 ***x*** 個 ***y*** 分鐘/小時/日的連續時段

指定在多少個連續期間內指定的值必須符合條件，Route 53 才會傳送通知。然後，指定期間的時間長度。

6. 當您選擇 Create (建立)，Amazon SNS 會傳送您一封電子郵件，其中包含有關新 SNS 主題的資訊。
7. 在電子郵件中，選擇 Confirm subscription (確認訂閱)。您必須確認訂閱，才能開始接收 CloudWatch 通知。

檢視 CloudWatch 警示狀態和編輯 Amazon Route 53 的警示 (主控台)

1. 在 Route 53 主控台的導覽窗格中，選擇 Health Checks (運作狀態檢查)。
2. 選擇任何運作狀態檢查的對應列。
3. 在詳細資訊窗格中 (在 x 個 Health Checks Selected (運作狀態檢查已選取) 後面)，選擇右插入號 ( ) 圖示。

   CloudWatch Alarms (CloudWatch 警示) 清單包含已使用目前的 AWS 帳戶建立的所有 Route 53 警示。

   State (狀態) 欄會顯示每個警示的狀態：

   OK (確定)

   CloudWatch 已從 Route 53 運作狀態檢查累積足夠的統計資料，判斷端點不符合警示閾值。

   INSUFFICIENT DATA (資料不足)

   CloudWatch 尚未累積足夠的統計資料，無法判斷端點是否符合警示閾值。這是新警示的初始狀態。如果 CloudWatch 指標變得無法使用，或者如果您刪除運作狀態檢查，但不刪除相關聯的警示，則警示狀態也會變更為 INSUFFICIENT DATA (資料不足)。

   ALARM (警示)

   CloudWatch 已從 Route 53 運作狀態檢查累積足夠的統計資料，判斷端點符合警示閾值，並傳送通知到指定的電子郵件地址。
4. 若要檢視或編輯警示的設定，請選擇警示的名稱。
5. 若要在 CloudWatch 主控台中檢視警示 (主控台提供警示的更多詳細資訊，例如，警示更新和狀態變化的歷史記錄)，請在該警示的 More Options (更多選項) 欄中選擇 View (檢視)。
6. 若要檢視已使用目前 AWS 帳戶建立的所有 CloudWatch 警示，包括其他 AWS 服務的警示，請選擇 View All CloudWatch Alarms (檢視所有 CloudWatch 警示)。
7. 若要檢視所有可用的 CloudWatch 指標，包括目前 AWS 帳戶未使用的指標，請選擇 View All CloudWatch Metrics (檢視所有 CloudWatch 指標)。

若要在 CloudWatch 主控台檢視 Route 53 指標

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/cloudwatch/ 的 CloudWatch 主控台。

2. 將目前區域變更為美國東部 (維吉尼亞北部)。如果您選擇任何其他區域做為目前的區域，Route 53 指標將無法使用。
3. 在導覽窗格中，選擇 Metrics (指標)。
4. 在 All metrics (所有指標) 標籤上，選擇 Route 53。
5. 選擇 Health Check Metrics (運作狀態檢查指標)。

設定 DNS 備援

當您有多個執行相同功能的資源 (例如，多個 HTTP 伺服器或郵件伺服器)，您可以設定 Amazon Route 53 檢查資源的運作狀態並僅使用正常的資源來回應 DNS 查詢。例如，假設您的網站 example.com 由六個伺服器託管，這些伺服器位於三個全球資料中心，每個資料中心兩個伺服器。您可以設定 Route 53 檢查這些伺服器的運作狀態，並僅使用目前正常的伺服器來回應對 example.com 的 DNS 查詢。

Route 53 可以檢查簡單和複雜組態中之資源的運作狀態：

- 在簡單組態中，您可以建立一組全含有相同名稱和類型的記錄 (例如 example.com 類型 A 的加權記錄群組)。然後，設定 Route 53 來檢查對應資源的運作狀態。Route 53 會根據資源的運作狀態來回應 DNS 查詢。如需更多詳細資訊，請參閱 簡單 Amazon Route 53 組態中運作狀態檢查的運作方式。
- 在較為複雜的組態中，您可以依據多項條件來建立記錄樹狀目錄以路由流量。例如，如果使用者的延遲狀態是您最重要的條件，您可以使用延遲別名記錄將流量路由到可提供最佳延遲性的區域。延遲別名記錄和別名目標一樣，在每個區域中都可以有加權記錄。加權記錄可根據執行個體類型，將流量路由到 EC2 執行個體。如同簡單的組態一樣，您可以將 Route 53 設為依據資源的運作狀態來路由流量。如需更多詳細資訊，請參閱 複雜 Amazon Route 53 組態中運作狀態檢查的運作方式。

主題

- 設定 DNS 備援的任務清單
- 簡單 Amazon Route 53 組態中運作狀態檢查的運作方式
- 複雜 Amazon Route 53 組態中運作狀態檢查的運作方式
- 當您已設定運作狀態檢查時，Amazon Route 53 會如何選擇記錄
- 主動-主動和主動-被動容錯移轉
- 在私有託管區域中設定容錯移轉
- Amazon Route 53 如何避免容錯移轉問題

設定 DNS 備援的任務清單

若要使用 Route 53 來設定 DNS 備援，請執行以下任務：

1. 繪製組態的樹狀圖，並指定要為每個節點建立的記錄類型 (加權別名、容錯移轉、延遲等等)。在樹狀目錄頂端，放置記錄的網域名稱 (例如 example.com)，以讓使用者用來存取您的網站或 Web 應用程式。

   此類型的記錄會依據組態的複雜性顯示在您的樹狀圖中：

   - 在簡單組態中，您的圖表可能不含任何別名記錄，或別名記錄會將流量直接路由到資源 (例如 ELB 負載平衡器)，而不是到另一個 Route 53 記錄。如需更多詳細資訊，請參閱 簡單 Amazon Route 53 組態中運作狀態檢查的運作方式。
   - 在複雜的組態，您的圖表會在多層級樹中包含別名記錄 (例如加權別名和容錯移轉別名) 和非別名記錄的組合，如 複雜 Amazon Route 53 組態中運作狀態檢查的運作方式 主題中的範例。

   > **Note**
   >
   > 若要快速且輕鬆地為複雜路由組態建立記錄，並將記錄與運作狀態檢查關聯，您可以使用流量流程視覺化編輯器，並將組態儲存為流量政策。然後，您可以將流量政策與相同託管區域或多個託管區域中的一或多個網域名稱 (例如 example.com) 或子網域名稱 (如 www.example.com) 關聯。此外，如果新組態執行不如預期，您可以復原更新。如需更多詳細資訊，請參閱 使用流量流程來路由 DNS 流量。

   如需詳細資訊，請參閱下列文件：

   - 選擇路由政策
   - 選擇別名或非別名記錄

2. 針對無法建立別名記錄的資源 (例如 Amazon EC2 伺服器與執行於資料中心的電子郵件伺服器)，建立運作狀態檢查。您會將這些運作狀態檢查與您的非別名記錄關聯。

   如需更多詳細資訊，請參閱 建立、更新和刪除運作狀態檢查。

3. 如有必要，請設定路由器和防火牆規則，讓 Route 53 可以將一般請求傳送給您在運作狀態檢查中指定的端點。如需更多詳細資訊，請參閱 為 Amazon Route 53 運作狀態檢查設定路由器和防火牆規則。

4. 在圖表中建立所有非別名記錄，並將步驟 2 中建立的運作狀態檢查與適用的記錄建立關聯。

如果您是在不含任何別名記錄的組態中設定 DNS 備援，請跳過其餘的任務。

5. 建立別名記錄以將流量路由到 AWS 資源，例如 ELB 負載平衡器和 CloudFront 分發。如果您希望 Route 53 在資源狀況不良時嘗試樹狀目錄的其他分支，請將每個別名記錄的 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)。(有些 AWS 資源不支援 Evaluate Target Health (評估目標運作狀態)。)
6. 從步驟 1 建立的樹狀圖底部開始，建立別名記錄以將流量路由到您在步驟 4 和 5 建立的記錄。如果您希望 Route 53 在樹狀目錄某個分支中的所有非別名記錄都是狀況不良時嘗試該樹狀目錄的其他分支，請將每個別名記錄的 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)。

   請記住，您必須先建立其他記錄之後，才能建立別名記錄來將流量路由到其他記錄。

簡單 Amazon Route 53 組態中運作狀態檢查的運作方式

當您有兩個或多個執行相同功能的資源 (例如兩個或多個 Web 伺服器用於 example.com)，您可以使用下列運作狀態檢查功能，僅將流量路由到正常運作的資源：

檢查 EC2 執行個體和其他資源的運作狀態 (非別名記錄)

如果您要將流量路由到無法建立別名記錄的資源 (例如 EC2 執行個體)，則可以為每個資源建立記錄和運作狀態檢查。然後，再將每個運作狀態檢查與適用的記錄建立關聯。運作狀態檢查會定期檢查對應資源的運作狀態，而 Route 53 只會將流量路由到運作狀態檢查回報為正常運作的資源。

評估 AWS 資源的運作狀態 (別名記錄)

如果您使用別名記錄，將流量路由到選取的 AWS 資源 (例如 ELB 負載平衡器)，您可以設定 Route 53 以評估資源的運作狀態，並將流量路由到正常運作的資源。當您設定別名記錄以評估資源的運作狀態時，即不需要建立資源的運作狀態檢查。

以下是如何設定 Route 53 以在簡單組態中檢查資源運作狀態的概觀：

1. 您識別出希望 Route 53 監控的資源。例如，您可能想要監控對 example.com 請求有所回應的所有 HTTP 伺服器。
2. 您可以針對無法建立別名記錄的資源 (例如 EC2 執行個體或您自己資料中心裡的伺服器)，建立運作狀態檢查。您可以指定如何傳送運作狀態檢查請求給資源：使用哪個通訊協定 (HTTP、HTTPS 或 TCP)、使用哪個 IP 地址和連接埠，以及網域名稱和路徑 (針對 HTTP/HTTPS 運作狀態檢查)。

> **Note**
>
> 如果您使用任何可以建立別名記錄的資源 (例如 ELB 負載平衡器)，請不要為這些資源建立運作狀態檢查。

常見組態是為每個資源建立一個運作狀態檢查，並對運作狀態檢查端點使用與資源相同的 IP 地址。運作狀態檢查會將請求傳送到指定的 IP 地址。

> **Note**
>
> 如果資源的 IP 地址位於本機、私有、不可路由或多點傳送範圍內，Route 53 就無法檢查這類資源的運作狀態。如需無法建立運作狀態檢查的 IP 地址詳細資訊，請參閱 RFC 5735, Special Use IPv4 Addresses 和 RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space。

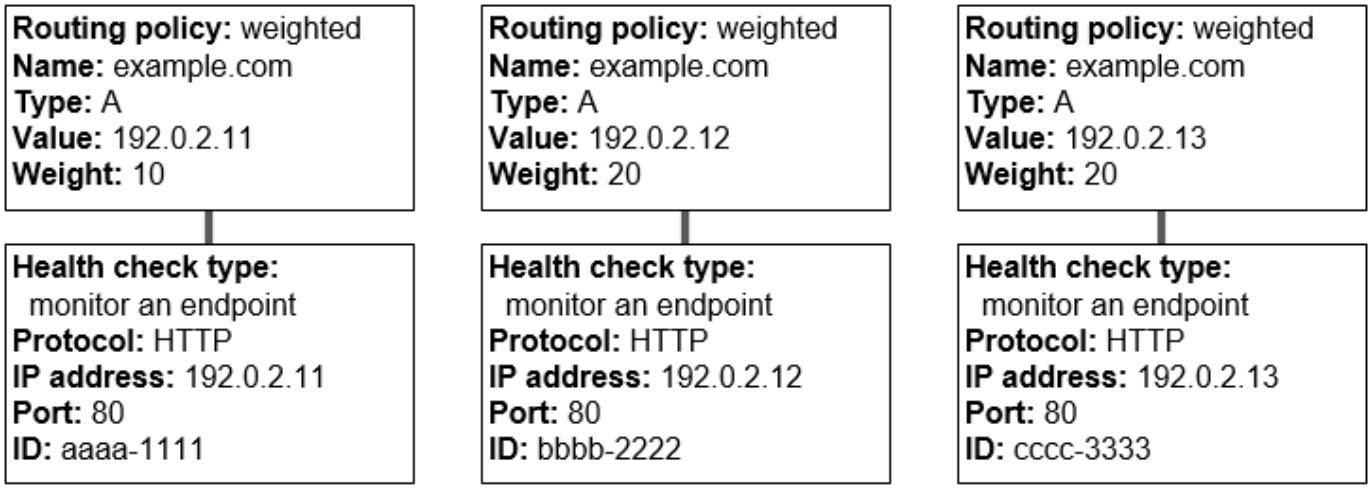
如需如何建立運作狀態檢查的詳細資訊，請參閱 建立、更新和刪除運作狀態檢查。

3. 您可能需要設定路由器和防火牆規則，讓 Route 53 可以向運作狀態檢查中指定的端點傳送一般請求。如需更多詳細資訊，請參閱 為 Amazon Route 53 運作狀態檢查設定路由器和防火牆規則。
4. 您可以建立資源的記錄群組，例如加權記錄群組。您可以混合別名和非別名記錄，但它們必須全擁有相同的 Name (名稱)、Type (類型) 和 Routing Policy (路由政策) 值。

   要如何設定 Route 53 以檢查資源運作的狀態，取決於您建立的是別名記錄或非別名記錄而定：

   - 別名記錄 – 將 Evaluate Target Health (評估目標運作狀態) 指定為 Yes (是)。
   - 非別名記錄 – 將步驟 2 建立的運作狀態檢查與對應的記錄建立關聯。

   完成後，您的組態如下圖所示，其中僅包含非別名記錄。



如需如何使用 Route 53 主控台建立記錄的詳細資訊，請參閱 使用 Amazon Route 53 主控台來建立記錄。

5. 如果您已建立運作狀態檢查，Route 53 會定期傳送請求給端點以進行每次運作狀態檢查，而不會在接收 DNS 查詢時執行運作狀態檢查。根據回應，Route 53 決定端點是否正常運作，並使用該資訊來確定如何回應查詢。如需更多詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

   Route 53 不會檢查記錄中所指定資源的運作狀態，例如 example.com 的 A 記錄中所指定的 IP 地址。當您將運作狀態檢查與記錄關聯時，Route 53 會開始檢查您在運作狀態檢查中所指定端點的運作狀態。您也可以設定 Route 53 來監控其他運作狀態檢查的運作狀態，或監控 CloudWatch 警示的資料串流。如需更多詳細資訊，請參閱 Amazon Route 53 運作狀態檢查的類型。

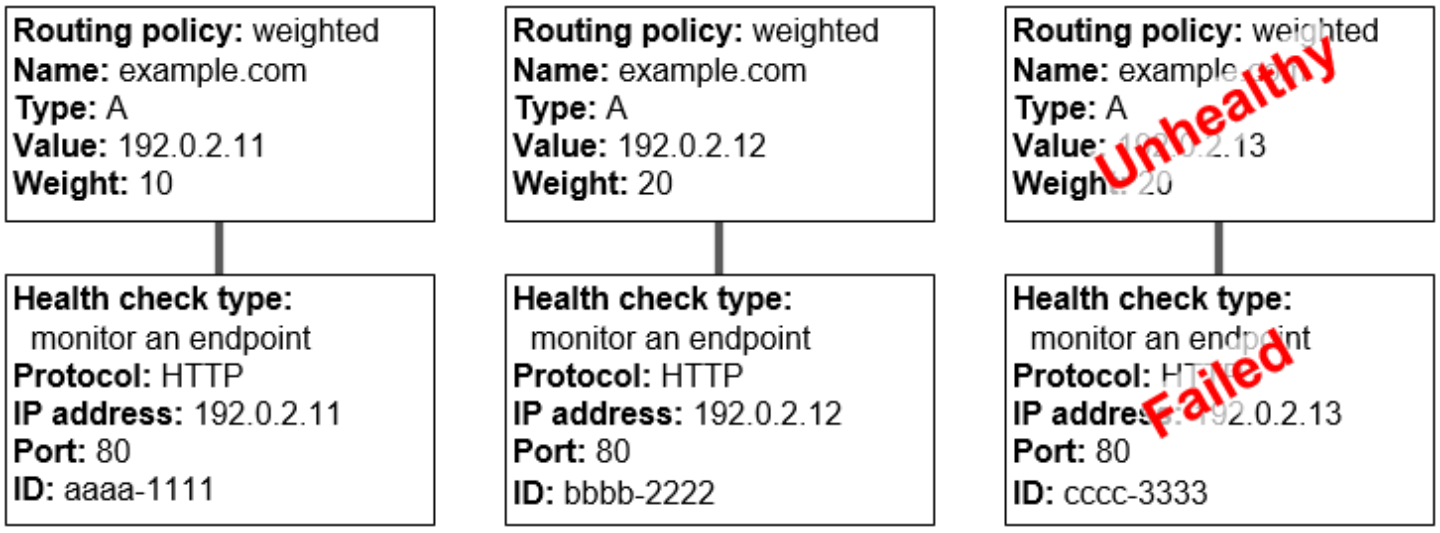
當 Route 53 收到對 example.com 的查詢，發生的情況如下：

1. Route 53 根據路由政策選擇記錄。在這種情況下，它會根據權重選擇記錄。
2. 它會檢查該記錄運作狀態檢查的狀態，來決定所選記錄的目前運作狀態。
3. 如果選取的記錄狀況不良，Route 53 會選擇不同的記錄。此時，不考慮狀況不良的記錄。

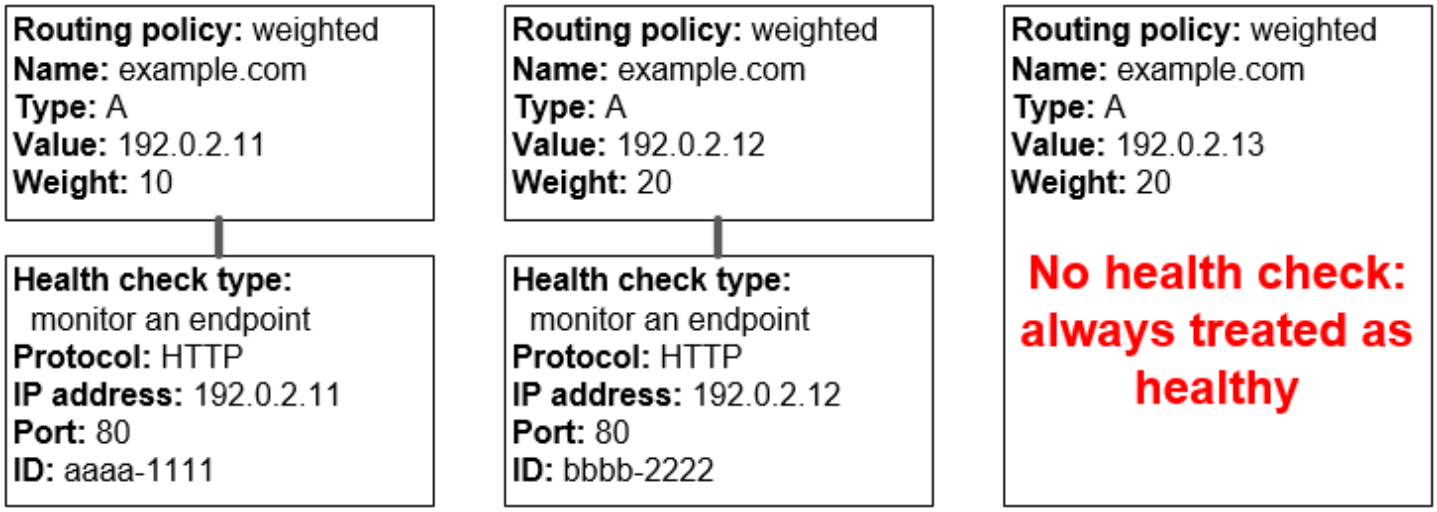
   如需更多詳細資訊，請參閱 當您已設定運作狀態檢查時，Amazon Route 53 會如何選擇記錄。
4. 當 Route 53 找到正常運作的記錄，即會以適用的值 (例如 A 記錄中的 IP 地址) 來回應查詢。

以下範例示範一組加權記錄，其中第三個記錄狀況不良。最初，Route 53 根據所有三個記錄的權重來選擇記錄。如果第一次碰巧選擇狀況不良的記錄，Route 53 會選擇另一個記錄，但這次從計算中省略第三個記錄的權重：

- 當 Route 53 最初從這三個記錄中選擇，在大約 20% 的時間內 (10/(10 + 20 + 20))，它會使用第一個記錄來回應請求。
- 當 Route 53 判斷第三個記錄狀況不良，在大約 33% 的時間內 (10/(10 + 20))，它會使用第一個記錄來回應請求。



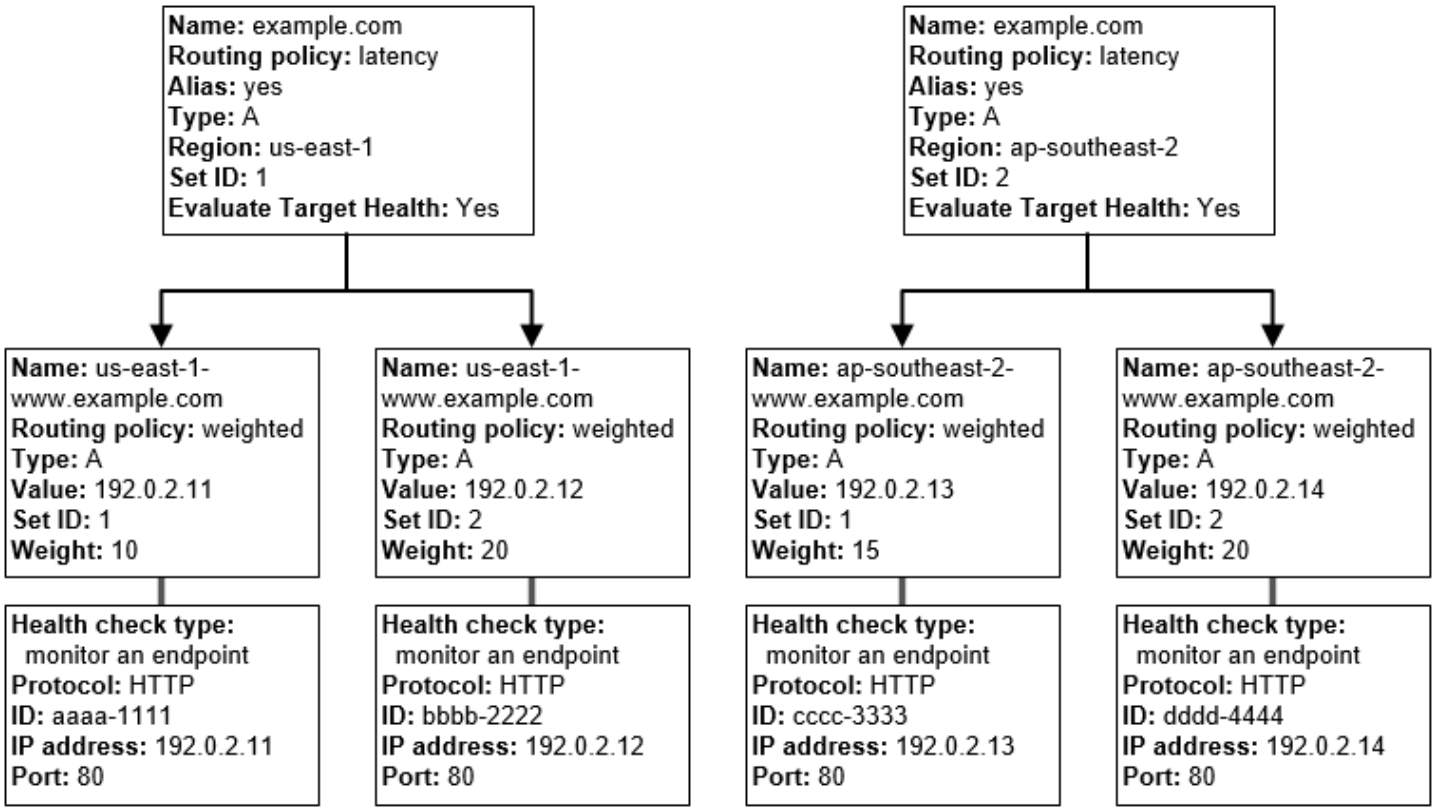
如果您忽略記錄群組的一或多個記錄的運作狀態檢查，Route 53 就無法判斷對應資源的運作狀態。Route 53 會將這些記錄視為正常運作。



複雜 Amazon Route 53 組態中運作狀態檢查的運作方式

在複雜組態中檢查資源運作狀態的運作方式和簡單組態大致相同。不過，在複雜組態中，您會使用別名記錄 (例如加權別名和容錯移轉別名) 和非別名記錄的組合來建置決策樹，以更一步控制 Route 53 回應請求的方式。

例如，您可以使用延遲別名記錄來選擇一個接近使用者的區域，並對每個區域內的兩個或多個資源使用加權記錄，以防止單一端點或可用區域故障。下圖顯示此組態。



以下是如何配置 Amazon EC2 和 Route 53 的方式。我們先從樹狀目錄的底端開始，因為這將是您建立記錄的順序：

- 您在 us-east-1 和 ap-southeast-2 這兩個區域中，各有兩個 EC2 執行個體。您想讓 Route 53 將流量路由到正常運作的 EC2 執行個體，所以您要為每個執行個體建立運作狀態檢查。您設定每個運作狀態檢查，以將運作狀態檢查請求傳送給對應的執行個體 (位於執行個體的彈性 IP 地址)。

  Route 53 是一項全球服務，因此您不必指定要建立運作狀態檢查的區域。

- 您想要根據執行個體類型，將流量路由到每個區域中的兩個執行個體，因此您建立每個執行個體的加權記錄，並為每個記錄設定權重。(您可以稍後變更權重，將更多或更少的流量路由到執行個體。) 您也可以將適用的運作狀態檢查與每個執行個體建立關聯。

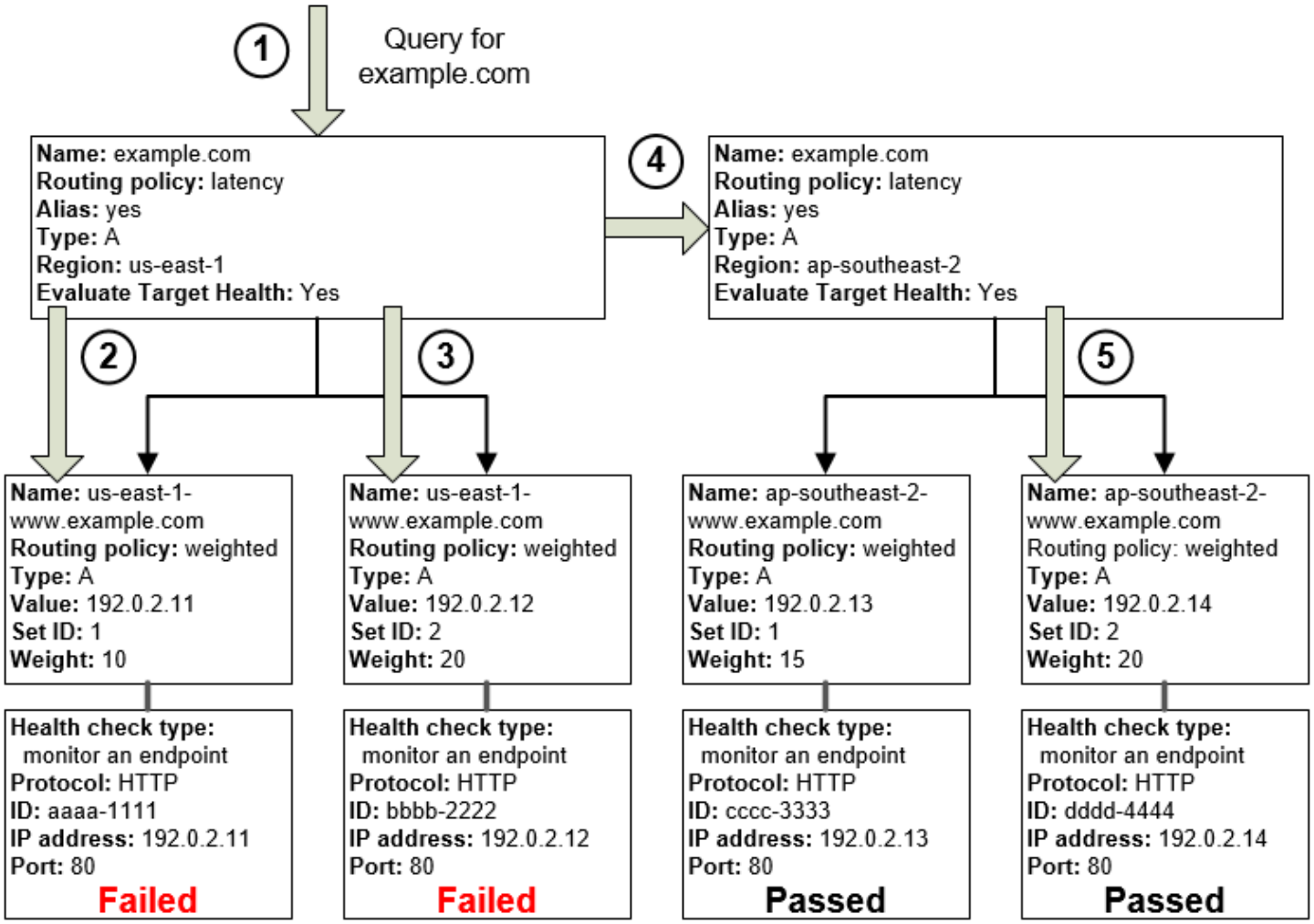
  當您建立記錄時，您會使用類似 as us-east-1-www.example.com. 和 ap-southeast-2-www.example.com 的名稱。等到您位於樹狀目錄頂端時，即可為記錄命名，以讓使用者用來存取您的網站或 Web 應用程式，例如 example.com。

- 您想要將流量路由到可為使用者提供最低延遲的區域，因此您針對樹狀目錄頂端的記錄，選擇延遲路由政策。

您想要將流量路由到每個區域中的記錄，而不是直接路由到每個區域中的資源 (加權記錄會處理這項作業)。因此，您可以建立延遲別名記錄。

當您建立別名記錄時，您可為其命名以讓使用者用來存取您的網站或 Web 應用程式，例如 example.com。別名記錄可將 example.com 的流量路由到 us-east-1-www.example.com 和 ap-southeast-2-www.example.com 記錄。

對於這兩個延遲別名記錄，您將 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)。這可讓 Route 53 先判斷區域中是否有任何正常運作的資源，再嘗試路由流量至此。如果沒有，Route 53 會選擇其他區域中正常運作的資源。



上圖說明下列事件序列：

1. Route 53 收到對 example.com 的查詢。根據使用者提出請求的延遲，Route 53 為 us-east-1 區域選擇延遲別名記錄。
2. Route 53 根據權重選擇加權記錄。延遲別名記錄的 Evaluate Target Health (評估目標運作狀態) 為 Yes (是)，因此 Route 53 會檢查所選加權記錄的運作狀態。
3. 運作狀態檢查失敗，因此 Route 53 根據權重選擇另一個加權記錄，並檢查其運作狀態。該記錄也是狀況不良。
4. Route 53 退出該樹分支，尋找具有次佳延遲的延遲別名記錄，並選擇 ap-southeast-2 的記錄。
5. Route 53 會再次根據權重選取記錄，然後檢查所選資源的運作狀態。資源正常運作，因此 Route 53 會傳回適用的值，以回應查詢。

主題

- 將運作狀態檢查與別名記錄關聯時會發生什麼情況？
- 當您忽略運作狀態檢查時會發生什麼情況？
- 當您將「evaluate target health (評估目標運作狀態)」設為「No (否)」時會發生什麼情況？

將運作狀態檢查與別名記錄關聯時會發生什麼情況？

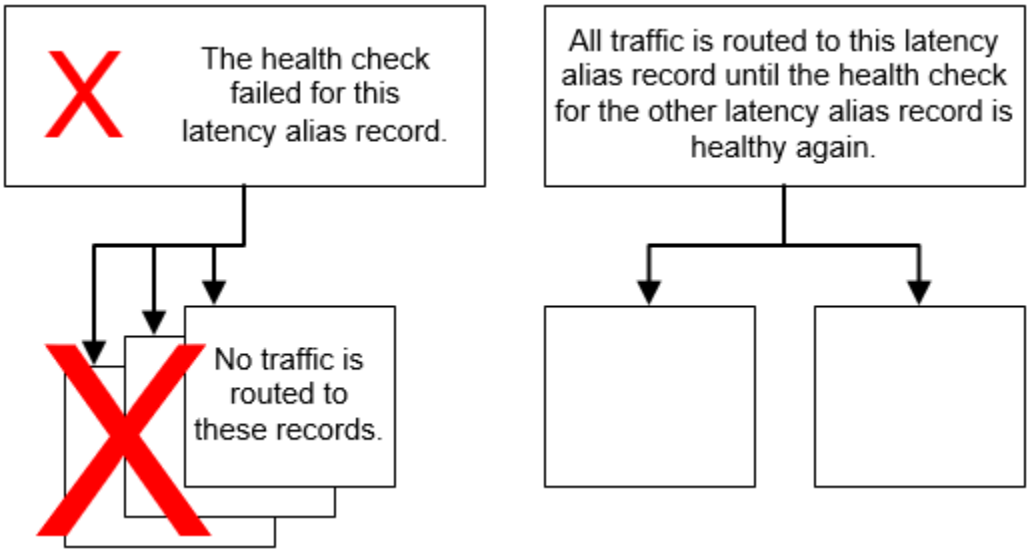
不論您是否要將 Evaluate Target Health (評估目標運作狀態) 的值設為 Yes (是)，您都可以將運作狀態檢查與別名記錄建立關聯。不過，如果 Route 53 根據基礎資源 (HTTP 伺服器、資料庫伺服器，以及別名記錄參照的其他資源) 的運作狀態來回應查詢，通常會更有用。例如，假設以下組態：

- 將運作狀態檢查指派至其別名目標是一組加權記錄的延遲別名記錄。
- 對於這個延遲別名記錄，將 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)。

在這個組態，以下兩個條件必須為真，Route 53 才會為加權記錄傳回適用的值：

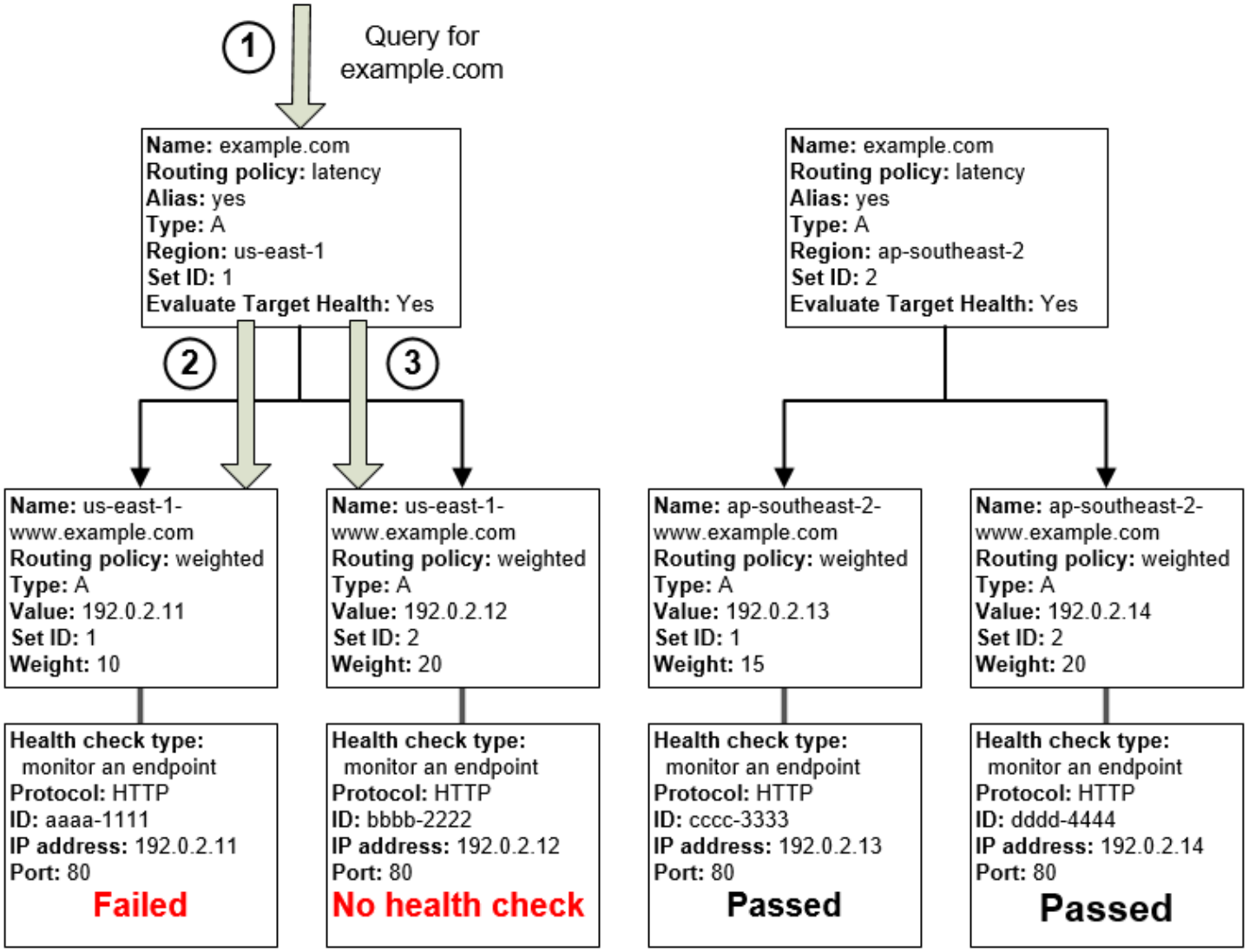
- 與延遲別名記錄相關的運作狀態檢查必須通過。
- 因為與已通過的運作狀態檢查關聯，或未與運作狀態檢查關聯，至少一個加權記錄必須被視為正常運作。在後一個案例中，Route 53 永遠會將加權記錄視為正常運作。

在下圖中，左上角延遲別名記錄的運作狀態檢查失敗。因此，如果查詢使用任何延遲別名記錄參考的加權記錄，即使它們都是正常運作，Route 53 也不再使用這些記錄來回應查詢。只有當延遲別名記錄的運作狀態檢查再次正常運作時，Route 53 才會再次開始參考這些加權記錄。(如需了解例外情況，請參閱 當您已設定運作狀態檢查時，Amazon Route 53 會如何選擇記錄。)



當您忽略運作狀態檢查時會發生什麼情況？

在複雜組態中，您必須將運作狀態檢查與所有非別名記錄建立關聯。在下列範例中，us-east-1 區域的其中一個加權記錄缺少運作狀態檢查：



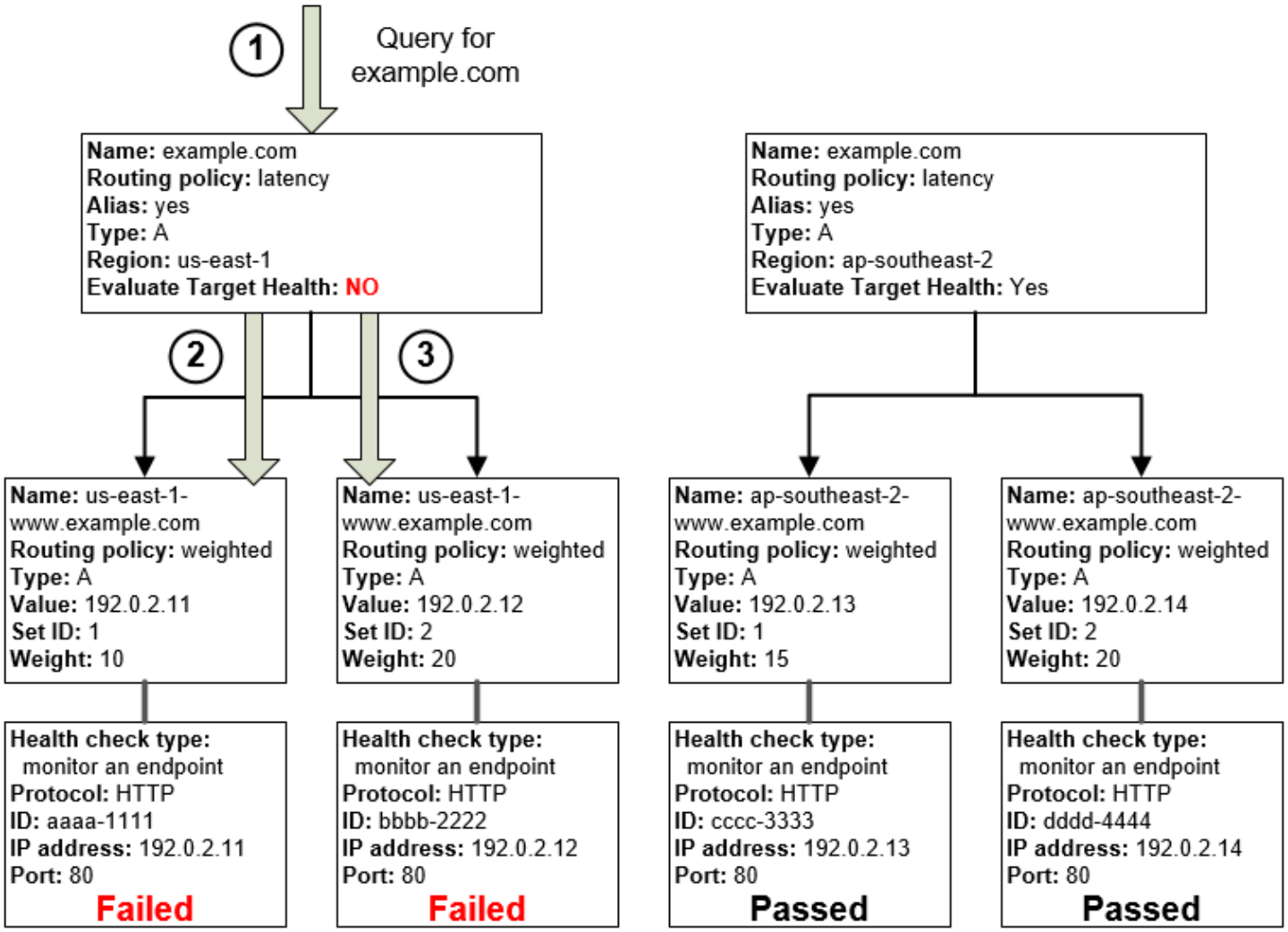
在這個組態，當您忽略非別名記錄的運作狀態檢查，發生的情況如下：

1. Route 53 收到對 example.com 的查詢。根據使用者提出請求的延遲，Route 53 為 us-east-1 區域選擇延遲別名記錄。
2. Route 53 為延遲別名記錄尋找別名目標，並檢查對應運作狀態檢查的狀態。一個加權記錄的運作狀態檢查失敗，因此不考慮該記錄。
3. us-east-1 區域的別名目標中的令一個加權記錄沒有運作狀態檢查。對應的資源可能正常運作或可能狀況不良，但沒有運作狀態檢查，Route 53 無從了解。Route 53 假設資源正常，並傳回適用的值，以回應查詢。

當您將「evaluate target health (評估目標運作狀態)」設為「No (否)」時會發生什麼情況？

一般而言，您應該將樹狀目錄中所有別名記錄的 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)。如果您將 Evaluate Target Health (評估目標運作狀態) 設為 No (否)，則即使別名記錄所參考記錄的運作狀態檢查失敗，Route 53 仍會持續將流量路由到這些記錄。

在下列範例中，所有加權記錄都有相關聯的運作狀態檢查，但 us-east-1 區域中延遲別名記錄的 Evaluate Target Health (評估目標運作狀態) 設為 No (否)：



在這個組態中，當您將別名記錄的 Evaluate Target Health (評估目標運作狀態) 設為 No (否) 時，發生的情況如下：

1. Route 53 收到對 example.com 的查詢。根據使用者提出請求的延遲，Route 53 為 us-east-1 區域選擇延遲別名記錄。

2. Route 53 判斷延遲別名記錄的別名目標，並檢查對應運作狀態檢查。兩個檢查都失敗。
3. 由於 us-east-1 區域中延遲別名記錄的 Evaluate Target Health (評估目標運作狀態) 值是 No (否)，Route 53 必須在這個分支中選擇一個記錄，而不是退出分支並在 ap-southeast-2 區域中尋找正常運作的記錄。

當您已設定運作狀態檢查時，Amazon Route 53 會如何選擇記錄

如果您為記錄群組中具有相同名稱、相同類型 (例如 A 或 AAAA) 和相同路由政策 (例如加權或容錯移轉) 的所有記錄設定運作狀態檢查，Route 53 會選擇正常運作的記錄，並從該記錄傳回適用的值以回應 DNS 查詢。

例如，假設您建立三個加權 A 記錄，並指派運作狀態檢查給這三個記錄。如果其中一個記錄的運作狀態檢查為狀況不良，則 Route 53 會使用另外兩個記錄其中之一的 IP 地址來回應 DNS 查詢。

Route 53 以下列方式選擇正常的記錄：

1. Route 53 一開始會根據路由政策以及您為每個記錄指定的值來選擇記錄。例如，若是加權記錄，Route 53 會根據您為每個記錄指定的權重來選擇記錄。
2. Route 53 可判斷記錄是否正常運作：
   - 非別名記錄與相關聯的運作狀態檢查 – 如果您將運作狀態檢查與非別名記錄建立關聯，Route 53 會查看運作狀態檢查的目前狀態。

     Route 53 會定期檢查在運作狀態檢查中所指定端點的運作狀態；當 DNS 查詢到達時，它不會執行運作狀態檢查。

     您可以將運作狀態檢查與別名記錄建立關聯，但我們建議您僅將運作狀態檢查與非別名記錄建立關聯。如需更多詳細資訊，請參閱 將運作狀態檢查與別名記錄關聯時會發生什麼情況？。
   - Evaluate Target Health (評估目標運作狀態) 設為 Yes (是) 的別名記錄 – Route 53 會檢查別名記錄參考的資源運作狀態，例如 ELB 負載平衡器或在相同託管區域中的其他記錄。
3. 如果記錄為正常運作，Route 53 即會以適用的值 (例如 IP 地址) 來回應查詢。

   如果記錄狀況不良，Route 53 會使用相同的條件選擇其他記錄，並重複程序直到找到正常運作的記錄為止。

Route 53 會在選擇記錄時使用以下條件：

如果記錄不具備運作狀態檢查，則一律正常運作

在具有相同名稱和類型的記錄群組中，如果某個記錄不具備相關聯的運作狀態檢查，則 Route 53 一律會將它視為正常運作，且一律將它包含在可能的查詢回應中。

如果沒有正常運作的記錄，則所有記錄都正常運作

如果記錄群組中的所有記錄都是狀況不良，Route 53 需要傳回某個項目以回應 DNS 查詢，但沒有用來選擇記錄的基礎。在這種情況下，Route 53 會將所有記錄視為正常運作，並依據路由政策和您為每個記錄指定的值選取一個記錄。

權重為 0 的加權記錄

如果您在加權記錄群組中新增所有記錄的運作狀態檢查，但您為某些記錄設定非零權重，而為其他記錄設定零權重，則運作狀態檢查的運作方式與所有記錄都是非零權重相同，除了以下例外：

- Route 53 最初只考量非零加權記錄 (如果有)。
- 如果權重大於 0 的所有記錄都是狀況不良，Route 53 會考慮零加權記錄。

由於 Route 53 在某些情況下會考慮零加權記錄，因此請務必確定零加權目標也有 DNS 查詢的可行答案。

如需加權記錄的詳細資訊，請參閱 運作狀態檢查和加權路由。

別名記錄

您也可以將每個別名記錄的 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)，以設定別名記錄的運作狀態檢查。這可讓 Route 53 評估記錄要將流量路由所至的資源運作狀態，例如 ELB 負載平衡器或相同託管區域中的其他記錄。

例如，假設別名記錄的別名目標是一組全部具有非零權重的加權記錄：

- 只要至少有一個加權記錄正常運作，Route 53 就會認為別名記錄正常運作。
- 如果所有加權記錄都狀況不良，Route 53 就會認為別名記錄狀況不良。
- Route 53 會停止考慮該樹分支中的記錄，直到至少有一個加權記錄再次正常運作。

如需更多詳細資訊，請參閱 複雜 Amazon Route 53 組態中運作狀態檢查的運作方式。

容錯移轉記錄

一般來說，容錯移轉記錄的運作方式與其他路由類型相同。您建立運作狀態檢查，並將它們與非別名記錄建立關聯，然後將別名記錄的 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)。注意下列事項：

- 主要記錄和次要記錄可以兩種都是非別名記錄或別名記錄。

- 如果您將運作狀態檢查與主要和次要容錯移轉記錄關聯，Route 53 回應請求的方式如下：
  - 如果 Route 53 將主要記錄視為正常運作 (如果運作狀態檢查端點正常運作的話)， Route 53 只會傳回主要記錄，以回應 DNS 查詢。
  - 如果 Route 53 將主要記錄視為狀況不良，將次要記錄視為正常運作，則 Route 53 會傳回次要記錄。
  - 如果 Route 53 將主要和次要記錄都視為狀況不良，Route 53 會傳回主要記錄。
- 當您設定次要記錄，新增運作狀態檢查是選用的。如果您省略次要記錄的運作狀態檢查，而且如果主要記錄的運作狀態檢查端點是狀況不良，Route 53 永遠會使用次要記錄來回應 DNS 查詢。即使次要記錄的狀況不良，也是如此。

如需詳細資訊，請參閱下列主題：

- 使用一個主要資源和一個次要資源來設定主動-被動容錯移轉
- 使用多個主要資源和次要資源來設定主動-被動容錯移轉

主動-主動和主動-被動容錯移轉

您可以使用 Route 53 運作狀態檢查，設定主動-主動和主動-被動容錯移轉組態。除了容錯移轉以外，您可以使用任何路由政策 (或路由政策的組合) 來設定主動-主動容錯移轉，並使用容錯移轉路由政策來設定主動-被動容錯移轉。

主題

- 主動-主動容錯移轉
- 主動-被動容錯移轉

主動-主動容錯移轉

當您希望所有資源在大部分的時間都可用時，可使用此容錯移轉組態。當某個資源無法使用時，Route 53 可以偵測到它狀況不良，並在回應查詢停止包含該資源。

在主動-主動容錯移轉中，具有相同名稱、相同類型 (例如 A 或 AAAA) 和相同路由政策 (例如加權或延遲) 的所有記錄都是主動的，除非 Route 53 將它們視為狀況不良。Route 53 可以使用任何正常運作的記錄來回應 DNS 查詢。

主動-被動容錯移轉

當您希望主要資源群組或其他資源群組在大部分的時間都可用，並希望次要資源或其他資源群組處於待命狀態，以防所有主要資源變成無法使用時，可使用主動-被動容錯移轉組態。當回應查詢，Route 53

只包含正常的主要資源。如果所有主要資源都是狀況不良，Route 53 就會只包含正常運作的次要資源以回應 DNS 查詢。

主題

- 使用一個主要資源和一個次要資源來設定主動-被動容錯移轉
- 使用多個主要資源和次要資源來設定主動-被動容錯移轉
- 使用加權記錄來設定主動-被動容錯移轉

使用一個主要資源和一個次要資源來設定主動-被動容錯移轉

若要使用一個主要記錄和一個次要記錄來建立主動-被動容錯移轉組態，您只要建立記錄，並指定 Failover (容錯移轉) 的路由政策。當主要資源正常運作時，Route 53 會使用主要記錄來回應 DNS 查詢。當主要資源狀況不良時，Route 53 會使用次要記錄來回應 DNS 查詢。

使用多個主要資源和次要資源來設定主動-被動容錯移轉

您也可以將多個資源與主要記錄、次要記錄或兩者建立關聯。在此組態中，只要至少有一個相關聯的資源正常運作，Route 53 就會認為主要容錯移轉記錄正常運作。如需更多詳細資訊，請參閱 當您已設定運作狀態檢查時，Amazon Route 53 會如何選擇記錄。

若要使用主要記錄或次要記錄的多個資源來設定主動-被動容錯移轉，請執行以下任務。

1. 針對您想要路由流量的每個資源建立運作狀態檢查，例如 EC2 執行個體或您資料中心內的 Web 伺服器。

   > **Note**
   >
   > 如果您要將流量路由到任何可以建立別名記錄的 AWS 資源，請不要為這些資源建立運作狀態檢查。當您建立別名記錄時，您反而要將 Evaluate Target Health (評估目標運作狀態) 設為 Yes (是)。

   如需更多詳細資訊，請參閱 建立和更新運作狀態檢查。
2. 為您的主要資源建立記錄，並指定以下值：
   - 為每個記錄設定相同的名稱、類型和路由政策。例如，您可以建立三個名稱均為 failover-primary.example.com 的加權 A 記錄。
   - 如果您使用可以建立別名記錄的 AWS 資源，請將 Evaluate Target Health (評估目標運作狀態) 指定為 Yes (是)。

如果您使用無法建立別名記錄的資源，請將步驟 1 的適用運作狀態檢查與每個記錄建立關聯。

如需更多詳細資訊，請參閱 使用 Amazon Route 53 主控台來建立記錄。

3. 為您的次要資源建立記錄 (如適用)，並指定以下值：
   - 為每個記錄設定相同的名稱、類型和路由政策。例如，您可以建立三個名稱均為 failover-secondary.example.com 的加權 A 記錄。
   - 如果您使用可以建立別名記錄的 AWS 資源，請將 Evaluate Target Health (評估目標運作狀態) 指定為 Yes (是)。

     如果您使用無法建立別名記錄的資源，請將步驟 1 的適用運作狀態檢查與每個記錄建立關聯。

   > **Note**
   >
   > 有些客戶將 Web 伺服器做為主要資源，並將 Amazon S3 儲存貯體設為網站端點以做為他們的次要資源。S3 儲存貯體包含一個簡單的「暫時無法使用」訊息。如果您使用的是上述組態，則可以略過此步驟，而只建立步驟 4 次要資源的容錯移轉別名記錄。

4. 建立兩個容錯移轉別名記錄 (一個主要記錄和一個次要記錄)，並指定以下值：

   主要記錄
   - Name (名稱) – 指定您希望 Route 53 為其路由流量的網域名稱 (example.com) 或子網域名稱 (www.example.com)。
   - Alias (別名) – 指定 Yes (是)。
   - Alias Target (別名目標) – 指定您在步驟 2 建立的記錄名稱。
   - Routing Policy (路由政策) – 指定 Failover (容錯移轉)。
   - Failover Record Type (容錯移轉記錄類型) – 指定 Primary (主要)。
   - Evaluate Target Health (評估目標運作狀態) – 指定 Yes (是)。
   - Associate with Health Check (與運作狀態檢查建立關聯) – 指定 No (否)。

   次要記錄
   - Name (名稱) – 指定您為主要記錄指定的相同名稱。
   - Alias (別名) – 指定 Yes (是)。
   - Alias Target (別名目標) – 如果您已在步驟 3 為您的次要資源建立記錄，請指定該記錄的名稱。如果您為次要資源使用 Amazon S3 儲存貯體，請指定網站端點的 DNS 名稱。
   - Routing Policy (路由政策) – 指定 Failover (容錯移轉)。
   - Failover Record Type (容錯移轉記錄類型) – 指定 Secondary (次要)。

- Evaluate Target Health (評估目標運作狀態) – 指定 Yes (是)。
- Associate with Health Check (與運作狀態檢查建立關聯) – 指定 No (否)。

使用加權記錄來設定主動-被動容錯移轉

您也可以將加權記錄用於主動-被動容錯移轉，並搭配警告。如果您為某些記錄指定非零權重，並為其他記錄指定零權重，則 Route 53 僅會使用具有非零權重的正常運作記錄來回應 DNS 查詢。如果權重大於 0 的所有記錄都是狀況不良，Route 53 會使用零加權記錄來回應查詢。

> **Note**
>
> 所有非零權重的記錄都必須為狀況不良，Route 53 才會開始使用零權重的記錄來回應 DNS 查詢。當其他資源無法使用時，如果最後一個正常運作的資源 (例如 Web 伺服器) 無法處理所有流量，這可能會讓您的 Web 應用程式或網站不穩定。

在私有託管區域中設定容錯移轉

如果您要在私有託管區域中建立容錯移轉記錄，請注意以下事項：

- Route 53 運作狀態檢查程式位於 VPC 外部。若要依 IP 地址檢查 VPC 中端點的運作狀態，您必須將公有 IP 地址指派給 VPC 中的執行個體。
- 您可以建立 CloudWatch 指標，將警示與指標建立關聯，然後建立以警示資料串流為依據的運作狀態檢查。例如，您可以建立一個用來檢查 EC2 `StatusCheckFailed` 指標狀態的 CloudWatch 指標，將警示新增至指標，然後建立以警示資料串流為依據的運作狀態檢查，以檢查僅具有私有 IP 地址的 Virtual Private Cloud (VPC) 中的執行個體。如需使用 CloudWatch 主控台建立 CloudWatch 指標和警示的資訊，請參閱 Amazon CloudWatch 使用者指南。

如需詳細資訊，請參閱使用私有託管區域及使用 CloudWatch 監控運作狀態檢查。

Amazon Route 53 如何避免容錯移轉問題

Route 53 實作的容錯移轉演算法不僅可用來將流量路由到正常運作的端點，還能避免因運作狀態檢查設定錯誤以及應用程式、端點超載和分割區失敗而使災難案例惡化。

主題

- Amazon Route 53 如何避免級聯故障

- Amazon Route 53 如何處理網際網路分割區

Amazon Route 53 如何避免級聯故障

做為避免串聯失敗的第一道防線，每個請求路由演算法 (如加權和容錯移轉) 都有最後解決方法的模式。在這個特殊模式中，當所有記錄都被視為狀況不良時，Route 53 演算法會回復為將所有記錄都視為正常運作。

例如，如果應用程式的所有執行個體在多個主機上都拒絕運作狀態檢查請求，Route 53 DNS 伺服器無論如何都會選擇並傳回回答，而不是不傳回 DNS 回答或傳回 NXDOMAIN (不存在的網域) 回答。應用程式可以回應使用者，但仍無法通過運作狀態檢查，因此這針對設定錯誤提供一些防護。

同樣地，如果應用程式超載，且三個端點的其中一個未通過運作狀態檢查而從 Route 53 的 DNS 回答中排除，則 Route 53 會在其餘的兩個端點之間分配回答。如果其餘的端點無法處理額外負載並失敗，Route 53 會回復為向全部三個端點請求散發。

Amazon Route 53 如何處理網際網路分割區

雖然不常見，但偶爾會有大型的網際網路分割事件，導致大型地理區域之間無法透過網際網路通訊的情況。在這些分割區，Route 53 位置可能會就端點的運作狀態達成不同結論，並可能不同於回報給 CloudWatch 的狀態。在每個 AWS 區域中的 Route 53 運作狀態檢查程式會持續傳送運作狀態檢查狀態至所有 Route 53 位置。在網際網路分割區，每個 Route 53 位置可能只存取這些狀態的部分集合，通常是來自最接近的區域。

例如，在影響南美洲往來連線的網際網路分割期間，Route 53 南美洲 (聖保羅) 位置中的 Route 53 DNS 伺服器可以正常存取南美洲 (聖保羅) AWS 區域中的運作狀態檢查端點，但無法存取其他位置的端點。同時，美國東部 (俄亥俄) 區域中的 Route 53 可能無法存取南美洲 (聖保羅) 區域中的運作狀態檢查端點，並斷定對應的記錄為狀況不良。

這類分割區可能會導致下列情況：Route 53 位置根據端點的本機可見性，得出有關端點運作狀態的不同結論。因此，只有一部分可連線的運作狀態檢查程式將端點視為正常運作時，每個 Route 53 位置都會將其視為正常運作。

命名和標記運作狀態檢查

您可以將標籤新增到 Amazon Route 53 運作狀態檢查，以便為每個運作狀態檢查指定比運作狀態檢查 ID 更有意義的名稱。這些是用於組織 AWS 帳單的相同標籤。 AWS Billing and Cost Management 如需使用標籤進行成本分配的詳細資訊，請參閱 AWS Billing 使用者指南中的將成本分配標籤用於自訂帳單報告。

每個標籤都包含您定義的金鑰 (標籤名稱) 和值。當您將標籤新增到運作狀態檢查時，我們建議您新增一個標籤，並對其中的鍵和值使用以下值：

- 金鑰 – Name (名稱)
- 值 – 您要為運作狀態檢查設定的名稱

Name (名稱) 標籤的值會出現在 Route 53 主控台的運作狀態檢查清單，讓您輕鬆區分各個運作狀態檢查。若要查看運作狀態檢查的其他標籤，您可以選擇運作狀態檢查，然後選擇 Tags (標籤) 標籤。

如需標籤的詳細資訊，請參閱下列主題：

- 若要在 Route 53 主控台中新增或編輯運作狀態檢查時，新增、編輯或刪除 Name (名稱) 標籤，請參閱 建立、更新和刪除運作狀態檢查。
- 如需標記 Route 53 資源的概觀，請參閱 標記 Amazon Route 53 資源。

標籤限制

以下基本限制適用於標籤：

- 每一資源最多標籤數 – 50
- Key (索引鍵) 長度上限 - 128 個 Unicode 字元
- Value (值) 長度上限 - 256 個 Unicode 字元
- Key (金鑰) 和 Value (值) 的有效值 – UTF-8 字元集中的大小寫字母、數字、空格和以下字元：_ . : / = + - 和 @
- 標記金鑰與值皆區分大小寫
- 不要將前`aws:`綴用於鍵或值; 它保留供 AWS 使用

新增、編輯和刪除運作狀態檢查的標籤

以下程序說明如何在 Route 53 主控台中使用運作狀態檢查的標籤。

主題

- 將標籤新增到運作狀態檢查 (主控台)
- 編輯運作狀態檢查的標籤 (主控台)
- 刪除運作狀態檢查的標籤 (主控台)

將標籤新增到運作狀態檢查 (主控台)

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
3. 選取一個運作狀態檢查，或選取多個運作狀態檢查 (如果您想要將同一個標籤新增至多個運作狀態檢查)。
4. 在底部窗格中，選擇 Tags (標籤) 標籤，然後選擇 Add/Edit Tags (新增/編輯標籤)。
5. 在 Add/Edit Tags (新增/編輯標籤) 對話方塊中，在 Key (鍵) 欄位中輸入標籤的名稱，並在 Value (值) 欄位中輸入值。
6. 選擇 Apply changes (套用變更)。

編輯運作狀態檢查的標籤 (主控台)

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
3. 選取運作狀態檢查。

   如果您選取多個共用相同標籤的運作狀態檢查，無法同時編輯所有標籤的值。不過請注意，如果您選取多個擁有相同標籤的運作狀態檢查，但至少其中一個運作狀態檢查沒有此標籤，則可以編輯出現在這些運作狀態檢查中的標籤的值。

   例如，假設您選取多個含有 Cost Center (成本中心) 標籤的運作狀態檢查，但其中一個不含此標籤。您可以選擇新增標籤，並指定 Cost Center (成本中心) 為鍵，777 為值。針對已有 Cost Center (成本中心) 標籤的所選運作狀態檢查，Route 53 會將值變更為 777。對於沒有 Cost Center (成本中心) 標籤的這個運作狀態檢查，Route 53 會新增一個標籤，並將值設為 777。
4. 在底部窗格中，選擇 Tags (標籤) 標籤，然後選擇 Add/Edit Tags (新增/編輯標籤)。
5. 在 Add/Edit Tags (新增/編輯標籤) 對話方塊中，編輯值。
6. 選擇儲存。

刪除運作狀態檢查的標籤 (主控台)

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

2. 在導覽窗格中，選擇 Health Checks (運作狀態檢查)。
3. 選取一個運作狀態檢查，或選取多個運作狀態檢查 (如果您想要從多個運作狀態檢查刪除相同的標籤)。
4. 在底部窗格中，選擇 Tags (標籤) 標籤，然後選擇 Add/Edit Tags (新增/編輯標籤)。
5. 在 Add/Edit Tags (新增/編輯標籤) 對話方塊中，選擇要刪除的標籤旁的 *X*。
6. 選擇儲存。

運作狀態檢查與早於 2012-12-12 的 Amazon Route 53 API 版本搭配使用

從 Amazon Route 53 API 2012-12-12 版本開始支援運作狀態檢查。如果託管區域包含已設定運作狀態檢查的記錄，我們建議您只使用 2012-12-12 API 或更新版本。將運作狀態檢查與之前的 API 版本搭配使用時，請注意以下限制。

- `ChangeResourceRecordSets` 動作無法建立或刪除包括 `EvaluateTargetHealth`、`Failover` 或 `HealthCheckId` 元素的記錄。
- `ListResourceRecordSets` 動作可以列出包含這些元素的記錄，但這些元素不包含在輸出中。相反地，回應的 `Value` 元素會包含訊息，指出記錄包含不支援的屬性。

Route 53 Resolver DNS 防火牆

使用 Route 53 Resolver DNS 防火牆，您可以篩選和調節 Virtual Private Cloud (VPC) 的傳出 DNS 流量。為此，您可以在 DNS 防火牆規則群組中建立可重複使用的篩選規則集合、將規則群組與 VPC 產生關聯，然後監控 DNS 防火牆日誌和指標中的活動。根據活動，您可以相應地調整 DNS 防火牆的行為。

DNS 防火牆為來自 VPC 的傳出 DNS 要求提供保護。這些要求會透過 Resolver 路由以進行網域名稱解析。DNS 防火牆保護的主要用途是協助防止 DNS 洩漏您的資料。當不良執行者危害 VPC 中的應用程式執行個體，然後使用 DNS 查詢將資料從 VPC 傳送到其控制的網域時，就可能發生 DNS 洩漏。透過 DNS 防火牆，您可以監控和控制應用程式可查詢的網域。您可以拒絕存取您已知行為不良的網域，並允許所有其他查詢通過。或者，您可以拒絕對除明確信任網域之外的所有網域的存取。您也可以允許或拒絕 DNS 查詢類型。例如，您可能想要封鎖特定網域的所有查詢類型，但允許 MX 記錄。

您也可以使用 DNS 防火牆來封鎖對私人託管區域 (共用或本機) 中資源 (包括 VPC 端點名稱) 的解析要求。它也可以封鎖對公有或私有 Amazon EC2 執行個體名稱的要求。

DNS 防火牆是 Route 53 Resolver 的一項功能，不需要執行任何其他 Resolver 設定即可使用。

AWS Firewall Manager 支援 DNS 防火牆

您可以使用 Firewall Manager，集中設定和管理 AWS Organizations 中各個賬戶的 VPC 的 DNS 防火牆規則群組關聯。Firewall Manager 會自動為歸屬於 Firewall Manager DNS 防火牆政策範圍的 VPC 新增關聯。如需詳細資訊，請參閱AWS WAF AWS Firewall Manager、和 AWS Shield Advanced 開發人員指南AWS Firewall Manager中的。

DNS 防火牆如何搭配使用 AWS Network Firewall

DNS 防火牆和 Network Firewall 都提供網域名稱篩選功能，但是針對不同類型的流量。透過 DNS 防火牆和 Network Firewall，您可以針對兩個不同的網路路徑上的應用程式層流量設定網域型篩選。

- DNS 防火牆針對從 VPC 內的應用程式透過 Route 53 Resolver 傳遞的傳出 DNS 查詢提供篩選功能。您也可以設定 DNS 防火牆，將查詢的自訂回應傳送至封鎖的網域名稱。
- Network Firewall 同時提供網路和應用程式層流量的篩選功能，但是沒有 Route 53 Resolver 所實現的查詢可見性。

如需詳細資訊，請參閱 Network Firewall 開發人員指南。

Route 53 Resolver DNS 防火牆的運作方式

Route 53 Resolver DNS 防火牆可讓您控制網站的存取，並針對透過 Route 53 Resolver 從 VPC 傳出的 DNS 查詢，封鎖 DNS 層級的威脅。使用 DNS 防火牆，您可以在與 VPC 關聯的規則群組中定義網域名稱篩選規則。您可以指定要允許或封鎖的網域名稱清單，也可以自訂要封鎖的 DNS 查詢的回應。您也可以透過微調網域清單，以允許某些查詢類型 (例如 MX-Records)。

DNS 防火牆只會篩選網域名稱。它不會將該名稱解析為要封鎖的 IP 地址。此外，DNS 防火牆會篩選 DNS 流量，但不會篩選其他應用程式層通訊協定，例如 HTTPS、SSH、TLS、FTP 等。

Route 53 Resolver DNS 防火牆的元件和設定

您可以使用下列中央元件和設定來管理 DNS 防火牆。

DNS 防火牆規則群組

定義具名、可重複使用的 DNS 防火牆規則集合，用於篩選 DNS 查詢。您可以使用篩選規則填入規則群組，然後將規則群組與一或多個 VPC 建立關聯。當您將規則群組與 VPC 建立關聯時，即啟用 VPC 的 DNS Firewall 篩選。然後，當 Resolver 收到具有與其相關聯的規則群組的 VPC 的 DNS 查詢時，Resolver 會將查詢傳遞至 DNS Firewall 進行篩選。

如果您將多個規則群組與單一 VPC 相關聯，則可以透過每個關聯中的優先順序設定來指出它們的處理順序。DNS 防火牆從最低數值優先順序設定開始處理 VPC 的規則群組。

如需詳細資訊，請參閱 DNS 防火牆規則群組與規則。

DNS 防火牆規則

為 DNS 防火牆規則群組中的 DNS 查詢定義篩選規則。每個規則都會指定一個網域清單，以及要對其網域符合清單中網域規格的 DNS 查詢採取的動作。您可以針對清單中的網域允許、封鎖或警示相符的查詢或查詢類型，例如，您可以封鎖或允許特定網域的 MX 查詢類型。您也可以為封鎖的查詢定義自訂回應。

規則群組中的每個規則都有該群組內唯一的優先順序設定。DNS 防火牆從最低數值優先順序開始處理規則群組中的規則。

DNS 防火牆規則只存在於定義這些規則群組的內容中。您無法重複使用規則，也無法獨立於規則群組參考規則。

如需詳細資訊，請參閱 DNS 防火牆規則群組與規則。

網域清單

定義用於 DNS 篩選的具名、可重複使用的網域規格集合。規則群組中的每個規則都需要單一網域清單。您可以選擇指定要允許存取的網域、要拒絕存取的網域或兩者的組合。您可以建立自己的網域清單，也可以使用為您 AWS 管理的網域清單。

如需詳細資訊，請參閱 Route 53 Resolver DNS 防火牆網域清單。

DNS 防火牆規則群組與 VPC 之間的關聯

使用 DNS 防火牆規則群組定義對 VPC 的保護，並啟用 VPC 的 Resolver DNS 防火牆設定。

如果您將多個規則群組與單一 VPC 相關聯，則可以透過關聯中的優先順序設定來指出它們的處理順序。DNS 防火牆從最低數值優先順序設定開始處理 VPC 的規則群組。

如需詳細資訊，請參閱 為 VPC 啟用 Route 53 Resolver DNS 防火牆保護。

VPC 的 Resolver DNS 防火牆設定

Resolver 解析程式在 VPC 層級處理 DNS 防火牆保護的方式。每當您至少有一個與 VPC 相關聯的 DNS 防火牆規則群組時，此設定就會生效。

此設定會指定當 DNS 防火牆無法篩選查詢時，Route 53 Resolver 如何處理查詢。根據預設，如果 Resolver 未收到來自 DNS 防火牆的查詢回應，則其會失敗關閉並封鎖查詢。

如需詳細資訊，請參閱 DNS 防火牆 VPC 組態。

監控 DNS 防火牆動作

您可以使 CloudWatch 用 Amazon 監控由 DNS 防火牆規則群組篩選的 DNS 查詢數目。CloudWatch 收集原始數據並將其處理為可讀的近乎實時的指標。

如需詳細資訊，請參閱 使用 Amazon 監控 Route 53 解析器 DNS 防火牆規則群組 CloudWatch。

您可以使用 Amazon EventBridge，這是一種使用事件將應用程式元件連接在一起的無伺服器服務，以建置可擴展的事件驅動應用程式。

如需詳細資訊，請參閱 使用管理 Route 53 解析程式 DNS 防火牆事件 Amazon EventBridge。

Route 53 Resolver DNS 防火牆如何篩選 DNS 查詢

當 DNS 防火牆規則群組與 VPC 的 Route 53 Resolver 相關聯時，防火牆會篩選下列流量：

- 源自該 VPC 的 DNS 查詢。
- 將 Resolver 端點從內部部署資源傳遞至具有與其解析程式相關聯的 DNS 防火牆相同 VPC 的 DNS 查詢。

當 DNS 防火牆收到 DNS 查詢時，它會使用您已設定的規則群組、規則和其他設定來篩選查詢，並將結果傳回 Resolver：

- DNS 防火牆會使用與 VPC 相關聯的規則群組來評估 DNS 查詢，直到找到相符項目或篩選所有規則群組為止。DNS 防火牆會根據您在關聯中設定的優先順序評估規則群組，從最低的數值設定開始。如需更多詳細資訊，請參閱 DNS 防火牆規則群組與規則 和 為 VPC 啟用 Route 53 Resolver DNS 防火牆保護。
- 在每個規則群組中，DNS 防火牆會根據每個規則的網域清單評估 DNS 查詢，直到找到符合項目或篩選所有規則為止。DNS 防火牆從最低數值設定開始，依照優先順序評估規則。如需詳細資訊，請參閱 DNS 防火牆規則群組與規則。
- 當 DNS 防火牆找到與規則的網域清單相符的項目時，它會終止查詢評估，並以結果回應 Resolver。如果相關動作是 `alert`，則 DNS 防火牆也會傳送警示至設定的 Resolver 日誌。如需更多詳細資訊，請參閱 DNS 防火牆中的規則動作 及 Route 53 Resolver DNS 防火牆網域清單。
- 如果 DNS 防火牆在未找到相符項目的情況下評估所有規則群組，它會正常回應該查詢。

Resolver 會根據來自 DNS 防火牆的回應路由查詢。在 DNS 防火牆無法回應的少見情況下，Resolver 會套用 VPC 設定的 DNS 防火牆失敗模式。如需詳細資訊，請參閱 DNS 防火牆 VPC 組態。

使用 Route 53 Resolver DNS 防火牆的高階步驟

若要在 Amazon Virtual Private Cloud VPC 中實作 Route 53 Resolver DNS 防火牆篩選，請執行以下高階步驟。

- 定義您的篩選方法和網域清單 - 決定篩選查詢的方式、識別您需要的網域規格，以及定義用來評估查詢的邏輯。例如，您可能想要允許除在已知惡意網域清單中的查詢外的所有查詢。或者，您可能想要執行相反操作，並封鎖除核准網域清單之外的所有查詢，這就是所謂的圍牆花園方法。您可以建立和管理自己的核可或封鎖的網域規格清單，也可以使用為您 AWS 管理的網域清單。如需網域清單的相關資訊，請參閱。Route 53 Resolver DNS 防火牆網域清單
- 建立防火牆規則群組 - 在 DNS 防火牆中，建立規則群組以篩選 VPC 的 DNS 查詢。您必須在想要使用規則群組的每個區域中建立規則群組。您也可能想要將篩選行為分成多個規則群組，以便在不同 VPC 的多個篩選案例中重複使用。如需規則群組的詳細資訊，請參閱 DNS 防火牆規則群組與規則。

- 新增和設定您的規則 - 針對您希望規則群組提供的每個網域清單和篩選行為，將規則新增至規則群組。設定規則的優先順序設定，以便它們在規則群組中以正確的順序得到處理，同時為您要先評估的規則提供最低的優先順序。如需規則的詳細資訊，請參閱 DNS 防火牆規則群組與規則。
- 將規則群組與 VPC 產生關聯 - 若要開始使用 DNS 防火牆規則群組，請將其與 VPC 產生關聯。如果您針對 VPC 使用多個規則群組，請設定每個關聯的優先順序，以便以正確的順序處理規則群組，同時為您要先評估的規則群組提供最低的優先順序。如需詳細資訊，請參閱 管理 VPC 與 Route 53 Resolver DNS 防火牆規則群組之間的關聯。
- (選用) 變更 VPC 的防火牆組態 - 如果您想要 Route 53 Resolver 在 DNS 防火牆無法傳回回應時封鎖查詢，請在 Resolver 中變更 VPC 的 DNS 防火牆設定。如需詳細資訊，請參閱 DNS 防火牆 VPC 組態。

在多個區域中使用 Route 53 Resolver DNS 防火牆規則群組

Route 53 解析器 DNS 防火牆是一種區域服務，因此您在一個 AWS 區域中創建的對象僅在該區域可用。若要在多個區域中使用相同的規則群組，您必須在每個區域中建立該規則。

建立規則群組的 AWS 帳戶可以與其他 AWS 帳戶共用。如需詳細資訊，請參閱 在帳戶之間共用 Route 53 解析程式 DNS 防火牆規則群組 AWS。

開始使用 Route 53 Resolver DNS 防火牆

包含精靈的 DNS 防火牆主控台會引導您完成以下步驟，開始使用 DNS 防火牆：

- 為您要使用的每一組規則建立規則群組。
- 針對每個規則，填入您要檢查的網域清單。您可以建立自己的網域清單，也可以使用 AWS 受管理的網域清單。
- 將規則群組與您要使用它們的 VPC 建立關聯。

Route 53 Resolver DNS 防火牆圍牆花園範例

在本教學課程中，您將建立一個規則群組，以封鎖所信任的選取網域群組以外的所有網域。這稱為封閉的平台或圍牆花園方法。

若要使用主控台精靈設定 DNS 防火牆規則群組

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

在導覽窗格中選擇 DNS 防火牆，以在 Amazon VPC 主控台上開啟 DNS 防火牆規則群組頁面。繼續步驟 3。

- 或 -

登入 AWS Management Console 並開啟

位於 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 主控台。

2. 在導覽窗格中的 DNS 防火牆下方，選擇規則群組。
3. 在導覽列中，選擇規則群組的區域。
4. 在 Rule groups (規則群組) 頁面中，選擇 Add rule group (新增規則群組)。
5. 針對規則群組名稱，輸入 **WalledGardenExample**。如果您需要其他描述，請也輸入該描述。
6. 選擇下一步。
7. 在 Add rules (新增規則) 頁面，選擇 Add rule (新增規則)。
   a. 在 Rule details (規則詳細資訊) 窗格中，輸入規則名稱 **BlockAll**。
   b. 在 Domain list (網域清單) 窗格中，選取 Add my own domain list (新增我自己的網域清單)。
   c. 在 Choose or create a new domain list (選擇或建立新網域清單) 下，選擇Create new domain list (建立新網域清單)。
   d. 輸入網域清單名稱 **AllDomains**，然後在文字方塊中輸入星號：*****。
   e. 對於動作，請選取 BLOCK (封鎖)，然後保留回應以 NODATA 的預設設定傳送。
   f. 選擇 Add rule (新增規則)。精靈會顯示規則群組的 [新增規則] 頁面，並列出您的規BlockAll則。
8. 再次選擇 Add rule (新增規則)，將第二個規則新增至規則群組。
   a. 在 Rule details (規則詳細資訊) 窗格中，輸入規則名稱 **AllowSelectDomains**，並將說明留空。
   b. 在 Domain list (網域清單) 窗格中，選取 Add my own domain list (新增我自己的網域清單)。
   c. 在 Choose or create a new domain list (選擇或建立新網域清單) 下，選取 Create new domain list (建立新網域清單)。
   d. 輸入網域清單名稱 **ExampleDomains**。
   e. 在文字方塊中，於第一行輸入 **example.com**，然後於第二行輸入 **example.org**。

> **Note**
>
> 如果您想要將規則套用至子網域，則也必須將這些網域新增至清單。例如，若要新增所有 example.com 的子網域，請將 **`*.example.com`** 新增至清單。

f. 對於動作，請選取 ALLOW (允許)。

g. 選擇 Add rule (新增規則)。精靈會顯示 Add rules (新增規則) 頁面，並列出您的兩個規則。

9. 選擇下一步。

10. 在 Set rule priority (設定規則優先順序) 頁面上，您可以調整規則群組中規則的評估順序。DNS 防火牆會評估以最低優先順序設定開始的規則，因此清單頂端的規則是第一個評估的規則。在此範例中，我們希望 DNS 防火牆先識別並允許選取的網域清單的 DNS 查詢，然後封鎖任何剩餘的查詢。

    選取並調整規則順序，AllowSelectDomains以便最先列出。

11. 選擇下一步。

12. 在 Add tags (新增標籤) 頁面中，選擇 Next (下一步)。標籤可協助您組織和管理 AWS 資源。如需詳細資訊，請參閱 標記 Amazon Route 53 資源。

13. 在 Review and create (檢閱和建立) 頁面中，確認您在前幾頁指定的設定值是正確的。如有必要，請針對適用的部分選擇 Edit (編輯)，並且更新設定。當您滿意設定時，請選擇 Create rule group (建立規則群組)。精靈會引導您返回 Rule groups (規則群組) 頁面，其中列出您的新規則群組。

您現在有一個規則群組，只允許特定的網域查詢通過。若要開始使用該規則群組，請將它與您要使用篩選行為的 VPC 產生關聯。如需詳細資訊，請參閱 管理 VPC 與 Route 53 Resolver DNS 防火牆規則群組之間的關聯。

Route 53 Resolver DNS 防火牆封鎖清單範例

在本教學課程中，您將建立封鎖已知為惡意網域的規則群組。您也會新增允許封鎖清單中網域使用的 DNS 查詢類型。規則群組允許所有其他傳送 DNS 要求通過 Route 53 Resolver。

使用主控台精靈設定 DNS 防火牆封鎖清單

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

在導覽窗格中選擇 DNS 防火牆，以在 Amazon VPC 主控台上開啟 DNS 防火牆規則群組頁面。繼續步驟 3。

- 或 -

登入 AWS Management Console 並開啟 Amazon VPC 主控台，網址為 https://console.aws.amazon.com/vpc/。

2. 在導覽窗格中的 DNS 防火牆下方，選擇規則群組。
3. 在導覽列中，選擇規則群組的區域。
4. 在 Rule groups (規則群組) 頁面中，選擇 Add rule group (新增規則群組)。
5. 針對規則群組名稱，輸入 **`BlockListExample`**。如果您需要其他描述，請也輸入該描述。
6. 選擇下一步。
7. 在 Add rules (新增規則) 頁面，選擇 Add rule (新增規則)。
   a. 在 Rule details (規則詳細資訊) 窗格中，輸入規則名稱 **`BlockList`**。
   b. 在 Domain list (網域清單) 窗格中，選取 Add my own domain list (新增我自己的網域清單)。
   c. 在 Choose or create a new domain list (選擇或建立新網域清單) 下，選取Create new domain list (建立新網域清單)。
   d. 輸入網域清單名稱 **`MaliciousDomains`**，然後在文字方塊中輸入您要封鎖的網域。例如：**`example.org`**。每行輸入一個網域。

      > **Note**
      > 如果您想要將規則套用至子網域，則也必須將這些網域新增至清單。例如，若要新增所有範例 .org 的子網域，請將 **`*.example.org`** 新增至清單。

   e. 對於動作，請選取 BLOCK (封鎖)，然後保留回應以 NODATA 的預設設定傳送。
   f. 選擇 Add rule (新增規則)。精靈會顯示規則群組的 [新增規則] 頁面，並列出您的規BlockList則。
8. 選擇下一步。
9. 在 Set rule priority (設定規則優先順序) 頁面上，您可以調整規則群組中規則的評估順序。DNS 防火牆會評估以最低優先順序設定開始的規則，因此清單頂端的規則是第一個評估的規則。

選取並調整規則順序，以便BlockList在您可能擁有的任何其他規則之前或之後進行評估。大多數情況下，應該先封鎖已知的惡意網域。也就是說，與這些網域相關的規則應具有最低的優先順序編號。

10. 在「新增標籤」頁面中，您可以選擇性地新增標籤，以便用於搜尋和篩選資 AWS 源。
11. 選擇 Next Step (下一步)，然後選擇 Create rule group (建立規則群組)。
12. 若要新增允許 BlockList 網域 MX 重複伺服器的規則，請在 [規則群組] 頁面上選擇連結**`BlockList`**，然後在 [規則] 索引標籤上選擇 [新增規則]。

    a. 在 Rule details (規則詳細資訊) 窗格中，輸入規則名稱 **`BlockList-allowMX`**。

    b. 在 Domain list (網域清單) 窗格中，選取 Add my own domain list (新增我自己的網域清單)。

    c. 在 [選擇或建立新網域清單] 下，選取BlockList。

    d. 在 [DNS 查詢類型] 清單中，選取 [MX: 指定郵件伺服器]。

    e. 針對動作，選取 [允許]。

    f. 選擇 Add rule (新增規則)。精靈會顯示規則群組的 [新增規則] 頁面，並列出您的 BlockList-AllowMX 規則。
13. 選擇下一步。
14. 在 Set rule priority (設定規則優先順序) 頁面上，您可以調整規則群組中規則的評估順序。DNS 防火牆會評估以最低優先順序設定開始的規則，因此清單頂端的規則是第一個評估的規則。

    選取並調整規則順序，以便在您可能擁有的任何其他規則之前或之後評估 BlockList-AllowMX。因為您想要允許 MX 查詢，請確定 BlockList-AllowMX 規則的優先順序低於. BlockList

您現在擁有一個規則群組，可封鎖特定的惡意網域查詢，但允許特定的 DNS 查詢類型。若要開始使用該規則群組，請將它與您要使用篩選行為的 VPC 產生關聯。如需詳細資訊，請參閱 管理 VPC 與 Route 53 Resolver DNS 防火牆規則群組之間的關聯。

DNS 防火牆規則群組與規則

本節說明您可以為 DNS 防火牆規則群組和規則進行的設定，以定義 VPC 的 DNS 防火牆行為。它也說明如何管理規則群組和規則的設定。

以所需的方式設定規則群組之後，您可以直接使用這些規則群組，而且可以在 AWS Organizations 中於帳戶之間和組織間共用和管理這些群組。

- 您可以將規則群組與多個 VPC 產生關聯，以便在整個組織中提供一致的行為。如需相關資訊，請參閱 管理 VPC 與 Route 53 Resolver DNS 防火牆規則群組之間的關聯。
- 您可以在帳戶之間共用規則群組，以便在整個組織中進行一致的 DNS 查詢管理。如需相關資訊，請參閱 在帳戶之間共用 Route 53 解析程式 DNS 防火牆規則群組 AWS。
- 您可以在 AWS Firewall Manager 政策中管理規則群組，以便在中使 AWS Organizations 用組織中的規則群組。如需有關「Firewall Manager 員」的資訊，請參閱AWS WAF AWS Firewall Manager、和 AWS Shield Advanced 開發人員指南AWS Firewall Manager中的。

DNS 防火牆中的規則群組設定

當您建立或編輯 DNS 防火墻規則群組時，請指定下列值：

名稱

獨特的名稱可讓您在儀表板中輕鬆找出規則群組。

(選用) 說明

為規則群組提供更多內容的簡短說明。

區域

您在建立規則群組時選擇的「 AWS 區域」。您在某個區域中建立的規則群組只能在該區域中使用。若要在多個區域中使用相同的規則群組，您必須在每個區域中建立該規則。

規則

規則群組篩選行為包含在其規則中。有關資訊，請參閱下一節。

標籤

指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

這些是用於組織 AWS 帳單的標籤。 AWS Billing and Cost Management 如需有關使用成本分配標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

DNS 防火牆中的規則設定

當您建立或編輯 DNS 防火墻規則群組中的規則時，請指定下列值：

名稱

規則群組中規則的唯一識別符。

(選用) 說明

提供規則詳細資訊的簡短說明。

網域清單

規則檢查的網域清單。您可以建立和管理自己的網域清單，也可以訂閱 AWS 會為您管理的網域清單。如需詳細資訊，請參閱 Route 53 Resolver DNS 防火牆網域清單。

查詢類型

規則檢查的 DNS 查詢類型清單。以下是有效值：

- 答：傳回 IPv4 位址。
- AAAA：返回一個 IPV6 地址。
- CAA：限制可為網域建立 SSL/TLS 認證的 CA。
- CNAME：返回另一個域名。
- DS：識別委派區域之 DNSSEC 簽署金鑰的記錄。
- MX：指定郵件伺服器。
- NAPR: 對域名進行egular-expression-based 重寫。
- NS：授權名稱伺服器。
- PTR：將 IP 位址對應至網域名稱。
- SOA：區域的權限記錄開始。
- SPF：列出授權從網域傳送電子郵件的伺服器。
- SRV：識別伺服器的應用程式特定值。
- TXT：驗證電子郵件發件人和應用程序特定的值。
- 您使用 DNS 類型識別碼定義的查詢類型，例如 AAAA 為 28。這些值必須定義為「類型##」，其中「##」可以是 1-65334，例如 TYPE28。如需詳細資訊，請參閱 DNS 記錄類型清單。

  您可以為每個規則建立一個查詢類型。

動作

您希望 DNS 防火牆處理其網域名稱符合規則網域清單中規格的 DNS 查詢的方式。如需詳細資訊，請參閱「DNS 防火牆中的規則動作」。

優先順序

在規則群組中決定處理順序的唯一正整數規則設定。DNS 防火墙會根據規則群組中的規則檢查 DNS 查詢，從最低數值優先順序設定開始處理。您可以隨時變更規則的優先順序，例如變更處理順序或為其他規則騰出空間。

DNS 防火牆中的規則動作

當 DNS 防火牆在規則中找到 DNS 查詢和網域規格之間的相符項目時，它會將規則中指定的動作套用至查詢。

您需要在建立的每個規則中指定下列其中一個選項：

- Allow - 停止檢查查詢並允許它通過。
- Alert - 停止檢查查詢，允許它通過，並在 Route 53 Resolver 日誌中記錄查詢的提醒。
- Block - 停止檢查查詢、封鎖查詢前往其預定目的地，並在 Route 53 Resolver 日誌中記錄查詢的封鎖動作。

  以如下內容回覆設定的封鎖回應：

  - NODATA – 回應表示查詢成功，但沒有可用的回應。
  - NXDOMAIN – 回應表示查詢的網域名稱不存在。
  - OVERRIDE –在回應中提供自訂覆寫。此選項需要下列附加設定：
    - Record value - 要傳回以回應查詢的自訂 DNS 記錄。
    - Record type - DNS 記錄的類型。這會決定記錄值的格式。這必須是 CNAME。
    - Time to live in seconds - DNS 解析程序或 Web 瀏覽器快取覆寫記錄並使用它來回應此查詢 (如果再次收到) 的建議時間。預設情況下，時間為零，而且不會快取記錄。

如需查詢日誌組態和內容的詳細資訊，請參閱 解析程式查詢日誌記錄 和 出現在 Resolver 查詢日誌中的值。

使用 Alert 來測試封鎖規則

當您第一次建立封鎖規則時，可以對其進行測試，方法是以設為 Alert 的動作設定該罪責。然後，您可以查看開啟規則提醒的查詢數目，以瞭解在將動作設定為 Block 時會封鎖的查詢數。

管理 DNS 防火牆中的規則群組和規則

若要在主控台中管理規則群組和規則，請遵循本主題中的指引。

當您變更 DNS 防火牆實體 (例如規則和網域清單) 時，DNS 防火牆會將變更傳播到儲存和使用該實體的所有位置。您的變更會在幾秒鐘內套用，但是當變更已經到達某些位置而不是在其他位置時，可能會有短暫的不一致的時間。因此，舉例而言，如果您將網域新增至封鎖規則所參考的網域清單中，新網域可能會在 VPC 的某個區域中短暫封鎖，而在另一個區域中仍然得到允許。當您第一次設定規則群組和 VPC 關聯，以及變更現有設定時，可能會發生此暫時不一致的情況。一般來說，這種類型的任何不一致只會持續幾秒鐘。

建立規則群組和規則

若要建立規則群組及其規則

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

   在導覽窗格中選擇 DNS 防火牆，以在 Amazon VPC 主控台上開啟 DNS 防火牆規則群組頁面。繼續步驟 3。

   - 或 -

   登入 AWS Management Console 並開啟

   位於 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 主控台。
2. 在導覽窗格中的 DNS 防火牆下方，選擇規則群組。
3. 在導覽列中，選擇規則群組的區域。
4. 選擇 Add rule group (新增規則群組)，然後依照精靈指引來指定規則群組和規則設定。

   如需有關規則群組值的資訊，請參閱 DNS 防火牆中的規則群組設定。

   如需有關規則值的資訊，請參閱 DNS 防火牆中的規則設定。

檢視并更新規則群組和規則

若要檢視和更新規則群組

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

在導覽窗格中選擇 DNS 防火牆，以在 Amazon VPC 主控台上開啟 DNS 防火牆規則群組頁面。繼續步驟 3。

- 或 -

登入 AWS Management Console 並開啟

位於 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 主控台。

2. 在導覽窗格中的 DNS 防火牆下方，選擇規則群組。
3. 在導覽列中，選擇該規則群組的區域。
4. 選取您要檢視或編輯的規則群組，然後選擇 View details (檢視詳細資訊)。
5. 在規則群組的頁面中，您可以檢視和編輯設定。

   如需有關規則群組值的資訊，請參閱 DNS 防火牆中的規則群組設定。

   如需有關規則值的資訊，請參閱 DNS 防火牆中的規則設定。

刪除規則群組

若要刪除規則群組，請執行以下程序。

> **Important**
>
> 如果您刪除與 VPC 相關聯的規則群組，DNS 防火牆會移除關聯，並停止規則群組提供給 VPC 的保護。

刪除 DNS 防火牆實體

當您刪除可在 DNS 防火牆中使用的實體 (例如規則群組中可能正在使用的網域清單) 或可能與 VPC 關聯的規則群組時，DNS 防火牆會檢查該實體目前是否正在使用中。如果發現該實體正在使用中，DNS 防火牆會警告您。DNS 防火墻幾乎總是能夠判斷實體是否正在使用中。但是在極少數的情況下，它也可能無法判斷。如果您需要確定目前沒有任何物件正在使用該實體，請在 DNS 防火墻組態中檢查它，然後予以刪除。如果實體是參考的網域清單，請檢查沒有規則群組正在使用它。如果實體是規則群組，請檢查該實體是否與任何 VPC 相關聯。

刪除規則群組

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

   在導覽窗格中選擇 DNS 防火牆，以在 Amazon VPC 主控台上開啟 DNS 防火牆規則群組頁面。繼續步驟 3。

   - 或 -

   登入 AWS Management Console 並開啟

   位於 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 主控台。
2. 在導覽窗格中的 DNS 防火牆下方，選擇規則群組。
3. 在導覽列中，選擇規則群組的區域。
4. 選取您要刪除的規則群組，然後選擇 Delete (刪除) 並確認刪除。

Route 53 Resolver DNS 防火牆網域清單

網域清單是一組可重複使用的網域規格，可在規則群組的 DNS Firewall 規則中使用。當您將規則群組與 VPC 建立關聯時，DNS 防火牆會比較您的 DNS 查詢與規則中使用的網域清單。如果找到相符項目，它會根據比對規則的動作處理 DNS 查詢。如需有關規則群組和規則的更多資訊，請參閱 DNS 防火牆規則群組與規則。

網域清單可讓您將明確的網域規格與想要對其採取的動作分開。您可以在多個規則中使用單一網域清單，而您對網域清單執行的任何更新都會自動影響使用該清單的所有規則。

網域清單可分為兩個主要類別：

- 受管理的網域清單，可為您 AWS 建立和維護。
- 您自己建立和維護的網域清單。

本節說明可供您使用的受管網域清單類型，並提供建立和管理自己的網域清單的指引 (如果您選擇這樣做)。

受管網域清單

受管理的網域清單包含與惡意活動或其他潛在安全威脅相關聯的網域名稱。 AWS 維護這些列表，以使 Route 53 解析器客戶在使用 DNS 防火牆時可以免費檢查對他們的出站 DNS 查詢。

為了保持在最新狀態以了解不斷變化的威脅趨勢，不僅費時而且耗錢。受管理的網域清單可以在您實作和使用 DNS 防火牆時節省您的時間。 AWS 當出現新的漏洞和威脅時，會自動更新列表。 AWS 通常會在公開揭露前通知有新的弱點，因此 DNS Firewall 甚至可以在新威脅被廣為人知之前為您部署緩和措施。

受管網域清單是用來協助您防範常見的 Web 威脅，並為您的應用程式增加另一層安全性。受 AWS 管理的網域清單會從內部 AWS 來源及來源取得資料 RecordedFuture，並持續更新。不過， AWS 受管理的網域清單並不是用來取代其他安全控制項，例如 Amazon GuardDuty，這些控制項是由您選取的 AWS 資源決定的。

最佳實務是在生產環境中使用受管網域清單之前，先在非生產環境中進行測試，並將規則動作設定為 `Alert`。使用 Amazon CloudWatch 指標結合 Route 53 解析器 DNS 防火牆取樣請求或 DNS 防火牆日誌來評估規則。當您對規則執行所需的動作感到滿意時，請視需要變更動作設定。

可用 AWS 受管理網域清單

本節說明目前可用的 受管網域清單。您在位於支援這些清單的區域時，如果您管理網域清單以及指定規則的網域清單，就會在主控台上看到這些清單。在日誌中，網域清單會記錄在 `firewall_domain_list_id field` 內。

AWS 為 Route 53 解析器 DNS 防火牆的所有使用者提供下列受管理的網域清單 (在可用的區域中)。

- `AWSManagedDomainsMalwareDomainList` –– 與傳送惡意軟體、託管惡意軟體或散佈惡意軟體相關聯的網域。
- `AWSManagedDomainsBotnetCommandandControl` - 與控制受到垃圾郵件惡意程式碼感染的電腦網路相關聯的網域。
- `AWSManagedDomainsAggregateThreatList`：與多種 DNS 威脅類別相關聯的網域，包括惡意軟體、勒索軟體、殭屍網路、間諜軟體和 DNS 通道，有助於封鎖多種類型的威脅。`AWSManagedDomainsAggregateThreatList` 包括 `AWSManagedDomainsAmazonGuardDutyThreatList`。
- `AWSManagedDomainsAmazonGuardDutyThreatList`— 與 Amazon GuardDuty DNS 安全發現相關聯的域. 這些網域僅來自威脅 GuardDuty情報系統，不包含來自外部第三方來源的網域。如需尋找項目中與網域相關之來源的詳細資訊，請參閱 GuardDuty API 參考資料ThreatIntelligenceDetail中的。只有搜尋結果中包`ThreatIntelligenceDetail`含「Amazon」的網域才會包含在受 AWS 管網域清單中。

  如需第三方合作夥伴威脅情報的詳細資訊，請參閱 Amazon GuardDuty 合作夥伴。

AWS 受管理的網域清單無法下載或瀏覽。為了保護智慧財產權，您無法檢視或編輯 AWS 受管理的網域清單中的個別網域規格。此限制也有助於防止惡意使用者設計可專門規避發佈的清單的威脅。

測試受管網域清單

我們提供以下網域集來測試受管網域清單：

AWSManagedDomainsBotnetCommandandControl

- controldomain1.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsMalwareDomainList

- controldomain1.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsAggregateThreatList 和 AWSManagedDomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

如果這些網域未遭到封鎖，則會解析為 1.2.3.4。如果您在 VPC 中使用受管網域清單，查詢這些網域會傳回規則中封鎖動作設定為的回應 (例如 NODATA)。

如需受管網域清單的詳細資訊，請聯絡 AWS Support 中心。

下表列出 AWS 受管理網域清單的區域可用性。

受管網域清單的區域可用性

區域	受管網域清單是否可用？
亞太區域 (孟買)	是
亞太區域 (首爾)	是
亞太區域 (新加坡)	是

區域	受管網域清單是否可用？
亞太區域 (雪梨)	是
亞太區域 (東京)	是
亞太 (大阪) 區域	是
加拿大 (中部) 區域	是
歐洲 (法蘭克福) 區域	是
歐洲 (愛爾蘭) 區域	是
歐洲 (倫敦) 區域	是
歐洲 (米蘭)	是
歐洲 (巴黎) 區域	是
歐洲 (斯德哥爾摩)	是
南美洲 (聖保羅)	是
美國東部 (維吉尼亞北部)	是
美國東部 (俄亥俄)	是
美國西部 (加利佛尼亞北部)	是

區域	受管網域清單是否可用？
美國西部 (奧勒岡)	是
亞太區域 (雅加達)	是
非洲 (開普敦)	是
中國 (北京)	是
中國 (寧夏)	是
AWS GovCloud (US)	是
亞太區域 (香港)	是
Middle East (Bahrain)	是

其他安全考慮事項

AWS 受管理的網域清單旨在協助保護您免於遭受常見的網路安全威脅。根據文件使用時，這些清單會為您的應用程式增加另一層安全性。不過，受管網域清單並非要用來取代其他安全性控制措施，這是由您選取的 AWS 資源決定的。若要確保中的資源受到適當 AWS 的保護，請參閱「共同責任模型」中的指引。

減少誤判案例

如果您在規則中遇到使用 受管網域清單封鎖查詢的誤判案例，請執行下列步驟：

1. 在 Resolver 日誌中，識別造成誤判的規則群組和受管網域清單。為此，您可以尋找日下查詢的日誌：其封鎖 DNS 防火牆，但您想要允許通過。該日誌記錄會列出規則群組、規則動作和受管清單。如需有關日誌的資訊，請參閱 出現在 Resolver 查詢日誌中的值。
2. 在規則群組中建立明確允許封鎖的查詢通過的新規則。建立規則時，您可以只使用想要允許的網域規格來定義自己的網域清單。遵循 建立規則群組和規則 中涉及規則群組和規則管理的指引。

3. 在規則群組內排定新規則的優先順序，使其在使用受管清單的規則之前執行。為此，請將新規則指定為較低的數值優先順序設定。

當您更新規則群組時，新規則會明確允許封鎖規則執行前要允許的網域名稱。

管理您自己的網域清單

您可以建立自己的網域清單，以指定在受管網域清單提供項目中無法找到或您偏好自行處理的網域類別。

除了本節所述的程序之外，您還可以在主控台中建立或更新規則時，於 Route 53 Resolver DNS 防火牆規則管理的內容中建立網域清單。

您網域清單中的每個網域規格都必須符合以下要求：

- 它可以選擇性地以 * (星號) 開頭。
- 除了選用的起始星號和句號之外，作為標籤之間的分隔符號，它只能包含下列字元：A-Z、a-z、0-9、- (連字號)。
- 長度必須為 1-255 個字元。

當您變更 DNS 防火牆實體 (例如規則和網域清單) 時，DNS 防火牆會將變更傳播到儲存和使用該實體的所有位置。您的變更會在幾秒鐘內套用，但是當變更已經到達某些位置而不是在其他位置時，可能會有短暫的不一致的時間。因此，舉例而言，如果您將網域新增至封鎖規則所參考的網域清單中，新網域可能會在 VPC 的某個區域中短暫封鎖，而在另一個區域中仍然得到允許。當您第一次設定規則群組和 VPC 關聯，以及變更現有設定時，可能會發生此暫時不一致的情況。一般來說，這種類型的任何不一致只會持續幾秒鐘。

在生產環境中使用之前，請先測試您的網域清單

最佳實務是在生產環境中使用規則群組之前，先在非生產環境中進行測試，並將規則動作設定為 Alert。使用 Amazon CloudWatch 指標和解析器日誌評估規則。日誌會提供所有警示和封鎖動作的網域清單名稱。當您對網域清單與您想要的 DNS 查詢相符感到滿意之後，請視需要變更規則動作設定。如需有關 CloudWatch 指標和查詢記錄檔的資訊使用 Amazon 監控 Route 53 解析器 DNS 防火牆規則群組 CloudWatch，請參閱出現在 Resolver 查詢日誌中的值、和管理 Resolver 查詢日誌記錄組態。

若要新增網域清單

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

在導覽窗格中選擇 DNS 防火牆，以在 Amazon VPC 主控台上開啟 DNS 防火牆規則群組頁面。繼續步驟 2。

- 或 -

登入 AWS Management Console 並開啟

位於 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 主控台。

2. 在導覽窗格中的 DNS 防火牆下方，選擇網域清單。在 Domain lists (網域清單) 頁面上，您可以選取和編輯現有網域清單，還可以新增自己的網域清單。
3. 要新增網域清單，請選擇 Add domain list (新增網域清單)。
4. 提供網域清單的名稱，然後在文字方塊中輸入網域規格 (每行一個)。

   如果您滑動 Switch to bulk upload (切換至大量上傳) 至 on (開啟)，請輸入您在其中建立網域清單的 Amazon S3 儲存貯體的 URI。此網域清單在每行中應該有一個網域名稱。
5. 選擇 Add domain list (新增網域清單)。Domain lists (網域清單) 頁面會列出您的新網域清單。

建立網域清單之後，您可以從 DNS 防火牆規則依名稱參考該清單。

刪除 DNS 防火墻實體

當您刪除可在 DNS 防火牆中使用的實體 (例如規則群組中可能正在使用的網域清單) 或可能與 VPC 關聯的規則群組時，DNS 防火牆會檢查該實體目前是否正在使用中。如果發現該實體正在使用中，DNS 防火牆會警告您。DNS 防火墻幾乎總是能夠判斷實體是否正在使用中。但是在極少數的情況下，它也可能無法判斷。如果您需要確定目前沒有任何物件正在使用該實體，請在 DNS 防火墻組態中檢查它，然後予以刪除。如果實體是參考的網域清單，請檢查沒有規則群組正在使用它。如果實體是規則群組，請檢查該實體是否與任何 VPC 相關聯。

若要刪除網域清單

1. 在導覽窗格中，選擇 Domain lists (網域清單)。
2. 在導覽列中，選擇網域清單的區域。
3. 選取您要刪除的網域清單，然後選擇 Delete (刪除) 並確認刪除。

為 DNS 防火牆設定日誌記錄

您可以使用 Amazon CloudWatch 指標和解析器查詢日誌來評估 DNS 防火牆規則。日誌會提供所有警示和封鎖動作的網域清單名稱。如需 Amazon 的詳細資訊 CloudWatch，請參閱使用 Amazon 監控 Route 53 解析器 DNS 防火牆規則群組 CloudWatch。

當您啟用 DNS 防火牆，將其與 VPC 建立關聯，並且已啟用記錄功能時，`firewall_rule_group_id`、`firewall_rule_action` 和 `firewall_domain_list_id` 是就是日誌中提供的 DNS 防火牆特定欄位。

> **Note**
>
> 只有遭到 DNS 防火牆規則封鎖的查詢，查詢日誌才會顯示額外的 DNS 防火牆欄位。

若要開始記錄源自 VPC 的 DNS 防火牆規則篩選的 DNS 查詢，請在 Amazon Route 53 主控台中執行下列任務：

設定 DNS 防火牆的 Resolver 查詢日誌記錄

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 展開 Route 53 主控台選單。在主控台的左上角，選擇三個水平橫條 (☰) 圖示。
3. 在 Resolver 選單中，選擇 Query logging (查詢日誌記錄)。
4. 在「地區」選取器中，選擇您要建立查詢記錄組態的「 AWS 區域」。

   此區域必須等同於您在其中建立與 DNS 防火牆相關聯且想要記錄查詢的 VPC 的區域。如果您在多個區域擁有 VPC，務必為每個區域至少建立一項查詢日誌記錄組態。
5. 選擇 Configure query logging (設定查詢日誌記錄)。
6. 指定下列值：

   查詢日誌記錄組態

   輸入查詢日誌記錄組態的名稱。名稱會顯示在主控台中的查詢日誌記錄組態清單。輸入稍後可以協助您尋找此組態的名稱。

查詢日誌目的地

選擇您希望解析器發送查詢日誌的 AWS 資源類型。如需如何在選項 (CloudWatch 日誌記錄群組、S3 儲存貯體和 Firehose 交付串流) 中進行選擇的相關資訊，請參閱AWS 您可以將解析器查詢日誌發送到的資源。

選擇資源類型後，您可以建立該類型的其他資源，或選擇目前 AWS 帳號建立的現有資源。

> **Note**
>
> 您只能選擇在步驟 4 中選取的 AWS 區域中建立的資源，即您要建立查詢日誌記錄組態的區域。如果您選擇建立新資源，則會在相同的區域中建立該資源。

要記錄查詢的 VPC

此查詢日誌記錄組態會記錄源自所選擇之 VPC 的 DNS 查詢。核取您要 Resolver 記錄查詢的目前區域中每個 VPC 的核取方塊，然後選擇 選擇。

> **Note**
>
> 針對特定目的地類型，只能啟用一次 VPC 日誌交付。日誌無法交付至相同類型的多個目的地。例如，VPC 日誌無法交付至兩個 Amazon S3 目的地。

7. 選擇 Configure query logging (設定查詢日誌記錄)。

> **Note**
>
> 您應該會在成功建立查詢日誌記錄組態後幾分鐘內開始看到由 VPC 資源進行的 DNS 查詢。

在帳戶之間共用 Route 53 解析程式 DNS 防火牆規則群組 AWS

您可以在 AWS 帳戶之間共用 DNS 防火牆規則群組。若要共用規則群組，請使用 AWS Resource Access Manager (AWS RAM)。DNS 防火牆主控台與主 AWS RAM 控台整合。如需有關的詳細資訊 AWS RAM，請參閱 Resource Access Manager 使用指南。

注意下列事項：

建立共用規則群組與 VPC 的關聯

如果其他 AWS 帳戶與您的帳戶共用規則群組，您可以使用與您建立的規則群組建立關聯的方式相同，將其與 VPC 建立關聯。如需詳細資訊，請參閱 管理 VPC 與 Route 53 Resolver DNS 防火牆規則群組之間的關聯。

刪除或停止共用規則群組

如果您與其他帳戶共用規則群組，然後刪除或停止共用該規則群組，DNS 防火墻會移除其他帳戶在規則群組與其 VPC 之間建立的所有關聯。

規則群組和關聯的最大設定值

共用規則群組及其與 VPC 的關聯會包含在共用規則群組之帳戶的計數中。

如需目前的 DNS 防火墻配額，請參閱 Route 53 Resolver DNS 防火墻上的配額。

許可

若要與其他 AWS 帳戶共用規則群組，您必須擁有使用該PutFirewallRuleGroupPolicy動作的權限。

規則群組共用的 AWS 帳戶限制

共用規則群組的帳戶無法變更或刪除規則群組。

標記

只有建立規則群組的帳戶可以新增、刪除或查看規則群組的標籤。

若要檢視規則群組目前的共用狀態 (包括共用規則群組的帳戶或接受共用的帳戶)，以及與其他帳戶共用規則群組，請執行以下程序。

檢視共用狀態並與其他 AWS 帳戶共用規則群組

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Rule groups (規則群組)。
3. 在導覽列上，選擇您建立規則群組的區域。

   Sharing status (共用狀態) 欄顯示規則群組目前的共用狀態，它們是目前帳戶建立的規則群組或與目前帳戶共用的規則群組：

   - 未共用：目前 AWS 帳戶已建立規則群組，且規則群組不會與任何其他帳戶共用。
   - Shared by me (由我共用)：目前的帳戶建立了規則群組，且與一或多個帳戶共用。

- Shared with me (與我共用)：另一個帳戶建立了規則群組，且與目前的帳戶共用。

4. 選擇您想要顯示共用資訊的規則群組名稱，或您想要與其他帳戶共用的規則群組名稱。

   在 Rule group: ***rule group name*** (規則群組：規則群組名稱) 頁面中，Owner (擁有者) 下的值會顯示建立規則群組的帳戶 ID。除非 Sharing status (共用狀態) 的值為 Shared with me (與我共用)，否則即為目前的帳戶。若是如此，Owner (擁有者) 即為建立了規則群組，且與目前帳戶共用規則群組的帳戶。

5. 選擇 Share (共用) 以檢視更多資訊，或與其他帳戶共用規則群組。視「共用狀態」的值而定，會顯示 AWS RAM 主控台中的頁面：

   - Not shared (不共用)：顯示 Create resource share (建立資源共用) 頁面。如需如何與其他帳戶、組織單位 (OU) 或組織共用規則群組的資訊，請移至後續的步驟。
   - Shared by me (由我共用)：Shared resources (共用的資源) 頁面會顯示目前帳戶所擁有的規則群組和其他資源，以及與其他帳戶共用的規則群組和資源。
   - Shared with me (與我共用)：Shared resources (共用的資源) 頁面會顯示其他帳戶所擁有的規則群組和其他資源，以及與目前帳戶共用的規則群組和資源。

6. 若要與其他 AWS 帳戶、OU 或組織共用規則群組，請指定下列值。

   > **Note**
   >
   > 您無法更新共用設定。如果您想要變更以下任一設定，則必須重新共用使用新設定的規則群組，然後移除舊的共用設定。

   描述

   輸入有助於您記憶為何共用規則群組的簡短描述。

   資源

   選擇您要共用之規則群組的核取方塊。

   主體

   輸入 AWS 帳號、OU 名稱或組織名稱。

   標籤

   指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

這些是用於組織 AWS 帳單的標籤；您也可以將標籤用於其他用途。 AWS Billing and Cost Management 如需有關使用成本分配標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

為 VPC 啟用 Route 53 Resolver DNS 防火牆保護

您可以透過將一或多個規則群組與 VPC 產生關聯來啟用 VPC 的 DNS 防火牆保護。每當 VPC 與 DNS 防火牆規則群組相關聯時，Route 53 Resolver 會提供下列 DNS 防火牆保護：

- Resolver 會透過 DNS 防火牆路由 VPC 的傳出 DNS 查詢，而 DNS 防火牆會使用相關聯的規則群組篩選查詢。
- Resolver 會強制執行 VPC 的 DNS 防火牆組態中的設定。

若要為 VPC 提供 DNS 防火牆保護，請執行下列動作：

- 建立及管理 DNS 防火牆規則群組與 VPC 之間的關聯。如需規則群組的詳細資訊，請參閱 DNS 防火牆規則群組與規則。
- 設定您希望 Resolver 在失敗期間處理 VPC 的 DNS 查詢的方式，例如，如果 DNS 防火牆未提供 DNS 查詢的回應。

管理 VPC 與 Route 53 Resolver DNS 防火牆規則群組之間的關聯

檢視規則群組的 VPC 關聯

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

   在導覽窗格中選擇 DNS 防火牆，以在 Amazon VPC 主控台上開啟 DNS 防火牆規則群組頁面。

   - 或 -

   登入 AWS Management Console 並開啟

   位於 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 主控台。
2. 在導覽窗格中的 DNS 防火牆下方，選擇規則群組。
3. 在導覽列中，選擇規則群組的區域。

4. 選取您要關聯的規則群組。
5. 請選擇 View Details (檢視詳細資訊)。隨即顯示規則群組頁面。
6. 在頁面底部，您可以看到包含規則和關聯 VPC 的標籤式詳細資料區域。選擇標籤 Associated VPCs (關聯的 VPC)。

將規則群組與 VPC 相關聯

1. 依照上述程序檢視規則群組的 VPC 關聯中的指示來尋找規則群組的 VPC 關聯。
2. 在 Associated VPCs (關聯的 VPC) 標籤中，選擇 Associate VPC (關聯 VPC)。
3. 在下拉式清單中找到您要與規則群組建立關聯的 VPC。選取該 VPC ，然後選擇 Associate (關聯)。

在規則群組頁面中，您的 VPC 會列在 Associated VPCs (關聯的 VPC) 標籤中。起初，該關聯的 Status (狀態) 報告為 Updating (更新中)。關聯完成時，狀態會變更為 Complete (完成)。

移除規則群組與 VPC 之間的關聯

1. 依照上述程序檢視規則群組的 VPC 關聯中的指示來尋找規則群組的 VPC 關聯。
2. 選取您要從清單中移除的 VPC，然後選擇Disassociate (解除關聯)。請驗證，然後確認該動作。

在規則群組頁面上，您的 VPC 會列在 Associated VPCs (關聯的 VPC) 標籤中，其狀態為 Disassociating (解除關聯中)。作業完成時，DNS 防火牆會更新清單以移除 VPC。

DNS 防火牆 VPC 組態

VPC 的 DNS 防火牆組態會決定 Route 53 Resolver 是否允許查詢或在失敗期間封鎖查詢，例如當 DNS 防火牆損壞、沒有回應，或未於區域中提供。每當您有一或多個與 VPC 相關聯的 DNS 防火牆規則群組時，Resolver 就會強制執行 VPC 的防火牆組態。

您可以將 VPC 設定為開啟失敗或關閉失敗。

- 根據預設，失敗模式會關閉，這表示 Resolver 會封鎖其未收到來自 DNS 防火牆回覆的任何查詢，並且會傳送 `SERVFAIL` DNS 回答。這種方法有利於安全性，而不是可用性。
- 如果您啟用開啟失敗，Resolver 會在未收到來自 DNS 防火牆的回覆時允許查詢。這種方法有利於可用性，而不是安全性。

若要變更 VPC (主控台) 的 DNS 防火牆組態

1. 登入 AWS Management Console 並開啟解析程式主控台，網址為 https://console.aws.amazon.com/route53resolver/。
2. 在導覽窗格的 Resolvers (解析程式) 下，選擇 VPCs。
3. 在 VPCs 頁面上，找出並編輯 VPC。視需要將 DNS 防火牆組態變更為開啟失敗或關閉失敗。

若要變更 VPC (API) 的 DNS 防火牆行為

- 透過呼叫UpdateFirewallConfig和啟用或停用`FirewallFailOpen`來更新您的 VPC 防火牆組態。

您可以透過呼叫 ListFirewallConfigsAPI 擷取 VPC 防火牆組態清單。

什麼是 Amazon Route 53 on Outposts？

AWS Outposts 是一項全受管服務，可將 AWS 基礎設施、服務、API 和工具擴展到客戶據點。這可讓客戶使用與 AWS 區域 中相同的程式設計介面，執行具有內部部署工作負載的 AWS 服務。如需詳細資訊，請參閱《AWS Outposts 使用者指南》中的什麼是 AWS Outposts？。

Route 53 on Outposts 提供兩種功能：

- 解析程式，其會快取源自 AWS Outposts 的所有 DNS 查詢。
- 在部署傳入和傳出端點時，在 Outpost 和內部部署 DNS 解析程式之間的混合式連線。

如需更多詳細資訊，請參閱 什麼是 Amazon Route 53 Resolver？。

此外，Route 53 on Outposts 透過允許在 Outpost 中解析查詢，而不是往返至最近的 AWS 區域，減少了網路延遲。

> **Note**
>
> 如果 AWS Outposts 機架版本與 Route 53 on Outposts 不相容，AWS 帳戶團隊會收到通知，並將與您聯絡以協助您升級 AWS Outposts。

Amazon Route 53 on Outposts 功能

下表描述 Route 53 on Outposts 功能與 Amazon Route 53 功能的比較情況。

Route 53 on Outposts 與 Route 53 的比較

功能	Route 53 on Outposts 的可用性
Route 53 Resolver	是。解析程式會為 Outpost 機架上託管的應用程式、AWS 區域 中的對等 VPC 以及任何可公開存取的主機名稱維護記錄的本機快取。
運作狀態檢查	否。運作狀態檢查的計算和報告皆是來自 AWS 區域。如果 Outpost 中斷與雲端的連線，端點會無法開啟，而且無法容錯移轉至備份。

功能	Route 53 on Outposts 的可用性
解析程式端點	是。Outpost 機架上的解析程式端點允許在內部部署的 DNS 伺服器轉送和接收 DNS 查詢。 僅可將 IPv4 端點類型用於端點。
Route 53 Resolver DNS 防火牆	不可用。
流量	不可用。

將 AWS Outposts 與 VPC 中斷連線時的 Route 53 Resolver 行為

如果 AWS Outposts 與 AWS 區域 中斷連線，則 Outpost 上的解析程式行為如下：

- 控制平面變更不可用。
- 無法使用運作狀態檢查和 DNS 備援功能。
- 在 Outposts 上本機託管的資源 DNS 查詢已經過解析，但在某些情況下，如果在 Outpost 處於中斷連線狀態時更新資源的 IP 地址，則回應可能會過時。
- 區域內 VPC 上託管的資源 DNS 查詢是可解析的。但是，在 AWS 區域 的 Outpost 連線恢復之前，將無法存取資源。
- 如果公用 DNS 資源的 DNS 查詢在 Outpost 的 Route 53 Resolver 快取中可用，則可以解析這些查詢。

開始在 AWS Outposts 上使用 Route 53 Resolver

在您訂購並收到交付的 AWS Outposts 機架後，您就可以如此處所述：《AWS Outposts 指南》中的 Create an AWS Outposts，在 Outpost 上設定解析程式。

您還可以使用 API 管理 Route 53 on Outposts。如需詳細資訊，請參閱 Resolver on Outpost actions。

> **Important**
>
> 最多可能需要 30-150 分鐘才能在 AWS Outposts 上建立解析程式快取。

AWS Outposts 機架交付後，您可以選擇加入 Route 53 on Outposts。

在 Outpost 上設定解析程式

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 在 Outpost 上的解析程式頁面上，選擇建立解析程式。
5. 在建立解析程式頁面上：
   - 在 AWS Outposts 下選取您要在其上建立解析程式的 AWS Outposts。
   - 在解析程式名稱文字方塊中輸入解析程式的名稱。
   - 在解析程式的建議執行個體類型中填入 Amazon EC2 執行個體之後，請選擇一個執行個體。

     如需有關執行個體類型的詳細資訊，請參閱 Outpost 上的解析程式配額。
   - 在執行個體數量中，選擇 VPC 解析程式的彈性介面執行個體數目。預設值為 4。

     如果 AWS Outposts 沒有支援解析程式的執行個體類型，則無法建立解析程式。
6. 選擇 Create Resolver (建立解析程式)。

   您可以在 Outpost 上的解析程式頁面上監控解析程式的建立。

建立傳入端點

在 Outpost 上建立解析程式之後，您可以新增傳入和傳出端點，以便解析內部部署網路之間的 DNS 查詢。

在 Outpost 上設定解析程式的傳入端點

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇檢視詳細資訊。
5. 在傳入端點資料表上，選擇建立傳入端點。
6. 在建立傳入端點頁面上，輸入適用的值。如需更多詳細資訊，請參閱 當您在 Outpost 上建立或編輯傳入端點時所指定的值。

7. 選擇 Create endpoint (建立端點)。

當您在 Outpost 上建立或編輯傳入端點時所指定的值

當您建立或編輯傳入端點時，請指定下列值：

Outpost ID

如果要在 AWS Outposts VPC 上為解析程式建立端點，則此為 AWS Outposts ID。

Endpoint name (端點名稱)

易記的名稱可讓您在儀表板中輕鬆找出傳入端點。

區域名稱區域中的 VPC

所有來自您網路的傳入 DNS 查詢，都會通過此 VPC 前往 Resolver。

此端點的安全群組

您想用來控制存取此 VPC 之一或多個安全群組的 ID。您指定的安全群組必須包含一或多個傳入規則。傳入規則必須允許連接埠 53 上的 TCP 和 UDP 存取權限。您無法在建立端點之後變更此值。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 安全群組規則。

IP 地址

您希望您網路上的 DNS 解析程式將 DNS 查詢轉送到這些 IP 地址。我們需要您至少指定兩個 IP 地址以供備援使用。注意下列事項：

多個可用區域

建議您至少在兩個可用區域中指定 IP 地址。您可以在那些或其他可用區域選擇性指定其他 IP 地址。

IP 地址和 Amazon VPC 彈性網路介面

針對您指定的可用區域、子網路和 IP 地址的各種組合，Resolver 會建立 Amazon VPC 彈性網路介面。如需了解端點中每個 IP 地址每秒的 DNS 查詢次數的目前上限，請參閱 Route 53 Resolver 的配額。如需有關每個彈性網路介面定價的資訊，請參閱 Amazon Route 53 定價頁面上的 Amazon Route 53。

> **Note**
>
> Resolver 端點具有私有 IP 地址。這些 IP 位址在端點的生命週期中不會變更。

針對每個 IP 地址，指定以下值。每個 IP 地址都必須位在您指定之 VPC 的可用區域內，您的 VPC 是在 VPC in the region-name Region (區域名稱區域中的 VPC) 中指定。

可用區域

您希望 DNS 查詢通往 VPC 途中所經過的可用區域。您指定的可用區域必須設定子網路。

子網

該子網路包含您想要將 DNS 查詢轉送到的 IP 地址。子網路必須有可用的 IP 地址。

指定 IPv4 地址的子網路。不支援 IPv6。

IP 地址

您想要將 DNS 查詢轉送到此 IP 地址。

選擇要讓 Resolver 從指定之子網路的可用 IP 地址當中為您選擇 IP 地址，還是您想要自己指定 IP 地址。

如果選擇自己指定 IP 地址，請輸入 IPv4 地址。不支援 IPv6。

Tags (標籤)

指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

AWS Billing and Cost Management 提供這些標籤供您組織 AWS 帳單，您也可以將這些標籤用於其他用途。如需有關使用成本配置標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

建立傳出端點

選擇加入和設定 Route 53 Resolver 後，您可以新增傳入和傳出端點，以便解析內部部署網路的 DNS 查詢。

在 Outpost 上設定解析程式的傳出端點

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。

4. 選取處於作業狀態的解析程式旁邊的核取記號，然後選擇檢視詳細資訊。
5. 在傳出端點資料表上，選擇建立傳出端點。
6. 在建立傳出端點頁面上，輸入適用的值。如需更多詳細資訊，請參閱 當您在 Outpost 上建立或編輯傳入端點時所指定的值。
7. 選擇 Create endpoint (建立端點)。

當您在 AWS Outposts 中建立或編輯傳出端點時所指定的值

當您建立或編輯傳入端點時，請指定下列值：

Outpost ID

如果要在 AWS Outposts VPC 上為解析程式建立端點，則此為 AWS Outposts ID。

Endpoint name (端點名稱)

易記的名稱可讓您在儀表板中輕鬆找出傳入端點。

區域名稱區域中的 VPC

所有來自您網路的傳入 DNS 查詢，都會通過此 VPC 前往 Resolver。

此端點的安全群組

您想用來控制存取此 VPC 之一或多個安全群組的 ID。您指定的安全群組必須包含一或多個傳入規則。傳入規則必須允許連接埠 53 上的 TCP 和 UDP 存取權限。您無法在建立端點之後變更此值。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 安全群組規則。

IP 地址

您希望您網路上的 DNS 解析程式將 DNS 查詢轉送到這些 IP 地址。我們需要您至少指定兩個 IP 地址以供備援使用。注意下列事項：

多個可用區域

建議您至少在兩個可用區域中指定 IP 地址。您可以在那些或其他可用區域選擇性指定其他 IP 地址。

IP 地址和 Amazon VPC 彈性網路介面

針對您指定的可用區域、子網路和 IP 地址的各種組合，Resolver 會建立 Amazon VPC 彈性網路介面。如需了解端點中每個 IP 地址每秒的 DNS 查詢次數的目前上限，請參閱 Route 53

Resolver 的配額。如需每個彈性網路介面的定價的相關資訊，請參閱 Amazon Route 53 定價頁面上的「Amazon Route 53」。

> **Note**
>
> Resolver 端點具有私有 IP 地址。這些 IP 位址在端點的生命週期中不會變更。

針對每個 IP 地址，指定以下值。每個 IP 地址都必須位在您指定之 VPC 的可用區域內，您的 VPC 是在 VPC in the region-name Region (區域名稱區域中的 VPC) 中指定。

可用區域

您希望 DNS 查詢通往 VPC 途中所經過的可用區域。您指定的可用區域必須設定子網路。

子網

該子網路包含您想要將 DNS 查詢轉送到的 IP 地址。子網路必須有可用的 IP 地址。

指定 IPv4 地址的子網路。不支援 IPv6。

IP 地址

您想要將 DNS 查詢轉送到此 IP 地址。

選擇要讓 Resolver 從指定之子網路的可用 IP 地址當中為您選擇 IP 地址，還是您想要自己指定 IP 地址。

如果選擇自己指定 IP 地址，請輸入 IPv4 地址。不支援 IPv6。

Tags (標籤)

指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

AWS Billing and Cost Management 提供這些標籤供您組織 AWS 帳單，您也可以將這些標籤用於其他用途。如需有關使用成本配置標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

建立傳出端點的轉送規則

您也可以為傳出端點建立轉送規則。如需詳細資訊，請參閱 建立轉送規則並建立規則與一或多個 VPC 的關聯

管理 Outpost 上的解析程式

若要管理 Outpost 上的解析程式，請執行適用的程序。

主題

- 編輯 Outpost 上的解析程式
- 檢視 Outpost 上的解析程式狀態
- 刪除 Outpost 上的解析程式

編輯 Outpost 上的解析程式

若要編輯 Outpost 上的解析程式，請執行下列程序。

編輯 Outpost 上的解析程式

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取記號，然後選擇編輯。
5. 您可以編輯下列資訊：
   - 解析程式名稱
   - 執行個體類型
   - 執行個體數量
6. 完成編輯後，選擇儲存變更。

檢視 Outpost 上的解析程式狀態

若要檢視 Outpost 上的解析程式狀態，請執行下列程序。

檢視傳入端點的狀態

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。

2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取記號，然後選擇檢視詳細資訊。
5. Outpost 上的解析程式頁面中的狀態欄包含下列其中一個值：

正在建立

Outpost 上的解析程式正在建立中。

可運作

Outpost 上的解析程式已正確設定。

正在更新

Outpost 上的解析程式正在更新執行個體類型。

需採取動作

此解析程式的運作狀態不佳，無法自動復原。若要解決此問題，建議您確定執行個體 AWS Outposts 可以支援 Outpost 上的解析程式。

正在刪除

Outpost 上的解析程式正在刪除中。

建立失敗

在 Outpost 上建立解析程式失敗。

刪除失敗

在 Outpost 上刪除解析程式失敗。若要修正此問題，請在幾分鐘後再試一次。

刪除 Outpost 上的解析程式

> **Note**
> 您必須先刪除與 Outpost 上的解析程式，才能刪除與其相關聯的任何端點。

若要刪除 Outpost 上的解析程式，請執行下列程序。

刪除 Outpost 上的解析程式

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇刪除。
5. 在刪除解析程式對話方塊中，在文字方塊內輸入 **delete**，然後選擇刪除。

在 Outpost 上管理解析程式上的傳入端點

若要在 Outpost 上管理解析程式上的傳入端點，請執行適用的程序。

主題

- 檢視和編輯傳入端點
- 檢視傳入端點的狀態
- 刪除傳入端點

檢視和編輯傳入端點

若要檢視及編輯傳入端點的設定，請執行下列程序。

檢視及編輯傳入端點的設定

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇檢視詳細資訊。
5. 在傳入端點清單中，選擇您想要檢視設定或想要編輯之端點的選項。
6. 選擇 View details (檢視詳細資訊) 或 Edit (編輯)。

   如需傳入端點值的資訊，請參閱當您在 Outpost 上建立或編輯傳入端點時所指定的值。
7. 如果您選擇 Edit (編輯)，請輸入適合的值，然後選擇 Save (儲存)。

檢視傳入端點的狀態

若要檢視傳入端點的狀態，請執行下列程序。

檢視傳入端點的狀態

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇檢視詳細資訊。
5. 傳入端點清單的狀態欄包含以下其中一個值：

   正在建立

   Resolver 正在為此端點建立和設定一或多個 Amazon VPC 網路介面。

   可運作

   此端點的 Amazon VPC 網路介面已正確設定，而且能夠在您的網路和 Resolver 之間傳送傳入或傳出 DNS 查詢。

   正在更新

   Resolver 正在建立或取消一或多個網路介面與此端點的關聯。

   自動復原

   Resolver 正在嘗試復原與此端點相關聯的一或多個網路介面。在復原過程中，由於每個 IP 地址 (每個網路介面) 的 DNS 查詢次數有所限制，端點會以有限容量運作。如需目前的限制，請參閱 Route 53 Resolver 的配額。

   需採取動作

   此端點運作狀態不佳，Resolver 無法自動復原它。若要解決該問題，建議您檢查與端點相關聯的每個 IP 地址。對於每個無法使用的 IP 地址，請新增另一個 IP 地址，然後刪除無法使用的 IP 地址。端點一定要包含至少兩個 IP 地址。狀態為 Action needed (需採取動作) 可能有各式各樣的原因。以下是兩個常見的原因：

   - 已使用 Amazon VPC 刪除與端點相關聯的一或多個網路介面。
   - 由於一些已超出 Resolver 所能控制的原因，而無法建立網路介面。

正在刪除

Resolver 正在刪除此端點和相關聯的網路介面。

刪除傳入端點

若要刪除傳入端點，請執行下列程序。

> **Important**
> 如果刪除傳入端點，您網路的 DNS 查詢即不再轉送到您於端點中指定之 VPC 中的 Resolver。

刪除傳入端點

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇檢視詳細資訊。
5. 勾選您要刪除的端點旁邊的核取方塊。
6. 選擇 Delete (刪除)。
7. 若要確認您要刪除該端點，請輸入端點名稱，然後選擇 Submit (提交)。

在 Outpost 上管理解析程式上的傳出端點

若要在 Outpost 上管理解析程式上的傳出端點，請執行適用的程序。

主題

- 檢視和編輯傳出端點
- 檢視輸出端點的狀態
- 刪除傳出端點

檢視和編輯傳出端點

若要檢視及編輯傳出端點的設定，請執行下列程序。

檢視及編輯傳出端點的設定

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇檢視詳細資訊。
5. 在傳出端點清單中，勾選您要檢視設定或編輯的端點旁邊的核取方塊。
6. 選擇 View details (檢視詳細資訊) 或 Edit (編輯)。

   如需傳出端點值的資訊，請參閱 當您在 AWS Outposts 中建立或編輯傳出端點時所指定的值。
7. 如果您選擇 Edit (編輯)，請輸入適合的值，然後選擇 Save (儲存)。

檢視輸出端點的狀態

若要檢視傳出端點的狀態，請執行下列程序。

檢視傳出端點的狀態

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。
3. 在導覽列中選擇 AWS Outposts 所在的區域。
4. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇檢視詳細資訊。
5. 在傳出端點清單中，狀態欄包含下列其中一個值：

   正在建立

   Resolver 正在為此端點建立和設定一或多個 Amazon VPC 網路介面。

   可運作

   此端點的 Amazon VPC 網路介面已正確設定，而且能夠在您的網路和 Resolver 之間傳送傳入或傳出 DNS 查詢。

正在更新

Resolver 正在建立或取消一或多個網路介面與此端點的關聯。

自動復原

Resolver 正在嘗試復原與此端點相關聯的一或多個網路介面。在復原過程中，由於每個 IP 地址 (每個網路介面) 的 DNS 查詢次數有所限制，端點會以有限容量運作。如需目前的限制，請參閱 Route 53 Resolver 的配額。

需採取動作

此端點運作狀態不佳，Resolver 無法自動復原它。若要解決該問題，建議您檢查與端點相關聯的每個 IP 地址。對於每個無法使用用的 IP 地址，請新增另一個 IP 地址，然後刪除無法使用的 IP 地址。(一個端點一定要包含至少兩個 IP 地址)。狀態為 Action needed (需採取動作) 可能有各式各樣的原因。以下是兩個常見的原因：

- 已使用 Amazon VPC 刪除與端點相關聯的一或多個網路介面。
- 由於一些已超出 Resolver 所能控制的原因，而無法建立網路介面。

正在刪除

Resolver 正在刪除此端點和相關聯的網路介面。

刪除傳出端點

在刪除端點之前，您必須先刪除與 VPC 相關聯的任何規則。

若要刪除傳出端點，請執行下列程序。

> **Important**
>
> 如果您刪除傳出端點，則針對指定已刪除傳出端點的那些規則，Resolver 會停止將 DNS 查詢從您的 VPC 轉送到您的網路。

刪除傳出端點

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在左側導覽窗格中，展開解析程式，然後導覽至 Outposts。

3. 選取處於作業狀態的解析程式旁邊的核取方塊，然後選擇檢視詳細資訊。
4. 在傳出端點清單中，選擇您要刪除之端點的選項。
5. 選擇 Delete (刪除)。
6. 若要確認您要刪除該端點，請輸入端點名稱，然後選擇 Submit (提交)。

使用 AWS CloudFormation 建立 Amazon Route 53 和 Amazon Route 53 Resolver 資源

Amazon Route 53 和 Amazon Route 53 Resolver 已與 AWS CloudFormation 整合，這項服務可協助您建立 AWS 資源的模型和設定，以減少建立和管理資源和基礎架構的時間。您可以建立一個範本，描述所有您想要的 AWS 資源，AWS CloudFormation 就會為您佈建和設定那些資源。

當您使用 AWS CloudFormation 時，您可以重複使用您的範本，重複、一致的設定您的 Route 53 和 Route 53 Resolver 資源。只需描述一次您的資源，即可在多個 AWS 帳戶 帳戶與區域內重複佈建相同資源。

Route 53、Route 53 Resolver 和 AWS CloudFormation 範本

若要佈建和設定 Route 53、Route 53 Resolver 與相關服務的資源，您必須了解 AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。而您亦可以透過這些範本的說明，了解欲在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation Designer 協助您開始使用 AWS CloudFormation 範本。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的什麼是 AWS CloudFormation Designer？。

Route 53 支援在 AWS CloudFormation 中建立如下資源類型：

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

如需更多詳細資訊 (包括 Route 53 資源的 JSON 和 YAML 範本範例)，請參閱 AWS CloudFormation 使用者指南中的 Amazon Route 53 資源類型參考。

Route 53 Resolver 支援在 AWS CloudFormation 中建立以下資源類型：

- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallDomainList`

- AWS::Route53Resolver::FirewallRuleGroupAssociation
- AWS::Route53Resolver::ResolverDNSSECConfig
- AWS::Route53Resolver::ResolverEndpoint
- AWS::Route53Resolver::ResolverQueryLoggingConfig
- AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation
- AWS::Route53Resolver::ResolverRule
- AWS::Route53Resolver::ResolverRuleAssociation

如需更多詳細資訊 (包括 Route 53 Resolver 資源的 JSON 和 YAML 範本範例)，請參閱 AWS CloudFormation 使用者指南中的 Amazon Route 53 Resolver 資源類型參考。

進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- 《AWS CloudFormation 使用者指南》https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
- AWS CloudFormation API 參考
- 《AWS CloudFormation 命令列介面使用者指南》https://docs.aws.amazon.com/cloudformation-cli/latest/userguide/what-is-cloudformation-cli.html

適用於使AWS用 SDK 的 Route 53 程式碼範例

下列程式碼範例示範如何使用 Route 53 搭配 AWS 軟體開發套件 (SDK)。

如需完整的 AWS SDK 開發人員指南和程式碼範例清單，請參閱 搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

程式碼範例

- 使用 AWS SDK 的路線 53 的程式碼範例
  - 使用 AWS SDK 執行路由 53 的動作
    - 使用 AWS SDK 獲取公共和私有 Route 53 託管區域的列表
- 使用 AWS SDK 進行 Route 53 網域註冊的程式碼範例
  - 使用 AWS SDK 進行路由 53 號線域註冊的操作
    - 使用 AWS SDK 檢查域的可用性
    - 使用 SDK 檢查域的可轉移性 AWS
    - 使用 AWS SDK 獲取 Route 53 域註冊域詳細信息
    - 使用 AWS SDK 獲取有關 Route 53 域註冊操作的詳細信息
    - 使用 AWS SDK 取得 Route 53 網域註冊網域名稱建議
    - 使用 AWS SDK 列出路由 53 域名註冊域名價格
    - 使用 AWS SDK 列出路由 53 域註冊註冊域
    - 使用 AWS SDK 列出路由 53 網域註冊作業
    - 使用 AWS SDK 使用 Route 53 網域註冊註冊網域
    - 使用 AWS SDK 檢視 Route 53 網域註冊帳單記錄
  - 使用 AWS SDK 進行路由 53 網域註冊的案例
    - 使用 AWS SDK 開始使用路線 53 網域註冊

使用 AWS SDK 的路線 53 的程式碼範例

下列程式碼範例說明如何搭配 AWS 軟體開發套件 (SDK) 使用 Route 53。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境和跨服務範例中查看內容中的動作。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

程式碼範例

- 使用 AWS SDK 執行路由 53 的動作
  - 使用 AWS SDK 獲取公共和私有 Route 53 託管區域的列表

使用 AWS SDK 執行路由 53 的動作

下列程式碼範例示範如何使用 AWS SDK 執行個別 Route 53 動作。這些摘錄會呼叫 Route 53 API，是必須在內容中執行之大型程式的程式碼摘錄。每個範例都包含一個連結 GitHub，您可以在其中找到設定和執行程式碼的指示。

下列範例僅包含最常使用的動作。如需完整清單，請參閱《Amazon Route 53 API 參考》。

範例

- 使用 AWS SDK 獲取公共和私有 Route 53 託管區域的列表

使用 AWS SDK 獲取公共和私有 Route 53 託管區域的列表

下列程式碼範例示範如何取得公有和私有託管區域的清單。

CLI

AWS CLI

列出與目前 AWS 帳號相關聯的託管區域

下列`list-hosted-zones`命令列出與目前 AWS 帳戶相關聯的前 100 個託管區域的摘要資訊。：

```
aws route53 list-hosted-zones
```

如果您具有 100 個以上的託管區域，或者要以小於 100 的群組列示它們，請包括 `--max-items` 參數。例如，若要一次列出一個託管區域，請使用下列命令：

```
aws route53 list-hosted-zones --max-items 1
```

若要檢視有關下一個託管區域的資訊，請從上一個命令的回應中取得 NextToken 值，並將其包含在 --starting-token 參數中，例如：

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考ListHostedZones中的。

Rust

適用於 Rust 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
async fn show_host_info(client: &aws_sdk_route53::Client) -> Result<(),
 aws_sdk_route53::Error> {
    let hosted_zone_count = client.get_hosted_zone_count().send().await?;

    println!(
        "Number of hosted zones in region : {}",
        hosted_zone_count.hosted_zone_count(),
    );

    let hosted_zones = client.list_hosted_zones().send().await?;

    println!("Zones:");

    for hz in hosted_zones.hosted_zones() {
        let zone_name = hz.name();
        let zone_id = hz.id();

        println!("  ID :   {}", zone_id);
        println!("  Name : {}", zone_name);
        println!();
    }

    Ok(())
}
```

- 如需 API 的詳細資訊，請參閱 AWS SDK ListHostedZones中的 Rust API 參考資料。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 進行 Route 53 網域註冊的程式碼範例

下列程式碼範例說明如何將 Route 53 網域註冊與 AWS 軟體開發套件 (SDK) 搭配使用。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境和跨服務範例中查看內容中的動作。

案例是向您展示如何呼叫相同服務中的多個函數來完成特定任務的程式碼範例。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含入門相關資訊和舊版 SDK 的詳細資訊。

開始使用

Hello Route 53 網域註冊

下列程式碼範例示範如何開始使用 Route 53 網域註冊。

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
```

```
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
 host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
 { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
 for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
            Console.WriteLine($"\tRegistration:
 {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {comPrices.RenewalPrice?.Price}
 {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考ListPrices中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the “com” type
 * and displays the prices for Registration and Renewal.
 *
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = "\n" +
                "Usage:\n" +
                "    <hostedZoneId> \n\n" +
                "Where:\n" +
                "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
 Route53DomainsClient.builder()
```

```
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .maxItems(10)
                    .tld(domainType)
                    .build();

            ListPricesResponse response =
route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
                System.out.println(
                        "Registration: " + pr.registrationPrice().price() + " " +
pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
+ pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
pr.changeOwnershipPrice().price() + " "
                        + pr.changeOwnershipPrice().currency());
                System.out.println(
                        "Restoration: " + pr.restorationPrice().price() + " " +
pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
```

```
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考ListPrices中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/**
 Before running this Kotlin code example, set up your development environment,
 including your credentials.

 For more information, see the following documentation topic:
 https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
           <domainType>

       Where:
           domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}
```

```
suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest = ListPricesRequest {
        maxItems = 10
        tld = domainType
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK ListPrices中的 Kotlin API 參考。

程式碼範例

- 使用 AWS SDK 進行路由 53 號線域註冊的操作
  - 使用 AWS SDK 檢查域的可用性
  - 使用 SDK 檢查域的可轉移性 AWS
  - 使用 AWS SDK 獲取 Route 53 域註冊域詳細信息
  - 使用 AWS SDK 獲取有關 Route 53 域註冊操作的詳細信息
  - 使用 AWS SDK 取得 Route 53 網域註冊網域名稱建議
  - 使用 AWS SDK 列出路由 53 域名註冊域名價格
  - 使用 AWS SDK 列出路由 53 域註冊註冊域
  - 使用 AWS SDK 列出路由 53 網域註冊作業
  - 使用 AWS SDK 使用 Route 53 網域註冊註冊網域
  - 使用 AWS SDK 檢視 Route 53 網域註冊帳單記錄

- 使用 AWS SDK 進行路由 53 網域註冊的案例
  - 使用 AWS SDK 開始使用路線 53 網域註冊

使用 AWS SDK 進行路由 53 號線域註冊的操作

下列程式碼範例示範如何使用 AWS SDK 執行個別 Route 53 網域註冊動作。這些摘錄會呼叫 Route 53 網域註冊 API，是必須在內容中執行之大型程式的程式碼摘錄。每個範例都包含一個連結 GitHub，您可以在其中找到設定和執行程式碼的指示。

下列範例僅包含最常使用的動作。如需完整清單，請參閱《Amazon Route 53 domain registration API 參考》。

範例

- 使用 AWS SDK 檢查域的可用性
- 使用 SDK 檢查域的可轉移性 AWS
- 使用 AWS SDK 獲取 Route 53 域註冊域詳細信息
- 使用 AWS SDK 獲取有關 Route 53 域註冊操作的詳細信息
- 使用 AWS SDK 取得 Route 53 網域註冊網域名稱建議
- 使用 AWS SDK 列出路由 53 域名註冊域名價格
- 使用 AWS SDK 列出路由 53 域註冊註冊域
- 使用 AWS SDK 列出路由 53 網域註冊作業
- 使用 AWS SDK 使用 Route 53 網域註冊註冊網域
- 使用 AWS SDK 檢視 Route 53 網域註冊帳單記錄

使用 AWS SDK 檢查域的可用性

下列程式碼範例示範如何檢查網域可用性。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/// <summary>
/// Check the availability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for availability.</param>
/// <returns>An availability result string.</returns>
public async Task<string> CheckDomainAvailability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
        new CheckDomainAvailabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Availability.Value;
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考CheckDomainAvailability中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainAvailabilityResponse response = route53DomainsClient
                    .checkDomainAvailability(availabilityRequest);
            System.out.println(domainSuggestion + " is " +
response.availability().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考CheckDomainAvailability中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest = CheckDomainAvailabilityRequest {
        domainName = domainSuggestion
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
    }
```

```
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK CheckDomainAvailability中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 SDK 檢查域的可轉移性 AWS

下列程式碼範例示範如何檢查網域的可轉移性。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/// <summary>
/// Check the transferability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for transferability.</param>
/// <returns>A transferability result string.</returns>
public async Task<string> CheckDomainTransferability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
        new CheckDomainTransferabilityRequest
        {
            DomainName = domain
        }
```

```
        );
        return result.Transferability.Transferable.Value;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考CheckDomainTransferability中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainTransferabilityResponse response = route53DomainsClient
                   .checkDomainTransferability(transferabilityRequest);
           System.out.println("Transferability: " +
response.transferability().transferable().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考CheckDomainTransferability中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest = CheckDomainTransferabilityRequest {
        domainName = domainSuggestion
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK CheckDomainTransferability中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 獲取 Route 53 域註冊域詳細信息

下列程式碼範例示範如何取得網域詳細資訊。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
{result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                          $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考GetDomainDetail中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
           System.out.println("The contact first name is " +
response.registrantContact().firstName());
           System.out.println("The contact last name is " +
response.registrantContact().lastName());
           System.out.println("The contact org name is " +
response.registrantContact().organizationName());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考GetDomainDetail中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest = GetDomainDetailRequest {
        domainName = domainSuggestion
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK GetDomainDetail中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 獲取有關 Route 53 域註冊操作的詳細信息

下列程式碼範例示範如何取得操作詳細資訊。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
```

```
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考GetOperationDetail中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
       try {
           GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                   .operationId(operationId)
                   .build();

           GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
           System.out.println("Operation detail message is " +
response.message());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考GetOperationDetail中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun getOperationalDetail(opId: String?) {
    val detailRequest = GetOperationDetailRequest {
        operationId = opId
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK GetOperationDetail中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 取得 Route 53 網域註冊網域名稱建議

下列程式碼範例示範如何取得網域名稱建議。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考GetDomainSuggestions中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                   .domainName(domainSuggestion)
                   .suggestionCount(5)
                   .onlyAvailable(true)
                   .build();

           GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
           List<DomainSuggestion> suggestions = response.suggestionsList();
           for (DomainSuggestion suggestion : suggestions) {
               System.out.println("Suggestion Name: " +
suggestion.domainName());
               System.out.println("Availability: " + suggestion.availability());
               System.out.println(" ");
           }

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考GetDomainSuggestions中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest = GetDomainSuggestionsRequest {
        domainName = domainSuggestion
        suggestionCount = 5
        onlyAvailable = true
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
            println(" ")
        }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK GetDomainSuggestions中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 列出路由 53 域名註冊域名價格

下列程式碼範例示範如何列出網域價格。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考ListPrices中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
       try {
           ListPricesRequest pricesRequest = ListPricesRequest.builder()
                   .tld(domainType)
                   .build();

           ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
           listRes.stream()
                   .flatMap(r -> r.prices().stream())
                   .forEach(content -> System.out.println(" Name: " +
content.name() +
                           " Registration: " +
content.registrationPrice().price() + " "
                           + content.registrationPrice().currency() +
                           " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考ListPrices中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun listAllPrices(domainType: String?) {
    val pricesRequest = ListPricesRequest {
        tld = domainType
```

```
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK ListPrices中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 列出路由 53 域註冊註冊域

下列程式碼範例示範如何列出已註冊網域。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
        }
        return results;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考ListDomains中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
+ content.domainName()));
```

```
        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考ListDomains中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun listDomains() {
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK ListDomains中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 列出路由 53 網域註冊作業

下列程式碼範例示範如何列出操作。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考ListOperations中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void listOperations(Route53DomainsClient route53DomainsClient)
{
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           localDateTime = localDateTime.minusYears(1);
           Instant myTime = localDateTime.toInstant(zoneOffset);

           ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
                   .submittedSince(myTime)
                   .build();

           ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
           listRes.stream()
                   .flatMap(r -> r.operations().stream())
                   .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                           " Status: " + content.statusAsString() +
                           " Date: " + content.submittedDate()));

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考ListOperations中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest = ListOperationsRequest {
        submittedSince = time2
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK ListOperations中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 使用 Route 53 網域註冊註冊網域

下列程式碼範例示範如何註冊網域。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
 and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
```

```
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
{domainName}");
            return null;
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考RegisterDomain中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
            String domainSuggestion,
            String phoneNumber,
            String email,
            String firstName,
            String lastName,
            String city) {
```

```
        try {
            ContactDetail contactDetail = ContactDetail.builder()
                    .contactType(ContactType.COMPANY)
                    .state("LA")
                    .countryCode(CountryCode.IN)
                    .email(email)
                    .firstName(firstName)
                    .lastName(lastName)
                    .city(city)
                    .phoneNumber(phoneNumber)
                    .organizationName("My Org")
                    .addressLine1("My Address")
                    .zipCode("123 123")
                    .build();

            RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                    .adminContact(contactDetail)
                    .registrantContact(contactDetail)
                    .techContact(contactDetail)
                    .domainName(domainSuggestion)
                    .autoRenew(true)
                    .durationInYears(1)
                    .build();

            RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
            System.out.println("Registration requested. Operation Id: " +
response.operationId());
            return response.operationId();

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考RegisterDomain中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun requestDomainRegistration(domainSuggestion: String?, phoneNumberVal:
 String?, emailVal: String?, firstNameVal: String?, lastNameVal: String?,
 cityVal: String?): String? {
    val contactDetail = ContactDetail {
        contactType = ContactType.Company
        state = "LA"
        countryCode = CountryCode.In
        email = emailVal
        firstName = firstNameVal
        lastName = lastNameVal
        city = cityVal
        phoneNumber = phoneNumberVal
        organizationName = "My Org"
        addressLine1 = "My Address"
        zipCode = "123 123"
    }

    val domainRequest = RegisterDomainRequest {
        adminContact = contactDetail
        registrantContact = contactDetail
        techContact = contactDetail
        domainName = domainSuggestion
        autoRenew = true
        durationInYears = 1
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK RegisterDomain中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 檢視 Route 53 網域註冊帳單記錄

下列程式碼範例示範如何檢視帳單記錄。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 網域入門

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
```

```
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考ViewBilling中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           LocalDateTime localDateTime2 = localDateTime.minusYears(1);
           Instant myStartTime = localDateTime2.toInstant(zoneOffset);
           Instant myEndTime = localDateTime.toInstant(zoneOffset);

           ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                   .start(myStartTime)
                   .end(myEndTime)
                   .build();

           ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
```

```
            listRes.stream()
                    .flatMap(r -> r.billingRecords().stream())
                    .forEach(content -> System.out.println(" Bill Date:: " +
 content.billDate() +
                            " Operation: " + content.operationAsString() +
                            " Price: " + content.price()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考ViewBilling中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest = ViewBillingRequest {
        start = timeStart
        end = timeEnd
    }
```

```
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK ViewBilling中的 Kotlin API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 進行路由 53 網域註冊的案例

下列程式碼範例會示範如何在使用 AWS SDK 的 Route 53 網域註冊中實作常見案例。這些案例會展示如何呼叫 Route 53 網域註冊中的多個函數，以完成特定任務。每個案例都包含一個連結 GitHub，您可以在其中找到如何設定和執行程式碼的指示。

範例

- 使用 AWS SDK 開始使用路線 53 網域註冊

使用 AWS SDK 開始使用路線 53 網域註冊

下列程式碼範例示範如何：

- 列出目前網域和過去一年的操作。
- 檢視過去一年的帳單和網域類型對應的價格。
- 取得網域建議。
- 檢查網域的可用性和可轉移性。
- 或者，要求網域註冊。
- 取得操作詳細資訊。
- 或者，取得網域詳細資訊。

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

在命令提示中執行互動式案例。

```
public static class Route53DomainScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.

    This .NET example performs the following tasks:
        1. List current domains.
        2. List operations in the past year.
        3. View billing for the account in the past year.
        4. View prices for domain types.
        5. Get domain suggestions.
        6. Check domain availability.
        7. Check domain transferability.
        8. Optionally, request a domain registration.
        9. Get an operation detail.
       10. Optionally, get a domain detail.
   */

    private static Route53Wrapper _route53Wrapper = null!;
    private static IConfiguration _configuration = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
```

```
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
                    .ConfigureServices((_, services) =>
            services.AddAWSService<IAmazonRoute53Domains>()
                .AddTransient<Route53Wrapper>()
            )
            .Build();

        _configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load settings from .json file.
            .AddJsonFile("settings.local.json",
                true) // Optionally, load local settings.
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(Route53DomainScenario));

        _route53Wrapper = host.Services.GetRequiredService<Route53Wrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the Amazon Route 53 domains example
scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            await ListDomains();
            await ListOperations();
            await ListBillingRecords();
            await ListPrices();
            await ListDomainSuggestions();
            await CheckDomainAvailability();
            await CheckDomainTransferability();
            var operationId = await RequestDomainRegistration();
            await GetOperationalDetail(operationId);
            await GetDomainDetails();
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
```

```
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("The Amazon Route 53 domains example scenario is
complete.");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List account registered domains.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomains()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"1. List account domains.");
        var domains = await _route53Wrapper.ListDomains();
        for (int i = 0; i < domains.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {domains[i].DomainName}");
        }

        if (!domains.Any())
        {
            Console.WriteLine("\tNo domains found in this account.");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain operations in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListOperations()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"2. List account domain operations in the past
year.");
        var operations = await _route53Wrapper.ListOperations(
            DateTime.Today.AddYears(-1));
        for (int i = 0; i < operations.Count; i++)
        {
            Console.WriteLine($"\tOperation Id: {operations[i].OperationId}");
            Console.WriteLine($"\tStatus: {operations[i].Status}");
```

```
            Console.WriteLine($"\tDate: {operations[i].SubmittedDate}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List billing in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListBillingRecords()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"3. View billing for the account in the past year.");
        var billingRecords = await _route53Wrapper.ViewBilling(
            DateTime.Today.AddYears(-1),
            DateTime.Today);
        for (int i = 0; i < billingRecords.Count; i++)
        {
            Console.WriteLine($"\tBill Date:
{billingRecords[i].BillDate.ToShortDateString()}");
            Console.WriteLine($"\tOperation: {billingRecords[i].Operation}");
            Console.WriteLine($"\tPrice: {billingRecords[i].Price}");
        }
        if (!billingRecords.Any())
        {
            Console.WriteLine("\tNo billing records found in this account for the
past year.");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List prices for a few domain types.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListPrices()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. View prices for domain types.");
        var domainTypes = new List<string> { "net", "com", "org", "co" };

        var prices = await _route53Wrapper.ListPrices(domainTypes);
        foreach (var pr in prices)
        {
```

```
            Console.WriteLine($"\tName: {pr.Name}");
            Console.WriteLine($"\tRegistration: {pr.RegistrationPrice?.Price}
{pr.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {pr.RenewalPrice?.Price}
{pr.RenewalPrice?.Currency}");
            Console.WriteLine($"\tTransfer: {pr.TransferPrice?.Price}
{pr.TransferPrice?.Currency}");
            Console.WriteLine($"\tChange Ownership:
{pr.ChangeOwnershipPrice?.Price} {pr.ChangeOwnershipPrice?.Currency}");
            Console.WriteLine($"\tRestoration: {pr.RestorationPrice?.Price}
{pr.RestorationPrice?.Currency}");
            Console.WriteLine();
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain suggestions for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomainSuggestions()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"5. Get domain suggestions.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to get available domain
suggestions.");
            domainName = Console.ReadLine();
        }

        var suggestions = await _route53Wrapper.GetDomainSuggestions(domainName,
true, 5);
        foreach (var suggestion in suggestions)
        {
            Console.WriteLine($"\tSuggestion Name: {suggestion.DomainName}");
            Console.WriteLine($"\tAvailability: {suggestion.Availability}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check availability for a domain name.
```

```
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainAvailability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Check domain availability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
availability.");
            domainName = Console.ReadLine();
        }

        var availability = await
_route53Wrapper.CheckDomainAvailability(domainName);
        Console.WriteLine($"\tAvailability: {availability}");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainTransferability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Check domain transferability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
transferability.");
            domainName = Console.ReadLine();
        }

        var transferability = await
_route53Wrapper.CheckDomainTransferability(domainName);
        Console.WriteLine($"\tTransferability: {transferability}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
```

```
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> RequestDomainRegistration()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. Optionally, request a domain registration.");

        Console.WriteLine($"\tNote: This example uses domain request settings in
 settings.json.");
        Console.WriteLine($"\tTo change the domain registration settings, set the
 values in that file.");
        Console.WriteLine($"\tRemember, registering an actual domain will incur
 an account billing cost.");
        Console.WriteLine($"\tWould you like to begin a domain registration? (y/
n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase))
        {
            string domainName = _configuration["DomainName"];
            ContactDetail contact = new ContactDetail();
            contact.CountryCode =
 CountryCode.FindValue(_configuration["Contact:CountryCode"]);
            contact.ContactType =
 ContactType.FindValue(_configuration["Contact:ContactType"]);

            _configuration.GetSection("Contact").Bind(contact);

            var operationId = await _route53Wrapper.RegisterDomain(
                domainName,
                Convert.ToBoolean(_configuration["AutoRenew"]),
                Convert.ToInt32(_configuration["DurationInYears"]),
                contact);
            if (operationId != null)
            {
                Console.WriteLine(
                    $"\tRegistration requested. Operation Id: {operationId}");
            }

            return operationId;
        }

        Console.WriteLine(new string('-', 80));
```

```
        return null;
    }

    /// <summary>
    /// Get details for an operation.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task GetOperationalDetail(string? operationId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Get an operation detail.");

        var operationDetails =
            await _route53Wrapper.GetOperationDetail(operationId);

        Console.WriteLine(operationDetails);

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Optionally, get details for a registered domain.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> GetDomainDetails()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Get details on a domain.");

        Console.WriteLine($"\tNote: you must have a registered domain to get
details.");
        Console.WriteLine($"\tWould you like to get domain details? (y/n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
StringComparison.InvariantCultureIgnoreCase))
        {
            string? domainName = null;
            while (domainName == null)
            {
                Console.WriteLine($"\tEnter a domain name to get details.");
                domainName = Console.ReadLine();
            }
```

```
            var domainDetails = await
 _route53Wrapper.GetDomainDetail(domainName);
            Console.WriteLine(domainDetails);
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }
}
```

Route 53 網域註冊動作案例使用的包裝函式方式。

```
public class Route53Wrapper
{
    private readonly IAmazonRoute53Domains _amazonRoute53Domains;
    private readonly ILogger<Route53Wrapper> _logger;
    public Route53Wrapper(IAmazonRoute53Domains amazonRoute53Domains,
 ILogger<Route53Wrapper> logger)
    {
        _amazonRoute53Domains = amazonRoute53Domains;
        _logger = logger;
    }


    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
 ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }
```

```
    /// <summary>
    /// Check the availability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for availability.</param>
    /// <returns>An availability result string.</returns>
    public async Task<string> CheckDomainAvailability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
            new CheckDomainAvailabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Availability.Value;
    }


    /// <summary>
    /// Check the transferability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for transferability.</param>
    /// <returns>A transferability result string.</returns>
    public async Task<string> CheckDomainTransferability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
            new CheckDomainTransferabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }


    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
```

```
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }


    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
```

```
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }


    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
 and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
 {domainName}");
            return null;
```

```
        }
    }


    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }


    /// <summary>
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
```

```
        }
        return results;
    }


    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }


    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
```

```
                            $"\tCreated on
 {result.CreationDate.ToShortDateString()}.\n" +
                            $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                            $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
}
```

- 如需 API 詳細資訊，請參閱《AWS SDK for .NET API 參考》中的下列主題。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example uses pagination methods where applicable. For example, to list
 * domains, the
 * listDomainsPaginator method is used. For more information about pagination,
 * see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/
pagination.html
 *
 * This Java code example performs the following operations:
 *
 * 1. List current domains.
 * 2. List operations in the past year.
 * 3. View billing for the account in the past year.
 * 4. View prices for domain types.
 * 5. Get domain suggestions.
 * 6. Check domain availability.
 * 7. Check domain transferability.
 * 8. Request a domain registration.
 * 9. Get operation details.
 * 10. Optionally, get domain details.
 */

public class Route53Scenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <domainType> <phoneNumber> <email> <domainSuggestion>
 <firstName> <lastName> <city>

                Where:
```

```
                    domainType - The domain type (for example, com).\s
                    phoneNumber - The phone number to use (for example,
+91.9966564xxx)      email - The email address to use.      domainSuggestion -
The domain suggestion (for example, findmy.accountants).\s
                    firstName - The first name to use to register a domain.\s
                    lastName -  The last name to use to register a domain.\s
                    city - the city to use to register a domain.\s
                    """;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        String phoneNumber = args[1];
        String email = args[2];
        String domainSuggestion = args[3];
        String firstName = args[4];
        String lastName = args[5];
        String city = args[6];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the Amazon Route 53 domains example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. List current domains.");
        listDomains(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. List operations in the past year.");
        listOperations(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. View billing for the account in the past year.");
```

```
        listBillingRecords(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. View prices for domain types.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Get domain suggestions.");
        listDomainSuggestions(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Check domain availability.");
        checkDomainAvailability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Check domain transferability.");
        checkDomainTransferability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Request a domain registration.");
        String opId = requestDomainRegistration(route53DomainsClient,
domainSuggestion, phoneNumber, email, firstName,
                lastName, city);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Get operation details.");
        getOperationalDetail(route53DomainsClient, opId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get domain details.");
        System.out.println("Note: You must have a registered domain to get
details.");
        System.out.println("Otherwise, an exception is thrown that states ");
        System.out.println("Domain xxxxxxx not found in xxxxxxx account.");
        getDomainDetails(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);
    }
```

```
   public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
           System.out.println("The contact first name is " +
response.registrantContact().firstName());
           System.out.println("The contact last name is " +
response.registrantContact().lastName());
           System.out.println("The contact org name is " +
response.registrantContact().organizationName());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }

   public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
       try {
           GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                   .operationId(operationId)
                   .build();

           GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
           System.out.println("Operation detail message is " +
response.message());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

```
   public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
           String domainSuggestion,
           String phoneNumber,
           String email,
           String firstName,
           String lastName,
           String city) {

       try {
           ContactDetail contactDetail = ContactDetail.builder()
                   .contactType(ContactType.COMPANY)
                   .state("LA")
                   .countryCode(CountryCode.IN)
                   .email(email)
                   .firstName(firstName)
                   .lastName(lastName)
                   .city(city)
                   .phoneNumber(phoneNumber)
                   .organizationName("My Org")
                   .addressLine1("My Address")
                   .zipCode("123 123")
                   .build();

           RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                   .adminContact(contactDetail)
                   .registrantContact(contactDetail)
                   .techContact(contactDetail)
                   .domainName(domainSuggestion)
                   .autoRenew(true)
                   .durationInYears(1)
                   .build();

           RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
           System.out.println("Registration requested. Operation Id: " +
response.operationId());
           return response.operationId();

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
       return "";
```

```
   }

   public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainTransferabilityResponse response = route53DomainsClient
                   .checkDomainTransferability(transferabilityRequest);
           System.out.println("Transferability: " +
response.transferability().transferable().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }

   public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainAvailabilityResponse response = route53DomainsClient
                   .checkDomainAvailability(availabilityRequest);
           System.out.println(domainSuggestion + " is " +
response.availability().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }

   public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
```

```
            GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                    .domainName(domainSuggestion)
                    .suggestionCount(5)
                    .onlyAvailable(true)
                    .build();

            GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .tld(domainType)
                    .build();

            ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
            listRes.stream()
                    .flatMap(r -> r.prices().stream())
                    .forEach(content -> System.out.println(" Name: " +
content.name() +
                            " Registration: " +
content.registrationPrice().price() + " "
                            + content.registrationPrice().currency() +
                            " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
```

```
            System.exit(1);
        }
    }

    public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            LocalDateTime localDateTime2 = localDateTime.minusYears(1);
            Instant myStartTime = localDateTime2.toInstant(zoneOffset);
            Instant myEndTime = localDateTime.toInstant(zoneOffset);

            ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                    .start(myStartTime)
                    .end(myEndTime)
                    .build();

            ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
            listRes.stream()
                    .flatMap(r -> r.billingRecords().stream())
                    .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                            " Operation: " + content.operationAsString() +
                            " Price: " + content.price()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listOperations(Route53DomainsClient route53DomainsClient)
{
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            localDateTime = localDateTime.minusYears(1);
            Instant myTime = localDateTime.toInstant(zoneOffset);
```

```
            ListOperationsRequest operationsRequest =
 ListOperationsRequest.builder()
                    .submittedSince(myTime)
                    .build();

            ListOperationsIterable listRes =
 route53DomainsClient.listOperationsPaginator(operationsRequest);
            listRes.stream()
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
 content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
 route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
 + content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- 如需 API 詳細資訊，請參閱《AWS SDK for Java 2.x API 參考》中的下列主題。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail

- GetDomainSuggestions
- GetOperationDetail
- ListDomains
- ListOperations
- ListPrices
- RegisterDomain
- ViewBilling

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This Kotlin code example performs the following operations:

1. List current domains.
2. List operations in the past year.
3. View billing for the account in the past year.
4. View prices for domain types.
5. Get domain suggestions.
6. Check domain availability.
7. Check domain transferability.
8. Request a domain registration.
9. Get operation details.
10. Optionally, get domain details.
 */
```

```
val DASHES: String = String(CharArray(80)).replace("\u0000", "-")
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType> <phoneNumber> <email> <domainSuggestion> <firstName>
 <lastName> <city>
        Where:
           domainType - The domain type (for example, com).
           phoneNumber - The phone number to use (for example, +1.2065550100)

           email - The email address to use.
           domainSuggestion - The domain suggestion (for example,
 findmy.example).
           firstName - The first name to use to register a domain.
           lastName -  The last name to use to register a domain.
           city - The city to use to register a domain.
    """

    if (args.size != 7) {
        println(usage)
        exitProcess(1)
    }

    val domainType = args[0]
    val phoneNumber = args[1]
    val email = args[2]
    val domainSuggestion = args[3]
    val firstName = args[4]
    val lastName = args[5]
    val city = args[6]

    println(DASHES)
    println("Welcome to the Amazon Route 53 domains example scenario.")
    println(DASHES)

    println(DASHES)
    println("1. List current domains.")
    listDomains()
    println(DASHES)

    println(DASHES)
    println("2. List operations in the past year.")
    listOperations()
    println(DASHES)
```

```
    println(DASHES)
    println("3. View billing for the account in the past year.")
    listBillingRecords()
    println(DASHES)

    println(DASHES)
    println("4. View prices for domain types.")
    listAllPrices(domainType)
    println(DASHES)

    println(DASHES)
    println("5. Get domain suggestions.")
    listDomainSuggestions(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("6. Check domain availability.")
    checkDomainAvailability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("7. Check domain transferability.")
    checkDomainTransferability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("8. Request a domain registration.")
    val opId = requestDomainRegistration(domainSuggestion, phoneNumber, email,
firstName, lastName, city)
    println(DASHES)

    println(DASHES)
    println("9. Get operation details.")
    getOperationalDetail(opId)
    println(DASHES)

    println(DASHES)
    println("10. Get domain details.")
    println("Note: You must have a registered domain to get details.")
    println("Otherwise an exception is thrown that states ")
    println("Domain xxxxxxx not found in xxxxxxx account.")
    getDomainDetails(domainSuggestion)
    println(DASHES)
```

```
}

suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest = GetDomainDetailRequest {
        domainName = domainSuggestion
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}

suspend fun getOperationalDetail(opId: String?) {
    val detailRequest = GetOperationDetailRequest {
        operationId = opId
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}

suspend fun requestDomainRegistration(domainSuggestion: String?, phoneNumberVal:
 String?, emailVal: String?, firstNameVal: String?, lastNameVal: String?,
 cityVal: String?): String? {
    val contactDetail = ContactDetail {
        contactType = ContactType.Company
        state = "LA"
        countryCode = CountryCode.In
        email = emailVal
        firstName = firstNameVal
        lastName = lastNameVal
        city = cityVal
        phoneNumber = phoneNumberVal
        organizationName = "My Org"
        addressLine1 = "My Address"
        zipCode = "123 123"
    }
```

```
    val domainRequest = RegisterDomainRequest {
        adminContact = contactDetail
        registrantContact = contactDetail
        techContact = contactDetail
        domainName = domainSuggestion
        autoRenew = true
        durationInYears = 1
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}

suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest = CheckDomainTransferabilityRequest {
        domainName = domainSuggestion
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}

suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest = CheckDomainAvailabilityRequest {
        domainName = domainSuggestion
    }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
    }
}

suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest = GetDomainSuggestionsRequest {
        domainName = domainSuggestion
        suggestionCount = 5
        onlyAvailable = true
    }
```

```
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
            println(" ")
        }
    }
}

suspend fun listAllPrices(domainType: String?) {
    val pricesRequest = ListPricesRequest {
        tld = domainType
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
}

suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest = ViewBillingRequest {
```

```
        start = timeStart
        end = timeEnd
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}

suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest = ListOperationsRequest {
        submittedSince = time2
    }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}

suspend fun listDomains() {
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient.listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
```

```
            }
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS 適用於 Kotlin 的 SDK API 參考中的下列主題。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 Route 53。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

Amazon Route 53 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同的責任。共同的責任模型 將此描述為雲端 本身 的安全和雲端內部的安全：

- 雲端本身的安全：AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Amazon Route 53 的合規計劃，請參閱合規計劃範圍內的 AWS 服務。
- 雲端內部的安全：您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Route 53 時套用共同責任模型。下列主題將示範如何設定 Route 53 以達到您的安全和合規目標。您也會了解如何使用其他 AWS 服務來協助監控並保護 Route 53 資源。

主題

- Route 53 中的資料保護
- Amazon Route 53 中的身分和存取管理
- 在 Amazon Route 53 中進行記錄和監控
- Amazon Route 53 的合規驗證
- Amazon Route 53 中的恢復能力
- Amazon Route 53 的基礎設施安全性

Route 53 中的資料保護

AWS 共同責任模型適用於 Amazon Route 53 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您必須負責維護在此基礎設施上託管之內容的控制權。您還要負責您所使用的 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如 Name (名稱) 欄位。這包括當您使用主控台、API、AWS CLI 或 AWS SDK 來利用 Route 53 或其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

防止在 Route 53 中懸置委派記錄

藉由 Route 53，您可以透過建立 NS 記錄將流量路由到子網域。當這些 NS 記錄指向 Route 53 名稱伺服器時，名稱伺服器預期會與子網域的授權託管區域委派集中的名稱伺服器相符。如果這些 NS 記錄未指向正確的名稱伺服器，則會暴露攻擊者可能會利用並控制子網域的風險。這些即稱為懸置的 NS 記錄。

例如，刪除子網域的 Route 53 託管區域時，其 NS 記錄在父網域中可能會懸置。發生這種情況時，攻擊者可以透過在已刪除區域的名稱服務器上建立新的託管區域來攔截子網域。Route 53 會嘗試防止這種情況發生，方法是追蹤子網域委派集配對，在移除懸置的 NS 記錄之前，不允許在這些名稱伺服器上建立任何子網域新區域。

但是，由於 NS 記錄設定錯誤，仍然可能會出現懸置的 NS 記錄。為了減輕此風險，我們建議您採取以下動作：

- 確定子網域授權 Route 53 託管區域的 Apex NS 記錄符合託管區域的委派集。您可以透過 Route 53 主控台或 AWS CLI 尋找託管區域的委派集。如需詳細資訊，請參閱 列出記錄 或 get-hosted-zone。
- 針對 Route 53 託管區域啟用 DNSSEC 簽署。DNSSEC 會驗證 DNS 回答來自授權來源，有效防止風險。如需詳細資訊，請參閱在 Amazon Route 53 中設定 DNSSEC 簽署。
- 從父託管區域的子網域 NS 記錄中移除不託管子網域的名稱伺服器。

  - 或 -

- 將名稱伺服器取代為子網域授權 Route 53 託管區域委派集中的四個名稱伺服器。這樣也可有效降低風險。

範例

在下面的範例中，我們假設您有一個父網域 parent-domain.com 和一個子網域 sub-domain.parent-domain.com，並說明存在懸置 NS 記錄的三個案例以及如何降低風險。

方案 1：

在父託管區域 parent-domain.com 中，您可以為 sub-domain.parent-domain.com 建立包含四個名稱伺服器 <ns1>、<ns2>、<ns3> 和 <ns4> 的 NS 記錄。且權威子網域的名稱伺服器為 <ns5>、<ns6>、<ns7> 和 <ns8>。因此，<ns1>、<ns2>、<ns3> 和 <ns4> 都是懸置的 NS 記錄，並且暴露出攻擊者可以獲得 sub-domain.parent-domain.com 控制權的風險。若要降低風險，請將子網域 NS 記錄取代為 <ns5>、<ns6>、<ns7> 和 <ns8>。

方案 2：

parent-domain.com 擁有指向 <ns1>、<ns2>、<ns3>、<ns4>、<ns5>、<ns6>、<ns7> 和 <ns8> 的 sub-domain.parent-domain.com NS 記錄。授權子網域託管區域的名稱伺服器為 <ns5>、<ns6>、<ns7> 和 <ns8>。因此，<ns1>、<ns2>、<ns3> 和 <ns4> 都再一次成為懸置的 NS 記錄。若要降低風險，請從 NS 記錄中移除 <ns1>、<ns2>、<ns3> 和 <ns4>。

案例 3：

您有可重複使用的委派集 <ns1>、<ns2>、<ns3> 和 <ns4>。您可以在父區域中建立 NS 記錄，並將子網域委派給可重複使用的委派集中的這些名稱伺服器。但是，您尚未在可重複使用的委派集上建立子網域區域。因此，<ns1>、<ns2>、<ns3> 和 <ns4> 都是懸置的 NS 記錄。若要降低風險，請使用可重複使用的委派集建立子網域託管區域。

Amazon Route 53 中的身分和存取管理

若要在 Amazon Route 53 資源上執行任何操作 (例如註冊網域或更新記錄)，AWS Identity and Access Management (IAM) 都會要求您進行身分驗證，確認您是已核准的 AWS 使用者。如果您使用 Route 53 主控台，可透過提供 AWS 使用者名稱和密碼來驗證您的身分。

在驗證您的身分之後，IAM 會透過確認您是否有執行操作和存取資源的許可，控制您對 AWS 的存取。如果您是帳戶管理員，您可以使用 IAM 控制其他使用者能否存取您的帳戶相關資源。

本章說明如何使用 IAM 和 Route 53，協助保護您的資源。

主題

- 使用身分驗證

- 存取控制
- 管理 Amazon Route 53 資源存取許可的概觀
- 將以身分為基礎的政策 (IAM 政策) 用於 Amazon Route 53
- 使用 Amazon Route 53 Resolver 的服務連結角色
- Amazon Route 53 的 AWS 受管政策
- 使用 IAM 政策條件進行精細定義存取控制，以便管理資源記錄集
- Amazon Route 53 API 許可：動作、資源和條件參考

使用身分驗證

身分驗證是使用身分憑證登入 AWS 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者身分，或擔任 IAM 角色進行 驗證 (登入至 AWS)。

您可以使用透過身分來源 AWS IAM Identity Center 提供的憑證，以聯合身分登入 AWS。(IAM Identity Center) 使用者、貴公司的單一登入身分驗證和您的 Google 或 Facebook 憑證都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。您 AWS 藉由使用聯合進行存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入至 AWS 的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

如果您是以程式設計的方式存取 AWS，AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的憑證透過密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 以提高帳戶的安全。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的在 AWS 中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者 (包括需要管理員存取權的使用者)搭配身分提供者使用聯合功能，使用暫時憑證來存取 AWS 服務。

聯合身分是來自您企業使用者目錄的使用者、Web 身分供應商、AWS Directory Service、Identity Center 目錄或透過身分來源提供的憑證來存取 AWS 服務 的任何使用者。聯合身分存取 AWS 帳戶時，會擔任角色，並由角色提供暫時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分來源中的一組使用者和群組，以便在您的所有 AWS 帳戶和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱《AWS IAM Identity Center 使用者指南》中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您 AWS 帳戶 中的一種身分，具備單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分登入。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的過程變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱《IAM 使用者指南》中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並取得由角色定義的許可。如需有關聯合角色

的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html中的為第三方身分供應商建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱《AWS IAM Identity Center 使用者指南》中的許可集。

- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳户存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳户存取權的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色作為代理)。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源類型政策的差異。
- 跨服務存取 – 有些 AWS 服務 會使用其他 AWS 服務 中的功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉發存取工作階段 (FAS)：當您使用 IAM 使用者或角色在 AWS 中執行動作時，系統會將您視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。只有在服務收到需要與其他 AWS 服務 或資源互動才能完成的請求之後，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色：服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務 服務。
  - 服務連結角色 – 服務連結角色是一種連結到 AWS 服務 的服務角色類型。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 AWS 帳戶 中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理暫時憑證。這是在 EC2 執行個體內儲存存取金鑰的較好方式。如需指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的建立 IAM 角色 (而非使用者) 的時機。

存取控制

若要建立、更新、刪除或列出 Amazon Route 53 資源，您需要有執行操作的許可，而且也需要有存取對應資源的許可。

以下章節說明如何管理 Route 53 的許可。我們建議您先閱讀概觀。

管理 Amazon Route 53 資源存取許可的概觀

每項 AWS 資源均由某個 AWS 帳戶所持有，而建立或存取資源的許可則由許可政策管理。

> **Note**
>
> 帳戶管理員 (或管理員使用者) 是具有管理員許可的使用者。如需管理員的詳細資訊，請參閱 IAM 使用者指南中的 IAM 最佳實務。

授予許可時，您會決定誰取得這些許可、取得許可的資源，以及他們有權執行的動作。

若使用者想要與 AWS Management Console 之外的 AWS 互動，則需要程式設計存取權。授予程式設計存取權的方式取決於存取 AWS 的使用者類型。

若要授予使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請依照您要使用的介面所提供的指示操作。 • 關於 AWS CLI，請參閱 AWS Command Line Interface使用者指南 中的 設定 AWS CLI 來使用 AWS IAM Identity Center。 • 關於 AWS SDKs、工具和 AWS APIs，請參閱 AWSSDKs 和工具參考指南

哪個使用者需要程式設計存取權？	到	By
		中的 IAM Identity Center 驗證。
IAM	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請遵循 IAM 使用者指南 中 使用臨時憑證搭配 AWS 資源 中的指示。
IAM	(不建議使用) 使用長期憑證簽署 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 關於 AWS CLI，請參閱 AWS Command Line Interface使用者指南 中的 使用 IAM 使用者憑證進行驗證。 • 關於 AWS SDKs 和工具，請參閱 AWSSDKs 和工具參考指南 中的 使用長期憑證進行驗證。 • 關於 AWS API，請參閱 IAM 使用者指南 中的 管理 IAM 使用者的存取金鑰。

主題

- Amazon Route 53 資源的 ARN
- 了解資源所有權
- 管理資源存取
- 指定政策元素：資源、動作、效果和委託人
- 在政策中指定條件

Amazon Route 53 資源的 ARN

Amazon Route 53 支援用於 DNS、運作狀態檢查和網域註冊的各種資源類型。在政策，您可以透過將 * 用於 ARN，授與或拒絕下列資源的存取：

- 運作狀態檢查
- 託管區域
- 可重複使用的委派組
- 資源記錄集變更批次的狀態 (API)
- 流量政策 (流量流程)
- 流量政策執行個體 (流量流程)

並不是所有 Route 53 資源都支援許可。您無法授與或拒絕以下資源的存取：

- 網域
- 個別記錄
- 網域的標籤
- 運作狀態檢查的標籤
- 託管區域的標籤

Route 53 提供 API 動作來處理這每一種類型的資源。如需詳細資訊，請參閱 Amazon Route 53 API 參考。如需為了授與或拒絕使用每個動作的許可而指定的動作和 ARN 清單，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

了解資源所有權

AWS 帳戶擁有在帳戶內所建立的資源，無論資源的建立者是誰。具體而言，資源擁有者就是對資源建立請求進行身分驗證的委託人實體 (即根帳戶或 IAM 角色) 的 AWS 帳戶。

下列範例說明其如何運作：

- 如果您使用 AWS 帳戶的根帳戶登入資料來建立託管區域，您的 AWS 帳戶即為資源擁有者。
- 如果您在 AWS 帳戶中建立使用者並授予該使用者建立託管區域的許可，該使用者就可以建立託管區域。但是您的 AWS 帳戶 (也是該使用者所屬的帳戶) 擁有該託管區域資源。
- 如果您在 AWS 帳戶中建立具有建立託管區域許可的 IAM 角色，則任何可以擔任該角色的人都能建立託管區域。您的 AWS 帳戶 (也是該角色所屬的帳戶) 擁有該託管區域資源。

管理資源存取

許可政策指定何人可存取何物。本節說明用來為 Amazon Route 53 建立許可政策的選項。如需 IAM 政策語法和說明的一般資訊，請參閱 IAM 使用者指南中的 AWS IAM 政策參考。

連接至 IAM 身分的政策稱為以身分為基礎的政策 (IAM 政策)，連接至資源的政策稱為以資源為基礎的政策。Route 53 僅支援以身分為基礎的政策 (IAM 政策)。

主題

- 身分類型政策 (IAM 政策)
- 資源型政策

身分類型政策 (IAM 政策)

您可以將政策連接到 IAM 身分。例如，您可以執行下列動作：

- 將許可政策連接至您帳戶中的使用者或群組 – 帳戶管理員可以使用與特定使用者相關聯的許可政策，來授與該使用者建立 Amazon Route 53 資源的許可。
- 將許可政策連接至角色 (授與跨帳戶許可) – 您可以對另一個 AWS 帳戶建立的使用者授予執行 Route 53 動作的許可。若要這樣做，請將許可政策連接至 IAM 角色，然後允許其他帳戶中的使用者擔任該角色。以下範例說明如何對兩個 AWS 帳戶 (帳戶 A 和帳戶 B) 執行此操作：
  1. 帳戶 A 管理員建立 IAM 角色，並將許可政策連接至該角色，來授予建立或存取帳戶 A 所擁有資源的許可。
  2. 帳戶 A 管理員將信任政策連接至該角色。信任政策識別帳戶 B 做為可擔任該角色的委託人。
  3. 然後，帳戶 B 管理員將擔任該角色的許可委派給帳戶 B 中的任何使用者或群組。這麼做可讓帳戶 B 中的使用者建立或存取帳戶 A 的資源。

  如需如何將許可委派給另一個 AWS 帳戶中的使用者的詳細資訊，請參閱 IAM 使用者指南中的存取管理。

以下範例政策可讓使用者執行 `CreateHostedZone` 動作，為任何 AWS 帳戶建立公有託管區域：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

如果您希望政策也套用至私有託管區域，您需要授與使用 Route 53 `AssociateVPCWithHostedZone` 動作和兩個 Amazon EC2 動作 (`DescribeVpcs` 和 `DescribeRegion`) 的許可，如下列範例所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegion"
            ],
            "Resource":"*"
        },
    ]
}
```

如需將政策連接至 Route 53 身分的詳細資訊，請參閱 將以身分為基礎的政策 (IAM 政策) 用於 Amazon Route 53。如需使用者、群組、角色和許可的詳細資訊，請參閱 IAM 使用者指南中的身分 (使用者、群組和角色)。

資源型政策

其他服務 (例如 Amazon S3) 也支援將許可政策連接到資源。例如，您可以將政策連接至 S3 儲存貯體，以管理該儲存貯體的存取許可。Amazon Route 53 不支援將政策連接到資源。

指定政策元素：資源、動作、效果和委託人

Amazon Route 53 包含 API 動作 (請參閱Amazon Route 53 API 參考)，您可以在每個 Route 53 資源上使用這些動作 (請參閱 Amazon Route 53 資源的 ARN)。您可以對使用者或聯合身分使用者授予執行任何或所有這些動作的許可。請注意，某些 API 動作 (例如註冊網域)，需要執行多個動作的許可。

以下是基本的政策元素：

- 資源 - 您使用 Amazon Resource Name (ARN) 識別欲套用政策的資源。如需詳細資訊，請參閱Amazon Route 53 資源的 ARN。
- 動作：使用動作關鍵字識別您要允許或拒絕的資源操作。例如，根據指定的 `Effect`，`route53:CreateHostedZone` 許可會允許或拒絕使用者執行 Route 53 `CreateHostedZone` 動作。
- 效果 - 您指定在使用者嘗試對指定資源執行動作時的效果 (允許或拒絕)。如果您不明確授與動作的存取權，將會隱含拒絕存取。您也可以明確拒絕資源存取，這樣做可確保使用者無法存取資源，即使不同政策授予存取也是一樣。
- 委託人：在以身分為基礎的政策 (IAM 政策) 中，政策所連接的使用者就是隱含委託人。對於資源型政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於資源型政策)。Route 53 不支援資源型政策。

如需 IAM 政策語法和說明的詳細資訊，請參閱 IAM 使用者指南中的 AWS IAM 政策參考。

如需顯示所有 Route 53 API 操作與其適用資源的清單，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

在政策中指定條件

當您授予許可時，您可以使用 IAM 政策語言指定政策生效時間。例如，建議只在特定日期之後套用政策。如需以政策語言指定條件的詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。

欲表示條件，您可以使用預先定義的條件金鑰。沒有 Route 53 特定的條件金鑰。不過，您可以視需要使用全 AWS 條件金鑰。如需全 AWS 金鑰的完整清單，請參閱 IAM 使用者指南中的可用的條件金鑰。

將以身分為基礎的政策 (IAM 政策) 用於 Amazon Route 53

本主題提供以身分為基礎的政策範例，此範例會示範帳戶管理員如何將許可政策連接至 IAM 身分，並藉此授與許可，以對 Amazon Route 53 資源執行操作。

> **Important**
>
> 建議您先檢閱簡介主題，這些主題說明管理 Route 53 資源存取的基本概念與選項。如需詳細資訊，請參閱 管理 Amazon Route 53 資源存取許可的概觀。

> **Note**
>
> 授與存取權時，託管區域和 Amazon VPC 必須屬於相同分割區。分割區是一組 AWS 區域。每個 AWS 帳戶 的範圍都限定在一個分割區。
> 以下是支援的分割區：
>
> - `aws` - AWS 區域
> - `aws-cn` - 中國區域
> - `aws-us-gov` - AWS GovCloud (US) Region
>
> 如需詳細資訊，請參閱 AWS 一般參考中的存取管理和 Amazon Route 53 端點和配額。

主題

- 使用 Amazon Route 53 主控台所需的許可
- 網域記錄擁有者的許可範例
- DNSSEC 簽署需要 Route 53 客戶受管金鑰許可
- 客戶受管政策範例

以下範例示範許可政策。`Sid` (陳述式 ID) 為選用：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "AllowPublicHostedZonePermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:UpdateHostedZoneComment",
                "route53:GetHostedZone",
```

```
                "route53:ListHostedZones",
                "route53:DeleteHostedZone",
                "route53:ChangeResourceRecordSets",
                "route53:ListResourceRecordSets",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZonesByName"
            ],
            "Resource": "*"
        },
        {
         "Sid" : "AllowHealthCheckPermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHealthCheck",
                "route53:UpdateHealthCheck",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:DeleteHealthCheck",
                "route53:GetCheckerIpRanges",
                "route53:GetHealthCheckCount",
                "route53:GetHealthCheckStatus",
                "route53:GetHealthCheckLastFailureReason"
            ],
            "Resource": "*"
        }
    ]
}
```

政策包含兩個陳述式：

- 第一個陳述式授予建立和管理公有託管區域及其記錄所需的動作的許可。Amazon Resource Name (ARN) 中的萬用字元 (*) 授與對目前 AWS 帳戶擁有的所有託管區域的存取權。
- 第二個陳述式授予建立和管理運作狀態檢查所需的動作的許可。

如需為了授與或拒絕使用每個動作的許可而指定的動作和 ARN 清單，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

使用 Amazon Route 53 主控台所需的許可

若要授予 Amazon Route 53 主控台的完整存取權，可在以下許可政策中授予許可：

```
{
```

```
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:*",
                "route53domains:*",
                "ssm:GetParametersByPath",
                "cloudfront:ListDistributions",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticbeanstalk:DescribeEnvironments",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketWebsite",
                "ec2:DescribeRegions",
                "ec2:DescribeVpcs",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic",
                "sns:CreateTopic",
                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:Sign",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/domainnames"
        }
```

```
    ]
}
```

需要許可的原因如下：

`route53:*`

可讓您執行以下除外的所有 Route 53 動作：

- 建立和更新別名目標值為 CloudFront 分配、Elastic Load Balancing 負載平衡器、彈性 Elastic Beanstalk 環境或 Amazon S3 儲存貯體的別名記錄。(透過這些許可，您可以建立 Alias Target (別名目標) 之值為相同託管區域中另一個記錄的別名記錄。)
- 使用私有託管區域。
- 使用網域。
- 建立、刪除和檢視 CloudWatch 警示。
- 在 Route 53 主控台中轉譯 CloudWatch 指標。

`route53domains:*`

可讓您使用網域。

> **Important**
>
> 如果您個別列出 `route53` 動作，則必須包含 `route53:CreateHostedZone` 才能使用網域。當您註冊網域，同時會建立託管區域，因此包含註冊網域許可的政策也需要建立託管區域的許可。

對於網域註冊，Route 53 不支援授與或拒絕個別資源許可。

`route53resolver:*`

可讓您使用 Route 53 Resolver。

`ssm:GetParametersByPath`

可讓您在建立新的別名記錄、私人託管區域和運作狀態檢查時擷取公開可用的區域。

`cloudfront:ListDistributions`

可讓您建立和更新別名目標值為 CloudFront 發佈的別名記錄。

如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的分佈清單。

elasticloadbalancing:DescribeLoadBalancers

可讓您建立和更新 Alias Target (別名目標) 之值為 ELB 負載平衡器的別名記錄。

如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的負載平衡器清單。

elasticbeanstalk:DescribeEnvironments

可讓您建立和更新 Alias Target (別名目標) 之值為 Elastic Beanstalk 環境的別名記錄。

如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的環境清單。

s3:ListAllMyBuckets、**s3:GetBucketLocation** 與 **s3:GetBucketWebsite**

可讓您建立和更新 Alias Target (別名目標) 之值為 Amazon S3 儲存貯體的別名記錄。(只有在儲存貯體設定為網站端點時，您才可以建立 Amazon S3 儲存貯體的別名； `s3:GetBucketWebsite` 會取得所需的組態資訊。)

如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的儲存貯體清單。

ec2:DescribeVpcs 和 **ec2:DescribeRegions**

可讓您使用私有託管區域。

所有列出的 **ec2** 許可

可讓您使用 Route 53 Resolver。

sns:ListTopics, **sns:ListSubscriptionsByTopic**, **sns:CreateTopic**, **cloudwatch:DescribeAlarms**, **cloudwatch:PutMetricAlarm**, **cloudwatch:DeleteAlarms**

可讓您建立、刪除和檢視 CloudWatch 警示。

cloudwatch:GetMetricStatistics

可讓您建立 CloudWatch 量度健康狀態檢查。

如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的統計資訊清單。

apigateway:GET

可讓您建立和更新 Alias Target (別名目標) 的值為 Amazon API Gateway API 的別名記錄。

如果未使用 Route 53 主控台，則不需要此許可。Route 53 只使用它來取得顯示在主控台中的 API 清單。

kms:*

可讓您使用 AWS KMS 以啟用 DNSSEC 簽署。

網域記錄擁有者的許可範例

透過資源記錄集許可，您可以設定 AWS 使用者的精細權限，限制其可以更新或修改哪些內容。如需詳細資訊，請參閱 使用 IAM 政策條件進行精細定義存取控制，以便管理資源記錄集。

在某些情況下，託管區域擁有者可能負責託管區域的整體管理，而組織中的其他人則負責這些任務的子集。例如，已啟用 DNSSEC 簽署的託管區域擁有者可能想要建立 IAM 政策，其中包含其他人在託管區域中新增和刪除資源集記錄 (RR) 的許可，以及執行其他任務的許可。託管區域擁有者選擇為記錄擁有者或其他人啟用的特定許可，將取決於其組織的政策。

以下是 IAM 政策範例，這些政策可讓記錄擁有者修改 RR、流量政策和運作狀態檢查。具有此政策的記錄擁有者不允許執行區域層級作業，例如建立或刪除區域、啟用或停用查詢日誌記錄、建立或刪除可重複使用的委派集，或變更 DNSSEC 設定。

```
{
      "Sid": "Do not allow zone-level modification ",
      "Effect": "Allow",
      "Action": [
        "route53:ChangeResourceRecordSets",
        "route53:CreateTrafficPolicy",
        "route53:DeleteTrafficPolicy",
        "route53:CreateTrafficPolicyInstance",
        "route53:CreateTrafficPolicyVersion",
        "route53:UpdateTrafficPolicyInstance",
        "route53:UpdateTrafficPolicyComment",
        "route53:DeleteTrafficPolicyInstance",
        "route53:CreateHealthCheck",
        "route53:UpdateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:List*",
        "route53:Get*"
      ],
      "Resource": [
        "*"
      ]
```

```
}
```

DNSSEC 簽署需要 Route 53 客戶受管金鑰許可

當您為 Route 53 啟用 DNSSEC 簽署時，Route 53 會根據客戶受管金鑰 AWS Key Management Service (AWS KMS) 建立金鑰簽署金鑰 (KSK)。您可以使用現有的客戶受管金鑰 (支援 DNSSEC 簽署) 或建立新的金鑰。Route 53 必須具有存取客戶受管金鑰的許可，才能為您建立 KSK。

若要啟用 Route 53 存取您的客戶受管金鑰，請確定您的客戶受管金鑰政策包含下列陳述式：

```
{
            "Sid": "Allow Route 53 DNSSEC Service",
            "Effect": "Allow",
            "Principal": {
                "Service": "dnssec-route53.amazonaws.com"
            },
            "Action": ["kms:DescribeKey",
                       "kms:GetPublicKey",
                       "kms:Sign"],
            "Resource": "*"
        },
        {
            "Sid": "Allow Route 53 DNSSEC to CreateGrant",
            "Effect": "Allow",
            "Principal": {
                "Service": "dnssec-route53.amazonaws.com"
            },
            "Action": ["kms:CreateGrant"],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
```

混淆代理問題屬於安全性議題，其中沒有動作許可的實體可以強制具有更多權限的實體執行該動作。若要保護您的 AWS KMS 以避免此情況，您可以選擇在資源型政策中限制服務對該資源所擁有的許可，方法是提供 aws:SourceAccount 和 aws:SourceArn 條件 (兩者或一個) 的組合。aws:SourceAccount 是一個託管區域擁有者的 AWS 帳戶 ID。aws:SourceArn 是託管區域的 ARN。

以下為您可以新增的許可的兩個示例：

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    }
},
```

- 或 -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

如需詳細資訊，請參閱《IAM 使用者指南》中的混淆代理問題。

客戶受管政策範例

您可以建立自訂 IAM 政策，授予執行 Route 53 動作的相關許可。您可以將這些自訂政策連接至需要指定許可的 IAM 群組。這些政策會在您使用 Route 53 API、AWS 開發套件或 AWS CLI 時運作。以下範例示範幾個常用案例的許可。如需授與使用者 Route 53完整存取權的政策，請參閱 使用 Amazon Route 53 主控台所需的許可。

範例

- 範例 1：允許讀取存取所有託管區域
- 範例 2：允許建立和刪除託管區域
- 範例 3：允許完整存取所有網域 (僅限公有託管區域)
- 範例 4：允許建立 Route 53 Resolver 端點的傳入和傳出

範例 1：允許讀取存取所有託管區域

以下許可政策為使用者授與列出所有託管區域和檢視託管區域中的所有記錄的許可。

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
    ]
}
```

範例 2：允許建立和刪除託管區域

以下許可政策允許使用者建立和刪除託管區域，以及追蹤變更進度。

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
```

```
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
}
```

範例 3：允許完整存取所有網域 (僅限公有託管區域)

以下許可政策允許使用者在網域註冊上執行所有動作，包括註冊網域和建立託管區域的許可。

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

當您註冊網域，同時會建立託管區域，因此包含註冊網域許可的政策也需要建立託管區域的許可。(對於網域註冊，Route 53 不支援授與個別資源許可。)

如需有關使用私有託管區域所需許可的詳細資訊，請參閱使用 Amazon Route 53 主控台所需的許可。

範例 4：允許建立 Route 53 Resolver 端點的傳入和傳出

下列許可政策可讓使用者使用 Route 53 主控台來建立 Resolver 傳入和傳出端點

其中一些許可僅在主控台中建立端點時才需要。如果您只是要以程式設計方式建立傳入和傳出端點而想要授與許可，可以忽略這些許可：

- route53resolver:ListResolverEndpoints 讓使用者查看傳入或傳出端點的清單，以便確認端點是否已建立。
- DescribeAvailabilityZones 是顯示可用區域清單的必要項。
- DescribeVpcs 是顯示 VPC 清單的必要項。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "route53resolver:CreateResolverEndpoint",
                "route53resolver:ListResolverEndpoints",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

使用 Amazon Route 53 Resolver 的服務連結角色

Route 53 Resolver 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 Resolver 的一種特殊 IAM 角色類型。服務連結角色由 Resolver 預先定義，內含該服務代您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 Resolver 更為簡單，因為您不必手動新增必要的許可。Resolver 定義其服務連結角色的許可，除非另有定義，否則僅有 Resolver 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須先刪除相關的資源，才能刪除服務連結角色。如此可保護您的 Resolver 資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的 AWS 服務，尋找 Service-Linked Role (服務連結角色) 欄顯示為是的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

主題

- Resolver 的服務連結角色許可
- 為 Resolver 建立服務連結角色
- 編輯 Resolver 的服務連結角色
- 刪除 Resolver 的服務連結角色
- Resolver 服務連結角色的支援區域

Resolver 的服務連結角色許可

Resolver 會使用 **AWSServiceRoleForRoute53Resolver** 服務連結角色，代表您傳遞查詢日誌。

角色許可政策允許 Resolver 在所有資源上完成下列動作：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 Resolver 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 Amazon Route 53 主控台、AWS CLI 或 AWS API 中建立解析器查詢日誌組態關聯時，Resolver 會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。另外，若您在 2020 年 8 月 12 日之前使用 Resolver 服務 (那時起開始支援服務連結角色)，Resolver 會於您的帳戶中建立 `AWSServiceRoleForRoute53Resolver` 角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立新的 Resolver 查詢日誌組態關聯時，會再度為您建立 `AWSServiceRoleForRoute53Resolver` 服務連結角色。

編輯 Resolver 的服務連結角色

Resolver 不允許您編輯 `AWSServiceRoleForRoute53Resolver` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Resolver 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 若 Resolver 服務在您試圖刪除資源時正在使用該角色，刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 **`AWSServiceRoleForRoute53Resolver`** 所使用的 Resolver 資源

1. 請登入 AWS Management Console，開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。

2. 展開 Route 53 主控台選單。在主控台的左上角，選擇三個水平橫條 (☰) 圖示。
3. 在 Resolver 選單內，選擇 Query logging (查詢日誌記錄)。
4. 選取查詢日誌記錄組態名稱旁的核取方塊，然後選擇 Delete (刪除)。
5. 在 Delete query logging configuration (刪除查詢日誌記錄組態) 文字方塊中，選取 Stop logging queries (停止日誌記錄查詢)。

   這將取消組態與 VPC 的關聯。您也可以透過程式設計方式取消查詢日誌記錄組態的關聯。如需詳細資訊，請參閱 disassociate-resolver-query-log-config。
6. 日誌記錄查詢停止後，您可以選擇性地在欄位中輸入 **delete**，然後選擇 Delete (刪除) 以刪除查詢日誌記錄組態。但是，刪除 `AWSServiceRoleForRoute53Resolver` 使用的資源不需要執行此操作。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、AWS CLI 或 AWS API 來刪除 `AWSServiceRoleForRoute53Resolver` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Resolver 服務連結角色的支援區域

Resolver 不支援在提供服務的每個區域中使用服務連結角色。您可以在下列區域中使用 `AWSServiceRoleForRoute53Resolver` 角色。

區域名稱	區域身分	Resolver 中的支援
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
亞太區域 (孟買)	ap-south-1	是
亞太區域 (大阪)	ap-northeast-3	是

區域名稱	區域身分	Resolver 中的支援
亞太區域 (首爾)	ap-northeast-2	是
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
歐洲 (巴黎)	eu-west-3	是
南美洲 (聖保羅)	sa-east-1	是
中國 (北京)	cn-north-1	是
中國 (寧夏)	cn-northwest-1	是
AWS GovCloud (US)	us-gov-east-1	是
AWS GovCloud (US)	us-gov-west-1	是

Amazon Route 53 的 AWS 受管政策

AWS 受管政策是由 AWS 建立和管理的獨立政策。AWS 受管政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授與您特定使用案例的最低權限許可，因為它們可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法更改 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies中的 AWS 受管政策。

AWS 受管政策：AmazonRoute53FullAccess

您可將 `AmazonRoute53FullAccess` 政策連接到 IAM 身分。

該政策將完整存取權授與 Route 53 資源，包括網域註冊和運作狀態檢查，但 Resolver 除外

許可詳細資訊

此政策包含以下許可。

- `route53:*` – 可讓您執行以下除外的所有 Route 53 動作：
  - 建立和更新 Alias Target (別名目標) 之值為 CloudFront 分佈、Elastic Load Balancing 負載平衡器、Elastic Beanstalk 環境或 Amazon S3 儲存貯體的別名記錄。(透過這些許可，您可以建立 Alias Target (別名目標) 之值為相同託管區域中另一個記錄的別名記錄。)
  - 使用私有託管區域。
  - 使用網域。
  - 建立、刪除和檢視 CloudWatch 警示。
  - 在 Route 53 主控台中轉譯 CloudWatch 指標。
- `route53domains:*` - 可讓您使用網域。
- `cloudfront:ListDistributions` – 可讓您建立和更新 Alias Target (別名目標) 之值為 CloudFront 分佈的別名記錄。

  如果未使用 Route 53 主控台，則不需要此許可。Route 53 只使用它來取得顯示在主控台中的分佈清單。
- `elasticloadbalancing:DescribeLoadBalancers` – 可讓您建立和更新 Alias Target (別名目標) 之值為 Elastic Load Balancing 負載平衡器的別名記錄。

  如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的負載平衡器清單。
- `elasticbeanstalk:DescribeEnvironments` – 可讓您建立和更新 Alias Target (別名目標) 之值為 Elastic Beanstalk 環境的別名記錄。

  如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的環境清單。

- `s3:ListBucket`、`s3:GetBucketLocation` 和 `s3:GetBucketWebsite` – 可讓您建立和更新 Alias Target (別名目標) 之值為 Amazon S3 儲存貯體的別名記錄。(只有在儲存貯體設定為網站端點時，您才可以建立 Amazon S3 儲存貯體的別名； `s3:GetBucketWebsite` 會取得所需的組態資訊。)

  如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的儲存貯體清單。
- `ec2:DescribeVpcs` – 可讓您顯示 VPC 清單。
- `ec2:DescribeVpcEndpoints` – 可讓您顯示 VPC 端點清單。
- `ec2:DescribeRegions` – 可讓您顯示可用區域清單。
- `sns:ListTopics`、`sns:ListSubscriptionsByTopic`、`cloudwatch:DescribeAlarms` - 可讓您建立、刪除和檢視 CloudWatch 警示。
- `cloudwatch:GetMetricStatistics` – 可讓您建立 CloudWatch 指標運作狀態檢查。

  如果未使用 Route 53 主控台，則不需要這些許可。Route 53 只使用它來取得顯示在主控台中的統計資訊清單。
- `apigateway:GET` – 可讓您建立和更新 Alias Target (別名目標) 的值為 Amazon API Gateway API 的別名記錄。

  如果未使用 Route 53 主控台，則不需要此許可。Route 53 只使用它來取得顯示在主控台中的儲存貯體清單。

如需許可的詳細資訊，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:*",
                "route53domains:*",
                "cloudfront:ListDistributions",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticbeanstalk:DescribeEnvironments",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketWebsite",
```

```
                "ec2:DescribeVpcs",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeRegions",
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/domainnames"
        }
    ]
}
```

AWS 受管政策：AmazonRoute53ReadOnlyAccess

您可將 AmazonRoute53ReadOnlyAccess 政策連接到 IAM 身分。

此政策將唯讀存取權授與 Route 53 資源，包括網域註冊和運作狀態檢查，但 Resolver 除外

許可詳細資訊

此政策包含以下許可。

- route53:Get* - 取得路由 Route 53 資源。
- route53:List* - 列出 Route 53 資源。
- route53:TestDNSAnswer - 取得 Route 53 為回應 DNS 要求所傳回的值。

如需許可的詳細資訊，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
```

```
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 受管政策：AmazonRoute53DomainsFullAccess

您可將 AmazonRoute53DomainsFullAccess 政策連接到 IAM 身分。

此政策授與 Route 53 網域註冊資源的完整存取權。

許可詳細資訊

此政策包含以下許可。

- route53:CreateHostedZone - 可讓您建立 Route 53 託管區域。
- route53domains:* - 可讓您註冊網域名稱並執行相關操作。

如需許可的詳細資訊，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 受管政策：AmazonRoute53DomainsReadOnlyAccess

您可將 AmazonRoute53DomainsReadOnlyAccess 政策連接到 IAM 身分。

此政策授與 Route 53 網域註冊資源的唯讀存取權。

許可詳細資訊

此政策包含以下許可。

- route53domains:Get* - 可讓您從 Route 53 擷取網域清單。
- route53domains:List* - 可讓您顯示 Route 53 網域的清單。

如需許可的詳細資訊，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 受管政策：AmazonRoute53ResolverFullAccess

您可將 AmazonRoute53ResolverFullAccess 政策連接到 IAM 身分。

此政策授與 Route 53 Resolver 資源的完整存取權。

許可詳細資訊

此政策包含以下許可。

- route53resolver:* - 可讓您在 Route 53 主控台上建立和管理 Resolver 資源。

- ec2:DescribeSubnets - 可讓您列出您的 Amazon VPC 子網路。
- ec2:CreateNetworkInterface、ec2:DeleteNetworkInterface h和 ec2:ModifyNetworkInterfaceAttribute - 可讓您建立、修改和刪除網路介面。
- ec2:DescribeNetworkInterfaces - 可讓您顯示網路介面清單。
- ec2:DescribeSecurityGroups - 可讓您顯示所有安全群組的清單。
- ec2:DescribeVpcs - 可讓您顯示 VPC 清單。
- ec2:DescribeAvailabilityZones - 可讓您列出可供您使用的區域。

如需許可的詳細資訊，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 受管政策：AmazonRoute53ResolverReadOnlyAccess

您可將 AmazonRoute53ResolverReadOnlyAccess 政策連接到 IAM 身分。

此政策授與 Route 53 解析程式資源的唯讀存取權。

許可詳細資訊

此政策包含以下許可。

- `route53resolver:Get*` - 可讓您擷取 Resolver 資源清單。
- `route53resolver:List*` - 可讓您顯示 Resolver 資源清單。
- `ec2:DescribeNetworkInterfaces` - 可讓您顯示網路介面清單。
- `ec2:DescribeSecurityGroups` - 可讓您顯示所有安全群組的清單。

如需許可的詳細資訊，請參閱 Amazon Route 53 API 許可：動作、資源和條件參考。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53resolver:Get*",
                "route53resolver:List*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 受管政策：Route53ResolverServiceRolePolicy

您無法連接 `Route53ResolverServiceRolePolicy` 至您的 IAM 實體。此政策會連接到服務連結角色，而該角色可讓 Route 53 Resolver 存取由 Resolver 使用或管理的 AWS 服務和資源。如需更多詳細資訊，請參閱 使用 Amazon Route 53 Resolver 的服務連結角色。

AWS 受管政策的 Route 53 更新項目

檢視自 Route 53 開始追蹤 AWS 受管政策變更以來的更新詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 Route 53 文件歷程記錄頁面上的 RSS 摘要。

變更	描述	日期
Route 53 開始追蹤變更	Route 53 開始追蹤其 AWS 受管政策的變更。	2021 年 7 月 14 日

使用 IAM 政策條件進行精細定義存取控制，以便管理資源記錄集

您在 Route 53 中授予資源記錄集的許可時，可以指定條件，以決定許可政策的生效方式。

您可在 Route 53 中指定使用 IAM 政策授予許可時的條件 (請參閱 存取控制)。例如，您可以：

- 授予許可以允許他人存取單一資源記錄集。
- 授予許可能讓使用者存取託管區域中特定 DNS 記錄類型的所有資源記錄集，例如 A 和 AAAA 記錄。
- 授予許可能讓使用者存取其名稱包含特定字串的資源記錄集。
- 授予權限以允許使用者僅在 Route 53 主控台上或使用 ChangeResourceRecordSetsAPI 時執行`CREATE | UPSERT | DELETE`動作的子集。

您也可以建立將任何精細權限合併在一起的權限。

使用 IAM `Condition` 元素來實作精細定義存取控制政策。在許可政策中新增 `Condition` 元素，即可根據業務需求而允許或拒絕對 Route 53 資源記錄集的存取行為。例如，您的 IAM 政策可以限制對託管區域中個別 DNS 記錄的存取行為。然後，您可以將政策套用至使用者、群組或角色。

正規化條件金鑰值

您在政策條件中輸入的值必須進行格式化或標準化，如下所示：

如果使用 **`route53:ChangeResourceRecordSetsNormalizedRecordNames`**：

- 所有字母必須小寫。
- DNS 名稱不可有行尾點號。
- a—z、0-9、- (連字號)、_ (底線) 和 . (用來分隔標籤的句點) 必須使用以下格式的逸出碼：\三位數八進位碼。例如，`\052` 是字元 * 的八進位碼。

如果使用 **route53:ChangeResourceRecordSetsActions**，則數值可能是下列任何一個值，且必須是大寫：

- CREATE
- UPSERT (更新插入)
- DELETE

如果使用 **route53:ChangeResourceRecordSetsRecordTypes**：

- 該值必須是大寫字母，並且可能是任何 Route 53 支援的 DNS 記錄類型。如需詳細資訊，請參閱 支援的 DNS 記錄類型。

> **Important**
>
> 您必須遵循這些慣例，才能授予別人許可，進而允許或限制別人能做的動作。

您可以使用 Access Analyzer 或 IAM 使用者指南中的政策模擬器來驗證您的政策是否如預期授予或限制他人權限。將 IAM 政策套用於要執行 Route 53 操作的測試使用者或測試角色也可以驗證許可。

指定條件：使用條件金鑰

AWS 為支援 IAM 的所有 AWS 服務提供一組預先定義的條件金鑰 (AWS 通用條件金鑰) 以進行存取控制。例如，您可以使用 `aws:SourceIp` 條件金鑰先檢查申請者的 IP 地址，再允許執行動作。如需詳細資訊以及 AWS 通用金鑰的清單，請參閱《IAM 使用者指南》中的可用條件金鑰。

> **Note**
>
> Route 53 不支援標籤型條件金鑰。

下表顯示適用於資源記錄集的 Route 53 服務專屬條件金鑰。

Route 53 條件金鑰	API 操作	值類型	描述
`route53:ChangeReso`		多重值	代表要求中的 DNS 記錄名稱清單ChangeResourceRecordSets。為了獲得預期反

Route 53 條件金鑰	API 操作	值類型	描述
urceRecordSetsNormalizedRecordNames	ChangeResourceRecordSets		應，IAM 政策中的 DNS 名稱必須依照下列方式進行標準化： • 所有字母必須小寫。 • DNS 名稱不可有行尾點號。 • a 到 z、0 到 9、- (連字號)、_ (底線) 和 . (用來分隔標籤的句點) 必須使用以下格式的逸出碼：\三位數八進位碼。
route53:ChangeResourceRecordSetsRecordTypes	ChangeResourceRecordSets	多重值	收到 ChangeResourceRecordSets 請求時，顯示 DNS 記錄類型清單。 ChangeResourceRecordSetsRecordTypes 可能是 Route 53 支援的任何 DNS 記錄類型。如需詳細資訊，請參閱 支援的 DNS 記錄類型。政策的所有內容都必須以大寫輸入。
route53:ChangeResourceRecordSetsActions	ChangeResourceRecordSets	多重值	收到 ChangeResourceRecordSets 請求時，顯示動作清單。 ChangeResourceRecordSetsActions 可能是下列任何一個值 (必須是大寫)： • CREATE • UPSERT (更新插入) • DELETE

範例政策：使用條件進行精細定義存取

本節中的每個範例都會將 Effect 子句設定為 Allow，而且只指定允許的動作、資源及參數。只允許存取 IAM 政策中明確列出的項目。

在某些情況下，有可能會重新撰寫這些政策，讓它們成為拒絕類型 (即，將 Effect 子句設定為 Deny，並反轉政策中的所有邏輯)。不過，建議您避免使用拒絕類型政策，因為它們與允許類型政策相較之下會較難正確地撰寫。對於需要文字正規化的 Route 53 而言尤其如此。

透過授予許可來限制他人對含特定名稱之 DNS 記錄的存取行為

下列許可政策授予的權限可允許他人對 example.com 和 marketing.example.com 上的託管區域 Z12345 執行 ChangeResourceRecordSets 動作。它使用 route53:ChangeResourceRecordSetsNormalizedRecordNames 條件金鑰來限制使用者僅能對符合指定名稱的記錄進行處置動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com", "marketing.example.com"]
                }
            }
          }
        ]
}
```

ForAllValues:StringEquals 是適用於多值金鑰的 IAM 條件運算子。上述政策中的條件僅在 ChangeResourceRecordSets 的所有變更都含有 example.com 的 DNS 名稱時才允許執行。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 條件運算子和具有多個索引鍵或值的 IAM 條件。

若要實作名稱中含有特定尾碼的權限，可在具有條件運算子 StringLike 或 StringNotLike 的政策中使用 IAM 萬用字元 (*)。以下策略會在當 ChangeResourceRecordSets 操作的所有變更都具有以「-beta.example.com」結尾的 DNS 名稱時允許執行。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringLike":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames": ["*-
beta.example.com"]
                }
            }
          }
        ]
}
```

> **Note**
>
> IAM 萬用字元與網域名稱萬用字元不同。如需有關在網域名稱中使用萬用字元的方式，請參閱下列範例。

授予他人可限制其對含萬用字元之網域名稱的 DNS 記錄進行存取的許可權限

下列許可政策授予的權限可允許他人對 example.com 上的託管區域 Z12345 執行 ChangeResourceRecordSets 動作。它會使用 route53:ChangeResourceRecordSetsNormalizedRecordNames 條件金鑰來限制使用者，使其只能對符合 *.example.com 的記錄採取處置動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames": ["\
\052.example.com"]
                }
            }
```

```
          }
        ]
}
```

\052 是 DNS 名稱中字元 * 的八進位碼，而 \052 中的 \ 則逸出為 \\，以便符合 JSON 語法。

透過授予許可權限來限制他人對特定 DNS 記錄的存取行為

下列許可政策授予的權限可允許他人對 example.com 上的託管區域 Z12345 執行 ChangeResourceRecordSets 動作。它使用三個條件金鑰的組合來限制使用者動作，只允許使用者建立或編輯具有特定 DNS 名稱和類型的 DNS 記錄。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com"],
                     "route53:ChangeResourceRecordSetsRecordTypes": ["MX"],
                     "route53:ChangeResourceRecordSetsActions": ["CREATE", "UPSERT"]
                }
            }
          }
        ]
}
```

授予許可權限以限制使用者的存取行為，使用者只能建立和編輯指定類型的 DNS 記錄

下列許可政策授予的權限可允許他人對 example.com 上的託管區域 Z12345 執行 ChangeResourceRecordSets 動作。它使用 route53:ChangeResourceRecordSetsRecordTypes 條件金鑰來限制使用者僅能對符合指定類型 (A 和 AAAA) 的記錄進行處置動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z1111111222222233333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
            }
          }
        ]
}
```

Amazon Route 53 API 許可：動作、資源和條件參考

當您設定 存取控制 並編寫可連接到 IAM 身分的許可政策 (以身分為基礎的政策) 時，可使用服務授權參考中的 Route 53 的動作、資源和條件金鑰、Route 53 網域的動作、資源和條件金鑰以及 Route 53 解析器的動作、資源和條件金鑰。這些頁面包含每個 Amazon Route 53 API 動作、您必須授與存取許可的動作，以及必須授與存取權的 AWS 資源。您在政策的 `Action` 欄位中指定動作，然後在政策的 `Resource` 欄位中指定資源值。

您可以在 Route 53 政策中使用 AWS 通用條件金鑰來表示條件。如需全 AWS 金鑰的完整清單，請參閱 IAM 使用者指南中的可用的金鑰。

> **Note**
>
> 授與存取權時，託管區域和 Amazon VPC 必須屬於相同分割區。分割區是一組 AWS 區域。每個 AWS 帳戶 的範圍都限定在一個分割區。
> 以下是支援的分割區：
>
> - `aws` - AWS 區域
> - `aws-cn` - 中國區域
> - `aws-us-gov` - AWS GovCloud (US) Region
>
> 如需詳細資訊，請參閱《AWS 一般參考》中的「存取管理」。

> **Note**
>
> 若要指定動作，請使用適用的字首 (`route53`、`route53domains` 或 `route53resolver`) 後接 API 操作名稱，例如：
>
> - `route53:CreateHostedZone`
> - `route53domains:RegisterDomain`
> - `route53resolver:CreateResolverEndpoint`

在 Amazon Route 53 中進行記錄和監控

Amazon Route 53 提供 DNS 查詢記錄，並可使用運作狀態來監控您的資源。此外，Route 53 會與其他的 AWS 整合，提供更多的記錄和監控功能：

記錄 DNS 查詢

可設定 Route 53 以記錄 Route 53 接收到的查詢相關資訊，例如提出請求的網域或子網域、請求的日期和時間，以及 DNS 記錄類型，例如 A 或 AAAA。

如需更多詳細資訊，請參閱 公有 DNS 查詢日誌記錄。

使用 AWS CloudTrail 來記錄主控台和程式設計動作

CloudTrail 會提供由使用者、角色或 AWS 服務所採取的 Route 53 動作的記錄。使用由 CloudTrail 收集的資訊時，您就可以追蹤所提出的請求、提出請求的 IP 地址、提出請求的對象、提出請求的時間，以及其他詳細資訊。如需更多詳細資訊，請參閱 使用日誌記錄 Amazon 路線 53 API 調用 AWS CloudTrail。

監控網域註冊

此 Route 53 儀表板會提供網域註冊狀態的相關詳細資訊，例如，網域傳輸狀態和即將過期的網域。

如需更多詳細資訊，請參閱 監控網域註冊。

使用 Route 53 運作狀態檢查和 Amazon CloudWatch 來監控您的資源

您可以透過建立 Route 53 運作狀態檢查來監控資源，這些運作狀態檢查使用 CloudWatch 收集原始資料並將其處理成為可讀取、近乎即時的指標。

如需更多詳細資訊，請參閱 使用 Amazon Route 53 健康檢查和 Amazon 監控您的資源 CloudWatch。

使用 Amazon CloudWatch 監控 Route 53 Resolver 端點

您可以使用 CloudWatch 來監控由 Resolver 端點轉發的 DNS 查詢數目。

如需更多詳細資訊，請參閱 使用 Amazon 監控 Route 53 解析器端點 CloudWatch。

使用 AWS Trusted Advisor

為 AWS 客戶提供服務的過程中，學習到的最佳實務，都體現在 Trusted Advisor 中。Trusted Advisor 可檢查您的 AWS 環境，並在有可能節省成本、提升系統可用性與效能或填補安全漏洞時向您提出建議。所有 AWS 客戶都能存取五項 Trusted Advisor 檢查。商業或企業支援方案客戶，可以檢視所有 Trusted Advisor 檢查。

如需更多詳細資訊，請參閱 Trusted Advisor。

Amazon Route 53 的合規驗證

在多個 AWS 合規計劃中，第三方稽核人員會評估 Amazon Route 53 的安全與合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內的 AWS 服務清單，請參閱合規計劃內的 AWS 服務。如需一般資訊，請參閱 AWS 合規計劃。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱在 AWS Artifact 中下載報告。

您使用 Route 53 的合規責任，取決於資料的機密性、您公司的合規目標及適用法律和法規。若您使用的 Route 53 必須遵循特定標準 (如 HIPAA、PCI 或 FedRAMP)，AWS 會提供資源予以協助：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心基準環境的架構考量和步驟。
- HIPAA 安全與合規架構白皮書 – 本白皮書說明公司可如何運用 AWS 來建立 HIPAA 合規的應用程式。
- AWS 合規資源 – 這組手冊和指南可能適用於您的產業和位置。
- AWS Config – 此 AWS 服務可評定資源組態與內部實務、業界準則和法規的合規狀態。
- AWS Security Hub：此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

Amazon Route 53 中的恢復能力

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS區域提供多個分開且隔離的實際可用區域，它們以低延遲、高輸送量和高度備援聯網功能相互連結。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

Route 53 將其功能劃分為控制和資料平面。如同大多數的 AWS 服務，Route 53 服務包含一個讓您能執行建立、更新和刪除資源等管理操作的控制平面，以及一個提供服務核心功能的資料平面。如需有關 Route 53 中控制與資料平面的詳細資訊，請參閱 控制和資料平面概念。

Route 53 主要是全球服務，但下列功能可支援 AWS 區域：

- 如果您將使用 Route 53 Resolver 來設定混合組態，則您要在自己所選定的 AWS 區域中建立端點，且您要在多個可用區域中指定 IP 地址。用於傳出端點時，您可以在與端點建立時所在的相同區域中建立規則。如需更多詳細資訊，請參閱 什麼是 Amazon Route 53 Resolver？。
- Route 53 運作狀態可設定成檢查您在特定區域中所建立資源的運作狀態，例如，Amazon EC2 執行個體和 Elastic Load Balancing 負載平衡器。
- 建立用於監控端點的運作狀態檢查時，您可以選擇性地指定希望 Route 53 在其中執行運作狀態檢查的區域。

如需有關 AWS 區域與可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

Amazon Route 53 的基礎設施安全性

Amazon Route 53 是一項受管服務，受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可使用 AWS 發佈的 API 呼叫，透過網路存取 Route 53。用戶端必須支援下列項目：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密 (PFS) 的密碼套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

監控 Amazon Route 53

監控是維持 AWS 解決方案可靠性、可用性和效能的重要組成部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。不過，在開始監控之前，您應該建立監控計劃，在其中回答下列問題：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

主題

- 公有 DNS 查詢日誌記錄
- 解析程式查詢日誌記錄
- 監控網域註冊
- 使用 Amazon Route 53 健康檢查和 Amazon 監控您的資源 CloudWatch
- 使用 Amazon 監控託管區域 CloudWatch
- 使用 Amazon 監控 Route 53 解析器端點 CloudWatch
- 使用 Amazon 監控 Route 53 解析器 DNS 防火牆規則群組 CloudWatch
- 使用管理 Route 53 解析程式 DNS 防火牆事件 Amazon EventBridge
- 使用日誌記錄 Amazon 路線 53 API 調用 AWS CloudTrail

公有 DNS 查詢日誌記錄

您可以將 Amazon Route 53 設定為記錄 Route 53 接收到的公有 DNS 查詢相關資訊，例如：

- 請求的網域或子網域
- 請求的日期和時間
- DNS 記錄類型 (例如 A 或 AAAA)

- 回應 DNS 查詢的 Route 53 節點。
- DNS 回答代碼，例如 `NoError` 或 `ServFail`

設定查詢記錄之後，Route 53 會將記錄檔傳送至記 CloudWatch 錄檔。您可以使用 CloudWatch 記錄檔工具來存取查詢記錄檔。

查詢日誌只包含 DNS 解析程式轉送至 Route 53 的查詢。如果 DNS 解析程式已快取對查詢的回應 (如 example.com 的負載平衡器的 IP 地址)，解析程式會繼續傳回快取的回應而不將查詢轉送到 Route 53，直到對應記錄的 TTL 到期為止。

根據為網域名稱 (example.com) 或子網域名稱 (www.example.com) 提交的 DNS 查詢數量、使用者正在使用的解析程式，以及記錄的 TTL，查詢日誌可能只包含提交到 DNS 解析程式的數千個查詢中的一個查詢的資訊。如需 DNS 運作方式的詳細資訊，請參閱 如何將網際網路流量路由到您的網站或 Web 應用程式。

如果您不需要詳細的記錄資訊，可以使用 Amazon CloudWatch 指標來查看 Route 53 針對託管區域回應的 DNS 查詢總數。如需詳細資訊，請參閱 檢視公有託管區域的 DNS 查詢指標。

主題

- 為 DNS 查詢設定日誌記錄
- 使用 Amazon CloudWatch 訪問 DNS 查詢日誌
- 變更日誌的保留期間並將日誌匯出到 Amazon S3
- 停止查詢日誌記錄
- 出現在 DNS 查詢日誌中的值
- 查詢日誌範例

為 DNS 查詢設定日誌記錄

若要開始記錄指定託管區域的 DNS 查詢，您需要在 Amazon Route 53 主控台執行下列任務：

- 選擇您希望 Route 53 發佈記錄檔的記錄檔群組，或建立新的記錄群組。 CloudWatch

> **Note**
>
> 日誌群組必須位於美國東部 (維吉尼亞北部)區域。

- 選擇 Create (建立政策) 以完成操作。

> **Note**
>
> 如果使用者正在提交對您網域的 DNS 查詢，您應該會在建立查詢日誌記錄組態後數分鐘內開始看到日誌中的查詢。

若要為 DNS 查詢設定日誌記錄

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇您要為其設定查詢日誌記錄的託管區域。
4. 在 Hosted zone details (託管區域詳細資訊) 窗格中，選擇 Configure query logging (設定查詢記錄)。
5. 選擇現有的日誌群組，或建立新的日誌群組。
6. 如果您收到有關許可的提醒 (如果您之前尚未使用新主控台設定查詢日誌記錄，就會發生這種情況)，請執行下列其中一項動作：
   - 如果您已經有 10 個資源政策，則無法再建立任何資源政策。選取任何資源政策，然後選取 Edit (編輯)。編輯會授予 Route 53 許可，將日誌寫入日誌群組。選擇儲存。提醒會消失，您可以繼續下一個步驟。
   - 如果您之前從未設定過查詢記錄 (或者您尚未建立 10 個資源原則)，則需要授與 Route 53 的權限，才能將記錄寫入記 CloudWatch 錄檔群組。選擇 授予許可。提醒會消失，您可以繼續下一個步驟。
7. 選擇權限-選用以查看表格，其中顯示資源原則是否符合記 CloudWatch 錄群組，以及 Route 53 是否具有將記錄發佈至的權限 CloudWatch。
8. 選擇建立。

使用 Amazon CloudWatch 訪問 DNS 查詢日誌

Amazon Route 53 會將查詢日誌直接傳送到 CloudWatch 日誌；這些日誌永遠無法透過 Route 53 存取。相反地，您可以使用 CloudWatch 日誌以近乎即時的方式檢視日誌、搜尋和篩選資料，以及將日誌匯出到 Amazon S3。

Route 53 會為每個 Route 53 邊緣位置建立一個 CloudWatch 記錄資料流，以回應指定託管區域的 DNS 查詢，並將查詢記錄傳送至適用的記錄資料流。每個記錄資料流的名稱格式為 *hosted-zone-id*/#### *ID*，例如。Z1D633PJN98FT9/DFW3

一個三字母代碼和任意指派的數字辨識每一節點，例如 DFW3。三字母代碼通常對應於節點附近機場的國際航空運輸協會機場代碼。(未來這些縮寫可能會改變。) 如需節點清單，請參閱 Route 53 產品詳細資訊上的「Route 53 全球網路」。

如需詳細資訊，請參閱適用的文件：

- Amazon CloudWatch 日誌用戶指南
- Amazon CloudWatch 日誌 API 參考
- CloudWatch 「 AWS CLI 指令參考」的「記錄」區段
- 出現在 DNS 查詢日誌中的值

變更日誌的保留期間並將日誌匯出到 Amazon S3

根據預設， CloudWatch 記錄會無限期儲存查詢記錄。您可以選擇性地指定保留期間，讓「 CloudWatch 記錄檔」刪除早於保留期間的記錄檔。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的變更 CloudWatch 日誌資料保留。

如果您想要保留日誌資料，但不需要 CloudWatch 日誌工具來檢視和分析資料，可以將日誌匯出到 Amazon S3，以降低儲存成本。如需詳細資訊，請參閱將日誌資料匯出到 Amazon S3。

如需有關定價的詳細資訊，請參閱適用的定價頁面：

- CloudWatch 定價頁面上的「Amazon CloudWatch 日誌」
- Amazon S3 定價

> **Note**
>
> 當您設定 Route 53 記錄 DNS 查詢時，不會產生任何 Route 53 費用。

停止查詢日誌記錄

如果您希望 Amazon Route 53 停止將查詢日誌傳送到 CloudWatch 日誌，請執行下列程序刪除查詢記錄組態。

若要刪除查詢日誌記錄組態

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 為您要為其刪除查詢日誌記錄組態的託管區域選擇名稱。
4. 在 Hosted zone details (託管區域詳細資訊) 窗格中，選擇 Delete query logging (刪除查詢日誌記錄)。
5. 選擇 Delete (刪除)，確認刪除。

出現在 DNS 查詢日誌中的值

針對 Amazon Route 53 從對應節點中的 DNS 解析程式收到的每個 DNS 查詢，每個日誌檔案都會包含一個日誌項目。每個日誌項目包含以下值：

日誌格式版本

此查詢日誌的版本編號。如果我們新增欄位至日誌或變更現有欄位的格式，我們會遞增這個值。

查詢時間戳記

Route 53 回應請求的日期和時間，採用 ISO 8601 格式和國際標準時間 (UTC)，例如 `2017-03-16T19:20:25.177Z`。

如需有關 ISO 8601 格式的資訊，請參閱 Wikipedia 文章 ISO 8601。如需有關 UTC 的資訊，請參閱 Wikipedia 文章國際標準時間。

託管區域 ID

與此日誌中的所有 DNS 查詢關聯的託管區域的 ID。

查詢名稱

請求中指定的網域或子網域

查詢類型

請求中指定的 DNS 記錄類型，或 ANY。如需有關 Route 53 支援的類型的資訊，請參閱 支援的 DNS 記錄類型。

回應代碼

Route 53 在對 DNS 查詢做出的回答中傳回的 DNS 回答代碼。

第 4 層通訊協定

用來提交查詢的通訊協定 (TCP 或 UDP)。

Route 53 節點

回應查詢的 Route 53 節點。每個節點是以三字母代碼和任意數字識別，例如 DFW3。三字母代碼通常對應於節點附近機場的國際航空運輸協會機場代碼。(未來這些縮寫可能會改變。)

如需節點清單，請參閱 Route 53 產品詳細資訊頁面上的「Route 53 全球網路」。

解析程式 IP 地址

向 Route 53 提交請求的 DNS 解析程式的 IP 地址。

EDNS 用戶端子網路

發起請求的用戶端的部分 IP 地址 (如果可從 DNS 解析程式取得)。

如需詳細資訊，請參閱 IETF 草稿 DNS 請求中的用戶端子網路。

查詢日誌範例

以下是查詢日誌示例 (區域是預留位置)：

```
1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP Region 192.168.1.1
 -
1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP Region
 192.168.3.1 192.168.222.0/24
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP Region
 2001:db8::1234 2001:db8:abcd::/48
1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP Region
 192.168.3.1 192.168.111.0/24
1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP Region
 192.168.1.2 -
```

解析程式查詢日誌記錄

您可以記錄下列 DNS 查詢：

- 源於您指定的 Amazon Virtual Private Cloud VPC 的查詢，以及對這些 DNS 查詢的回應。
- 來自使用傳入 Resolver 端點的內部部署資源的查詢。
- 使用傳出 Resolver 端點進行遞迴 DNS 解析的查詢。

- 使用 Route 53 Resolver DNS 防火牆規則來封鎖、允許或監控網域清單的查詢。

Resolver 查詢日誌包含下列值：

- 建 AWS 立 VPC 所在的區域
- 查詢源自其中的 VPC 的 ID
- 查詢源自其中的執行個體的 IP 地址
- 查詢源自其中的資源的執行個體 ID
- 第一次進行查詢的日期和時間
- 要求的 DNS 名稱 (例如 prod.example.com)
- DNS 記錄類型 (例如 A 或 AAAA)
- DNS 回答代碼，例如 `NoError` 或 `ServFail`
- DNS 回答資料，例如，在對 DNS 查詢做出的回答中傳回的 IP 地址
- 對 DNS 防火牆規則動作的回應

如需所有記錄值的詳細清單和範例，請參閱 出現在 Resolver 查詢日誌中的值。

> **Note**
>
> 與 DNS 解析器的標準一樣，解析器會在解析器 time-to-live （TTL）確定的時間長度內緩存 DNS 查詢。Route 53 Resolver 會快取源自 VPC 的查詢，並儘可能從快取回應以加速回應。解析程式查詢日誌記錄只會記錄唯一的查詢，而不會記錄解析程式能夠從快取回應的查詢。例如，假設其中一個 VPC 中的 EC2 執行個體正在記錄查詢的查詢，則會提交 account.example.com 的要求。解析程式會快取該查詢的回應，並記錄查詢。如果相同執行個體的彈性網路介面在 Resolver 快取的 TTL 內對 account.example.com 進行查詢，解析程式會回應來自快取的查詢。未記錄第二個查詢。

您可以將記錄檔傳送至下列其中一個 AWS 資源：

- Amazon CloudWatch 日誌（CloudWatch 日誌）日誌群組
- Amazon S3 (S3) 儲存貯體
- Firehose 交付串流

如需詳細資訊，請參閱 AWS 您可以將解析器查詢日誌發送到的資源。

主題

- AWS 您可以將解析器查詢日誌發送到的資源
- 管理 Resolver 查詢日誌記錄組態

AWS 您可以將解析器查詢日誌發送到的資源

> **Note**
>
> 如果您希望為每秒高查詢 (QPS) 的工作負載記錄查詢，則應使用 Amazon S3 來確保查詢日誌在寫入目的地時不會受節制。如果您使用 Amazon CloudWatch，則可以增加`PutLogEvents`操作的每秒請求限制。若要進一步了解如何提高 CloudWatch 限制，請參閱 Amazon CloudWatch 使用者指南中的CloudWatch 日誌配額。

您可以將解析器查詢日誌發送到以下 AWS 資源：

Amazon CloudWatch 日誌（Amazon CloudWatch 日誌）日誌組

您可以使用 Logs Insights 來分析日誌，並建立指標和警示。

如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。

Amazon S3 (S3) 儲存貯體

S3 儲存貯體是經濟實惠的長期日誌存檔方式。延遲通常較高。

支援所有 S3 伺服器端加密選項。如需詳細資訊，請參閱《Amazon S3 使用者指南》中的使用伺服器端加密保護資料。

如果 S3 儲存貯體位於您擁有的帳戶中，所需的許可會自動新增至儲存貯體政策。如果您想將日誌發送到您未擁有的帳戶中的 S3 儲存貯體，則 S3 儲存貯體的擁有者必須在其儲存貯體政策中為您的帳戶新增許可。例如：

```
{
    "Version": "2012-10-17",
    "Id": "CrossAccountAccess",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::your_bucket_name/AWSLogs/your_caller_account/
*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your_bucket_name"
        },
         {
            "Effect": "Allow",
            "Principal": {
                "AWS": "iam_user_arn_or_account_number_for_root"
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::your_bucket_name"
        }
    ]
}
```

> **Note**
>
> 如果您想要將記錄儲存在組織的中央 S3 儲存貯體中，建議您從集中式帳戶設定查詢日誌記錄組態 (具有寫入中央儲存貯體的必要許可)，然後使用 RAM 以跨帳戶共用組態。

如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南。

Firehose 交付串流

您可以將日誌即時串流到 Amazon OpenSearch 服務、Amazon Redshift 或其他應用程式。

如需詳細資訊，請參閱 Amazon 資料 Firehose 開發人員指南。

如需解析器查詢記錄定價的相關資訊，請參閱 Amazon CloudWatch 定價。

CloudWatch 使用解析器日誌時需支付日誌費用，即使日誌直接發佈到 Amazon S3 也是如此。如需詳細資訊，請參閱以 Amazon CloudWatch 定價將日誌交付到 S3。

管理 Resolver 查詢日誌記錄組態

設定 (Resolver 查詢日誌記錄)

若要開始記錄源自 VPC 的 DNS 查詢，您需要在 Amazon Route 53 主控台執行下列任務：

若要設定 Resolver 查詢日誌記錄

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 展開 Route 53 主控台選單。在主控台的左上角，選擇三個水平橫條 (☰) 圖示。
3. 在 Resolver 選單中，選擇 Query logging (查詢日誌記錄)。
4. 在「地區」選取器中，選擇您要建立查詢記錄組態的「 AWS 區域」。這必須是與您建立要為其記錄 DNS 查詢的 VPC 的相同區域。如果您在多個區域擁有 VPC，務必為每個區域至少建立一項查詢日誌記錄組態。
5. 選擇 Configure query logging (設定查詢日誌記錄)。
6. 指定下列值：

   查詢日誌記錄組態

   輸入查詢日誌記錄組態的名稱。名稱會顯示在主控台中的查詢日誌記錄組態清單。輸入稍後可以協助您尋找此組態的名稱。

   查詢日誌目的地

   選擇您希望解析程式傳送查詢記錄檔的 AWS 資源類型。如需如何在選項 (CloudWatch 日誌記錄群組、S3 儲存貯體和 Firehose 交付串流) 中進行選擇的相關資訊，請參閱AWS 您可以將解析器查詢日誌發送到的資源。

   選擇資源類型後，您可以建立該類型的其他資源，或選擇目前 AWS 帳號建立的現有資源。

   > **Note**
   >
   > 您只能選擇在步驟 4 (建立查詢記錄設定的 AWS 區域) 中選擇的區域中建立的資源。如果您選擇建立新資源，則會在相同的區域中建立該資源。

要記錄查詢的 VPC

此查詢日誌記錄組態會記錄源自所選擇之 VPC 的 DNS 查詢。核取您要 Resolver 記錄查詢的目前區域中每個 VPC 的核取方塊，然後選擇 選擇。

> **Note**
>
> 針對特定目的地類型，只能啟用一次 VPC 日誌交付。日誌無法交付到相同類型的多個目的地，例如，VPC 日誌無法交付至 2 個 Amazon S3 目的地。

7. 選擇 Configure query logging (設定查詢日誌記錄)。

> **Note**
>
> 您應該會在成功建立查詢日誌記錄組態後幾分鐘內開始看到由 VPC 資源進行的 DNS 查詢。

出現在 Resolver 查詢日誌中的值

針對 Amazon Route 53 從對應節點中的 DNS 解析程式收到的每個 DNS 查詢，每個日誌檔案都會包含一個日誌項目。每個日誌項目包含以下值：

version

此查詢日誌格式的版本編號。目前版本是 `1.1`。

版本值是以 **`major_version.minor_version`** 形式的主要和次要版本。例如，您可以有一個值為 `version` 的 `1.7`，其中 `1` 是主要版本，而 `7` 是次要版本。

如果對不向下相容的日誌結構進行變更，Route 53 就會增加主要版本。這包括已經存在的 JSON 欄位，或變更欄位內容的呈現方式 (例如，日期格式)。

如果變更將新欄位新增至日誌檔案，Route 53 會增加次要版本。如果 VPC 內的部分或所有現有 DNS 查詢都有新資訊，就會發生這種情況。

account_id

建立 VPC 之 AWS 帳戶的識別碼。

region

您在其中建立 VPC 的 AWS 區域。

vpc_id

查詢源自其中的 VPC 的 ID。

query_timestamp

提交查詢的日期和時間，採用 ISO 8601 格式和國際標準時間 (UTC)，例如 `2017-03-16T19:20:177Z`。

如需有關 ISO 8601 格式的資訊，請參閱 Wikipedia 文章 ISO 8601。如需有關 UTC 的資訊，請參閱 Wikipedia 文章國際標準時間。

query_name

查詢中指定的網域名稱 (example.com) 或子網域名稱 (www.example.com)。

query_type

請求中指定的 DNS 記錄類型，或 ANY。如需有關 Route 53 支援的類型的資訊，請參閱 支援的 DNS 記錄類型。

query_class

查詢的類別。

rcode

Resolver 在對 DNS 查詢做出的回答中傳回的 DNS 回答代碼。此回應代碼指出查詢是否有效。最常見的回應代碼是 NOERROR，表示查詢有效。如果回應無效，Resolver 會傳回說明無效原因的回應代碼。如需可能的回應代碼清單，請參閱 IANA 網站上的 DNS RCODES。

answer_type

Resolver 為了回應查詢而傳回的值的 DNS 記錄類型 (例如 A、MX 或 CNAME)。如需有關 Route 53 支援的類型的資訊，請參閱 支援的 DNS 記錄類型。

rdata

Resolver 在對 DNS 查詢做出的回應中傳回的值。例如，對於 A 記錄，這是 IPv4 格式的 IP 地址。對於 CNAME 記錄，這是 CNAME 記錄中的網域名稱。

answer_class

Resolver 回應查詢的類別。

scaddr

查詢源自其中的執行個體的 IP 地址。

srcport

查詢源自其中的執行個體上的連接埠。

transport

用來提交 DNS 查詢的通訊協定。

scids

DNS 查詢來源其中或通過其中的 `instance`、`resolver_endpoint` 和 `resolver_network_interface` 的 ID。

instance

查詢來源其中的執行個體的 ID。

resolver_endpoint

將 DNS 查詢傳遞至內部部署 DNS 伺服器的解析程式端點的 ID。

firewall_rule_group_id

符合查詢中網域名稱的 DNS 防火牆規則群組的 ID。只有當 DNS 防火牆找到符合動作設定為警示或封鎖的規則時，才會填入此選項。

如需防火牆規則群組的詳細資訊，請參閱 DNS 防火牆規則群組與規則。

firewall_rule_action

由符合查詢中網域名稱的規則指定的動作。只有當 DNS 防火牆找到符合動作設定為警示或封鎖的規則時，才會填入此選項。

firewall_domain_list_id

由符合查詢中網域名稱的規則使用的網域清單。只有當 DNS 防火牆找到符合動作設定為警示或封鎖的規則時，才會填入此選項。

additional_properties

日誌交付事件的其他資訊。is_delayed：如果交付日誌時發生延遲。

Route 53 Resolver 查詢日誌範例

以下是解析程式查詢日誌範例：

```
    {
      "srcaddr": "4.5.64.102",
      "vpc_id": "vpc-7example",
      "answers": [
          {
              "Rdata": "203.0.113.9",
              "Type": "PTR",
              "Class": "IN"
          }
      ],
      "firewall_rule_group_id": "rslvr-frg-01234567890abcdef",
      "firewall_rule_action": "BLOCK",
      "query_name": "15.3.4.32.in-addr.arpa.",
      "firewall_domain_list_id": "rslvr-fdl-01234567890abcdef",
      "query_class": "IN",
      "srcids": {
          "instance": "i-0d15cd0d3example"
      },
      "rcode": "NOERROR",
      "query_type": "PTR",
      "transport": "UDP",
      "version": "1.100000",
      "account_id": "111122223333",
      "srcport": "56067",
      "query_timestamp": "2021-02-04T17:51:55Z",
      "region": "us-east-1"
  }
```

與其他帳戶共享解析器查詢日誌配置 AWS

您可以與其 AWS 他帳戶共用您使用一個 AWS 帳戶建立的查詢記錄設定。若要共用組態，Route 53 解析程式主控台會與 Res AWS ource Access Manager 整合。如需 Resource Access Manager 的詳細資訊，請參閱 Resource Access Manager 使用者指南。

注意下列事項：

將 VPC 與共用查詢日誌記錄組態建立關聯

如果其他 AWS 帳戶與您的帳戶共用了一或多個組態，您可以使 VPC 與組態產生關聯，方式與您建立的組態相同。

刪除或解除共用組態

如果您與其他帳戶共用組態，然後刪除或停止共用該組態，並且如果一或多個 VPC 與組態建立關聯，則 Route 53 Resolver 會停止記錄源自這些 VPC 的 DNS 查詢。

查詢日誌記錄組態以及可以這些組態建立關聯的 VPC 數量上限

當某個帳戶建立了組態並與一或多個其他帳戶共用此組態時，可與該組態建立關聯的 VPC 數量上限會套用至相關帳戶。例如，如果您的組織中有 10,000 個帳戶，您可以在中央帳戶中建立查詢記錄設定，並透過共用，以 AWS RAM 便將其共用至組織帳戶。然後，組織帳戶會建立組態與其 VPC 之間的關聯，根據其帳戶的查詢日誌組態來計算所建立的 VPC 關聯數量，每個 AWS 區域 建立的 VPC 關聯數量最多不能超過 100。但是，如果所有 VPC 都在單一帳戶中，則可能需要提高帳戶的服務上限。

如需目前的 Resolver 配額，請參閱 Route 53 Resolver 的配額。

許可

若要與其他 AWS 帳號共用規則，您必須擁有使用該PutResolverQueryLogConfigPolicy動作的權限。

規則共用的 AWS 帳戶限制

共用規則的帳戶無法變更或刪除規則。

標記

只有建立規則的帳戶可以新增、刪除或檢視規則的標籤。

若要檢視規則目前的共用狀態 (包括共用規則的帳戶或與之共用規則的帳戶)，以及與其他帳戶共用規則，請執行以下程序。

檢視共用狀態並與另一個 AWS 帳戶共用查詢日誌記錄組態

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Query Logging (查詢日誌記錄)。
3. 在導覽列上，選擇您建立規則的區域。

   Sharing status (共用狀態) 欄顯示規則目前的共享狀態，它們是目前帳戶建立的規則或與目前帳戶共用的規則：

   - 未共用：目前 AWS 帳戶已建立規則，且該規則不會與任何其他帳戶共用。

- Shared by me (由我共用)：目前的帳戶建立了規則，且與一或多個帳戶共用。
- Shared with me (與我共用)：另一個帳戶建立了規則，且與目前的帳戶共用。

4. 選擇您想要顯示共用資訊的規則名稱，或您想要與其他帳戶共用的規則名稱。

   在 Rule: ***rule name*** (規則：規則名稱) 頁面中，Owner (擁有者) 下的值會顯示建立規則的帳戶 ID。除非 Sharing status (共用狀態) 的值為 Shared with me (與我共用)，否則即為目前的帳戶。若是如此，Owner (擁有者) 即為建立了規則，且與目前帳戶共用規則的帳戶。

5. 選擇 Share (共用) 以檢視更多資訊，或與其他帳戶共用規則。Resource Access Manager 主控台會顯示一個頁面，視 Sharing status (共用狀態) 的值而定：

   - Not shared (不共用)：顯示 Create resource share (建立資源共用) 頁面。如需如何與其他帳戶、OU 或組織共用規則的資訊，請跳到步驟 6。
   - Shared by me (由我共用)：Shared resources (共用的資源) 頁面會顯示目前帳戶所擁有的規則和其他資源，以及與其他帳戶共用的規則和資源。
   - Shared with me (與我共用)：Shared resources (共用的資源) 頁面會顯示其他帳戶所擁有的規則和其他資源，以及與目前帳戶共用的規則和資源。

6. 若要與其他 AWS 帳戶、OU 或組織共用查詢記錄組態，請指定下列值。

   > **Note**
   >
   > 您無法更新共用設定。如果您想要變更以下任一設定，您必須重新共用使用新設定的規則，然後移除舊的共用設定。

   描述

   輸入有助於您記憶為何共用查詢日誌記錄組態的簡短描述。

   資源

   選擇您要共用之組態的核取方塊。

   主體

   輸入 AWS 帳號、OU 名稱或組織名稱。

   標籤

   指定一或多個金鑰和對應的值。例如，您可以為 Key (金鑰) 指定 Cost center (成本中心)，為 Value (值) 指定 456。

這些是用於組織 AWS 帳單的標籤；您也可以將標籤用於其他用途。 AWS Billing and Cost Management 如需有關使用成本配置標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

監控網域註冊

Amazon Route 53 儀表板提供網域註冊狀態的詳細資訊，包括下列項目：

- 新網域註冊的狀態
- 網域轉移至 Route 53 的狀態
- 過期日期在即的網域清單

我們建議您定期檢查 Route 53 主控台的儀表板，尤其是在註冊新網域或將網域轉移至 Route 53 之後，以確認沒有需要處理的問題。

我們也建議您確認網域的聯絡資訊是最新的。當網域過期日期在即，我們會向網域的註冊聯絡人傳送電子郵件，其中包含網域過期時間和續約方法的相關資訊。

使用 Amazon Route 53 健康檢查和 Amazon 監控您的資源 CloudWatch

您可以透過建立 Amazon Route 53 運作狀態檢查來監控資源，這些檢查可用 CloudWatch 來收集原始資料並將其處理為可讀且接近即時的指標。這些統計資料會保存兩週的期間，以便您存取歷史資訊，並更清楚資源的執行方式。根據預設，Route 53 健康狀態檢查的指標資料會以一分鐘的間隔自動傳送到 CloudWatch 。

如需 Route 53 運作狀態檢查的詳細資訊，請參閱 使用 CloudWatch 監控運作狀態檢查。如需詳細資訊 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 在 Amazon 用 CloudWatch 戶指南。

Route 53 運作狀態檢查指標與維度

建立運作狀態檢查時，Amazon Route 53 會開始每分鐘傳送一次指標和維度至您指定的資源 CloudWatch 相關資源。Route 53 主控台可讓您檢視運作狀態檢查的狀態。您也可以使用下列程序在 CloudWatch 主控台中檢視測量結果，或使用 AWS Command Line Interface (AWS CLI) 來檢視測量結果。

使用 CloudWatch 主控台檢視指標

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 Metrics (指標)。
3. 在 All Metrics (所有指標) 標籤上，選擇 Route 53。
4. 選擇 Health Check Metrics (運作狀態檢查指標)。

若要使用 AWS CLI

- 在命令提示中，使用下列命令：

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

主題

- CloudWatch 53 號路線健康狀態檢查的指標
- Route 53 運作狀態檢查指標的維度

CloudWatch 53 號路線健康狀態檢查的指標

AWS/Route53 命名空間包含 Route 53 運作狀態檢查的下列指標。

ChildHealthCheckHealthyCount

適用於計算的運作狀態檢查， 運作狀態檢查中，運作狀態為正常的數量。

有效統計：平均 (建議)、最小值、最大值

單位：計數

ConnectionTime

Route 53 運作狀態檢查程式與端點建立 TCP 連線所花的平均時間 (毫秒)。您可以檢視 ConnectionTime 以查看所有區域或選取的地理區域的運作狀態檢查。

有效統計：平均 (建議)、最小值、最大值

單位：毫秒

HealthCheckPercentageHealthy

認定選取端點是正常的 Route 53 運作狀態檢查程式的百分比。

有效統計：平均、最小值、最大值

單位：百分比

HealthCheckStatus

正在檢查的健全狀況檢查端點 CloudWatch 的狀態。 1 表示健康，0 表示不健康。

有效的統計資訊：下限、平均和上限

單位：無

SSL HandshakeTime

Route 53 運作狀態檢查程式完成 SSL 交握所花的平均時間 (毫秒)。您可以檢視 `SSLHandshakeTime` 以查看所有區域或選取的地理區域的運作狀態檢查。

有效統計：平均 (建議)、最小值、最大值

單位：毫秒

TimeToFirstByte

Route 53 運作狀態檢查程式接收回應 HTTP 或 HTTPS 請求的第一個位元組所花的平均時間 (毫秒)。您可以檢視 `TimeToFirstByte` 以查看所有區域或選取的地理區域的運作狀態檢查。

有效統計：平均 (建議)、最小值、最大值

單位：毫秒

Route 53 運作狀態檢查指標的維度

運作狀態檢查的 Route 53 指標使用 `AWS/Route53` 命名空間，並提供 `HealthCheckId` 的指標。擷取指標時，您必須提供 `HealthCheckId` 維度。

此外，針對 `ConnectionTime`、`SSLHandshakeTime` 及 `TimeToFirstByte`，您可以選擇性指定 `Region`。如果省略`Region`，則 CloudWatch 會傳回所有區域的量度。如果包含`Region`，則僅 CloudWatch 傳回指定區域的量度。

如需詳細資訊，請參閱 使用 CloudWatch 監控運作狀態檢查。

使用 Amazon 監控託管區域 CloudWatch

您可以使用 Amazon 收集原始資料並將其處理 CloudWatch 為可讀且近乎即時的指標，藉此監控公有託管區域。Route 53 收到指標所依據的 DNS 查詢後不久，即可使用量度。 CloudWatch Route 53 託管區域的度量資料粒度為一分鐘。

如需詳細資訊，請參閱下列文件

- 如需有關如何在 Amazon CloudWatch 主控台中檢視指標以及如何使用 AWS Command Line Interface (AWS CLI) 擷取指標的概觀和資訊，請參閱 檢視公有託管區域的 DNS 查詢指標
- 如需有關指標保留期的資訊，請參閱 Amazon CloudWatch API 參考GetMetricStatistics中的。
- 如需詳細資訊 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 在 Amazon 用 CloudWatch 戶指南。
- 如需有關指 CloudWatch 標的詳細資訊，請參閱 Amazon 使用者指南中的使 CloudWatch 用 Amazon 指 CloudWatch 標。

主題

- CloudWatch Route 53 公共託管區域的度量
- CloudWatch Route 53 公共託管區域量度的維度

CloudWatch Route 53 公共託管區域的度量

`AWS/Route53` 命名空間包含下列 Route 53 託管區域的指標：

DNSQueries

針對託管區域，在指定期間內 Route 53 回應的 DNS 查詢數量。

有效統計數據：總和， SampleCount

單位：計數

區域：Route 53 是全球服務。若要取得託管區域指標，您必須為該區域指定 US East (N. Virginia) (美國東部 (維吉尼亞北部))。

DNSSC InternalFailure

如果託管區域中的任何物件為 INTERNAL_FAILURE 狀態，則值為 1。否則，值為 0。

有效的統計資訊：總和

單位：計數

容量：每 4 個小時每個託管區域 1 個

區域：Route 53 是全球服務。若要取得託管區域指標，您必須為該區域指定 US East (N. Virginia) (美國東部 (維吉尼亞北部))。

DNSSC KeySigningKeysNeedingAction

具有 ACTION_NEEDED 狀態 (因為 KMS 失敗) 的金鑰簽署金鑰 (KSK) 數目。

有效統計數據：總和， SampleCount

單位：計數

容量：每 4 個小時每個託管區域 1 個

區域：Route 53 是全球服務。若要取得託管區域指標，您必須為該區域指定 US East (N. Virginia) (美國東部 (維吉尼亞北部))。

DNSSC KeySigningKeyMaxNeedingActionAge

自金鑰簽署金鑰 (KSK) 設定為 ACTION_NEEDED 狀態以來經過的時間。

有效的統計資訊：上限

單位：秒

容量：每 4 個小時每個託管區域 1 個

區域：Route 53 是全球服務。若要取得託管區域指標，您必須為該區域指定 US East (N. Virginia) (美國東部 (維吉尼亞北部))。

DNSSC KeySigningKeyAge

建立金鑰簽署金鑰 (KSK) 後經過的時間 (並非自其啟動以來的時間)。

有效的統計資訊：上限

單位：秒

容量：每 4 個小時每個託管區域 1 個

區域：Route 53 是全球服務。若要取得託管區域指標，您必須為該區域指定 US East (N. Virginia) (美國東部 (維吉尼亞北部))。

CloudWatch Route 53 公共託管區域量度的維度

託管區域的 Route 53 指標使用 AWS/Route53 命名空間，並提供 HostedZoneId 的指標。若要取得 DNS 查詢的數量，您必須在 HostedZoneId 維度中指定託管區域的 ID。

使用 Amazon 監控 Route 53 解析器端點 CloudWatch

您可以使 CloudWatch 用 Amazon 監控由 Route 53 解析器端點轉發的 DNS 查詢數量。Amazon CloudWatch 會收集原始資料並將其處理為可讀且近乎即時的指標。這些統計資料會保存兩週的期間，以便您存取歷史資訊，並更清楚資源的執行方式。依預設，解析器端點的測量結果資料會以五分鐘的CloudWatch間隔自動傳送到。五分鐘的間隔也是可以傳送度量資料的最小間隔。

如需 Resolver 的詳細資訊，請參閱 什麼是 Amazon Route 53 Resolver？。如需詳細資訊 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 在 Amazon 用 CloudWatch 戶指南。

Route 53 Resolver 的指標與維度

當您設定解析器將 DNS 查詢轉寄至您的網路 (反之亦然) 時，Resolver 會開始每五分鐘傳送一次度量和維度至 CloudWatch 轉送的查詢數目。您可以使用下列程序在 CloudWatch 主控台中檢視測量結果，或使用 AWS Command Line Interface (AWS CLI) 來檢視測量結果。

使用主控台檢視解析器測量結果 CloudWatch

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽列上，選擇您建立端點的區域。
3. 在導覽窗格中，選擇 指標。
4. 在 All metrics (所有指標) 標籤中，選擇 Route 53 Resolver (Route 53 解析程式)。
5. 選擇 By Endpoint (依端點)，以檢視指定端點的查詢計數。然後選擇要查看查詢數量的端點。

   選擇「跨所有端點」可檢視所有輸入端點的查詢計數，或目前 AWS 帳號建立的所有輸出端點的查詢計數。然後選擇InboundQueryVolume或OutboundQueryVolume以檢視所需的計數。

若要使用 AWS CLI

- 在命令提示中，使用下列命令：

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

主題

- CloudWatch Route 53 解析器的度量
- Route 53 Resolver 指標的維度

CloudWatch Route 53 解析器的度量

AWS/Route53Resolver 命名空間包含 Route 53 Resolver 端點和 IP 地址的指標。

主題

- Resolver 端點的指標
- Resolver IP 地址的指標

Resolver 端點的指標

此 AWS/Route53Resolver 命名空間包含 Route 53 Resolver 端點的下列指標。

EndpointHealthy英尼康

處於 OPERATIONAL 狀態的彈性網路介面數量。這意味著端點 (由 EndpointId 指定) 的 Amazon VPC 網路介面已正確設定，而且能夠在您的網路和 Resolver 之間傳送傳入或傳出 DNS 查詢。

有效統計資訊：下限、上限、平均數

單位：計數

EndpointUnhealthy英尼康

處於 AUTO_RECOVERING 狀態的彈性網路介面數量。

這表示解析程式正在嘗試復原與端點相關聯的一或多個 Amazon VPC 網路介面 (由 EndpointId 指定)。在復原過程中，端點會以有限容量運作，而且無法處理 DNS 查詢，直到完全復原。

有效統計資訊：下限、上限、平均數

單位：計數

InboundQueryVolume

對於傳入端點，DNS 查詢數量會透過 EndpointId 指定的端點，從您的網路轉送到 VPC。

有效的統計資訊：總和

單位：計數

OutboundQueryVolume

對於傳出端點，DNS 查詢數量會透過 EndpointId 指定的端點，從您的 VPC 轉送到網路。

有效的統計資訊：總和

單位：計數

OutboundQueryAggregateVolume

對於傳出端點，從 Amazon VPC 轉送到您網路的 DNS 查詢總數包括下列項目：

- DNS 查詢數量會透過 EndpointId 指定的端點，從您的 VPC 轉送到網路。
- 當目前帳戶與其他帳戶共用 Resolver 規則時，由其他帳戶建立的 VPC 查詢將透過 EndpointId 指定的端點轉送到您的網路。

有效的統計資訊：總和

單位：計數

Resolver IP 地址的指標

AWS/Route53Resolver 命名空間包含與 Resolver 傳入或傳出端點相關聯之每個 IP 地址的以下指標。(當您指定端點時，Resolver 會建立 Amazon VPC 彈性網路介面。)

InboundQueryVolume

對於傳入端點的每個 IP 地址，從網路轉送到指定 IP 地址的 DNS 查詢數目。每個 IP 地址由 IP 地址 ID 識別。您可以使用 Route 53 主控台獲取此值。在適用端點之頁面的 IP 地址區段中，查看 IP address ID (IP 地址 ID) 欄。您也可以使用編程方式獲取值ListResolverEndpointIpAddresses。

有效的統計資訊：總和

單位：計數

OutboundQueryAggregateVolume

對於傳出端點的每個 IP 地址，從 Amazon VPC 轉送至您網路的 DNS 查詢總數包括下列項目：

- 使用指定的 IP 地址從 VPC 轉送到網路的 DNS 查詢數目。
- 當目前帳戶與其他帳戶共用 Resolver 規則時，由其他帳戶建立的 VPC 查詢會透過使用指定的 IP 地址轉送到您的網路。

每個 IP 地址由 IP 地址 ID 識別。您可以使用 Route 53 主控台獲取此值。在適用端點之頁面的 IP 地址區段中，查看 IP address ID (IP 地址 ID) 欄。您也可以使用編程方式獲取值ListResolverEndpointIpAddresses。

有效的統計資訊：總和

單位：計數

Route 53 Resolver 指標的維度

傳入和傳出端點的 Route 53 Resolver 指標會使用 `AWS/Route53Resolver` 命名空間，並提供 `EndpointId` 的指標。如果您為`EndpointId`維度指定值，則會 CloudWatch 傳回指定端點的 DNS 查詢數目。如果未指定`EndpointId`，則會 CloudWatch 傳回目前帳戶所建立之所有端點的 DNS 查詢數 AWS 目。

支援 `OutboundQueryAggregateVolume` 和 `InboundQueryVolume` 指標的 `RniId` 維度。

使用 Amazon 監控 Route 53 解析器 DNS 防火牆規則群組 CloudWatch

您可以使用 Amazon CloudWatch 監控由 Route 53 解析器 DNS 防火牆規則群組篩選的 DNS 查詢數量。Amazon CloudWatch 會收集原始資料並將其處理為可讀且近乎即時的指標。這些統計資料會保存兩週的期間，以便您存取歷史資訊，並更清楚資源的執行方式。根據預設，DNS 防火牆規則群組的度量資料會自動傳送 CloudWatch 至每五分鐘一次。

如需 DNS 防火牆的詳細資訊，請參閱 Route 53 Resolver DNS 防火墻。如需詳細資訊 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 在 Amazon 用 CloudWatch 戶指南。

Route 53 Resolver DNS Firewall 的指標和維度

當您將 Route 53 解析器 DNS 防火牆規則群組與 VPC 建立 CloudWatch 關聯以篩選 DNS 查詢時，DNS 防火牆會開始每 5 分鐘向其篩選的查詢傳送一次度量和維度。如需 DNS 防火墻的指標和維度的詳細資訊，請參閱 CloudWatch Route 53 解析器 DNS 防火牆的度量。

您可以使用下列程序在 CloudWatch 主控台中檢視測量結果，或使用 AWS Command Line Interface (AWS CLI) 來檢視測量結果。

使用 CloudWatch 主控台檢視 DNS 防火牆度量

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽列上，選擇您要檢視的區域。
3. 在導覽窗格中，選擇 指標。
4. 在 All metrics (所有指標) 標籤中，選擇 Route 53 Resolver (Route 53 解析程式)。
5. 選擇您感興趣的指標。

若要使用 AWS CLI

- 在命令提示中，使用下列命令：

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

主題

- CloudWatch Route 53 解析器 DNS 防火牆的度量

CloudWatch Route 53 解析器 DNS 防火牆的度量

此 AWS/Route53Resolver 命名空間包含 Route 53 Resolver DNS 防火牆規則群組的指標。

主題

- Route 53 Resolver DNS 防火牆規則群組的指標
- VPC 的指標
- 防火牆規則群組和 VPC 關聯的指標
- 防火牆規則群組中網域清單的指標

Route 53 Resolver DNS 防火牆規則群組的指標

FirewallRuleGroupQueryVolume

符合防火牆規則群組的 DNS 防火牆查詢數目 (由 FirewallRuleGroupId 指定)。

維度：FirewallRuleGroupId

有效的統計資訊：總和

單位：計數

VPC 的指標

VpcFirewallQueryVolume

來自 VPC 的 DNS 防火牆查詢數目 (由 VpcId 指定)。

維度：VpcId

有效的統計資訊：總和

單位：計數

防火牆規則群組和 VPC 關聯的指標

FirewallRuleGroupVpcQueryVolume

VPC 中符合防火牆規則群組 (由 FirewallRuleGroupId 指定) 的 DNS 防火牆查詢數目 (由 VpcId 指定)。

維度：FirewallRuleGroupId, VpcId

有效的統計資訊：總和

單位：計數

防火牆規則群組中網域清單的指標

FirewallRuleGroupVpcQueryVolume

符合防火牆規則群組中防火牆網域清單 (由 FirewallDomainListId 指定) 的 DNS 防火牆查詢數目 (由 FirewallRuleGroupId 指定)。

維度：FirewallRuleGroupId, FirewallDomainListId

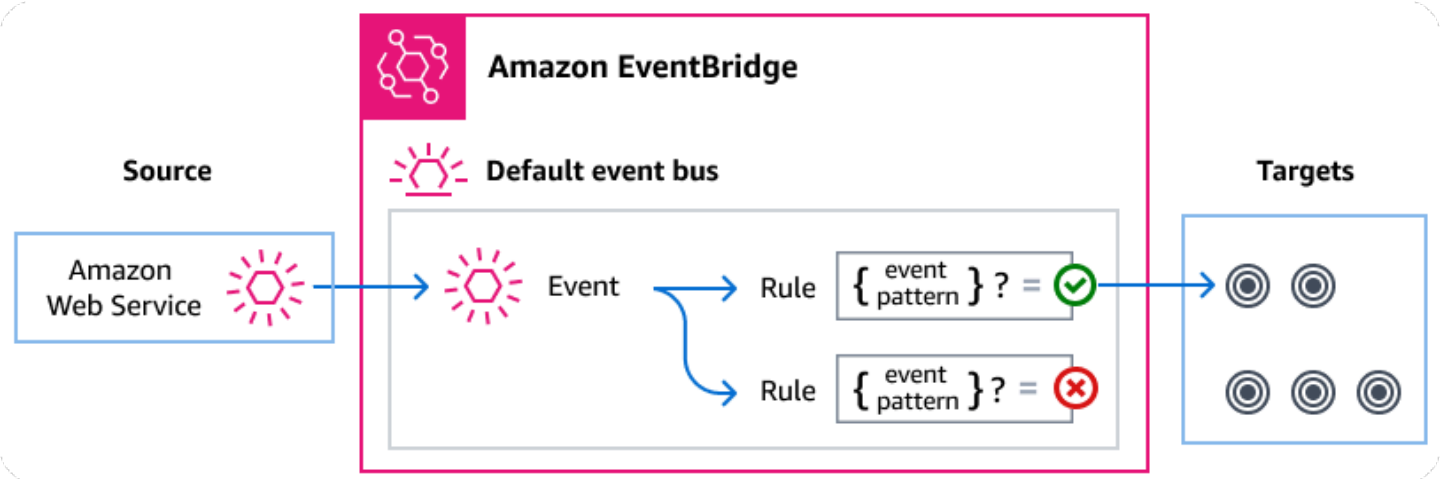
有效的統計資訊：總和

單位：計數

使用管理 Route 53 解析程式 DNS 防火牆事件 Amazon EventBridge

Amazon EventBridge 是一種使用事件將應用程式元件連接在一起的無伺服器服務，讓您更輕鬆地建置可擴充的事件驅動型應用程式。事件驅動架構是一種建置鬆耦合軟體系統的方式，透過發出和回應事件來協作。事件代表資源或環境中的變化。

與許多 AWS 服務一樣，DNS 防火牆會產生事件並將其傳送至 EventBridge 預設事件匯流排。預設事件匯流排會在每個 AWS 帳戶中自動佈建。) 事件匯流排是接收事件，並將事件傳遞至零個或多個目的地或目標的路由器。您為事件匯流排指定的規則會在事件到達時進行評估。每個規則都會檢查事件是否符合規則的事件模式。如果事件不相符，則事件匯流排會將事件傳送到指定的目標。



主題

- Route 53 解析程式 DNS 防火牆事件
- 使用規則傳送 Route 53 解析程式 DNS 防火牆事件 EventBridge
- Amazon EventBridge 權限
- 其他 EventBridge 資源
- Route 53 解析程式 DNS 防火牆事件詳細資料參考

Route 53 解析程式 DNS 防火牆事件

Route 53 解析程式會自動將 DNS 防火牆事件傳送至預設 EventBridge 事件匯流排。您可以在事件匯流排上建立規則；每個規則都包含一個事件模式和一或多個目標。符合規則事件模式的事件會盡最大努力傳遞至指定的目標。活動可能無序交付。

DNS 防火牆會產生下列事件。若要取得更多資訊，請參閱《Amazon EventBridge 使用指南》EventBridge中的。 。

事件明細類型	描述
DNS 防火牆封鎖	對網域執行的任何封鎖動作。
DNS 防火牆警報	對網域執行的任何警示動作。

使用規則傳送 Route 53 解析程式 DNS 防火牆事件 EventBridge

若要讓 EventBridge 預設事件匯流排將 DNS 防火牆事件傳送至目標，您必須建立包含符合所需 DNS 防火牆事件中資料之事件模式的規則。

建立規則包含下列一般步驟：

1. 為指定下列項目的規則建立事件模式：
   - Route 53 解析器是規則評估的事件的來源。
   - (選擇性)：要比對的任何其他事件資料。

   如需更多資訊，請參閱 ???
2. (選擇性)：建立輸入轉換器，在將資訊 EventBridge 傳送至規則目標之前自訂事件中的資料。

   如需詳細資訊，請參閱《EventBridge 使用指南》中的〈輸入轉換〉。
3. 指定要 EventBridge 傳遞符合事件模式之事件的目標。

   目標可以是其他 AWS 服務、 software-as-a-service (SaaS) 應用程式、API 目標或其他自訂端點。如需詳細資訊，請參閱《EventBridge 使用者指南》中的目標。

如需建立事件匯流排規則的完整指示，請參閱《使用指南》中的〈建立對事件做出反應的規則EventBridge 〉。

建立 Route 53 解析程式 DNS 防火牆事件的事件模式

當 DNS 防火牆將事件傳遞至預設事件匯流排時， EventBridge 會使用為每個規則定義的事件模式來判斷是否應將事件傳遞至規則的目標。事件模式符合所需 DNS 防火牆事件中的資料。每個事件模式都是一個 JSON 對象，其中包含：

- 識別傳送事件之服務的 `source` 屬性。對於 DNS 防火牆事件，來源為`aws.route53resolver`。
- (選擇性)：包含要比對之事件類型陣列的 `detail-type` 屬性。

- (選擇性)：包含要比對的任何其他事件資料的 `detail` 屬性。

例如，下列事件模式會比對來自 DNS 防火牆的警示和封鎖事件：

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

以下事件模式與 BLOCK 操作匹配：

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

DNS 防火牆只會在 6 小時的時間內針對同一個網域傳送相同的事件一次。例如：

1. 執行個體 i-123 在時間 T1 傳送 DNS 查詢範例網域。DNS 防火牆會傳送警示或封鎖事件，因為這是第一次發生。
2. 執行個體 i-123 在 T1+30 分鐘的時間傳送一個 DNSquery 範例網域網站。DNS 防火牆不會傳送警示或封鎖事件，因為這是 6 小時視窗內重複發生的事件。
3. 執行個體 i-123 在 T1+7 小時的時間傳送 DNS 查詢範例網域。DNS 防火牆會傳送警示或封鎖事件，因為這發生在 6 小時的視窗之外。

如需撰寫事件模式的詳細資訊，請參閱EventBridge 使用指南中的事件模式。

測試 DNS 防火牆事件的事件模式 EventBridge

您可以使用 S EventBridge andbox 來快速定義和測試事件模式，而無需完成建立或編輯規則的較大程序。您可以使用 Sandbox 定義事件模式，並使用範例事件來確認模式符合所需的事件。 EventBridge 提供您直接從沙箱中使用該事件模式建立新規則的選項。

如需詳細資訊，請參閱使用指南中的使用 EventBridge 沙箱測試事件模式。EventBridge

建立 DNS 防火牆的 EventBridge 規則和目標

下列程序說明如何建立可 EventBridge 傳送所有 DNS 防火牆警示和封鎖動作事件的規則，以及如何將 AWS Lambda 函數新增為規則的目標。

1. 用 AWS CLI 於建立 EventBridge 規則：

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. 附加 Lambda 函數作為規則的目標：

```
AWS events put-targets --rule dns-firewall-rule --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. 若要新增呼叫目標所需的權限，請執行下列 Lambda AWS CLI 命令：

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge 權限

DNS 防火牆不需要任何其他權限即可將事件傳遞給 Amazon EventBridge。

您指定的目標可能需要特定的權限或組態。如需有關針對目標使用特定服務的詳細資訊，請參閱《使Amazon EventBridge 用指南》中的Amazon EventBridge 目標。

其他 EventBridge 資源

如需有關如何使Amazon EventBridge 用處理和管理事件的詳細資訊，請參閱《使 EventBridge 用指南》中的下列主題。

- 如需事件匯流排如何運作的詳細資訊，請參閱Amazon EventBridge 事件匯流排。
- 如需有關事件結構的資訊，請參閱事件。
- 如需建構事件模式以便在符合規則時 EventBridge 使用的相關資訊，請參閱事件模式。
- 如需建立規則以指定 EventBridge 處理哪些事件的相關資訊，請參閱規則。
- 如需指定 EventBridge 將相符事件傳送至哪些服務或其他目的地的資訊，請參閱目標。

Route 53 解析程式 DNS 防火牆事件詳細資料參考

來自 AWS 服務的所有事件都有一組共同的欄位，其中包含事件的相關中繼資料，例如做為事件來源的 AWS 服務、產生事件的時間、發生事件的帳戶和地區，以及其他。如需這些一般欄位的定義，請參閱《Amazon EventBridge 使用指南》中的「事件結構參考」。

此外，每個事件都有一個 `detail` 欄位，其中包含該特定事件的特定資料。下面的參考定義了各種 DNS 防火牆事件的詳細信息字段。

使用 EventBridge 來選取和管理 DNS 防火牆事件時，請牢記下列事項：

- DNS 防火牆中所有事件的`source`欄位都設定為`aws.route53resolver`。
- `detail-type` 欄位指定事件類型。

  例如 `DNS Firewall Block` 或 `DNS Firewall Alert`。
- `detail` 欄位包含該特定事件的特定資料。

如需建構啟用規則以符合 DNS 防火牆事件的事件模式的詳細資訊，請參閱《Amazon EventBridge 使用手冊》中的事件模式。

如需有關事件及其 EventBridge 處理方式的詳細資訊，請參閱《Amazon EventBridge 使用指南》中的Amazon EventBridge 事件。

主題

- DNS 防火牆警示事件詳情
- DNS 防火牆封鎖事件詳細資

DNS 防火牆警示事件詳情

以下是「警示狀態」事件詳細資料的詳細資料欄位。

`source`和`detail-type`欄位會包含在內，因為它們包含 Route 53 事件的特定值。

```
{...,
 "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
 ...,
 "detail": {
```

```
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

識別事件的類型。

對於此事件，此值為`DNS Firewall Alert`。

`source`

識別產生事件的服務。對於 DNS 防火牆事件，此值為`aws.route53resolver`。

`detail`

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

對於此事件，此資料包括：

`account-id`

建立 VPC 的識別碼。 AWS 帳戶

`last-observed-at`

在 VPC 中進行「警示/區塊」查詢時的時間戳記。

`query-name`

查詢中指定的網域名稱 (example.com) 或子網域名稱 (www.example.com)。

`query-type`

要求中指定的 DNS 記錄類型，或任何。如需有關 Route 53 支援的類型的資訊，請參閱 支援的 DNS 記錄類型。

`query-class`

查詢的類別。

`transport`

用來提交 DNS 查詢的通訊協定。

`firewall-rule-action`

由符合查詢中網域名稱的規則指定的動作。ALERT 或 BLOCK。

`firewall-rule-group-id`

符合查詢中網域名稱的 DNS 防火牆規則群組的 ID。如需防火牆規則群組的詳細資訊，請參閱 DNS 防火牆DNS 防火牆規則群組與規則。

`firewall-domain-list-id`

由符合查詢中網域名稱的規則使用的網域清單。

`resourcese`

包含資源類型及其他相關詳細資訊。

`resource-type`

指定資源類型，例如解析程式端點或 VPC 執行個體。

`resource-type``-detail`

有關資源的其他詳細資訊。

Example DNS 防火牆警示事件

以下是警示事件範例。

```
{
 "version": "1.0",
```

```
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Alert",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "ALERT",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0",
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0"
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```


DNS 防火牆封鎖事件詳細資

下面是####的詳細字段。

source和detail-type欄位會包含在內，因為它們包含 Route 53 事件的特定值。


```
{...,
```

```
 "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

識別事件的類型。

對於此事件，此值為`DNS Firewall Alert`。

`source`

識別產生事件的服務。對於 DNS 防火牆事件，此值為`aws.route53resolver`。

`detail`

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

對於此事件，此資料包括：

`account-id`

建立 VPC 的識別碼。 AWS 帳戶

`last-observed-at`

在 VPC 中進行「警示/區塊」查詢時的時間戳記。

`query-name`

查詢中指定的網域名稱 (example.com) 或子網域名稱 (www.example.com)。

`query-type`

要求中指定的 DNS 記錄類型，或任何。如需有關 Route 53 支援的類型的資訊，請參閱 支援的 DNS 記錄類型。

`query-class`

查詢的類別。

`transport`

用來提交 DNS 查詢的通訊協定。

`firewall-rule-action`

由符合查詢中網域名稱的規則指定的動作。ALERT 或 BLOCK。

`firewall-rule-group-id`

符合查詢中網域名稱的 DNS 防火牆規則群組的 ID。如需防火牆規則群組的詳細資訊，請參閱 DNS 防火牆DNS 防火牆規則群組與規則。

`firewall-domain-list-id`

由符合查詢中網域名稱的規則使用的網域清單。

`resourcese`

包含資源類型及其他相關詳細資訊。

`resource-type`

指定資源類型，例如解析程式端點或 VPC 執行個體。

`resource-type``-detail`

有關資源的其他詳細資訊。

Example 範例事件

以下是區塊事件的範例。

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Block",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "BLOCK",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0"
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0",
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```


使用日誌記錄 Amazon 路線 53 API 調用 AWS CloudTrail

Route 53 與一項服務整合 AWS CloudTrail，可提供 Route 53 中使用者、角色或服務所採取之動作記錄的 AWS 服務。CloudTrail 將 Route 53 的所有 API 呼叫擷取為事件，包括來自 Route 53 主控台的

呼叫，以及從 Route 53 API 的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Route 53 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 Route 53 提出的要求、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

主題

- 53 號路線資訊 CloudTrail
- 檢視事件歷史記錄中的 Route 53 事件
- 了解 Route 53 日誌檔案項目

53 號路線資訊 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當活動在 Route 53 中發生時，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需 AWS 帳戶中持續記錄事件 (包括 Route 53 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立權杖時，權杖會套用到所有區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件和從多個帳戶接收 CloudTrail 日誌文件

所有的 Route 53 動作都由記錄下來， CloudTrail 並記錄在 Amazon 路線 53 API 參考中。例如，呼叫`CreateHostedZone`、`CreateHealthCheck`、和`RegisterDomain`動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 IAM 使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

檢視事件歷史記錄中的 Route 53 事件

CloudTrail 可讓您在事件歷史記錄中檢視最近的事件。若要檢視 Route 53 API 請求的事件，您必須在主控台上方的區域選擇器中選擇美國東部 (維吉尼亞北部))。如需詳細資訊，請參閱AWS CloudTrail 使用指南中的檢視具有 CloudTrail 事件歷程記錄的事件。

了解 Route 53 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

`eventName` 元素會識別發生的動作。(在 CloudTrail 記錄檔中，網域註冊動作的第一個字母為小寫，即使其在動作名稱中為大寫。 例如，`UpdateDomainContact`顯示為`updateDomainContact`在日誌中）。 CloudTrail 支援所有路由 53 API 動作。下列範例顯示示範下列動作的 CloudTrail 記錄項目：

- 列出與 AWS 帳戶關聯的託管區域
- 建立運作狀態檢查
- 建立 2 筆記錄
- 刪除託管區域
- 更新已註冊網域的資訊
- 建立 Route 53 Resolver 傳出端點


```
{
    "Records": [
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "1cdbea14-e162-43bb-8853-f9f86d4739ca",
            "eventName": "ListHostedZones",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2015-01-16T00:41:48Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "741e0df7-9d18-11e4-b752-f9c6311f3510",
```

```
            "requestParameters": null,
            "responseElements": null,
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "45ec906a-1325-4f61-b133-3ef1012b0cbc",
            "eventName": "CreateHealthCheck",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:57Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "79915168-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "callerReference": "2014-05-06 64832",
                "healthCheckConfig": {
                    "iPAddress": "192.0.2.249",
                    "port": 80,
                    "type": "TCP"
                }
            },
            "responseElements": {
                "healthCheck": {
                    "callerReference": "2014-05-06 64847",
                    "healthCheckConfig": {
                        "failureThreshold": 3,
                        "iPAddress": "192.0.2.249",
                        "port": 80,
                        "requestInterval": 30,
                        "type": "TCP"
                    },
                    "healthCheckVersion": 1,
                    "id": "b3c9cbc6-cd18-43bc-93f8-9e557example"
```

```
                },
                "location": "https://route53.amazonaws.com/2013-04-01/healthcheck/
b3c9cbc6-cd18-43bc-93f8-9e557example"
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "additionalEventData": {
                "Note": "Do not use to reconstruct hosted zone"
            },
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "883b14d9-2f84-4005-8bc5-c7bf0cebc116",
            "eventName": "ChangeResourceRecordSets",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:43Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "7081d4c6-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "changeBatch": {
                    "changes": [
                        {
                            "action": "CREATE",
                            "resourceRecordSet": {
                                "name": "prod.example.com.",
                                "resourceRecords": [
                                    {
                                        "value": "192.0.1.1"
                                    },
                                    {
                                        "value": "192.0.1.2"
                                    },
                                    {
```

```
                                "value": "192.0.1.3"
                            },
                            {
                                "value": "192.0.1.4"
                            }
                        ],
                        "tTL": 300,
                        "type": "A"
                    }
                },
                {
                    "action": "CREATE",
                    "resourceRecordSet": {
                        "name": "test.example.com.",
                        "resourceRecords": [
                            {
                                "value": "192.0.1.1"
                            },
                            {
                                "value": "192.0.1.2"
                            },
                            {
                                "value": "192.0.1.3"
                            },
                            {
                                "value": "192.0.1.4"
                            }
                        ],
                        "tTL": 300,
                        "type": "A"
                    }
                }
            ],
            "comment": "Adding subdomains"
        },
        "hostedZoneId": "Z1PA6795UKMFR9"
    },
    "responseElements": {
        "changeInfo": {
            "comment": "Adding subdomains",
            "id": "/change/C156SRE0X2ZB10",
            "status": "PENDING",
            "submittedAt": "Jan 16, 2018 12:41:43 AM"
        }
```

```
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "0cb87544-ebee-40a9-9812-e9dda1962cb2",
            "eventName": "DeleteHostedZone",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:37Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "6d5d149f-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "id": "Z1PA6795UKMFR9"
            },
            "responseElements": {
                "changeInfo": {
                    "id": "/change/C1SIJYUYIKVJWP",
                    "status": "PENDING",
                    "submittedAt": "Jan 16, 2018 12:41:36 AM"
                }
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
```

```
        {
            "eventVersion": "1.05",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "userName": "smithj",
                "sessionContext": {
                    "attributes": {
                        "mfaAuthenticated": "false",
                        "creationDate": "2018-11-01T19:43:59Z"
                    }
                },
                "invokedBy": "test"
            },
            "eventTime": "2018-11-01T19:49:36Z",
            "eventSource": "route53domains.amazonaws.com",
            "eventName": "updateDomainContact",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
            "requestParameters": {
                "domainName": {
                    "name": "example.com"
                }
            },
            "responseElements": {
                "requestId": "034e222b-a3d5-4bec-8ff9-35877ff02187"
            },
            "additionalEventData": "Personally-identifying contact information is not
logged in the request",
            "requestID": "015b7313-bf3d-11e7-af12-cf75409087f6",
            "eventID": "f34f3338-aaf4-446f-bf0e-f72323bac94d",
            "eventType": "AwsApiCall",
            "recipientAccountId": "444455556666"
        },
        {
            "eventVersion": "1.05",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
```

```
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "sessionContext": {
                    "attributes": {
                        "mfaAuthenticated": "false",
                        "creationDate": "2018-11-01T14:33:09Z"
                    },
                    "sessionIssuer": {
                        "type": "Role",
                        "principalId": "AROAIUZEZLWWZOEXAMPLE",
                        "arn": "arn:aws:iam::123456789012:role/Admin",
                        "accountId": "123456789012",
                        "userName": "Admin"
                    }
                }
            },
            "eventTime": "2018-11-01T14:37:19Z",
            "eventSource": "route53resolver.amazonaws.com",
            "eventName": "CreateResolverEndpoint",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "192.0.2.176",
            "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
            "requestParameters": {
                "creatorRequestId": "123456789012",
                "name": "OutboundEndpointDemo",
                "securityGroupIds": [
                    "sg-05618b249example"
                ],
                "direction": "OUTBOUND",
                "ipAddresses": [
                    {
                        "subnetId": "subnet-01cb0c4676example"
                    },
                    {
                        "subnetId": "subnet-0534819b32example"
                    }
                ],
                "tags": []
            },
            "responseElements": {
                "resolverEndpoint": {
                    "id": "rslvr-out-1f4031f1f5example",
```

```
                    "creatorRequestId": "123456789012",
                    "arn": "arn:aws:route53resolver:us-west-2:123456789012:resolver-
endpoint/rslvr-out-1f4031f1f5example",
                    "name": "OutboundEndpointDemo",
                    "securityGroupIds": [
                        "sg-05618b249example"
                    ],
                    "direction": "OUTBOUND",
                    "ipAddressCount": 2,
                    "hostVPCId": "vpc-0de29124example",
                    "status": "CREATING",
                    "statusMessage": "[Trace id: 1-5bd1d51e-f2f3032eb75649f71example]
 Creating the Resolver Endpoint",
                    "creationTime": "2018-11-01T14:37:19.045Z",
                    "modificationTime": "2018-11-01T14:37:19.045Z"
                }
            },
            "requestID": "3f066d98-773f-4628-9cba-4ba6eexample",
            "eventID": "cb05b4f9-9411-4507-813b-33cb0example",
            "eventType": "AwsApiCall",
            "recipientAccountId": "123456789012"
        }
    ]
}
```

疑難排解 Amazon Route 53

此章節的主題可協助您排除網域註冊和 DNS 組態的問題。

主題

- 我的網域在網際網路上不可用
- 我的網域已暫停使用 (狀態為 ClientHold)
- 我的網域轉移到 Amazon Route 53 失敗
- 我變更 DNS 設定，但沒有生效
- 我的瀏覽器顯示「找不到伺服器」錯誤
- 我無法將流量路由到為網站託管而設定的 Amazon S3 儲存貯體
- 同一個託管區域被收費兩次
- 我的網域收取了多張發票費用
- 我的 AWS 帳戶已關閉、暫停或終止，且我的網域已在 Route 53 註冊

我的網域在網際網路上不可用

您的網域在網際網路不可用，有以下幾個最常見的可能原因。

主題

- 您註冊新的網域，但沒有按一下確認電子郵件中的連結
- 您將網域註冊轉移到 Amazon Route 53，但未轉移 DNS 服務
- 您轉移網域註冊並在網域設定中指定錯誤的名稱伺服器
- 您先轉移 DNS 服務，但沒有等待足夠長時間就轉移網域註冊
- 刪除 Route 53 用於路由網域網際網路流量的託管區域
- 您的網域已暫停

您註冊新的網域，但沒有按一下確認電子郵件中的連結

當您註冊新的網域，ICANN 會要求我們確認註冊聯絡人的電子郵件地址是否有效。為取得確認，我們會傳送一封內含連結的電子郵件。(如果您未回應第一封電子郵件，我們會重新傳送相同的電子郵件，

最多再傳送兩次。) 您有 3 到 15 天的時間來按一下該連結，具體時間取決於頂層網域。在這之後，該連結將失效。

如果您沒有在規定的時間內按一下電子郵件中的連結，ICANN 會要求我們暫停該網域。如需如何向註冊聯絡人重新傳送確認電子郵件的資訊，請參閱重新傳送授權和確認電子郵件。

您將網域註冊轉移到 Amazon Route 53，但未轉移 DNS 服務

如果您之前的註冊商隨網域註冊提供免費的 DNS 服務，該註冊商可能在您將網域註冊轉移到 Route 53 時即停止提供 DNS 服務。執行以下步驟，判斷是否為此問題，如果是，請予以解決。

還原 DNS 服務 – 如果您之前的註冊商在您將網域註冊轉移到 Route 53 後取消 DNS 服務

1. 聯絡您之前的註冊商，確認他們是否取消您網域的 DNS 服務。如果是，則執行下面三個最快速的方法 (按必要性排序)，來還原網域的 DNS 服務：

   - 如果之前的註冊商提供付費 DNS 服務，請他們使用您的網域的舊 DNS 記錄和名稱伺服器還原 DNS 服務。
   - 如果之前的註冊商規定不進行網域註冊就不提供付費 DNS 服務，則詢問是否可以將網域註冊轉移回去，然後使用您的網域的舊 DNS 記錄和名稱伺服器還原 DNS 服務。
   - 如果您可以將網域註冊轉移回以前的註冊商，但他們沒有保留您的 DNS 記錄，則詢問是否可以將網域註冊轉移回去，並取得以前指派給您的網域的同一組名稱伺服器。如果可以，您將需要重新建立舊 DNS 記錄。不過，一旦您完成此操作，您的網域將再次變得可用。

   如果您之前的註冊商無法幫助您完成以上任一選項，請繼續執行步驟 2。

   > **Important**
   >
   > 如果您無法使用在將網域轉移到 Route 53 時所指定的名稱伺服器來還原 DNS 服務，則在您完成此程序中的其餘步驟後兩天，您的網域在網際網路上才會變得再次可用。DNS 解析程式通常會將網域名稱伺服器的名稱快取 24 到 48 個小時，在此之後所有 DNS 解析程式才能取得新名稱伺服器的名稱。

2. 選擇新的 DNS 服務，例如 Route 53。
3. 使用新 DNS 服務提供的方法來建立託管區域和記錄：

   a. 建立一個與您的網域 (如 example.com) 同名的託管區域。

   b. 使用以前的註冊商提供的區域檔案建立記錄。

如果您選擇 Route 53 做為新的 DNS 服務，可以透過匯入區域檔案建立記錄。如需詳細資訊，請參閱 透過匯入區域檔案建立記錄。

4. 取得新託管區域的名稱伺服器。如果您選擇 Route 53 做為 DNS 服務，請參閱 取得公有託管區域的名稱伺服器。
5. 將網域的名稱伺服器變更為您在步驟 4 中取得的名稱伺服器。如需詳細資訊，請參閱 新增或變更網域的名稱伺服器和黏附記錄。

您轉移網域註冊並在網域設定中指定錯誤的名稱伺服器

當您將網域註冊轉移到 Amazon Route 53 時，您為網域指定的設定之一是將回應網域的 DNS 查詢的一組名稱伺服器。這些名稱伺服器來自於和網域名稱同名的託管區域。託管區域包含有關您如何路由網域流量的資訊，如 www.example.com 的 Web 伺服器的 IP 地址。

您可能無意中為錯誤的託管區域指定名稱伺服器，如果您有多個和網域同名的託管區域，尤其容易發生這種錯誤。若要確認網域是否使用正確託管區域的名稱伺服器，並在必要時更新網域的名稱伺服器，請執行以下程序。

> **Important**
>
> 如果在將網域轉移到 Route 53 時指定錯誤的名稱伺服器記錄，則在更正網域的名稱伺服器後，可能需要長達兩天時間 DNS 服務才能完全還原。因為分佈在網際網路上的 DNS 解析程式通常每兩天請求一次名稱伺服器，並快取回應。

若要取得託管區域的名稱伺服器

1. 如果您對網域使用另一個 DNS 服務，則使用該 DNS 服務提供的方法取得託管區域的名稱伺服器。然後跳到下一個程序。

   如果您使用路由 53 做為網域的 DNS 服務，請登入 AWS Management Console 並開啟路由 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted Zones (託管區域)。
3. 在 Hosted Zones (託管區域) 頁面上，選擇託管區域的選項按鈕 (而非名稱)。

> **Important**
>
> 如果您有多個同名的託管區域，請確保選擇正確託管區域的名稱伺服器。

4. 在右窗格中，記下 Name Servers (名稱伺服器) 下所列的四個伺服器。

若要確認網域使用正確的名稱伺服器

1. 如果您正在為網域使用其他 DNS 服務，請登入 AWS Management Console 並開啟路由 53 主控台，網址為 https://console.aws.amazon.com/route53/

   如果您使用 Route 53，請跳到下一個步驟。
2. 在導覽窗格中，選擇 Registered Domains (已註冊的網域)。
3. 選擇要為其編輯設定的網域名稱。
4. 選擇 Add or Edit Name Servers (新增或編輯名稱伺服器)。
5. 將在上一個程序中取得的名稱伺服器清單，與 Edit Name Servers for domain name (編輯網域名稱的名稱伺服器) 對話方塊中列出的名稱伺服器進行比較。
6. 如果此處所列的名稱伺服器，與在上一個程序中取得的名稱伺服器不相符，則變更此處的名稱伺服器，然後選擇 Update (更新)。

您先轉移 DNS 服務，但沒有等待足夠長時間就轉移網域註冊

當您將 DNS 服務轉移到 Amazon Route 53 或另一個 DNS 服務時，您向網域註冊商更新了網域組態，以使用新 DNS 服務的名稱伺服器。

回應請求的 DNS 解析程式通常會將名稱伺服器的名稱快取 24 到 48 小時。如果您變更某個網域的 DNS 服務，將一個 DNS 服務的名稱伺服器取代為另一個 DNS 服務的名稱伺服器，則最多 48 個小時後，DNS 解析程式才開始使用新名稱伺服器，並進而使用新的 DNS 服務。

以下說明在轉移 DNS 服務後太早轉移網域會導致網域在網際網路上不可用的原因：

1. 您轉移網域的 DNS 服務。
2. 在 DNS 解析程式開始使用您的新 DNS 服務的名稱伺服器之前，您將網域轉移到 Route 53。
3. 當您將網域轉移到 Route 53 後，您以前的註冊商隨即取消您的網域的 DNS 服務。
4. DNS 解析程式還在將查詢路由到您的舊 DNS 服務，但不再有任何記錄告訴它們如何路由您的流量。

當舊 DNS 服務的名稱伺服器的快取到期時，DNS 將開始使用新的 DNS 服務。遺憾的是，目前無法加速此程序。

刪除 Route 53 用於路由網域網際網路流量的託管區域

如果 Route 53 是您網域的 DNS 服務，且如果您刪除用於路由網域網際網路流量的託管區域，則網域將無法在網際網路上使用。無論網域是否透過 Route 53 註冊，都會發生此情況。

> **Important**
>
> 還原網域的網際網路服務可能需要 48 小時。

如果您刪除 Route 53 用於路由網域網際網路流量的託管區域，還原網際網路服務的方式

1. 建立另一個與該網域同名的託管區域。如需詳細資訊，請參閱 建立公有託管區域。
2. 重新建立已刪除託管區域中的記錄。如需詳細資訊，請參閱 處理記錄。
3. 取得 Route 53 指派給新託管區域之名稱伺服器的名稱。如需詳細資訊，請參閱 取得公有託管區域的名稱伺服器。
4. 更新網域註冊以使用您在步驟 3 中取得的名稱伺服器：
   - 如果此網域已向 Route 53 註冊，請參閱 新增或變更網域的名稱伺服器和黏附記錄。
   - 如果此網域已向其他網域註冊商註冊，請使用註冊商提供的方法來更新網域註冊，以使用新的名稱伺服器。
5. 等候名稱伺服器的 TTL 傳遞給遞迴解析程式，該解析程式快取已刪除託管區域之名稱伺服器的名稱。在 TTL 傳遞後，當瀏覽器或應用程式為網域或其子網域之一提交 DNS 查詢時，遞迴解析程式會將查詢轉發到新託管區域的 Route 53 名稱伺服器。如需詳細資訊，請參閱 Amazon Route 53 如何為您的網域路由流量。

   名稱伺服器的 TTL 可能需要 48 小時，取決於網域的 TLD。

您的網域已暫停

因為我們必須暫停您的網域，所以網域在網際網路上可能無法使用。如需詳細資訊，請參閱 我的網域已暫停使用 (狀態為 ClientHold)。

我的網域已暫停使用 (狀態為 ClientHold)

如果 Amazon Route 53暫停您的網域，該網域在網際網路上會變得無法使用。您可以使用下列其中一種方法來判斷網域是否已暫停：

- 在 Route 53 主控台，在 Registered domains (已註冊的網域) 頁面底部的 Alerts (提醒) 表格中尋找該網域名稱。如果 Status (狀態) 欄的值為 clientHold，則該網域已暫停。
- 針對該網域傳送 WHOIS 查詢。如果 Domain Status (網域狀態) 的值為 clientHold，則該網域已暫停。WHOIS 命令在許多作業系統中都可用，在許多網站上也會以 Web 應用程式的形式提供。

此外，當我們暫停網域時，通常會向該網域的註冊聯絡人的電子郵件地址傳送一封電子郵件。不過，如果暫停該網域是基於法院判決，法院可能不允許我們通知註冊聯絡人。

為了讓網域在網際網路上再次可用，您必須解除暫停。以下是網域被暫停的原因以及解除暫停的方法。

> **Note**
>
> 如果您需要取消停用網域的協助，可以免費聯絡 Sup AWS port 務。如需詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

主題

- 您註冊新的網域，但沒有按一下確認電子郵件中的連結
- 您已停用網域自動續約，而且網域已過期
- 您已變更註冊申請人的聯絡人電子郵件地址，但您尚未驗證新的電子郵件地址是有效的
- 我們無法處理您的自動網域續約付款，而且網域已過期
- 使用者違反 AWS 可接受的使用政策，因此我們暫停網域
- 由於法院判決而暫停網域

您註冊新的網域，但沒有按一下確認電子郵件中的連結

當您第一次向網域註冊時，ICANN 要求我們確認註冊人聯絡人的電子郵件地址是否有 AWS 效。為取得確認，我們會傳送一封內含連結的電子郵件。您有 3 到 15 天的時間來按一下該連結，具體時間取決於頂層網域。在這之後，該連結將失效。

> **Note**
>
> 如果您已向 Amazon Route 53 註冊一或多個網域，並使用相同的註冊聯絡人電子郵件地址，則我們不會傳送確認電子郵件。

如果您沒有在規定的時間內按一下電子郵件中的連結，ICANN 會要求我們暫停該網域。如需如何向註冊聯絡人重新傳送確認電子郵件的資訊，請參閱重新傳送授權和確認電子郵件。當您確認電子郵件地址是有效的，我們會自動對網域解除暫停。

您已停用網域自動續約，而且網域已過期

如果為網域啟用自動續約 (新網域或轉移網域的預設值)，我們會在過期日期之前不久自動續約網域註冊。如果您停用自動續約，我們會向註冊聯絡人的電子郵件地址傳送三封提醒電子郵件，以提醒網域註冊即將到期。在網域到期前 45 天，我們就開始傳送這些電子郵件。

如果您停用網域自動續約，而且沒有手動延長網域註冊期間，我們通常會在過期日期當天暫停網域。請注意，有些網域的註冊機構甚至會在過期日期之前刪除網域。

如需有關如何續約已過期網域的資訊，請參閱續約網域的註冊。

您已變更註冊申請人的聯絡人電子郵件地址，但您尚未驗證新的電子郵件地址是有效的

如果您將註冊申請人的聯絡人電子郵件地址變更為您先前尚未驗證的電子郵件地址，ICANN 會要求我們確認註冊申請人的該電子郵件地址是有效的。為取得確認，我們會傳送一封內含連結的電子郵件。您有 3 到 15 天的時間來按一下該連結，具體時間取決於頂層網域。在這之後，該連結將失效。

如果您不在 TLD 註冊商允許的時間內，按一下電子郵件中的連結，ICANN 會要求我們暫停該網域。如需如何向註冊聯絡人重新傳送確認電子郵件的資訊，請參閱重新傳送授權和確認電子郵件。當您確認電子郵件地址是有效的，我們會自動對網域解除暫停。

我們無法處理您的自動網域續約付款，而且網域已過期

如果已啟用網域自動續約，但我們無法處理您的付款 (例如，因為您的信用卡過期)，我們會向網域註冊聯絡人的電子郵件地址傳送多封電子郵件。如果我們沒有收到付款，我們通常會在過期日期當天暫停網域。請注意，有些網域的註冊機構甚至會在過期日期之前刪除網域。

如需有關如何續約已過期網域的資訊，請參閱續約網域的註冊。

使用者違反 AWS 可接受的使用政策，因此我們暫停網域

如果因為使用者違反 AWS 可接受的使用政策而導致我們暫停網域，我們會向網域的註冊聯絡人傳送電子郵件通知。如果 AWS 帳戶因詐騙而遭到停權，我們不會傳送通知電子郵件。)

如果對暫停有異議，請傳送電子郵件至 abuse@amazon.com。

由於法院判決而暫停網域

如果暫停網域是出於法院判決結果，則我們無法對網域解除暫停，直到法院撤銷判決。如果對法院判決的有效性有異議，請傳送電子郵件至 abuse@amazon.com，並附加適用的文件。

我的網域轉移到 Amazon Route 53 失敗

以下是網域轉移到 Amazon Route 53 失敗的一些常見原因。

主題

- 沒有按一下授權電子郵件中的連結
- 您從目前註冊商取得的授權碼無效
- 嘗試將 .es 網域轉移到 Amazon Route 53 時出現「請求中的參數無效」錯誤
- 您要轉移到 Amazon Route 53 的國際化網域名稱是否列在 Punycode 中？

沒有按一下授權電子郵件中的連結

當您將網域註冊轉移到 Amazon Route 53 時，按照 ICANN (網域註冊管理機構) 的要求，網域的註冊聯絡人必須向我們提供轉移授權。為取得授權，我們會向您傳送一封內含連結的電子郵件。您有 5 到 15 天的時間來按一下該連結，具體時間取決於頂層網域。在這之後，該連結將失效。

如果您沒有在規定的時間內按一下電子郵件中的連結，ICANN 會要求我們取消網域轉移。如需如何向註冊聯絡人重新傳送授權電子郵件的資訊，請參閱重新傳送授權和確認電子郵件。

您從目前註冊商取得的授權碼無效

如果您請求將網域轉移到 Amazon Route 53，但沒有收到授權電子郵件，請檢查 Route 53 主控台中的狀態頁面。如果狀態頁面顯示您從註冊商取得的轉移授權碼無效，請執行以下步驟：

1. 聯絡網域目前的註冊商，並請求新授權碼。請確認以下內容：

- 新的授權碼保持有效狀態的時間。必須在該代碼到期之前請求網域轉移。
- 新的授權碼不同於無效的代碼。如果仍相同，請要求目前的註冊商重新整理授權碼。

2. 提交另一個請求以轉移網域。如需詳細資訊，請參閱 將網域註冊轉移到 Amazon Route 53 主題中的 步驟 5：請求轉移。

嘗試將 .es 網域轉移到 Amazon Route 53 時出現「請求中的參數無效」錯誤

當您嘗試將 .es 網域轉移到 Route 53，而註冊聯絡人的聯絡人類型是 Company (公司) 時，Amazon Route 53 將傳回 "Parameters in request are not valid" (請求中的參數無效) 錯誤。若要完成轉移，請將註冊商的聯絡人類型變更為個人，然後重新提交。

您要轉移到 Amazon Route 53 的國際化網域名稱是否列在 Punycode 中？

當您註冊新的網域名稱或建立託管區域和記錄，您可以指定 a-z 之外的字母 (例如法語中的 ç)、其他字母 (例如斯拉夫字母或阿拉伯字母) 中的字元，以及中文、日文或韓文等語言中的字元。Amazon Route 53 會用 Punycode 儲存這些國際化網域名稱 (IDN) (將 Unicode 字元轉換為 ASCII 字串表示)。

如果您在將 IDN 轉移到 Route 53 時遇到錯誤，請使用 Punycode 來表示它，然後再試一次。如需詳細資訊，請參閱 設定國際化網域名稱的格式。

我變更 DNS 設定，但沒有生效

如果您變更 DNS 設定，而變更沒有生效，以下是一些常見原因。

主題

- 您在過去 48 小時將 DNS 服務轉移到 Amazon Route 53，所以 DNS 仍在使用您之前的 DNS 服務
- 您最近將 DNS 服務轉移到 Amazon Route 53，但沒有向網域註冊商更新名稱伺服器
- DNS 解析程式仍使用記錄的舊設定
- 您有多個託管區域使用相同名稱，且您更新了未與網域關聯的託管區域

您在過去 48 小時將 DNS 服務轉移到 Amazon Route 53，所以 DNS 仍在使用您之前的 DNS 服務

當您將 DNS 服務轉移到 Amazon Route 53 時，您使用網域註冊商提供的方法，將先前 DNS 服務的名稱伺服器取代為 Route 53 的四個名稱伺服器。

> **Note**
>
> 如果您不確定是否完成這一部分工作，請參閱[您最近將 DNS 服務轉移到 Amazon Route 53，但沒有向網域註冊商更新名稱伺服器](#)。

網域註冊商通常對名稱伺服器使用 24 到 48 個小時的 TTL (存留時間)。這意味著當某個 DNS 解析程式在取得您的網域名稱伺服器時，會在長達 48 小時的時間內使用該資訊，之後才會提交對於網域的目前名稱伺服器的另一個請求。如果您在過去 48 小時內將 DNS 服務轉移到 Route 53，然後變更 DNS 設定，則有些 DNS 解析程式仍在使用您的舊 DNS 服務來路由網域流量。

您最近將 DNS 服務轉移到 Amazon Route 53，但沒有向網域註冊商更新名稱伺服器

您的網域註冊商擁有網域的各種資訊，包括網域的 DNS 服務的名稱伺服器。網域註冊商通常也是您的 DNS 服務，因此與您的網域關聯的名稱伺服器屬於註冊商。這些名稱伺服器告知 DNS，從何處取得有關您希望如何路由網域流量的資訊，例如，路由到您的網域的 Web 伺服器的 IP 地址。

當您將 DNS 服務轉移到 Amazon Route 53 時，需要使用網域註冊商提供的方法來變更與網域關聯的名稱伺服器。通常，您需要將註冊商提供的名稱伺服器取代為四個 Route 53 名稱伺服器，它們與您為網域建立的託管區域相關聯。

如果您為網域建立新的託管區域和記錄，並指定與先前 DNS 服務不同的設定，但 DNS 仍在將流量路由到舊資源，則有可能您沒有向網域註冊商更新名稱伺服器。若要判斷註冊商是否使用 Route 53 託管區域的名稱伺服器，並在必要時更新網域的名稱伺服器，請執行以下程序：

若要取得您的託管區域的名稱伺服器，並向網域註冊商更新名稱伺服器設定

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在導覽窗格中，選擇 Hosted Zones (託管區域)。
3. 在 Hosted Zones (託管區域) 頁面上，選擇託管區域的名稱 (而非選項按鈕)。

   > **Important**
   >
   > 如果您有多個同名的託管區域，請確保選擇正確託管區域的名稱伺服器。

4. 在 Record name (記錄名稱) 清單中，記下 Name Servers (名稱伺服器) 下所列的四個伺服器。

5. 使用網域註冊商提供的方法，顯示網域名稱伺服器的清單。
6. 如果網域名稱伺服器和您在步驟 4 中取得的名稱伺服器相符，則表示網域組態正確。

   如果網域名稱伺服器和您在步驟 4 中取得的名稱伺服器不相符，請更新網域以使用 Route 53 名稱伺服器。
7.

> **Important**
>
> 如果您將網域名稱伺服器變更為來自 Route 53 託管區域的名稱伺服器，可能需要兩天時間變更才會生效，讓 Route 53 成為您的 DNS 服務。因為分佈在網際網路上的 DNS 解析程式通常每兩天請求一次名稱伺服器，並快取回應。

DNS 解析程式仍使用記錄的舊設定

如果您變更記錄中的設定，但您的流量仍被路由到舊資源 (如您的網站的 Web 伺服器)，一個可能的原因是 DNS 仍快取以前的設定。每個記錄都有 TTL (存留時間) 值，用來指定您希望 DNS 解析程式快取記錄中的資訊 (如 Web 伺服器的 IP 地址) 的時間 (以秒為單位)。直到經過 TTL 所指定的時間後，DNS 解析程式才繼續傳回舊值以回應 DNS 查詢。如果您想知道記錄的 TTL 值，請執行下列程序。

> **Note**
>
> 對於別名記錄，TTL 由記錄路由流量的 AWS 資源決定。如需詳細資訊，請參閱 選擇別名或非別名記錄。

若要檢視記錄的 TTL

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在 Hosted Zones (託管區域) 頁面上，選擇包含該記錄的託管區域的名稱。
3. 在記錄清單中，尋找您想要 TTL 值的記錄，並檢查 TTL 欄的值。

> **Note**
>
> 現在變更 TTL 不會讓變更更快生效。DNS 解析程式已將此值快取，因此，在經過舊設定所指定的時間之前，它們不會得到新的設定。

您有多個託管區域使用相同名稱，且您更新了未與網域關聯的託管區域

您可以使用相同帳戶或多個帳戶，來建立多個有相同名稱的託管區域。為了指定 Route 53 用來為您網域路由網際網路流量的託管區域，您會獲得該託管區域的四個 Route 53 名稱，請將網域註冊更新為使用這些名稱伺服器。

如果您新增、變更或刪除一個託管區域中的記錄，但網域註冊卻在另一個託管區域使用名稱伺服器，則 DNS 查詢的 Route 53 回應不會反映您的變更。如果要判斷您的網域註冊是否有為您更新記錄的託管區域使用名稱伺服器，請執行以下任務：

1. 判斷有哪些名稱伺服器與您的網域註冊建立關聯。請參閱 新增或變更名稱伺服器或黏附記錄。
2. 比較您在步驟 1 中獲得的名稱伺服器，以及 Route 53 指派至您更新記錄之託管區域的名稱伺服器。請參閱 取得公有託管區域的名稱伺服器。

如果網域註冊的名稱伺服器與您更新記錄之託管區域的名稱伺服器不相符，有兩種做法：

變更目前與網域關聯之託管區域中的記錄 (建議)

請記下您在目前未與網域註冊關聯的託管區域中，所做的變更。接著，前往與網域註冊關聯的託管區域並進行相同的變更。因為變更幾乎會立即生效，所以是首選方法。如需詳細資訊，請參閱 編輯記錄。

將網域註冊更新為使用不同的名稱伺服器

將網域註冊更新為使用您更新之託管區域中的名稱伺服器。

> **Important**
>
> 如果您變更了與網域註冊關聯的名稱伺服器，則網域在網際網路上最高會無法使用 2 天。這是因為 DNS 解析程式通常會快取伺服器的名稱 2 天。如果需要 DNS 運作方式的概觀 (包含解析工具快取的資訊)，請參閱 Amazon Route 53 如何為您的網域路由流量。

變更與您網域註冊關聯的名稱伺服器，基本上就是變更網域的 DNS 服務。您有兩種做法，視網域目前是否正在使用而定：

- 如果網域正在使用中，請參閱將 Route 53 做為使用中網域的 DNS 服務。
- 如果網域目前不在使用中，請執行以下任務：
  1. 取得您要用來將流量路由至網域之託管區域的名稱伺服器。請參閱 取得公有託管區域的名稱伺服器。
  2. 在您於步驟 1 取得名稱伺服器的託管區域中，確認 NS 記錄有在使用相同的四個名稱伺服器。如果沒有，請更新 NS 記錄。請參閱 編輯記錄。
  3. 更新網域註冊以使用您在步驟 1 中取得的名稱伺服器。請參閱 新增或變更名稱伺服器或黏附記錄。

我的瀏覽器顯示「找不到伺服器」錯誤

當您嘗試瀏覽網域 (example.com) 或子網域 (www.example.com) 時，如果您的瀏覽器顯示 "Server not found" (找不到伺服器) 錯誤，以下是一些常見的原因說明。

主題

- 您未建立網域或子網域名稱的記錄
- 您建立記錄，但指定錯誤的值
- 流量路由到的資源不可用

您未建立網域或子網域名稱的記錄

如果沒有為網域或子網域建立記錄，那麼如果有人在瀏覽器中輸入該名稱，DNS 就不知道該將流量路由到哪裡。如需詳細資訊，請參閱 處理記錄。

您建立記錄，但指定錯誤的值

當您建立記錄時，很容易指定錯誤的值，例如 Web 伺服器的 IP 位址或指 CloudFront 派給 Web 分發的網域名稱。如果記錄存在，但您仍收到 "Server not found" (找不到伺服器) 錯誤，我們建議您確認值是否正確。

流量路由到的資源不可用

如果記錄指定不可用的資源 (例如 Web 伺服器)，瀏覽器會傳回 "Server not found" (找不到伺服器) 錯誤。我們建議您檢查流量路由到的資源的狀態。

我無法將流量路由到為網站託管而設定的 Amazon S3 儲存貯體

當您為網站託管設定 Amazon S3 儲存貯體時，該儲存貯體的名稱必須與您用來將流量路由到儲存貯體的記錄名稱相同。例如，如果您要將 example.com 的流量路由到為網站託管而設定的某個 S3 儲存貯體，則該儲存貯體的名稱必須為 example.com。

如果您想要將流量路由到為網站託管設定的 S3 儲存貯體，但儲存貯體的名稱未出現在 Amazon Route 53 主控台的別名目標清單中，或者如果您嘗試以程式設計方式建立別名記錄，並且收到 Route 53 API 的 InvalidInput 錯誤訊息，或者 AWS CLI AWS Tools for Windows PowerShell，請檢查以下內容：AWS

- 儲存貯體名稱與記錄名稱完全相符，例如 example.com 或 www.example.com。
- S3 儲存貯體已正確設定，用於網站託管。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的「在 Amazon S3 上託管靜態網站」。

同一個託管區域被收費兩次

如果您在建立託管區域後的 12 小時內刪除它，我們不會向您收費。在 12 小時後，我們會立即針對託管區域收取標準月費。對於不是整月的情況，託管區域的月費不會依比例分配。(此費用同樣適用於您註冊網域時我們自動建立的託管區域。)

如果您在某月的最後一天 (例如 1 月 31 日) 建立一個託管區域，則 1 月的費用可能隨 2 月的費用一起出現在 2 月的發票上。請注意，Amazon Route 53 使用國際標準時間 (UTC) 做為時區來確定託管區域的建立時間。

我的網域收取了多張發票費用

當您註冊訂閱，支付註冊費，轉讓費或續訂費用（包括前期費用）時，將生成唯一的發票。即使付款交易不成功，此發票仍會保留在帳單控制台上。相關的帳單行項目會顯示為 [x] 數量，在 [帳單主控台] 的 [依服務分類的帳單詳細資料] 索引標籤的 [註冊商-全域] 子區段下方。

若要檢視豁免的商業發票，請完成以下步驟：

在帳單主控台上檢視豁免的發票

1. 請登入 AWS Management Console 並開啟 AWS Billing 主控台，網址為 https://console.aws.amazon.com/billing/。
2. 在導覽窗格中，選擇 Bills (帳單)。

3. 選擇「商業發票」以查看任何豁免商業發票的明細。

若要在帳單主控台上檢視成功的付款和退款，請完成以下步驟：

確認已成功處理的付款或退款

1. 在導覽窗格中，選擇付款。
2. 選擇「異動」頁標，以檢視具有的所有已完成交易的「異動」表格 AWS。

我的 AWS 帳戶已關閉、暫停或終止，且我的網域已在 Route 53 註冊

如果您關閉了 AWS 帳戶，或者帳戶被暫停或終止，並且已開啟自動續約，Route 53 將嘗試續約網域註冊，但續約將會失敗。您可以聯絡 Sup AWS port 部門，並向他們尋求下列選項的協助：

- 如果您不想保留網域註冊，Sup AWS port 人員可以停用網域的自動續約功能。這樣可防止您收到有關網域續約的提醒電子郵件。
- 如果您確實想要保留網域註冊，Sup AWS port 人員可以協助您重新啟用帳戶，或將網域轉移到其他網域註冊商。

> **Note**
>
> 在您關閉的 90 天後，您將無法再重新開啟帳戶。如需詳細資訊，請參閱我可以重新開啟已關閉的嗎 AWS 帳戶？ 。

如需更多詳細資訊，請參閱 就網域註冊問題聯絡 S AWS upport。

Amazon Route 53 伺服器的 IP 地址範圍

Amazon Web Services (AWS) 會以 JSON 格式發佈目前的 IP 地址範圍。如果您的防火牆或安全群組根據來源 IP 地址來限制傳入的流量，則請確認您的組態允許來自適用 IP 地址範圍的流量。

如果要檢視 Route 53 目前的 IP 地址範圍，請下載 ip-ranges.json，並使用以下值搜尋檔案：

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

如需有關資 AWS 源 IP 位址的詳細資訊，請參閱AWS Amazon Web Services 一般參考.

Route 53 名稱伺服器的 IP 地址範圍

`"service": "ROUTE53"`：Route 53 名稱伺服器會使用這些 IP 地址範圍。如果您要將 Route 53 用做一或多個網域的 DNS 服務，且想要用 `dig` 或 `nslookup` 命令查詢 名稱伺服器，請將這些範圍列入允許的 IP 地址範圍清單。

> **Note**
>
> 我們很少變更名稱伺服器的 IP 地址；如果需要變更 IP 地址，我們會提前通知您。

Route 53 運作狀態檢查的 IP 地址範圍

`"service": "ROUTE53_HEALTHCHECKS"`：Route 53 運作狀態檢查程式會使用這些 IP 地址範圍。如果您使用 Route 53 運作狀態檢查來檢查網路上資源的運作狀態，請將這些範圍新增至允許的 IP 位址範圍清單。

> **Note**
>
> 我們很少更改健康檢查器的 IP 地址範圍；如果我們需要更改 IP 地址範圍，我們會提前通知您。

如需運作狀態檢查的 IP 地址的詳細資訊，請參閱為 Amazon Route 53 運作狀態檢查設定路由器和防火牆規則。

參考字首清單

字首清單是一個或多個 CIDR 區塊項目的集合，您可用來設定安全群組。Amazon EC2 執行個體的路由器和防火牆規則必須允許來自 Route 53 運作狀態檢查程式所使用 IP 地址的傳入流量。字首清單的參考可協助您簡化規則中 CIDR 區塊的管理。如果您經常在多個規則中使用相同的 CIDR，則您可以在單一字首清單中管理這些 CIDR，而不是在每個規則中重複參照相同的 CIDR。如果您需要移除 CIDR 區塊，則可以從字首清單中移除其項目，而不是從每個受影響的規則中移除該 CIDR。如需有關一般字首清單的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用受管字首清單對 CIDR 區塊分組。

AWS管理前綴列表是 AWS 服務的 IP 地址範圍集。 AWS-managed 前綴列表由 AWS 創建和維護，任何擁有 AWS 帳戶的人都可以使用。您無法建立、修改、共用或刪除 AWS-managed 前置詞清單。

如需有關 AWS-managed 前置詞清單的詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 AWS受管前置詞清單。

Route 53 運作狀態檢查的內部 IP 地址範圍

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`：Route 53 只會在內部使用這些 IP 地址範圍。您不需要將這些範圍新增到允許的範圍清單中。

標記 Amazon Route 53 資源

標籤是您指派給 AWS 資源的標籤。每個標籤皆包含由您定義的索引鍵和值。例如，索引鍵可能是「網域」，而值可能是「example.com」。標籤具有多種用途；一個常見的用途是對 Amazon Route 53 成本進行分類和追蹤。當您將標籤套用至 Route 53 託管區域、網域和運作狀態檢查，AWS 會以逗號分隔值 (CSV) 檔案格式產生一份成本分配報告，其中包含按標籤匯總的用量與成本。您可以套用代表業務類別 (例如成本中心、應用程式名稱或擁有者) 的標籤，來整理多個服務中的成本。如需有關使用成本分配標籤的詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

為了易用性和最佳結果，請使用 AWS Management Console 中的標籤編輯器，此編輯器可讓您集中、整合地建立和管理標籤。如需詳細資訊，請參閱 AWS Management Console 入門中使用標籤編輯器。您也可以使用 Route 53 主控台來套用部分資源的標籤：

- 運作狀態檢查 – 如需詳細資訊，請參閱 命名和標記運作狀態檢查。
- Route 53 Resolver 傳入端點 - 如需詳細資訊，請參閱 當您建立或編輯傳入端點時所指定的值。
- Resolver 傳出端點 - 如需詳細資訊，請參閱 當您建立或編輯傳出端點時所指定的值。
- Resolver 規則 - 如需詳細資訊，請參閱 當您建立或編輯規則時所指定的值。
- 託管區域 - 如需詳細資訊，請參閱 使用託管區域。

> **Note**
>
> Resolver 費用有一部份取決於 VPC 彈性網路界面，分別對應於您為傳入和傳出端點所指定的 IP 地址。您目前無法標記 Resolver 建立的彈性網路界面，因此您無法使用標籤來分配 Resolver 的成本。如需 Resolver 定價的資訊，請參閱 Amazon Route 53 定價。

您也可以藉由使用 Route 53 API 將標籤套用到資源。如需詳細資訊，請參閱 Amazon Route 53 API 參考的依功能的 Route 53 API 動作主題中與標籤有關的動作。

教學課程

以下教學說明如何使用 Amazon Route 53 做為子網域的 DNS 服務，同時使用網域的另一個 DNS 服務，以及如何將 Route 53 用於與加權和延遲記錄相關的多種使用案例。

主題

- 將 Amazon Route 53 做為子網域的 DNS 服務，而不需遷移父系網域
- 轉換到 Amazon Route 53 中的以延遲為基礎的路由
- 在 Amazon Route 53 中將另一個區域新增到以延遲為基礎的路由
- 使用 Amazon Route 53 中的延遲和加權記錄，將流量路由至區域中的多個 Amazon EC2 執行個體
- 在 Amazon Route 53 中管理超過 100 個加權記錄
- 在 Amazon Route 53 中對容錯多記錄回答進行加權

將 Amazon Route 53 做為子網域的 DNS 服務，而不需遷移父系網域

您可以使用 Amazon Route 53 做為新子網域或現有子網域的 DNS 服務，並繼續對父系網域使用其他 DNS 服務。如需詳細資訊，請參閱適用的主題。

主題

- 無需遷移父系網域，建立使用 Amazon Route 53 做為 DNS 服務的子網域
- 無需遷移父系網域，將子網域的 DNS 服務遷移到 Amazon Route 53

無需遷移父系網域，建立使用 Amazon Route 53 做為 DNS 服務的子網域

您可以建立使用 Amazon Route 53 做為 DNS 服務的子網域，而不需從其他 DNS 服務遷移父系網域。

此程序具有下列基本步驟：

1. 了解您是否應該使用此程序。
2. 為子網域建立 Route 53 託管區域。
3. 將新子網域的記錄新增到 Route 53 託管區域。
4. 僅限 API：確認您的變更已傳播到所有 Route 53 DNS 伺服器。

> **Note**
>
> 目前唯一能驗證變更是否已傳播的方式，就是使用 GetChange API 方法。變更通常會在 60 秒內傳播至所有 Route 53 名稱伺服器。

5. 透過為子網域新增名稱伺服器記錄，更新父系網域的 DNS 服務。

決定用於建立子網域的程序

本主題中的程序說明如何執行少見的操作。如果您目前正在使用 Route 53 做為網域的 DNS 服務，並且只希望將流量路由至子網域 (例如 www.example.com) 或您的資源 (例如在 EC2 執行個體上執行的 Web 伺服器)，請參閱 路由傳送子網域的流量。

唯有當您使用網域 (例如 example.com) 的另一個 DNS 服務，而您希望開始使用 Route 53 做為該網域之新子網域 (例如 www.example.com) 的 DNS 服務時，才會使用此程序。

為新子網域建立託管區域

如果您要將 Amazon Route 53 做為子網域的 DNS 服務，而不遷移父系網域，請先為子網域建立託管區域。Route 53 會將子網域的相關資訊存放在託管區域中。

如需有關如何使用 Route 53 主控台建立託管區域的詳細資訊，請參閱 建立公有託管區域。

建立記錄

您可以使用 Amazon Route 53 控制台或 Route 53 API 建立記錄。將子網域的責任委派給 Route 53 之後，在 Route 53 中建立的記錄會成為 DNS 所使用的記錄，如本程序稍後的 使用子網域的名稱伺服器記錄來更新您的 DNS 服務 一節中所說明。

> **Important**
>
> 請勿在 Route 53 託管區域中建立其他名稱伺服器 (NS) 或起始授權 (SOA) 記錄，也請勿刪除現有的 NS 和 SOA 記錄。

若要使用 Route 53 主控台建立記錄，請參閱 處理記錄。若要使用 Route 53 API 建立記錄，請使用 `ChangeResourceRecordSets`。如需詳細資訊，請參閱 Amazon Route 53 API 參考 中的 ChangeResourceRecordSets。

檢查變更的狀態 (僅限 API)

建立新託管區域和變更記錄需要一些時間傳播到 Route 53 DNS 伺服器。如果您使用 ChangeResourceRecordSets 建立記錄，則可以使用 GetChange 動作判斷您的變更是否已傳播。(ChangeResourceRecordSets 會傳回 ChangeId 的值，您可以將其包含在後續 GetChange 請求中。如果您使用主控台建立記錄，則無法使用 ChangeId。) 如需詳細資訊，請參閱 Amazon Route 53 API 參考中的 GET GetChange。

> **Note**
>
> 變更通常會在 60 秒內傳播至所有 Route 53 名稱伺服器。

使用子網域的名稱伺服器記錄來更新您的 DNS 服務

Amazon Route 53 記錄的變更傳播之後 (請參閱 檢查變更的狀態 (僅限 API))，請透過為子網域新增 NS 記錄，更新父系網域的 DNS 服務。這稱為將子網域的責任委派給 Route 53。例如，如果父系網域 example.com 是透過另一個 DNS 服務託管，而且您在 Route 53 中建立子網域 test.example.com，則必須使用 test.example.com 的新 NS 記錄來更新 example.com 的 DNS 服務。

請執行以下程序。

1. 使用您的 DNS 服務提供的方法，備份父系網域的區域檔案。
2. 在 Route 53 主控台中，取得 Route 53 託管區域的名稱伺服器：
   a. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
   b. 在導覽窗格中，按一下 Hosted zones (託管區域)。
   c. 在 Hosted zones (託管區域) 頁面上，選擇託管區域的選項按鈕 (而非名稱)，然後選擇 View details (檢視詳細資訊)。
   d. 在託管區域的詳細資訊頁面上，選擇託管區域詳細資訊。
   e. 記下 Name Servers (名稱伺服器) 下所列的四個名稱。

   或者也可使用 GetHostedZone 動作。如需詳細資訊，請參閱 Amazon Route 53 API 參考中的 GetHostedZone。
3. 使用父系網域的 DNS 服務提供的方法，將子網域的 NS 記錄新增至父系網域的區域檔案。在這些 NS 記錄中，指定四個與您在步驟 1 中建立的託管區域關聯的 Route 53 名稱伺服器。

> **Important**
>
> 請勿將起始授權 (SOA) 記錄新增至父系網域的區域檔案。由於子網域將使用 Route 53，所以父系網域的 DNS 服務不是子網域的授權單位。
> 如果您的 DNS 服務為子網域自動新增 SOA 記錄，請刪除子網域的記錄。不過，請勿刪除父系網域的 SOA 記錄。

無需遷移父系網域，將子網域的 DNS 服務遷移到 Amazon Route 53

您可以遷移子網域以便使用 Amazon Route 53 做為 DNS 服務，而不需從其他 DNS 服務遷移父系網域。

此程序具有下列基本步驟：

1. 了解您是否應該使用此程序。
2. 為子網域建立 Route 53 託管區域。
3. 從父系網域目前的 DNS 服務提供者取得目前 DNS 組態。
4. 將子網域的記錄新增至 Route 53 託管區域。
5. 僅限 API：確認您的變更已傳播到所有 Route 53 DNS 伺服器。

   > **Note**
   >
   > 目前唯一能驗證變更是否已傳播的方式，就是使用 GetChange API 方法。變更通常會在 60 秒內傳播至所有 Route 53 名稱伺服器。

6. 透過為子網域新增名稱伺服器記錄，使用父系網域的 DNS 服務提供者更新 DNS 組態。

決定用於建立子網域的程序

本主題中的程序說明如何執行少見的操作。如果您目前正在使用 Route 53 做為網域的 DNS 服務，並且只希望將流量路由至子網域 (例如 www.example.com) 或您的資源 (例如在 EC2 執行個體上執行的 Web 伺服器)，請參閱 路由傳送子網域的流量。

唯有當您使用網域 (例如 example.com) 的另一個 DNS 服務，而您希望開始使用 Route 53 做為該網域之現有子網域 (例如 www.example.com) 的 DNS 服務，才應使用此程序。

為子網域建立託管區域

如果您要將子網域從其他 DNS 服務遷移至 Amazon Route 53，但不想遷移父系網域，請先為子網域建立託管區域。Route 53 會將子網域的相關資訊存放在託管區域中。

如需有關如何使用 Route 53 主控台建立託管區域的詳細資訊，請參閱 建立公有託管區域。

從您的 DNS 服務提供者取得目前的 DNS 組態

為了簡化將現有子網域遷移至 Route 53 的程序，可從目前提供網域服務的 DNS 服務提供者取得網域目前的 DNS 組態。您可以使用這項資訊做為基礎，來設定 Route 53 做為網域的 DNS 服務。

要求和格式取決於目前做為您的 DNS 服務提供者的公司。在理想情況下，他們將為您提供區域檔案，其中包含有關您目前的組態中所有記錄的資訊。(記錄會告知 DNS 為您的網域和子網域路由流量的方式。例如，當有人在 Web 瀏覽器中輸入您的網域名稱，您希望流量路由到資料中心的 Web 伺服器、Amazon EC2 執行個體、CloudFront 分佈或其他位置？) 如果您可以從目前的 DNS 服務提供者取得區域檔案，您可以編輯區域檔案，以移除您不想遷移到 Amazon Route 53 的記錄。然後，您可以將剩餘記錄匯入 Route 53 託管區域，大幅簡化此程序。請嘗試詢問您目前 DNS 服務提供者的客戶支援如何取得「區域檔案」或「記錄清單」。

建立記錄

使用從目前 DNS 服務提供者取得的記錄做為起點，在為網域所建立的 Amazon Route 53 託管區域中建立對應的記錄。將子網域的責任委派給 Route 53 之後，在 Route 53 中建立的記錄會成為 DNS 所使用的記錄，如本程序稍後的 使用子網域的名稱伺服器記錄來更新您的 DNS 服務 一節中所說明。

> **Important**
>
> 請勿在 Route 53 託管區域中建立其他名稱伺服器 (NS) 或起始授權 (SOA) 記錄，也請勿刪除現有的 NS 和 SOA 記錄。

若要使用 Route 53 主控台建立記錄，請參閱 處理記錄。若要使用 Route 53 API 建立記錄，請使用 `ChangeResourceRecordSets`。如需詳細資訊，請參閱 Amazon Route 53 API 參考 中的 ChangeResourceRecordSets。

檢查變更的狀態 (僅限 API)

建立新託管區域和變更記錄需要一些時間傳播到 Route 53 DNS 伺服器。如果您使用 ChangeResourceRecordSets 建立記錄，則可以使用 `GetChange` 動作判斷您的變更是否已傳播。(`ChangeResourceRecordSets` 會傳回 `ChangeId` 的值，您可以將其包含在後續 `GetChange` 請求

中。如果您使用主控台建立記錄，則無法使用 ChangeId。) 如需詳細資訊，請參閱 Amazon Route 53 API 參考中的 GET GetChange。

> **Note**
>
> 變更通常會在 60 秒內傳播至所有 Route 53 名稱伺服器。

使用子網域的名稱伺服器記錄來更新您的 DNS 服務

Amazon Route 53 記錄的變更傳播之後 (請參閱 檢查變更的狀態 (僅限 API))，請透過為子網域新增 NS 記錄，更新父系網域的 DNS 服務。這稱為將子網域的責任委派給 Route 53。例如，假設父系網域 example.com 透過另一個 DNS 服務託管，並且您要將子網域 test.example.com 遷移到 Route 53。您必須為 test.example.com 建立託管區域，然後使用 Route 53 為 test.example.com 的新託管區域指派的 NS 記錄來更新 example.com 的 DNS 服務。

請執行以下程序。

1. 使用您的 DNS 服務提供的方法，備份父系網域的區域檔案。
2. 如果之前的 DNS 服務提供者有方法為其名稱伺服器變更 TTL 設定，則我們建議您將設定變更為 900 秒。這樣會限制用戶端請求嘗試使用過時的名稱伺服器來解析網域名稱的時間。如果目前的 TTL 是 172800 秒 (兩天，這是常見的預設設定)，您仍需要等待兩天，解析程式和用戶端才能停止使用以前的 TTL 快取 DNS 記錄。TTL 設定過期後，您可以安全地刪除儲存在之前提供者的記錄，並僅對 Route 53 進行變更。
3. 在 Route 53 主控台中，取得 Route 53 託管區域的名稱伺服器：

    a. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。

    b. 在導覽窗格中，按一下 Hosted zones (託管區域)。

    c. 在 Hosted zones (託管區域) 頁面上，選擇託管區域的選項按鈕 (而非名稱)，然後選擇 View details (檢視詳細資訊)。

    d. 在託管區域的詳細資訊頁面上，選擇託管區域詳細資訊。

    e. 記下 Name Servers (名稱伺服器) 下所列的四個名稱。

    或者也可使用 GetHostedZone 動作。如需詳細資訊，請參閱 Amazon Route 53 API 參考中的 GetHostedZone。

4. 使用父系網域的 DNS 服務提供的方法，將子網域的 NS 記錄新增至父系網域的區域檔案。為 NS 記錄指定與子網域相同的名稱。對於 NS 記錄中的值，指定四個與您在步驟 2 中建立的託管區域關聯的 Route 53 名稱伺服器。請注意，不同的 DNS 服務使用不同的術語。您可能需要聯絡您的 DNS 服務技術支援，了解如何執行此步驟。

   > **Important**
   >
   > 請勿將起始授權 (SOA) 記錄新增至父系網域的區域檔案。由於子網域將使用 Route 53，所以父系網域的 DNS 服務不是子網域的授權單位。
   > 如果您的 DNS 服務為子網域自動新增 SOA 記錄，請刪除子網域的記錄。不過，請勿刪除父系網域的 SOA 記錄。

   根據父系網域的名稱伺服器的 TTL 設定的不同，傳播對 DNS 解析程式的變更可能需要 48 小時或更長的時間。在此期間，DNS 解析程式可能仍使用父系網域 DNS 服務的名稱伺服器來回答請求。此外，用戶端電腦的快取中可能還是子網域以前的名稱伺服器。

5. 在網域註冊商的 TTL 設定過期後 (請參閱步驟 2)，從父系網域的區域檔案中刪除以下記錄：

   - 您新增至 Route 53 中的記錄，如 建立記錄 中所述。
   - 您的 DNS 服務的 NS 記錄。當您完成刪除 NS 記錄後，區域檔案中僅有的 NS 記錄將是您在步驟 4 中建立的 NS 記錄。

轉換到 Amazon Route 53 中的以延遲為基礎的路由

使用以延遲為基礎的路由，Amazon Route 53 可以將使用者導向到最低延遲的 AWS 端點。例如，您可以將 DNS 名稱 (如 `www.example.com`) 與 ELB Classic Load Balancer、Application Load Balancer 或 Network Load Balancer 建立關聯，或與美國東部 (俄亥俄) 和歐洲 (愛爾蘭) 區域中託管的 Amazon EC2 執行個體或彈性 IP 地址建立關聯。Route 53 DNS 伺服器會根據過去幾週的網路條件來判斷哪些區域中的哪些執行個體應該服務特定使用者。在倫敦的使用者可能被導向到歐洲 (愛爾蘭) 執行個體，在芝加哥的使用者可能被導向到美國東部 (俄亥俄) 執行個體，以此類推。Route 53 支援以延遲為基礎的路由，用於 A、AAAA、TXT 和 CNAME 記錄，以及 A 和 AAAA 記錄的別名。

> **Note**
>
> 使用者和資源之間延遲的相關資料，完全以使用者和 AWS 資料中心之間的流量為基準。如果您不使用 AWS 區域中的資源，則使用者和資源之間的實際延遲可能和 AWS 延遲資料有很大的差異。即使您的資源與 AWS 區域位於同一個城市，也是如此。

為實現平順、低風險的轉換，您可以結合加權和延遲記錄，逐步從標準路由遷移到每個階段都具有完全控制和轉返功能的 Latency Based Routing。例如，我們假設 `www.example.com` 目前託管於美國東部 (俄亥俄) 區域中的 Amazon EC2 執行個體。該執行個體有彈性 IP 地址 `W.W.W.W`。假設您要繼續將流量路由到美國東部 (俄亥俄) 區域 (如適用)，同時開始將使用者導向美國西部 (加利佛尼亞北部) 區域中 (彈性 IP `X.X.X.X`) 和歐洲 (愛爾蘭) 區域 (彈性 IP `Y.Y.Y.Y`) 中的其他 Amazon EC2 執行個體。`www.example.com` 的 Route 53 託管區域已有 `example.com` 的記錄，其 Type (類型) 為 A 且 Value (值) (IP 地址) 為 `W.W.W.W`。

當您完成以下範例，您將會有兩個加權別名記錄：

- 將 `www.example.com` 的現有記錄轉換為加權別名記錄，以持續將大部分的流量導向到美國東部 (俄亥俄) 區域中的現有 Amazon EC2 執行個體。
- 建立另一個加權別名記錄，該記錄最初只將一小部分的流量導向到您的延遲記錄，後者再將流量路由到所有三個區域。

透過更新這些加權別名記錄中的權重，您可以逐步從僅將流量路由到美國東部 (俄亥俄) 區域，轉移為路由到具有 Amazon EC2 執行個體的所有三個區域。

若要轉換至以延遲為基礎的路由

1. 複製 `www.example.com` 的記錄，但使用新的網域名稱，例如，`copy-www.example.com`。為新記錄指定與 記錄相同的 Type (類型) (A) 和 Value`W.W.W.W` (值) (`www.example.com`)。
2. 更新 `www.example.com` 的現有 A 記錄，使其成為加權別名記錄：

   - 對於 Value/Route traffic to (值/將流量路由到)，選擇 Alias to another record in this hosted zone (此託管區域中其他記錄的別名)，然後指定 `copy-www.example.com`。
   - 對於 Weight (權重)，指定 100。

   當您完成更新，Route 53 會繼續使用此記錄，將所有流量路由至 IP 地址為 `W.W.W.W` 的資源。
3. 為每個 Amazon EC2 執行個體建立延遲記錄，例如：

- 美國東部 (俄亥俄)，彈性 IP 地址 W.W.W.W
- 美國西部 (加利佛尼亞北部)，彈性 IP 地址 X.X.X.X
- 歐洲 (愛爾蘭)，彈性 IP 地址 Y.Y.Y.Y

為所有延遲記錄指定相同的網域名稱 (例如，www-lbr.example.com) 和相同的 A 類型。

當您完成建立延遲記錄，Route 53 會繼續使用您在步驟 2 中更新的記錄來路由流量。

您可以使用 www-lbr.example.com 來執行諸如驗證測試等工作，以確保每個端點都可以接受請求。

4. 現在將 www-lbr.example.com 延遲記錄新增至 www.example.com 加權記錄，並開始將有限流量路由至對應的 Amazon EC2 執行個體。這表示美國東部 (俄亥俄) 區域中的 Amazon EC2 執行個體會從兩個加權記錄取得流量。

   為 www.example.com 建立另一個加權別名記錄：

   - 對於 Value/Route traffic to (值/將流量路由到)，選擇 Alias to another record in this hosted zone (此託管區域中其他記錄的別名)，然後指定 www-lbr.example.com.
   - 對於 Weight (權重)，指定 1。

   當您完成以上程序，且變更已同步到 Route 53 伺服器，Route 53 會開始將一小部分的流量 (1/101) 路由至您在步驟 3 中為其建立延遲記錄的 Amazon EC2 執行個體。
5. 當您確信端點為傳入流量進行了適當的擴展時，據此調整權重。例如，如果您需要 10% 的請求以 Latency Based Routing 為基礎，則將權重分別變更為 90 和 10。

如需建立延遲記錄的詳細資訊，請參閱使用 Amazon Route 53 主控台來建立記錄。

在 Amazon Route 53 中將另一個區域新增到以延遲為基礎的路由

如果您使用 Latency Based Routing，而且要在新區域中新增執行個體，可以透過轉換到 Amazon Route 53 中的以延遲為基礎的路由中逐步將流量轉移至 Latency Based Routing 的相同方式，逐步將流量轉移至新區域。

例如，假設您使用以延遲為基礎的路由來路由 www.example.com 的流量，並且要將亞太區域 (東京) 中的 Amazon EC2 執行個體新增到美國東部 (俄亥俄)、美國西部 (加利佛尼亞北部) 和歐洲 (愛爾蘭) 的執行個體。以下範例程序說明如何在另一個區域中新增執行個體的方式。

在此範例中，www.example.com 的 Amazon Route 53 託管區域已有 example.com 的加權別名記錄，可將流量路由至 www-lbr.example.com 的以延遲為基礎的路由：

- 美國東部 (俄亥俄)，彈性 IP 地址 W.W.W.W
- 美國西部 (加利佛尼亞北部)，彈性 IP 地址 X.X.X.X
- 歐洲 (愛爾蘭)，彈性 IP 地址 Y.Y.Y.Y

加權別名記錄的權重為 100。在您轉換至 Latency Based Routing 之後，假設您刪除用於轉換的另一個加權記錄。

若要在 Route 53 中將另一個區域新增到以延遲為基礎的路由

1. 建立四個新的延遲為基礎的記錄，包括三個原始區域，以及一個要開始向其路由流量的新區域。

   - 美國東部 (俄亥俄)，彈性 IP 地址 W.W.W.W
   - 美國西部 (加利佛尼亞北部)，彈性 IP 地址 X.X.X.X
   - 歐洲 (愛爾蘭)，彈性 IP 地址 Y.Y.Y.Y
   - 亞太區域 (東京)，彈性 IP 地址 Z.Z.Z.Z

   為所有延遲記錄指定相同的新網域名稱 (例如，www-lbr-2012-04-30.example.com) 和相同的 A 類型。

   當您完成建立延遲記錄，Route 53 會繼續使用原始加權別名記錄 (www.example.com) 和延遲記錄 (www-lbr.example.com) 來路由流量。

   您可以使用 www-lbr-2012-04-30.example.com 記錄來執行諸如驗證測試等工作，以確保每個端點都可以接受請求。
2. 為新的延遲記錄建立加權別名記錄：

   - 對於網域名稱，指定現有加權別名記錄的名稱 www.example.com。
   - 對於 Value/Route traffic to (值/將流量路由到)，選擇 Alias to another record in this hosted zone (此託管區域中其他記錄的別名)，然後指定 www-lbr-2012-04-30.example.com。
   - 對於 Weight (權重)，指定 1。

完成後，Route 53 會開始將一小部分的流量 (1/101) 路由至您在步驟 1 中為其建立 www-lbr-2012-04-30.example.com 延遲記錄的 Amazon EC2 執行個體。其餘流量會持續路由到 www-lbr.example.com 延遲記錄，不包含亞太區域 (東京) 區域中的 Amazon EC2 執行個體。

3. 當您確信端點為傳入流量進行了適當的擴展時，據此調整權重。例如，如果您希望 10% 的請求路由到包括東京區域的延遲記錄，請將 www-lbr.example.com 的權重從 100 變更為 90，並將 www-lbr-2012-04-30.example.com 的權重從 1 變更為 10。

如需建立記錄的詳細資訊，請參閱使用 Amazon Route 53 主控台來建立記錄。

使用 Amazon Route 53 中的延遲和加權記錄，將流量路由至區域中的多個 Amazon EC2 執行個體

如果您的應用程式是在二或多個 Amazon EC2 區域的 Amazon EC2 執行個體上執行，並且如果在一或多個區域中有多個 Amazon EC2 執行個體，您可以使用以延遲為基礎的路由將流量路由至正確的區域，然後使用加權記錄，根據指定的權重將流量路由至區域內的執行個體。

例如，假設您在美國東部 (俄亥俄) 區域中有三個具有彈性 IP 地址的 Amazon EC2 執行個體，而且您希望針對使用者 (美國東部 (俄亥俄) 是其適當區域) 在所有三個 IP 之間平均分配請求。在其他區域一個 Amazon EC2 執行個體就足夠，但其實您可以同時對多個區域套用相同技術。

使用 Amazon Route 53 中的延遲和加權記錄，將流量路由至區域中的多個 Amazon EC2 執行個體

1. 為區域中的 Amazon EC2 執行個體建立一組加權記錄。注意下列事項：

   - 為每個加權記錄指定相同的 Record name (記錄名稱) (例如 us-east.example.com) 和 Record type (記錄類型) 值。
   - 針對 Value/Route traffic to (值/路由流量至)，選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)，然後指定某個彈性 IP 地址的值。
   - 如果您想要為 Amazon EC2 執行個體指定同等加權值，請為 Weight (權重) 指定相同的值。
   - 為每個記錄的 Set ID (集合 ID) 指定唯一值。

   如需加權記錄值的詳細資訊，請參閱 加權路由

2. 如果您在其他區域中有多個 Amazon EC2 執行個體，針對其他區域重複步驟 1。為每個區域中的 Name (名稱) 指定不同值。

3. 針對每個您在其中擁有多個 Amazon EC2 執行個體的區域 (例如美國東部 (俄亥俄))，建立延遲別名記錄。對於 Value/Route traffic to (值/將流量路由到)，選擇 Alias to another record in this hosted zone (此託管區域中其他記錄的別名)，然後指定 Record name (記錄名稱) 欄位的值 (例如，`us-east.example.com`)，您將此值指派給該區域中的加權記錄。
4. 對於您有一個 Amazon EC2 執行個體的每個區域，建立延遲記錄。針對 Record name (記錄名稱) 值，請指定您在步驟 3 中建立之延遲別名記錄指定的相同值。針對 Value/Route traffic to (值/路由流量至)，選擇 IP address or another value depending on the record type (IP 地址或其他值，視記錄類型而定)，，然後指定該區域中 Amazon EC2 執行個體的彈性 IP 地址。

   如需有關新增別名記錄至 Amazon EC2 執行個體的詳細資訊，請參閱 將流量路由到 Amazon EC2 執行個體

如需建立記錄的詳細資訊，請參閱使用 Amazon Route 53 主控台來建立記錄。

在 Amazon Route 53 中管理超過 100 個加權記錄

Amazon Route 53 可讓您設定加權記錄。對於指定的名稱和類型 (例如 `www.example.com`，類型 A)，您可以設定高達 100 個替代回應，而且每個回應都有自己的權重。回應 `www.example.com` 的查詢時，Route 53 DNS 伺服器會選取加權的隨機回應，來傳回給 DNS 解析程式。傳回權數為 2 的加權記錄值，平均來說，傳回頻率是權數為 1 的加權記錄值的兩倍。

如果您需要將流量導向到超過 100 個端點，達成此目標的一個方法是使用加權別名記錄和加權記錄樹。例如，樹狀的第一「層」最多可以包含 100 個加權別名記錄，每個加權別名記錄可以指向高達 100 個加權記錄。Route 53 最多允許三個層級的遞迴，讓您能夠管理高達 1,000,000 個唯一的加權端點。

簡單的兩層樹可能如下所示：

加權別名記錄

- `www.example.com` 的 `www-a.example.com` 別名，權重為 1
- `www.example.com` 的 `www-b.example.com` 別名，權重為 1

加權記錄

- `www-a.example.com`，類型 A，值 192.0.2.1，權重 1。
- `www-a.example.com`，類型 A，值 192.0.2.2，權重 1。

- www-b.example.com，類型 A，值 192.0.2.3，權重 1。
- www-b.example.com，類型 A，值 192.0.2.4，權重 1。

如需建立記錄的詳細資訊，請參閱處理記錄。

在 Amazon Route 53 中對容錯多記錄回答進行加權

> **Note**
>
> 使用多值回答路由政策的記錄與此教學課程中記載的設定具有非常相似的行為。主要差別是，教學課程中的設定可讓您指定權重，這在您的端點具有不同容量時很有用。如需更多詳細資訊，請參閱 多值回答路由。

Amazon Route 53 加權記錄只能與一個記錄建立關聯，即一個名稱 (例如 example.com) 和另一個記錄類型 (例如，A) 的組合。但是，通常需要對包含多個記錄的 DNS 回答進行加權。

例如，對於一個服務，您可能有八個 Amazon EC2 執行個體或彈性 IP 端點。如果該服務的用戶端支援連線重試 (就像所有常見的瀏覽器一樣)，則在 DNS 回答中提供多個 IP 地址會在任何特定端點發生故障時為這些用戶端提供替代端點。如果將回應設定包含兩個或多個可用區域中託管的 IP 組合，您甚至可以保範可用區域故障。

當大量用戶端 (例如，行動 Web 應用程式) 共用一小組 DNS 快取，多記錄回答也十分實用。在這種情況下，多記錄回答允許用戶端將請求導向到多個端點，即使用戶端從共享快取收到通用 DNS 回答。

透過使用記錄和加權別名記錄的組合，可實現這些類型的加權多記錄回答。您可以將八個端點分為兩組不同的記錄集，每組包含四個 IP 地址：

endpoint-a.example.com，類型 A，具有下列值：

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

endpoint-b.example.com，類型 A，具有下列值：

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

然後，您可以建立指向每個群組的加權別名記錄：

- www.example.com 的 endpoint-a.example.com 別名，類型 A，權重 1
- www.example.com 的 endpoint-b.example.com 別名，類型 A，權重 1

如需建立記錄的詳細資訊，請參閱處理記錄。

Amazon Route 53 的最佳實務

設定 Route 53 時，請遵循這些最佳實務。

主題

- Amazon Route 53 DNS 的最佳實務
- Resolver 的最佳實務
- Amazon Route 53 運作狀態檢查的最佳實務

Amazon Route 53 DNS 的最佳實務

使用 Amazon Route 53 DNS 服務時，請遵循以下最佳實務以獲得最佳結果。

使用資料平面功能進行 DNS 備援和應用程式復原

Route 53 的資料平面 (包括運作狀態檢查) 以及 Amazon Route 53 應用程式恢復控制器路由控制在全球範圍內進行分佈，並且專為實現 100% 的可用性和功能而設計，即使在嚴重事件中也是如此。它們互相整合，且不依賴於控制平面功能。這些服務的控制平面 (包括其主控台) 通常非常可靠，但它們的設計方式更集中，並優先考慮耐用性和一致性，而不是高可用性。對於災難復原過程中的容錯移轉等情況，我們推薦您使用 Route 53 運作狀態檢查和 Route 53 ARC 路由控制等功能，這些功能依賴於資料平面功能來更新 DNS。如需詳細資訊，請參閱 控制和資料平面概念 和部落格：使用 Amazon Route 53 建立災難復原機制。

為 DNS 記錄選擇 TTL 值

DNS TTL 是數值 (以秒為單位)，DNS 解析程式用來判斷在不對 Route 53 進行另一個查詢的情況下，可以快取多長時間的記錄。所有 DNS 記錄都必須具有為其指定的 TTL。TTL 值的建議範圍為 60 秒到 172,800 秒。

選擇 TTL 是為了在延遲和可靠性以及對變化的回應能力之間進行權衡。如果記錄上的 TTL 較短，DNS 解析程式會更快地注意到記錄的更新，因其必須更頻繁地查詢。這會增加查詢量 (以及成本)。當您延長 TTL 時，DNS 解析程式會更頻繁地從快取中回答查詢，這樣通常更快、更便宜，而且在某些情況下更可靠，因為這樣可以避免透過網際網路進行查詢。沒有正確的值，但值得考慮的是，對您來說更重要的是否是回應能力或可靠性。

設定 TTL 值時需要考慮的項目包括：

- 將 DNS 記錄 TTL 設定為您能夠等待變更生效的時間長度。在委派 (NS 記錄集) 或其他很少變更的記錄 (例如 MX 記錄) 上更是如此。對於這些記錄，建議選擇較長的 TTL。通常可選擇介於一小時 (3,600 秒) 到一天 (86,400 秒) 之間的值。
- 對於作為快速容錯移轉機制的一部分而需要更改的記錄 (特別是經過運作狀態檢查的記錄)，較短的 TTL 更為合適。在這種情況下，將 TTL 設為 60 秒或 120 秒是常見的選擇。
- 當您想要變更關鍵 DNS 條目時，我們建議您暫時縮短 TTL。然後，如果有需要，您就可以快速進行變更、觀察和回復。在最終確定變更並如預期運作之後，您可以增加 TTL。

如需詳細資訊，請參閱 TTL (秒)。

CNAME 記錄

DNS CNAME 記錄是一種將一個網域名稱指向另一個網域名稱的方法。如果 DNS 解析程式解析 domain-1.example.com 並找到指向 domain-2.example.com 的 CNAME，則 DNS 解析程式必須繼續解析 domain-2.example.com，之後才能做出回應。這些記錄在許多情況下都很有用，例如，可用於在網站具有多個網域名稱時確保一致性。

但是，DNS 解析程式必須進行更多查詢才能回答 CNAME，這會增加延遲和成本。在可能的情況下，更快且更便宜的替代方案是使用 Route 53 別名記錄。別名記錄可讓 Route 53 以 AWS 資源 (例如負載平衡器) 和相同託管區域內其他網域的直接回應回應。

如需詳細資訊，請參閱 將網際網路流量路由到您的 AWS 資源。

進階 DNS 路由

- 使用地理位置、地理位置鄰近性或以延遲為基礎的路由時，請務必設定預設值，除非您想要某些用戶端收到無回答的回應。
- 若要最大限度地減少應用程式延遲，請使用以延遲為基礎的路由。這種類型的路由資料可能會經常變更。
- 若要提供路由穩定性和可預測性，請使用地理位置或地理位置鄰近性路由。

如需詳細資訊，請參閱 地理位置路由、地理鄰近路由 及 以延遲為基礎的路由。

DNS 變更傳播

當您使用 Route 53 主控台或 API 建立或更新記錄或託管區域時，需要一些時間才能在網際網路上反映變更。這就是所謂的變更傳播。雖然全域性的傳播通常需要不到一分鐘的時間，但偶爾會出現延遲的情況，例如，由於同步到一個位置的問題，或者在極少數情況下，中央控制平面內出現問題。如果您正在建立自動化佈建工作流程，並且在繼續下一個工作流程步驟之前等待變更傳播完成很重要，請使用 GetChangeAPI 確認 DNS 變更已生效 (`Status =INSYNC`)。

DNS 委派

當您在 DNS 中委派多個級別的子網域時，務必始終從父區域委派。例如，如果您正在委派 www.dept.example.com，您應該從 dept.example.com 區域而不是從 example.com 區域執行此操作。從祖父至子區域的委派可能根本無法運作，或只能在不一致的情況下運作。如需詳細資訊，請參閱 路由傳送子網域的流量。

DNS 回答大小

避免建立大型單一回應。如果回應大於 512 位元組，許多 DNS 解析程式必須透過 TCP (而不是 UDP) 重試，這可能會降低可靠性並導致回應速度較慢。我們建議使用多值回答路由，此會選擇 8 個運作正常的隨機 IP 地址，以將回應保持在 512 位元組的界線內。

如需詳細資訊，請參閱 多值回答路由 和 DNS 回覆大小測試伺服器。

Resolver 的最佳實務

遵循這些最佳實務以最佳化 Route 53 Resolver。

主題

- 避免對 Resolver 端點使用迴圈組態
- Resolver 端點擴展
- Resolver 端點的高可用性
- DNS 區域遍歷

避免對 Resolver 端點使用迴圈組態

請勿將相同的 VPC 與 Resolver 規則及其傳入端點建立關聯 (無論是端點的直接目標，還是透過內部部署 DNS 伺服器)。當 Resolver 規則中的傳出端點指向與規則共用 VPC 的傳入端點時，可能會造成迴圈，其中查詢會持續在傳入端點和傳出端點之間傳遞。

轉送規則仍可以使用 AWS Resource Access Manager (AWS RAM) 與其他帳戶共用的其他 VPC 產生關聯。與樞紐或中央 VPC 相關聯的私有託管區域仍會從查詢解析到傳入端點，因為轉送解析程式規則不會變更此解決方案。

Resolver 端點擴展

Resolver 端點安全群組使用連線追蹤來來收集傳入和流出端點的相關資訊。每個端點截面都有可以追蹤的連線數目上限，而且大量的 DNS 查詢可能會超過連線數，引發調節和查詢丟失。若要減少追蹤的

連線數，請實作安全群組規則，以根據流量的連線狀態允許流量。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的安全群組和連線追蹤。

即使安全性群組組態不需要 AWS Transit Gateway 追蹤，也會自動追蹤透過 Network Load Balancer 和 AWS Lambda (如需完整清單，請參閱自動追蹤的連線) 所建立的連線。

如果透過使用限制性安全群組規則強制執行連線追蹤，或者透過 Transit Gateway 或 Network Load Balancer 路由查詢，則輸入端點每個 IP 位址每秒的整體查詢上限可低至 1500。

傳入和傳出 Resolver 安全群組建議

傳入規則		
通訊協定類型	連接埠號碼	來源 IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0
傳出規則		
通訊協定類型	連接埠號碼	目標 IP
TCP	All	0.0.0.0/0
UDP	All	0.0.0.0/0

傳入 Resolver 端點

對於使用傳入 Resolver 端點的用戶端，如果您有超過 40,000 個唯一 IP 地址和連接埠組合產生 DNS 流量，彈性網路介面的容量就將受到影響。

Resolver 端點的高可用性

當您建立 Route 53 Resolver 傳入端點時，Route 53 會要求您建立至少兩個 IP 地址，網路上的 DNS 解析程式會將查詢轉送至這些地址。您也應該在至少兩個可用區域中指定 IP 地址以進行備援。

如果您需要多個始終可用的彈性網路介面端點，建議您至少建立一個超過所需的網路介面，以確保有額外的容量可用於處理可能的流量激增。額外的網路介面也可確保維護或升級等維修作業期間的可用性。

如需詳細資訊，請參閱 當您建立或編輯傳入端點時所指定的值。

DNS 區域遍歷

DNS 區域遍歷攻擊會嘗試從 DNSEC 簽署的 DNS 區域取得所有內容。如果 Route 53 Resolver 團隊偵測到與在端點上遍歷 DNS 區域時產生的流量模式相符的情況，服務團隊將會調節端點上的流量。因此，您可能會觀察到高百分比的 DNS 查詢逾時。

如果您觀察到端點上的容量降低，並且認為端點已錯誤地進行調節，請前往 https://console.aws.amazon.com/support/home#/ 建立支援案例。

Amazon Route 53 運作狀態檢查的最佳實務

遵循最佳實務來最佳化 Amazon Route 53 運作狀態檢查。

主題

- 適用於運作狀態檢查的彈性 IP 地址的最佳實務

適用於運作狀態檢查的彈性 IP 地址的最佳實務

運作狀態檢查端點的最佳實務是使用彈性 IP 地址。不過，請務必刪除任何與您不再擁有的彈性 IP 地址相關聯的運作狀況檢查。例如，如果您不再使用 Amazon EC2 執行個體，請確保刪除與其彈性 IP 地址相關聯的任何運作狀態檢查。這是因為彈性 IP 地址可以分配給不同的用戶 AWS 帳戶，或者可能會損害您的健康狀態檢查數據。

配額

Amazon Route 53 API 請求和實體受下列配額 (先前稱為「限制」) 的約束。

主題

- 使用 Service Quotas 來檢視和管理配額
- 實體的配額
- API 請求的上限

使用 Service Quotas 來檢視和管理配額

您可以使用 Service Quotas 服務來檢視配額，並為許多 AWS 服務請求提高配額。如需詳細資訊，請參閱 Service Quotas 使用者指南。(您目前可以使用 Service Quotas 來檢視及管理網域、Route 53 和 Route 53 Resolver 配額。)

> **Note**
>
> 若要檢視 Route 53 的配額並要求提高配額，您必須將區域變更為美國東部 (維吉尼亞北部)。若要檢視 Resolver 的配額並要求提高配額，請變更至適用的區域。

實體的配額

Amazon Route 53 實體受下列配額的約束。

如需取得目前配額 (先前稱為「限制」) 的相關資訊，請參閱下列 Route 53 動作：

- GetAccountLimit— 取得運作狀態檢查、託管區域、可重複使用的委派集、流量原則和流量原則記錄的配額
- GetHostedZoneLimit— 在託管區域和 Amazon VPC 上取得可與私有託管區域建立關聯的記錄配額
- GetReusableDelegationSetLimit— 取得可與可重複使用委派集建立關聯的託管區域數量配額

主題

- 網域的配額
- 託管區域的配額

- 記錄的配額
- Route 53 Resolver 的配額
- 運作狀態檢查的配額
- 查詢日誌組態的配額
- 流量流程政策和政策記錄的配額
- 可重複使用委派組的配額

網域的配額

實體	配額
網域	每 AWS 個帳號 20* 申請提高配額。

*截至 2021 年 3 月，新客戶的上限為 20。

如果您擁有現有的帳戶，且預設限額目前為 50，它將保持在 50。

託管區域的配額

實體	配額
託管區域	每個 AWS 帳戶的初始配額為 500，但您可以根據需要要求更高的配額。 申請提高配額。
可以使用相同可重複使用委派組的託管區域	100 申請提高配額。
可以與私有託管區域關聯的 Amazon VPC (每個託管區域)	300

實體	配額
	申請提高配額。
可與 VPC 建立關聯的私有託管區域	沒有配額*
您可以建立的授權，以便將某個帳戶建立的 VPC 與另一個帳戶建立的託管區域相關聯	1000
每個託管區域可以建立的金鑰簽署金鑰 (KSK) 數量	2

* 您可以將 VPC 與您透過 AWS 帳戶控制的任何或所有私有託管區域建立關聯。例如，假設您有三個 AWS 帳戶，而這三個帳戶的預設配額為 500 個託管區域。如果您為這三個帳戶各建立 500 個私有託管區域，您可以建立 VPC 與所有 1,500 個私有託管區域的關聯。

記錄的配額

實體	配額
記錄	每個託管區域 10,000 個 申請提高配額。 在託管區域中如需大於 10,000 個記錄的配額，會產生額外費用。如需詳細資訊，請參閱 Amazon Route 53 定價。
記錄集中的記錄	每個記錄集 400 個
地理位置、延遲、多值回答、加權和以 IP 為基礎的記錄	具有相同名稱和類型的 100 個記錄
地理位置鄰近性記錄	具有相同名稱和類型的 30 個記錄

實體	配額
CIDR 集合	每個 5 個 AWS 帳戶。 申請提高配額。
CIDR 區塊	每個 CIDR 集合 1000 次。 申請提高配額。

Route 53 Resolver 的配額

本節包含所有 Route 53 Resolver 配額

Route 53 Resolver 的配額

請使用下列程序來增加 Route 53 Resolver 的配額。

若要增加 Resolver 的配額

1. 開啟位於 https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas 的 Service Quotas 主控台。
2. 請前往您要提高限額的區域。
3. 選取您想要增加的 Route 53 Resolver 配額名稱。
4. 選擇 Request quota increase (申請提高配額)，輸入配額值，然後選取 Request (申請)。

Route 53 Resolver 端點上的配額

實體	配額
每個 AWS 區域的端點	每個 AWS 帳號 4 個 申請提高配額。
每個端點的 IP 地址	6

實體	配額
	申請提高配額。
每個規則的 IP 地址	6
每個 AWS 區域的規則	每個 AWS 帳號為 1000 元 申請提高配額。
每 AWS 個區域的規則與 VPC 之間的關聯	每個 AWS 帳戶 2000 年 申請提高配額。
端點中每個 IP 地址每秒的查詢	10,000*

* 端點中的每個 IP 位址每秒最多可處理 10,000 個 DNS 查詢 (QPS)。DNS QPS 數目依據查詢類型、回應大小、目標名稱伺服器的運作狀態、查詢回應時間、往返延遲、和正在使用的通訊協定而變化。例如，對於回應速度緩慢的目標名稱伺服器的查詢可以大幅降低網路介面的容量。此外，為了確保高可用性，Route 53 Resolver 會為它接收的每個 DNS 要求產生備援的傳出查詢。因此，每個傳出網路介面的 QPS 將與傳送至 Route 53 Resolver 的 QPS 不相符。使用 CloudWatch 指標來測量傳送至每個網路介面的查詢數目。如需詳細資訊，請參閱 Resolver IP 地址的指標。如果您的最大查詢速率超過端點中任何網路介面容量的 50%，則可以新增更多網路介面來增加端點容量。

即使安全性群組組態不需要 AWS Transit Gateway 追蹤，也會自動追蹤透過 Network Load Balancer 和 AWS Lambda (如需完整清單，請參閱自動追蹤的連線) 所建立的連線。

如果透過使用限制性安全群組規則強制執行連線追蹤，或者透過 Transit Gateway 或 Network Load Balancer 路由查詢，則輸入端點每個 IP 位址每秒的整體查詢最高可低至 1500 次。

Route 53 Resolver 查詢日誌上的配額

實體	配額
每個 AWS 區域的查詢記錄組態	20

實體	配額
每個 AWS 區域的查詢日誌組態 VPC 關聯*	100
共用組態之帳戶所屬的每個 AWS 區域中的每個帳戶能在查詢日誌組態和 VPC 之間建立的關聯數量 (透過 RAM 共用)。	100

* 此為硬性限制。您無法在同一個項目中建立另一個查詢記錄檔組態，AWS 區域 並將其他 100 個 VPC 與其關聯。

Route 53 Resolver DNS 防火牆上的配額

實體	配額
每個 AWS 區域針對單一帳戶與 VPC 相關聯的規則群組數目	5
每個 AWS 區域的單一帳戶，單一 Amazon S3 檔案中的 DNS 防火牆網域數目	250,000 申請提高配額。
每個 AWS 區域之單一帳戶的 DNS 防火牆規則群組數目	1,000 申請提高配額。
每個 AWS 區域之單一帳戶的規則群組內的規則數目	100 申請提高配額。
每個 AWS 區域單一帳戶的網域清單數目	1000 申請提高配額。

實體	配額
每個 AWS 區域的單一帳戶，您可以在所有網域清單中指定的網域數目上限	100,000 申請提高配額。

Outpost 上的解析程式配額

實體	配額
Outpost 上的解析程式執行個體限制	6 個 (至少需要 4 個)

Outpost 執行個體類型的解析程式，以及每個執行個體類型每秒可容納的 DNS 查詢數量：

執行個體類型	每秒查詢數
c5.large	最高 7,000
c5.xlarge	最高 12,000
c5.2xlarge	最高 24,000
c5.4xlarge	最高 56,000
c5d.large	最高 7,000
c5d.xlarge	最高 12,000
c5d.2xlarge	最高 24,000
c5d.4xlarge	最高 56,000
m5.large	最高 7,000

執行個體類型	每秒查詢數
m5.xlarge	最高 12,000
m5.2xlarge	最高 24,000
m5.4xlarge	最高 56,000
m5d.large	最高 7,000
m5d.xlarge	最高 12,000
m5d.2xlarge	最高 24,000
m5d.4xlarge	最高 56,000
r5.large	最高 7,000
r5.xlarge	最高 12,000
r5.2xlarge	最高 24,000
r5.4xlarge	最高 56,000
r5d.large	最高 7,000
r5d.xlarge	最高 12,000
r5d.2xlarge	最高 24,000

執行個體類型	每秒查詢數
r5d.4xlarge	最高 56,000

Outpost 端點執行個體類型的解析程式，以及每個執行個體類型每秒可容納的 DNS 查詢次數：

執行個體類型	每秒查詢數
c5.large	最高 5,000
c5.xlarge	最高 10,000
c5.2xlarge	最高 18,000
c5.4xlarge	最高 30,000
c5d.large	最高 5,000
c5d.xlarge	最高 10,000
c5d.2xlarge	最高 18,000
c5d.4xlarge	最高 30,000
m5.large	最高 5,000
m5.xlarge	最高 10,000
m5.2xlarge	最高 18,000
m5.4xlarge	最高 30,000

執行個體類型	每秒查詢數
m5d.large	最高 5,000
m5d.xlarge	最高 10,000
m5d.2xlarge	最高 18,000
m5d.4xlarge	最高 30,000
r5.large	最高 5,000
r5.xlarge	最高 10,000
r5.2xlarge	最高 18,000
r5.4xlarge	最高 30,000
r5d.large	最高 5,000
r5d.xlarge	最高 10,000
r5d.2xlarge	最高 18,000
r5d.4xlarge	最高 30,000

運作狀態檢查的配額

實體	配額
運作狀態檢查	每個 AWS 帳戶 200 次有效健康檢查

實體	配額
	申請提高配額。
計算的運作狀態檢查可監控的子級運作狀態檢查	255
回應運作狀態檢查請求的標頭長度上限	16,384 位元組 (16K)

查詢日誌組態的配額

實體	配額
查詢日誌組態	每個託管區域 1 個

流量流程政策和政策記錄的配額

實體	配額
流量政策 如需 Route 53 流量流程的詳細資訊，請參閱 使用流量流程來路由 DNS 流量。	每個 AWS 帳號 50 元 申請提高配額。
流量政策版本	每個流量政策 1,000 個
流量政策記錄 (在路線 53 API、 AWS SDK 和 AWS Tools for Windows PowerShell中稱為「政策執行個體」) AWS Command Line Interface	每個 AWS 帳號 5 個 申請提高配額。

可重複使用委派組的配額

實體	配額
可重複使用的委派組	每個 AWS 帳號 100 元 申請提高配額。

API 請求的上限

Amazon Route 53 API 請求受下列配額的約束。

主題

- ChangeResourceRecordSets 請求中元素和字元的數目
- Amazon Route 53 API 請求的頻率
- Route 53 Resolver API 請求的頻率

`ChangeResourceRecordSets` 請求中元素和字元的數目

`ResourceRecord` 元素

一個請求不能包含超過 1,000 個 `ResourceRecord` 元素 (包括別名記錄)。當 `Action` 元素的值為 `UPSERT`，每個 `ResourceRecord` 元素會計數兩次。

最大字元數

一個請求的所有 `Value` 元素中的字元總數 (包括空格) 不能超過 32,000 個字元。當 `Action` 元素的值為 `UPSERT`，`Value` 元素中的每個字元會計數兩次。

Amazon Route 53 API 請求的頻率

所有 Amazon Route 53 API 請求

對於 Amazon 路線 53 API，每個 AWS 帳戶每秒有五個請求。如果每秒提交超過 5 個請求，Amazon Route 53 會傳回 HTTP 400 錯誤 (`Bad request`)。回應標頭還包含值為 `Code` 的 `Throttling` 元素以及值為 `Message` 的 `Rate exceeded` 元素。

> **Note**
>
> 如果您的應用程式超過此限制，我們建議您實作重試的指數退避。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 AWS中的錯誤重試與指數退避。

`ChangeResourceRecordSets` 請求

如果 Route 53 在下一個請求到達之前無法處理請求，它會拒絕同一託管區域的後續請求，並傳回 HTTP 400 錯誤 (`Bad request`)。回應標頭還包含值為 `Code` 的 `PriorRequestNotComplete` 元素以及值為 `Message` 的 `The request was rejected because Route 53 was still processing a prior request.` 元素。

`CreateHealthCheck` 請求

您可以每 2 秒提交一個`CreateHealthCheck`請求 AWS 帳戶。

Route 53 Resolver API 請求的頻率

所有請求

每個區域每個 AWS 帳戶每秒有五個請求。如果區域中每秒提交超過 5 個請求，Resolver 會傳回 HTTP 400 錯誤 (`Bad request`)。回應標頭還包含值為 `Code` 的 `Throttling` 元素以及值為 `Message` 的 `Rate exceeded` 元素。

> **Note**
>
> 如果您的應用程式超過此限制，我們建議您實作重試的指數退避。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 AWS中的錯誤重試與指數退避。

相關資訊

以下相關資源可協助您使用此服務。

主題

- AWS 資源
- 第三方工具和程式庫
- 圖形使用者介面

AWS 資源

Amazon Web Services 中提供一些有用的指南、論壇和其他資源。

- Amazon Route 53 API 參考指南 – 該參考指南中包含結構描述位置；API 動作、參數和資料類型的完整說明；以及該服務傳回的錯誤清單。
- AWS CloudFormation 使用者指南中的 AWS::Route53::RecordSet 類型 - 該屬性用於將 Amazon Route 53 與 AWS CloudFormation 結合使用以建立 AWS CloudFormation 堆疊的自訂 DNS 名稱。
- 開發論壇 – 由社群參與的論壇，可讓開發人員討論 Route 53 的相關技術問題。
- AWS 支援中心 – 此網站匯集了關於您近期支援案例的資訊，和 AWS Trusted Advisor 與運作狀態檢查的結果，並提供連結，可連到開發論壇、技術常見問答集、服務運作狀態儀表板，以及 AWS 支援方案的相關資訊。
- AWS Premium Support 資訊 – 提供 AWS Premium Support 相關資訊的主要網頁，這是一對一的快速回應支援服務管道，可幫助您在 AWS Infrastructure Services 上建置和執行應用程式。
- 聯絡我們 – 用來查詢帳單或帳戶相關問題的連結。對於技術問題，請使用上述開發論壇或支援連結。
- Route 53 產品資訊 – 主要網頁提供 Route 53 的相關資訊，包括其功能與定價資訊等。

- 課程和研討會 – 連結至以角色為基礎的專門課程以及自主進度實驗室，協助加強您的 AWS 技能，並取得實際體驗。
- AWS 開發人員中心 – 研究教學課程、下載工具，以及瞭解 AWS 開發人員活動。
- AWS 開發人員工具 – 連結至開發人員工具、軟體開發套件、IDE 工具組和命令列工具，用來開發及管理 AWS 應用程式。
- 入門資源中心 – 瞭解如何設定 AWS 帳戶、加入 AWS 社群，並啟動您的第一個應用程式。

- 實用的教學課程 - 按照逐步教學課程在 AWS 上啟動第一個應用程式。
- AWS 白皮書 – 連結至完整的技術 AWS 白皮書清單，其中涵蓋了架構、安全和成本等主題，並由 AWS 解決方案架構師或其他技術專家撰寫。
- AWS Support 中心 – 建立和管理您的 AWS Support 案例的中心。這也包含與其他實用資源的連結，例如論壇、技術常見問答集、服務運作狀態以及 AWS Trusted Advisor。
- AWS Support – AWS Support 相關資訊的主要網頁，為一對一的快速回應支援頻道，可協助您在雲端中建置並執行應用程式。
- 聯絡我們 – 查詢有關 AWS 帳單、帳戶、事件、濫用與其他問題的聯絡中心。
- AWS 網站條款 – 我們的著作權與商標；您的帳戶、授權與網站存取；以及其他主題的詳細資訊。

第三方工具和程式庫

除了 AWS 資源，您還可以找到各種可搭配 Amazon Route 53 使用的第三方工具和程式庫。

- AmazonRoute53AppsScript (透過 webos-goodies)

  Amazon Route 53 的 Google 試算表管理。
- AWS適用於 .NET 的 元件 (透過 SprightlySoft)

  適用於 Amazon Web Services 的 SprightlySoft .NET 元件，支援 REST 操作和 Route 53。
- Boto API 下載 (透過 github)

  用於存取 Amazon Web Services 的 Boto Python 介面。
- cli53 (透過 github)

  適用於 Route 53 的命令列介面。
- Dasein Cloud API

  以 Java 為基礎的 API。
- R53.py (透過 github)

  維持來源控制下的 DNS 組態正式版本，並計算組態變更所需的最小變更集。
- route53d

  DNS 前端至 Route 53 API (啟用增量區域轉移 (IXFR))。
- Route53Manager (透過 github)

以 Web 為基礎的介面。

- Ruby Fog (透過 github)

  Ruby 雲端服務程式庫。

- WebService::Amazon::Route53 (透過 CPAN)

  Amazon Route 53 API Perl 介面。

圖形使用者介面

以下第三方工具提供使用 Amazon Route 53 的圖形使用者介面 (GUI)：

- R53 Fox
- Ylastic

文件歷史記錄

以下項目說明每個 Route 53 文件版本的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

主題

- 新聞稿
- 2023 新聞稿
- 2022 年發佈
- 2021 版本
- 2020 版本
- 2018 年版本
- 2017 年版本
- 2016 年版本
- 2015 年版本
- 2014 年版本
- 2013 年版本
- 2012 年版本
- 2011 年版本
- 2010 年版本

新聞稿

2024年2月5 日

您現在可以使 EventBridge 用 Amazon 與 DNS 防火牆實時提醒。如需詳細資訊，請參閱 使用管理 Route 53 解析程式 DNS 防火牆事件 Amazon EventBridge。

2024 年 1 月 9 日

您現在可以使用 DNS 查詢類型作為 DNS 防火牆規則的選用值，以區分規則對特定 DNS 查詢類型的回應。如需詳細資訊，請參閱 Route 53 Resolver DNS 防火墻的元件和設定 及 DNS 防火牆中的規則設定。

2024 年 1 月 9 日

您現在可以使用「快速建立記錄」或「建立記錄」精靈來建立地理鄰近路由記錄。如需詳細資訊，請參閱 地理鄰近路由、地理鄰近度記錄的特定值 及 地理鄰近別名記錄的特定值。

2023 新聞稿

2023 年 12 月 20 日

您現在可以將 DNS over HTTPS 與 Route 53 Resolver 端點搭配使用。如需詳細資訊，請參閱 選擇端點的協定。

2023 年 7 月 20 日

Outposts 上的 Amazon Route 53 現已在 AWS Outposts 機架推出。其中包括一個解析程式，用於快取源自 AWS Outposts 的所有 DNS 查詢。您也可以在部署傳入和傳出端點時，在 Outpost 和內部部署 DNS 解析程式之間設定混合式連線。如需詳細資訊，請參閱 什麼是 Amazon Route 53 on Outposts？。

2023 年 7 月 19 日

您現在可以在啟用 Local Zone 後，將其與地理位置鄰近性路由 (僅限流量) 搭配使用。如需詳細資訊，請參閱 地理鄰近路由 和 Traffic Policy Document Format。

2023 年 3 月 22 日

以全新的網域主控台體驗更新整個 Route 53 指南。您也可以使用全新的主控台體驗，將網域從一個 AWS 帳戶 轉移到另一個 AWS 帳戶。如需詳細資訊，請參閱 註冊新網域 及 轉移網域。

2023 年 3 月 10 日

您現可透過將 IPv4、IPv6 或雙堆疊端點與 Amazon Route 53 Resolver 搭配使用，連線至資源。如需詳細資訊，請參閱 當您建立或編輯傳入端點時所指定的值 及 當您建立或編輯傳出端點時所指定的值。

2022 年發佈

2022 年 9 月 21 日

您現在可以使用政策條件，為使用者提供更新 Amazon Route 53 中資源記錄集的更新權限。如需詳細資訊，請參閱 資源記錄集許可。

2022 年 8 月 30 日

Amazon Route 53 現在支援 2022 年 8 月 1 日之後所建立 AWS App Runner 服務的別名記錄。如需詳細資訊，請參閱 將流量路由到 AWS App Runner 服務。

2022 年 6 月 1 日

以 IP 為基礎的路由選項現在可在 Amazon Route 53 中使用。如需詳細資訊，請參閱 以 IP 為基礎的路由。

2022 年 3 月 16 日

Amazon Route 53 中的私有託管區域現在支援地理位置和以延遲為基礎的路由選項。如需詳細資訊，請參閱 Supported routing policies for records in a private hosted zone。

2022 年 1 月 25 日

已簡化變更 .com.au 和 .net.au TLD 所有權的程序為包括回應兩封電子郵件 (舊註冊者以及新註冊者），且不包括填寫表格。如需更多詳細資訊，請參閱 .com.au (澳洲) 及 .net.au (澳洲)。

2021 版本

2021 年 10 月 26 日

加入了對使用 Amazon Route 53 停用預設反向 DNS 規則的支援。您現在可以停用這些規則的建立，並且將反向 DNS 命名空間的查詢改為轉送至外部伺服器 (如有需要)。如需詳細資訊，請參閱 Resolver 中反向 DNS 查詢的轉送規則。

2021 年 9 月 1 日

添加了一個新的入門主題，引導您完成為靜態網站創建 Amazon CloudFront 分發。如需詳細資訊，請參閱 使用 Amazon CloudFront 分發服務靜態網站。

2021 年 7 月 14 日

開始追蹤 Amazon Route 53 的 AWS 受管政策。如需詳細資訊，請參閱 Amazon Route 53 的 AWS 受管政策。

2021 年 3 月 31 日

新增 Route 53 Resolver DNS 防火墻 透過 DNS 防火牆，您可以針對來自 VPC 的傳出 DNS 要求提供保護。如需詳細資訊，請參閱 Route 53 Resolver DNS 防火墻。

2020 版本

2020 年 12 月 17 日

新增對 Route 53 Resolver 的 DNSSEC 簽署的支援。如需詳細資訊，請參閱 在 Amazon Route 53 中設定 DNSSEC 簽署。

新增對 Route 53 Resolver 的 DNSSEC 簽署的支援。如需詳細資訊，請參閱 在 Amazon Route 53 中啟用 DNSSEC 驗證。

2020 年 9 月 23 日

以新的主控台體驗更新整個 Route 53 指南。如需詳細資訊，請參閱 什麼是 Amazon Route 53？。

2020 年 9 月 1 日

新增對 Resolver 查詢日誌的支援。如需詳細資訊，請參閱 解析程式查詢日誌記錄。

2018 年版本

2018 年 12 月 20 日

您可以建立 Route 53 別名記錄，將流量路由到 API Gateway API 或 Amazon VPC 介面端點。如需詳細資訊，請參閱 值/將流量路由到。

2018 年 11 月 28 日

Route 53 自動命名 (亦稱為服務探索) 現在是一項獨立的服務，即 AWS Cloud Map。如需詳細資訊，請參閱 AWS Cloud Map 開發人員指南。

2018 年 11 月 19 日

您可以使用 Route 53 Resolver 設定 VPC 與網路之間透過 Direct Connect 或 VPN 連接的 DNS 解析。(Resolver 是 Amazon Virtual Private Cloud (Amazon VPC) 在預設情況下提供給所有客戶的遞迴 DNS 服務的新名稱。) 這可讓您將網路上的解析程式的 DNS 查詢轉送到 Route 53 Resolver。Resolver 還可讓您將所選網域名稱 (example.com) 和子網域名稱 (api.example.com) 的查詢，從 VPC 轉送到網路上的解析程式。如需詳細資訊，請參閱 什麼是 Amazon Route 53 Resolver？。

2018 年 11 月 7 日

使用 Route 53 流量和地理鄰近性路由時，您可以使用互動式地圖來將最終使用者路由到全球各地之端點的方式進行視覺化。如需詳細資訊，請參閱 檢視顯示地理位置鄰近性設定效果的地圖。

2018 年 10 月 18 日

您可以使用 Route 53 主控台和 API 來暫時停用 Route 53 運作狀態檢查。這可讓您輕鬆暫停對端點 (例如 Web 伺服器) 的監控，以便在端點上執行維護，而不觸發警示或產生不必要的日誌或狀態訊息。如需詳細資訊，請參閱 您在建立或更新運作狀態檢查時指定的值 中的「停用」。此功能適用於所有三種 Route 53 健康狀態檢查：監控端點的健康狀態檢查、監控其他健康狀態檢查的健全狀況檢查，以及監控 CloudWatch 警示的健康狀態檢查。

2018 年 3 月 13 日

如果您使用自動命名，您現在可以使用第三方運作狀態檢查程式評估資源的運作狀態。在無法透過網際網路使用資源 (例如由於執行個體位於 Amazon VPC) 時，此功能非常實用。如需詳細資訊，請HealthCheckCustomConfig參閱 Amazon 路線 53 API 參考中的。

2018 年 3 月 9 日

IAM 現在包含適用於自動命名的 IAM 受管政策。如需詳細資訊，請參閱 Amazon Route 53 的 AWS 受管政策。

2018 年 2 月 6 日

您現在可以設定自動命名來建立將流量路由至 ELB 負載平衡器的別名記錄，或者建立 CNAME 記錄。如需詳細資訊，請參閱 Amazon 路線 53 RegisterInstanceAPI 參考中 API 文件中的屬性。

2017 年版本

2017 年 12 月 5 日

您現在可以使用 Route 53 自動命名 API 來佈建微服務執行個體。自動命名可讓您自動建立 DNS 記錄，並選擇性地根據您定義的範本建立運作狀態檢查。如需詳細資訊，請參閱 AWS Cloud Map 開發人員指南中的什麼是 AWS Cloud Map？。

2017 年 11 月 16 日

您現在可以透過程式設計方式，取得 Route 53 資源 (例如託管區域和運作狀態檢查) 的目前配額，以及您目前正在使用的每個資源的數目。如需詳細資訊 GetAccountLimitGetHostedZoneLimit，請參閱 Amazon 路線 53 API 參考GetReusableDelegationSetLimit中的、和。

2017 年 10 月 3 日

Route 53 現為 HIPAA 合格服務。如需詳細資訊，請參閱 Amazon Route 53 的合規驗證。

2017 年 9 月 29 日

您現在可以透過程式設計方式檢查網域是否可以轉移到 Route 53。如需詳細資訊，請CheckDomainTransferability參閱 Amazon 路線 53 API 參考中的。

2017 年 9 月 11 日

您現在可以建立 Route 53 別名記錄，該記錄將網際網路流量路由到 Elastic Load Balancing Network Load Balancers。如需別名記錄的詳細資訊，請參閱 選擇別名或非別名記錄。

2017 年 9 月 7 日

如果您使用 Route 53 做為公有、授權 DNS 服務，您現在可以記錄 Route 53 收到的 DNS 查詢。如需詳細資訊，請參閱 公有 DNS 查詢日誌記錄。

2017 年 9 月 1 日

如果您使用 Route 53 流量流程，您現在可以使用地理位置鄰近性，根據使用者和資源之間的實際距離來路由流量。您也可以透過指定正偏差或負偏差，將更多或更少的流量路由到每個資源。如需詳細資訊，請參閱 地理鄰近路由。

2017 年 8 月 21 日

您現在可以使用 Route 53 建立憑證授權單位授權 (CAA) 記錄，該記錄可讓您為網域和子網域指定發出憑證的憑證授權單位。如需詳細資訊，請參閱 CAA 記錄類型。

2017 年 8 月 18 日

您現在可以使用 Route 53 主控台將大量網域轉移到 Route 53。如需詳細資訊，請參閱 將網域註冊轉移到 Amazon Route 53。

2017 年 8 月 4 日

當您註冊網域，有些頂層網域 (TLD) 的註冊機構要求您驗證為註冊聯絡人指定有效的電子郵件。您現在可以在網域註冊程序中傳送驗證電子郵件並確認已成功驗證電子郵件地址。如需詳細資訊，請參閱 註冊新網域。

2017 年 6 月 21 日

如果您要將流量以近乎隨機的方式路由到多個資源 (例如 Web 伺服器)，您現在可以為每個資源建立一個多值回答記錄，並選擇性地將 Route 53 運作狀態檢查關聯至每個記錄。Route 53 最多使用八個正常記錄來回應每個 DNS 查詢，並向不同的 DNS 解析程式提供不同的回應。如需詳細資訊，請參閱 多值回答路由。

2017 年 4 月 10 日

使用 Route 53 主控台將網域註冊轉移到 Route 53 時，您現在可以選擇下列其中一個選項，將網域 DNS 服務的名稱伺服器與已轉移網域註冊建立關聯：

- 使用所選擇的 Route 53 託管區域的名稱伺服器
- 使用網域目前的 DNS 服務的名稱伺服器
- 使用您指定的名稱伺服器

Route 53 會自動將這些名稱伺服器與被轉移的網域註冊關聯。

2016 年版本

2016 年 11 月 21 日

您現在可以建立運作狀態檢查，使用 IPv6 地址檢查端點的運作狀態。如需詳細資訊，請參閱 建立和更新運作狀態檢查。

2016 年 11 月 15 日

您現在可以使用 Route 53 API 動作，將您用一個帳戶建立的 Amazon VPC 與用另一個帳戶建立的私有託管區域相關聯。如需詳細資訊，請參閱 將您用不同 AWS 帳戶建立的 Amazon VPC 與私有託管區域關聯。

2016 年 8 月 30 日

在此版本，Route 53 新增以下新功能：

- 名稱授權單位指標 (NAPTR) 記錄 – 您現在可以建立 NAPTR 記錄，動態委派探索系統 (DDDS) 應用程式會使用該記錄將某個值轉換為另一個值，或將一個值取代為另一個值。例如，一個常見用途是將電話號碼轉換為 SIP URI。如需詳細資訊，請參閱 NAPTR 記錄類型。
- DNS 查詢測試工具 – 您現在可以模擬記錄的 DNS 查詢，並查看 Route 53 傳回的值。對於地理位置及延遲記錄，您也可以模擬來自特定 DNS 解析程式和/或用戶端 IP 地址的請求，了解 Route 53 會向具有該解析程式和/或 IP 地址的用戶端傳回的回應。如需詳細資訊，請參閱 檢查來自 Route 53 的 DNS 回答。

2016 年 8 月 11 日

在此版本，您可以建立將流量路由到 ELB Application Load Balancer 的別名記錄。此程序和 Classic Load Balancer 的程序相同。如需詳細資訊，請參閱 值/將流量路由到。

2016 年 8 月 9 日

在此版本，Route 53 新增 DNSSEC 支援以進行網域註冊。DNSSEC 可讓您保護您的網域免受 DNS 詐騙攻擊 (也稱為攻擊) 的攻擊。 man-in-the-middle 如需詳細資訊，請參閱 設定網域的 DNSSEC。

2016 年 7 月 7 日

您現在可以手動延長網域註冊，用長於註冊機構所指定的最短註冊期間的初始註冊期間來註冊網域。如需詳細資訊，請參閱 延長網域的註冊期間。

2016 年 7 月 6 日

如果您是聯絡地址在印度的 AISPL 客戶，現在可以使用 Route 53 註冊網域。如需詳細資訊，請參閱管理印度帳戶。

2016 年 5 月 26 日

在此版本，Route 53 新增以下新功能：

- 網域帳單報告 – 您現在可以在指定時段內，下載依網域列出所有網域註冊費用的報告。該報告包含產生費用的所有網域註冊操作，包括註冊網域、將網域轉移至 Route 53、續約網域註冊以及 (適用於某些 TLD) 變更網域擁有者。如需詳細資訊，請參閱下列 文件：
  - Route 53 主控台 – 請參閱 下載網域帳單報告。
  - 路線 53 API — 請參閱 Amazon 路線 53 API 參考ViewBilling中的。
- 新的 TLD – 您現在可以註冊具有下列 TLD 的網域：.college、.consulting、.host、.name、.online、.republican、.rocks、.sucks、.trade、.website 和 .uk。如需詳細資訊，請參閱 可向 Amazon Route 53 註冊的網域。
- 用於網域註冊的新 API – 針對需要確認註冊聯絡人電子郵件地址是否有效的操作 (如註冊新網域時)，您現在可以透過程式設計方式，判斷註冊聯絡人是否已按一下確認電子郵件中的連結；如果未按，則會判斷該連結是否仍然有效。您也可以透過程式設計方式請求我們傳送另一封確認電子郵件。如需詳細資訊，請參閱 Amazon Route 53 API 參考中的下列文件：
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

2016 年 4 月 5 日

在此版本，Route 53 新增以下新功能：

- 根據 CloudWatch 指標的 Health 狀態檢查 — 您現在可以根據任何 CloudWatch 測量結果的警示狀態建立健全狀況檢查。對於標準 Route 53 運作狀態檢查無法存取的端點 (例如 Amazon Virtual

Private Cloud (VPC) 中僅有私有 IP 地址的執行個體)，這種運作狀態檢查方法很有用。如需詳細資訊，請參閱下列 文件：

- Route 53 主控台 – 請參閱「建立或更新運作狀態檢查時指定的值」主題中的 監控 CloudWatch 警示。
- 路線 53 API — 請參閱 Amazon 路線 53 API 參考UpdateHealthCheck中的CreateHealthCheck和。

- 可設定的運作狀態檢查位置 – 您現在可以選擇用於檢查資源運作狀態的 Route 53 運作狀態檢查區域，從而減輕運作狀態檢查端點的負載。如果您的客戶集中在一個或幾個地理區域，此功能很有用。如需詳細資訊，請參閱下列 文件：
  - Route 53 主控台 – 請參閱「建立或更新運作狀態檢查時指定的值」主題中的 Health checker regions。
  - 路線 53 API — 請參閱 Amazon 路線 53 API 參考UpdateHealthCheck中的CreateHealthCheck和中的`Regions`元素。
- 私有託管區域中的容錯移轉 – 您現在可以在私有託管區域中建立容錯移轉和容錯移轉別名記錄。此功能與以指標為基礎的運作狀態檢查結合時，您甚至可以為只有私有 IP 地址且使用標準 Route 53 運作狀態檢查無法存取的端點設定 DNS 備援。如需詳細資訊，請參閱下列 文件：
  - Route 53 主控台 - 請參閱 在私有託管區域中設定容錯移轉。
  - 路線 53 API — 請參閱 Amazon 路線 53 API 參考ChangeResourceRecordSets中的。
- 私有託管區域中的別名記錄 – 過去，您可以建立只將 DNS 查詢路由至相同託管區域中其他 Route 53 記錄的別名記錄。在此版本，您還可以建立別名記錄，將 DNS 查詢路由到具有區域化子網域、Elastic Load Balancing 負載平衡器和 Amazon S3 儲存貯體的 Elastic Beanstalk 環境。您仍然無法建立別名記錄，將 DNS 查詢路由到 CloudFront 發行版。) 如需詳細資訊，請參閱下列 文件：
  - Route 53 主控台 - 請參閱 選擇別名或非別名記錄。
  - 路線 53 API — 請參閱 Amazon 路線 53 API 參考ChangeResourceRecordSets中的。

2016 年 2 月 23 日

當您建立或更新 HTTPS 運作狀態檢查，您現在可以設定 Route 53 在 TLS 交涉期間將主機名稱傳送到端點。這允許端點使用適用的 SSL/TLS 憑證來回應 HTTPS 請求。如需詳細資訊，請參閱「建立或更新運作狀態檢查時指定的值」主題中Enable SNI 欄位的描述。如需有關如何在使用 API 建立或更新運作狀態檢查時啟用 SNI 的詳細資訊，請參閱 Amazon Route 53 API 參考UpdateHealthCheck中的CreateHealthCheck和。

2016 年 1 月 27 日

您現在可以為 100 多個附加頂層網域 (TLD) (例如 .accountants、.band 和 .city) 註冊網域。如需支援的 TLD 的完整清單，請參閱可向 Amazon Route 53 註冊的網域。

2016 年 1 月 19 日

您現在可以建立將流量路由至 Elastic Beanstalk 環境的別名記錄。如需如何使用 Route 53 主控台建立記錄的資訊，請參閱 使用 Amazon Route 53 主控台來建立記錄。如需使用 API 建立記錄的相關資訊，請參閱 Amazon 路線 53 API 參考ChangeResourceRecordSets中的。

2015 年版本

2015 年 12 月 3 日

Route 53 主控台現在包含視覺化編輯器，可讓您快速建立使用 Route 53 加權、延遲、容錯移轉和地理位置路由政策組合的複雜路由組態。然後，您可以將組態與相同託管區域或多個託管區域中的一或多個網域名稱 (例如 example.com) 或子網域名稱 (如 www.example.com) 關聯。此外，如果新組態執行不如預期，您可以復原更新。使用 Route 53 API、AWS 開發套件、AWS CLI 和 AWS Tools for Windows PowerShell，可取得此相同功能。如需使用視覺化編輯器的相關資訊，請參閱使用流量流程來路由 DNS 流量。如需使用 API 建立流量流程組態的詳細資訊，請參閱 Amazon Route 53 API 參考。

2015 年 10 月 19 日

在此版本，Route 53 新增以下新功能：

- 透過 Amazon Registrar, Inc. 註冊 .com 和 .net 網域 - Amazon 現在是 ICANN 認可的註冊商，可透過 Amazon Registrar, Inc. 註冊 .com 和 .net 頂層網域 (TLD)。使用 Route 53 註冊 .com 或 .net 網域時，Amazon Registrar 將是記錄有案的註冊商，並將在 Whois 查詢結果中列為「贊助註冊商」。如需使用 Route 53 註冊網域的資訊，請參閱 使用 Amazon Route 53 註冊和管理網域。
- .com 和 .net 網域的隱私權保護 – 現在當您使用 Route 53 註冊 .com 或 .net 網域時，會隱藏所有個人資訊 (包括名字和姓氏)。使用 Route 53 註冊其他網域時，不會隱藏名字和姓氏。如需隱私權保護的詳細資訊，請參閱 為網域的聯絡資訊啟用或停用隱私權保護。

2015 年 9 月 15 日

在此版本，Route 53 新增以下新功能：

- 計算的運作狀態檢查 – 您現在可以建立運作狀態檢查，其狀態由其他運作狀態檢查的運作狀態來判斷。如需詳細資訊，請參閱 建立和更新運作狀態檢查。此外，請參閱 CreateHealthCheckAmazon 路線 53 API 參考。
- 運作狀態檢查的延遲測量 – 您現在可以設定 Route 53 測量運作狀態檢查程式和端點之間的延遲。延遲資料會顯示在路由 53 主控台的 Amazon CloudWatch 圖形中。若要為新運作狀態檢查啟用延遲測量，請參閱主題 您在建立或更新運作狀態檢查時指定的值 中 進階組態 (僅限 "Monitor an endpoint") 下的延遲測量設定。(您無法為現有的運作狀態檢查啟用延遲測量。) 此外，請參閱 MeasureLatencyAmazon 路線 53 API 參考CreateHealthCheck中的主題。
- Route 53 主控台中運作狀態檢查儀表板的更新 — 用於監控運作狀態檢查的儀表板已透過多種方式改進，包括用於監控 Route 53 健全狀況檢查程式和端點之間延遲的 CloudWatch 圖形。如需詳細資訊，請參閱 監控運作狀態檢查狀態和取得通知。

2015 年 3 月 3 日

Amazon Route 53 開發人員指南現在解釋如何為 Route 53 託管區域設定白標籤名稱伺服器。如需詳細資訊，請參閱 設定白標籤名稱伺服器。

2015 年 2 月 26 日

您現在可以使用 Route 53 API，以名稱字母順序列出與 AWS 帳戶關聯的託管區域。您也可以取得與帳戶關聯的託管區域計數。如需詳細資訊 ListHostedZonesByName，請參閱 Amazon 路線 53 API 參考GetHostedZoneCount中的和。

2015 年 2 月 11 日

在此版本，Route 53 新增以下新功能：

- 運作狀態檢查狀態 – Route 53 主控台的運作狀態檢查頁面現在包含 Status (狀態) 欄，可讓您查看所有運作狀態檢查的整體狀態。如需詳細資訊，請參閱 檢視運作狀態檢查狀態和運作狀態檢查失敗的原因。
- 與集成 AWS CloudTrail — Route 53 現在可 CloudTrail 以與以捕獲有關您的AWS帳戶發送到 Route 53 API 的每個請求的信息。整合 Route 53，並 CloudTrail 可讓您判斷向 Route 53 API 發出哪些要求、發出每個要求的來源 IP 位址、提出要求的人員、提出要求的時間等。如需詳細資訊，請參閱 使用日誌記錄 Amazon 路線 53 API 調用 AWS CloudTrail。
- 運作 Health 態檢查的快速警示 — 當您使用 Route 53 主控台建立運作狀態檢查時，您現在可以同時建立運作狀態檢查的 Amazon CloudWatch 警示，並指定 Route 53 認為端點運作狀態不良一分鐘時要通知誰。如需詳細資訊，請參閱 建立和更新運作狀態檢查。
- 託管區域和網域的標記 – 您現在可以將通常用於成本分配的標籤指派至 Route 53 託管區域和網域。如需詳細資訊，請參閱 標記 Amazon Route 53 資源。

2015 年 2 月 5 日

您現在可以使用 Route 53 主控台更新網域的聯絡資訊。如需詳細資訊，請參閱 註冊或轉移網域時所指定的值。

2015 年 1 月 22 日

您現在可以在向 Route 53 註冊新網域時指定國際化網域名稱。(Route 53 已經支援國際化網域名稱用於託管區域和記錄。) 如需詳細資訊，請參閱 DNS 網域名稱格式。

2014 年版本

2014 年 11 月 25 日

在此版本中，您現在可以編輯建立託管區域時為其指定的註解。在主控台中，按一下 Comment (註解) 欄位旁邊的鉛筆圖示，然後輸入新值。如需有關使用路線 53 API 變更註解的詳細資訊，請參閱 Amazon 路線 53 API 參考UpdateHostedZoneComment中的。

2014 年 11 月 5 日

在此版本，Route 53 新增以下新功能：

- 私有 DNS，用於使用 Amazon Virtual Private Cloud 建立的 VPC – 您現在可以使用 Route 53 管理 VPC 的內部網域名稱，而不用將 DNS 資料暴露於公有網際網路。如需詳細資訊，請參閱 使用私有託管區域。
- 運作狀態檢查失敗原因 – 您現在可以看到所選運作狀態檢查的目前狀態，以及上一次運作狀態檢查失敗的詳細原因，如每個 Route 53 運作狀態檢查程式所報告。狀態包含 HTTP 狀態碼，而失敗原因包含有關多種失敗原因的資訊，例如字串比對失敗和回應逾時。如需詳細資訊，請參閱 檢視運作狀態檢查狀態和運作狀態檢查失敗的原因。
- 可重複使用的委派組 – 您現在可以將同一組四個授權名稱伺服器 (統稱為委派組) 套用至多個對應於不同網域名稱的託管區域。這可大幅簡化將 DNS 服務遷移至 Route 53 和管理大量託管區域的程序。使用可重複使用的委派組目前要求您使用 Route 53 API 或 AWS 開發套件。如需詳細資訊，請參閱 Amazon Route 53 API 參考。
- 改進了地理定位路由 — 我們通過添加對 EDNS0 edns-client-subnet 擴展的支持進一步提高了地理定位路由的準確性。如需詳細資訊，請參閱 地理位置路由。
- 對 Signature v4 的支援 – 您現在可以使用 Signature 版本 4 簽署所有 Route 53 API 請求。如需詳細資訊，請參閱 Amazon Route 53 API 參考中的簽署 Route 53 API 要求。

2014 年 7 月 31 日

在此版本中，您現在可以執行以下動作：

- 使用 Route 53 註冊網域名稱 如需詳細資訊，請參閱 使用 Amazon Route 53 註冊和管理網域。
- 設定 Route 53，根據查詢來自的地理位置來回應 DNS 查詢。如需詳細資訊，請參閱 地理位置路由。

2014 年 7 月 2 日

在此版本中，您現在可以執行以下動作：

- 編輯運作狀態檢查中的大多數值。如需詳細資訊，請參閱 建立、更新和刪除運作狀態檢查。
- 使用 Route 53 API 取得 Route 53 運作狀態檢查程式用於檢查資源運作狀態的 IP 範圍清單。可以使用這些 IP 地址來設定您的路由器和防火牆規則，以允許運作狀態檢查程式檢查資源的運作狀態。如需詳細資訊，請GetCheckerIpRanges參閱 Amazon 路線 53 API 參考中的。
- 將成本分配標籤指派至運作狀態檢查，也可讓您指派運作狀態檢查的名稱。如需詳細資訊，請參閱 命名和標記運作狀態檢查。
- 使用 Route 53 API 取得與您的 AWS 帳戶相關的運作狀態檢查數目。如需詳細資訊，請GetHealthCheckCount參閱 Amazon 路線 53 API 參考中的。

2014 年 4 月 30 日

在此版本中，您現在可以建立運作狀態檢查，並使用網域名稱 (而非 IP 地址)來指定端點。當端點的 IP 地址不固定或由多個 IP 提供時 (例如 Amazon EC2 或 Amazon RDS 執行個體)，此功能很有幫助。如需詳細資訊，請參閱 建立和更新運作狀態檢查。

此外，以前包含在 Amazon Route 53 開發人員指南中有關使用 Route 53 API 的一些資訊已移動。現在 Amazon Route 53 API 參考虹包含所有 API 文件。

2014 年 4 月 18 日

在此版本中，當運作狀態檢查 Port (連接埠) 值是 443 且 Protocol (通訊協定) 值是 HTTPS 時，Route 53 會在 `Host` 標頭中傳遞不同的值。在運作狀態檢查期間，Route 53 現在會向端點傳遞一個包含 Host Name (主機名稱) 欄位值的 `Host` 標頭。如果您使用 `CreateHealthCheck` API 動作建立運作狀態檢查，這是 `FullyQualifiedDomainName` 元素的值。

如需詳細資訊，請參閱 建立、更新和刪除運作狀態檢查。

2014 年 4 月 9 日

在此版本中，您現在可以檢視目前報告某個端點正常運作的 Route 53 運作狀態檢查程式百分比。

此外，Amazon 中運作狀態檢查 Health 態指標的行為 CloudWatch 現在僅顯示零 (如果您的端點在指定時間段內運作狀況不良) 或一個 (如果端點在該時段內運作良好)。此指標不再顯示介於 0 至 1 之間的值，反映 Route 53 運作狀態檢查報告端點為正常運作的部分。

如需詳細資訊，請參閱 使用 CloudWatch 監控運作狀態檢查。

2014 年 2 月 18 日

在此版本中，Route 53 新增以下功能：

- 運作狀態檢查容錯移轉閾值：您現在可以指定端點必須失敗的連續運作狀態檢查數目 (介於 1 和 10 次連續檢查之間)，才會讓 Route 53 將該端點視為狀況不良。狀況不良的端點必須通過相同數量的檢查，才會被視為正常運作。如需詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。
- 運作狀態檢查請求間隔：您現在可以指定 Route 53 傳送請求至端點的頻率，以判斷端點是否正常運作。有效設定為 10 秒和 30 秒。如需詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

2014 年 1 月 30 日

在此版本中，Route 53 新增以下功能：

- HTTP 和 HTTPS 字串比對運作狀態檢查：Route 53 現在支援根據回應本文中是否出現指定的字串，來判斷端點運作狀態的運作狀態檢查。如需詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。
- HTTPS 運作狀態檢查：Route 53 現在支援運作狀態檢查用於安全、僅限 SSL 的網站。如需詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。
- **`ChangeResourceRecordSets`** API 動作的 **`UPSERT`**：在使用 `ChangeResourceRecordSets` API 動作建立或變更記錄時，您現在可以使用 UPSERT 動作來建立新的記錄 (如果指定名稱和類型的記錄不存在)，或更新現有的記錄。如需詳細資訊，請ChangeResourceRecordSets參閱 Amazon 路線 53 API 參考中的。

2014 年 1 月 7 日

在此版本，Route 53 支援根據回應本文中是否出現指定字串來判斷端點運作狀態的運作狀態檢查。如需詳細資訊，請參閱 Amazon Route 53 決定運作狀態檢查是否良好的方式。

2013 年版本

2013 年 8 月 14 日

在此版本，Route 53 支援透過匯入 BIND 格式的區域檔案來建立記錄。如需詳細資訊，請參閱 透過匯入區域檔案建立記錄。

此外，Route 53 健康狀態檢查的 CloudWatch 指標已整合到 Route 53 主控台中，並且簡化。如需詳細資訊，請參閱 使用 CloudWatch 監控運作狀態檢查。

2013 年 6 月 26 日

在此版本中，Route 53 新增了整合運作狀態檢查與 CloudWatch 指標的支援，因此您可以執行下列動作：

- 驗證運作狀態檢查已適當設定。
- 檢閱運作狀態檢查端點在指定期間內的運作狀態。
- 設定 CloudWatch 為在所有 Route 53 運作狀態檢查程式都認為您指定的端點運作狀況不良時，傳送 Amazon 簡單通知服務 (Amazon SNS) 警示。

如需詳細資訊，請參閱 使用 CloudWatch 監控運作狀態檢查。

2013 年 6 月 11 日

在此版本中，Route 53 新增了對建立別名記錄的支援，將 DNS 查詢路由到 Amazon CloudFront 分發的替代網域名稱。您可以為 Zone Apex 的替代網域名稱 (example.com) 和子網域的替代網域名稱 (www.example.com) 使用此功能。如需詳細資訊，請參閱 使用您的網域名稱將流量路由到 Amazon CloudFront 分發。

2013 年 5 月 30 日

在此版本中，Route 53 支援評估 ELB 負載平衡器及相關聯 Amazon EC2 執行個體的運作狀態。如需詳細資訊，請參閱 建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。

2013 年 3 月 28 日

重寫有關運作狀態檢查和容錯移轉的文件，以提高可用性。如需詳細資訊，請參閱 建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。

2013 年 2 月 11 日

在此版本，Route 53 新增對容錯移轉和運作狀態檢查的支援。如需詳細資訊，請參閱 建立 Amazon Route 53 運作狀態檢查和設定 DNS 備援。

2012 年版本

2012 年 3 月 21 日

在此版本，Route 53 可讓您建立延遲記錄。如需詳細資訊，請參閱 以延遲為基礎的路由。

2011 年版本

2011 年 12 月 21 日

在此版本中，AWS Management Console 中的 Route 53 主控台可讓您從清單中選擇 Elastic Load Balancer 來建立別名記錄，而不必手動輸入託管區域 ID 和負載平衡器的 DNS 名稱。新功能記載在 Amazon Route 53 開發人員指南中。

2011 年 11 月 16 日

在此版本中，您可以使用 AWS Management Console 中的 Route 53 主控台建立和刪除託管區域，以及建立、變更和刪除記錄。Amazon Route 53 開發人員指南中適時地記載了新功能。

2011 年 10 月 18 日

此 Amazon Route 53 入門指南已合併到 Amazon Route 53 開發人員指南中，並且此開發人員指南已重新整理以增強可用性。

2011 年 5 月 24 日

此版 Amazon Route 53 引進別名記錄，別名記錄可讓您建立 Zone Apex 別名、加權記錄、新的 API (2011-05-05)，以及服務水準協議。此外，在六個月 Beta 測試之後，Route 53 現在已正式上市。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的 Amazon Route 53 產品頁面和 選擇別名或非別名記錄。

2010 年版本

2010 年 12 月 5 日

這是 Amazon Route 53 開發人員指南的第一個版本。

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。